Physics Open 24 (2025) 100298

Contents lists available at ScienceDirect

Physics Open

journal homepage: www.elsevier.com/locate/physo

Orbits of one-dimensional cellular automata induced by symmetry transformations

Martin Schaller [a], Karl Svozil [b,*]

[a] Vienna, Austria
[b] Institute for Theoretical Physics, TU Wien, Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria

ARTICLE INFO

Handling Editor: Gabriele Coniglio

Keywords:
One-dimensional cellular automata
Symmetry transformations
G-isomorphism

ABSTRACT

Using a group-theoretic approach, a method for determining the equivalence classes (also called orbits) of the set of rules of one-dimensional cellular automata induced by the symmetry operations of reflection and permutation and their product is presented. Orbits are classified by their isomorphism type. Results for the number of orbits and the number of orbits by type for state sets of size two and three are included.

1. Introduction

1.1. The physical relevance of cellular automata

Cellular Automata (CAs) are mathematical constructs that model systems composed of discrete components evolving over time according to simple local rules. Despite their simplicity, CAs exhibit remarkable phenomenological complexity, making them powerful tools for studying a wide range of natural and computational phenomena. Beyond their abstract utility, CAs hold profound potential physical relevance as models for discrete universes and simulations, offering insights into the fundamental principles underlying locally governed (though not necessarily spatially localized) universes and the dynamics of complex systems. Their capacity for Church-Turing universal computation, including the self-reproduction of universal devices within their framework, provides metaphors that may extend to continuous physical models.

Historically, Konrad Zuse, in his seminal work *Rechnender Raum* (Calculating Space) [1–3], proposed the bold hypothesis that the universe itself could be interpreted as a vast computational structure evolving through local updates. Zuse's digital physics posits that space, time, and matter are inherently discrete, with their evolution governed by computational rules analogous to those of CAs. This perspective suggests that physical laws are emergent properties of an underlying computational substrate, where local interactions among discrete elements produce global patterns. In this context, CAs serve as ideal candidates for modelling a digital universe, offering a conceptual framework for exploring the computational essence of reality.

Independently, John von Neumann, utilizing their algorithmic and computational aspects, provided another profound perspective on the significance of CAs, emphasizing their universality and self-replication capabilities [4]. Motivated by questions of biological self-reproduction and universal computation, von Neumann designed a CA capable of replicating itself. This achievement demonstrated that even within a simple, rule-based system, it is possible to encode the complexity of life-like processes and achieve computational universality. Von Neumann's work laid the foundation for studying self-reproducing systems, influencing fields ranging from artificial life to nanotechnology, and underscoring the potential of CAs to model the interplay between computation and dynamics.

CAs have also found extensive applications as models of dynamical systems. Their discrete, rule-driven structure makes them particularly suited for simulating phenomena where local interactions give rise to emergent behaviour, such as fluid dynamics, traffic flow, biological growth, and even aspects of quantum mechanics. Unlike continuum-based models requiring analysis, CAs inherently capture the often granular, stepwise nature of many physical processes.

In sum, CAs embody a profound duality, functioning both as abstract computational models and as physically relevant systems. From Zuse's vision of a computational universe to von Neumann's pioneering work on self-reproduction, CAs have reshaped our understanding of computation, biology, and the dynamics of physical systems. This interplay between simplicity and complexity places CAs at the heart of efforts to unify computational theory with the physical world.

* Corresponding author.
E-mail addresses: martin.roman.schaller@gmail.com (M. Schaller), karl.svozil@tuwien.ac.at (K. Svozil).
URL: http://tph.tuwien.ac.at/~svozil (K. Svozil).

https://doi.org/10.1016/j.physo.2025.100298
Received 10 February 2025; Received in revised form 7 July 2025; Accepted 18 July 2025
Available online 29 July 2025

Their characterization in terms of equivalence through transformations such as reflection, state permutation, and their combinations represents a critical step toward understanding their potential. This study is motivated by such physical motivations.

1.2. Outline and previous work

A one-dimensional CA operates on a bi-infinite lattice of cells where each cell is in one state from a finite set of possible states. A computational step of the automaton comprises the following operations. For each cell the automaton reads the states of a small set of neighbouring cells including the cell itself. The values of the states read are used as input of a lookup table, called the local rule, that determines the new state of the cell. Then all cells are updated synchronously. The net effect of one computational step is the calculation of a new bi-infinite sequence of states.

Multiple iterative computational steps of the CA leads to a sequence of configurations, termed the evolution of the CA. If each configuration of a CA's evolution is shifted the same number of cells to the left or to the right, the CA's evolution is still governed by the same local rule. This fundamental property of CA is called shift invariance.

Other symmetry operations transform the local rule. If the CA's evolution is reflected (or mirrored), the resulting evolution is governed by the reflected rule, which, in general, is different, to the unmirrored one. Reflection is thus a symmetry operation that transforms rules.

Similarly, since the states of a CA are merely labels, permutating the labels does not change the dynamic behaviour of the CA, but will in general result in a different local rule. Rules that can be transformed into each other under reflection or permutation or their product are considered equivalent. Consequently, the set of all CA rules splits up into classes of equivalent rules.

Wolfram [5] designated the family of one-dimensional CAs with two states and three neighbours as elementary. In [6], pp. 485–557, he gave a table that divided the 256 rules of the elementary CA into 88 equivalence classes with respect to the symmetry operations of reflecting the lattice, permutation of the state set, and the product of these operations. A mathematical derivation of this result was carried out by Li and Packard [7]. Cattaneo et al. [8] studied a variety of transformations of the set of local rules, in particular, also the symmetry operations of two-state CAs to be discussed in this work. They gave, inter alias, the general result for the equivalence classes of two-state CAs with $2r + 1$ neighbours, where r is a nonnegative integer. The properties of symmetry transformations acting on CA rules have also been investigated, see e.g., [9]. Symmetry transformations were even extended to generalized CAs over groups, see [10].

Determining the equivalence classes is an elementary classification and serves both to understand the set of local rules in terms of symmetry operations and to reduce the number of non-equivalent rules. There are a variety of other classification schemes. For instance, Wolfram's classification [11] is based on the phenomenological behaviour of the dynamic evolution, the Culik-Yu classification [12] captures the computational complexity of the limit sets; see [13] for an overview. The classification by symmetry operations precedes these higher-level classifications as rules in an equivalence class are all in the same class of other classification schemes (at least they should be).

This study focuses on the equivalence classes of one-dimensional CAs induced by the symmetry transformations of reflection and permutation and their product. The set of symmetry transformations forms a group which acts on the set of CA rules. Therefore group-theoretical concepts are applied to determine the equivalence classes of CAs. In group-theoretical notation, equivalence classes induced by group actions are called orbits, and this term is used in the following. One of the main results of this study is the provision of formulas that give the number of orbits for a state set of size two and three for any size of the neighbourhood. This study goes beyond the scope of previous work by classifying the orbits according to their isomorphism type and deriving the cardinalities of these classes.

The organization of this study is as follows. Section 2 provides definitions on CAs and symmetry operators. Section 3 presents a method based on group actions to determine the number of orbits. Sections 4 and 5 contains the calculations for a state set of size two and size three respectively. Section 6 presents a brute-force algorithm that can be used to validate the results for small numbers of states and neighbours. Conclusion remarks are made in Section 7.

2. Definitions

2.1. One-dimensional cellular automata

The states of a CA are represented by symbols from a finite set, also called an alphabet. As the symbols only serve to designate the states, any finite set will do, so we choose the set $\Sigma = \{0, 1, \dots, k-1\}$ to represent a state set of size k. The size (or cardinality) of an arbitrary set A is denoted by $|A|$.

A word $w = x_0 x_1 \dots x_{m-1}$ over an alphabet Σ is a finite sequence of symbols from Σ juxtaposed. The length of a word w, denoted $|w|$, is the length of the sequence, that is $|x_0 x_1 \dots x_{m-1}| = m$ (the notation $|.|$ denotes both the size of a set and the length of a word). The set of all words of length m over the alphabet Σ is denoted by Σ^m. A configuration x is a bi-infinite sequence over the alphabet Σ, defined as a mapping of $\mathbb{Z}$ into Σ. The ith element, $i \in \mathbb{Z}$, of a configuration x is denoted by x_i.

Definition 1.

A one-dimensional CA is a triple (k, N, f), where

$k \geq 2$ is an integer, the number of states in the state set $\Sigma = \{0, 1, \dots, k-1\}$;

N is the neighbourhood, a finite nonempty set of integers such that $-N = N + d$ for an integer d;

f is the local rule, a function from Σ^n to Σ.

Let $n = |N|$ and $N = \{j_0, j_1, \dots, j_{n-1}\}$ such that $j_0 < j_1 < \dots < j_{n-1}$. The local mapping f induces the global mapping on the set of configurations $\Phi_f^N : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$, defined by $\Phi_f^N(x)_i = f(x_{i+j_0} x_{i+j_1} \dots x_{i+j_{n-1}})$.

We have used the notation $-N = \{-j \mid j \in N\}$ and $N + d = \{j + d \mid j \in N\}$. If N is given, we will write Φ_f instead of Φ_f^N. Definition 1 is similar to the one used in [14,15] or [16], apart that we always use the first nonnegative integers as state set and more important that we introduce the constraint $-N = N + d$ to later define the reflection operator in a meaningful way. If the CA is initialized with the configuration x, the CA computes in one step the configuration $\Phi_f(x)$.

The shift operator σ operates on the set of configurations, it shifts a configuration one cell to the left, formally defined by $\sigma(x)_i = x_{i+1}$. By the definition of the CA, the global mapping commutes with the shift operator: $\Phi_f(\sigma(x)) = \sigma(\Phi_f(x))$. A fundamental result of Hedlund [17] shows that an alternative, topological definition of an one-dimensional CA based on the shift operator and continuous mappings is equivalent to the one above. We contrast Definition 1 with another definition that is frequently found in literature, e.g. [18] or [11]. If p and q are integers, let $[p, q]$ denote the integer interval $\{p, p+1, \dots, q\}$.

Definition 2. A radius-based CA is a CA (k, N, f) such that $N = [-r, r]$, where r is a nonnegative integer, called the radius of the CA.

The local mapping f induces the global mapping $\Phi_f(x)_i = f(x_{i-r} x_{i-r+1} \dots x_{i+r})$. Definition 2 encompasses only CAs with an odd $(2r + 1)$ number of neighbours. The generalization to an even number of neighbours becomes cumbersome, e.g. by shifting the output configuration a half cell and introducing half-integers to index the configuration, see Kari [16], or by loss of symmetry, see Ruivo [19],

while Definition 1 enables a uniform treatment of all neighbourhood sizes.

If $k = |\Sigma|$, then the set $L(k,n) = \{f \mid f : \Sigma^n \to \Sigma\}$ is called the local rule space of the family of CAs with k states and n neighbours. The size of $L(k,n)$ is k^{k^n}. If $k > 1$, $|L(k,n)|$ grows extremely fast as function of n: $|L(k,0)| = k$, and $|L(k,n+1)| = |L(k,n)|^k$. The set $G(k,N) = \{\Phi_f \mid f \in L(k,|N|)\}$ is called the global rule space of the family of CAs with k states and neighbourhood N.

Proposition 3. *If $G(k_1,N_1) = G(k_2,N_2)$, then $k_1 = k_2$ and $N_1 = N_2$.*

Proof. If $k_1 \neq k_2$, then clearly $G(k_1,N_1) \neq G(k_2,N_2)$. Suppose now that $k_1 = k_2$ and $N_1 \neq N_2$. Then $N_1 \setminus N_2 \cup N_2 \setminus N_1$ is not empty. Without loss of generality, suppose $N_1 = \{j_0,\ldots,j_{n-1}\}$ and $j_p \in N_1 \setminus N_2$. Define a local rule f by $f(a_0 \ldots a_{n-1}) = 1$ only if $a_p = 1$ and $a_i = 0$ for $i \neq p$, and a configuration x by $x_{j_p} = 1$ and $x_i = 0$ if $i \neq j_p$. Then $\Phi_f^{N_1}(x)_i$ is 1 if $i = 0$ and 0 otherwise. Let $g \in L(k,n)$ be arbitrary. If $\Phi_g^{N_2}(x)_0 = 0$ then $\Phi_f^{N_1} \neq \Phi_g^{N_2}$. If $\Phi_g^{N_2}(x)_0 = 1$, we conclude that $g(0\ldots0) = 1$ and $\Phi_g^{N_2}(x)$ contains infinitely many 1's, so also $\Phi_f^{N_1} \neq \Phi_g^{N_2}$. Thus, we have shown that $\Phi_f^{N_1} \notin G(k,N_2)$. □

Note the following two cases. First, if $N_2 = N_1 + q$ for an integer q, then $G(k,N_1) = \{\sigma^q \Phi_f \mid \Phi_f \in G(k,N_2)\}$. Second, if $N_2 \subseteq N_1$, then $G(k,N_2) \subseteq G(k,N_1)$.

2.2. Symmetry operations

The notion of the equivalence of one-dimensional CAs is based on two classes of symmetry operations: permutations of the state set and reflection of the configuration.

Let S_k be the symmetric group of degree k, that is the set of all permutations of the set $\Sigma = \{0,1,\ldots,k-1\}$, and suppose $\alpha \in S_k$. If $a \in \Sigma$ we write the image of a under α as product αa. The extension of α to words and configurations is defined by elementwise application. If $w = a_0 \ldots a_{n-1} \in \Sigma^n$ is a word, set $\alpha w = (\alpha a_0)\ldots(\alpha a_{n-1})$. If x is a configuration, set $(\alpha x)_i = \alpha(x_i)$. Suppose f is a local rule that maps Σ^n to Σ. The permutation operator $\hat{\alpha}$ is defined by $\hat{\alpha} f(w) = \alpha f(\alpha^{-1} w)$ for all words $w \in \Sigma^n$. It represents a transformation of the set of local rules. Note that the "hat" on the operator is necessary, because αf and $\hat{\alpha} f$ are distinct entities. The first one is the composite function $\alpha \circ f$, whereas the second represents the composite function $\alpha \circ f \circ \alpha^{-1}$. If Φ_f is the induced global mapping of f, we define $\hat{\alpha}\Phi_f$ similarly: $\hat{\alpha}\Phi_f(x) = \alpha\Phi_f(\alpha^{-1}x)$ for all configurations x. From

$$\begin{aligned}\left(\hat{\alpha}\Phi_f(x)\right)_i &= \left(\alpha\Phi_f(\alpha^{-1}x)\right)_i = \alpha f\left(\alpha^{-1}(x_{i+j_0}\ldots x_{i+j_{n-1}})\right)\\ &= \hat{\alpha} f(x_{i+j_0}\ldots x_{i+j_{n-1}}) = \Phi_{\hat{\alpha}f}(x)_i\end{aligned}$$

follows $\hat{\alpha}\Phi_f = \Phi_{\hat{\alpha}f}$.

The second type of operator is the reflection operator. If $w = a_0 \ldots a_{n-1} \in \Sigma^n$ is a word over Σ, define $rw = a_{n-1}\ldots a_0$. Note that $ra = a$ for all $a \in \Sigma$. If x is a configuration, set $(rx)_i = x_{-i}$. The reflection operator $\hat{r}$ is defined by $\hat{r} f(w) = f(rw)$ and $\hat{r}\Phi_f(x) = r\Phi_f(rx)$. Since r is self-inverse, that is $r^{-1} = r$, we can also write $\hat{r} f(w) = r f(r^{-1}w)$, making the notation consistent with the one of the permutation operator.

From

$$\begin{aligned}\left(\hat{r}\Phi_f(x)\right)_i &= \left(r\Phi_f(rx)\right)_i = \left(\Phi_f(rx)\right)_{-i} = f\left((rx)_{-i+j_0}\ldots(rx)_{-i+j_{n-1}}\right)\\ &= f\left(x_{i-j_0}\ldots x_{i-j_{n-1}}\right) = f\left(x_{i+j_{n-1}+d}\ldots x_{i+j_0+d}\right)\\ &= f\left(r(x_{i+j_0+d}\ldots x_{i+j_{n-1}+d})\right) = \hat{r} f\left(x_{i+j_0+d}\ldots x_{i+j_{n-1}+d}\right)\\ &= \left(\Phi_{\hat{r}f}(x)\right)_{i+d};\end{aligned}$$

we conclude that $\hat{r}\Phi_f = \sigma^d\Phi_{\hat{r}f}$. If the CA complies with Definition 2 the relation simplifies to $\hat{r}\Phi_f = \Phi_{\hat{r}f}$.

We call $R = \{1, r\}$, the reflection group. The direct product of S_k and R, written as $S_k R$, is the group that contains all permutations, the reflection and their products. Suppose that $\hat{\alpha}$ and $\hat{\beta}$ are two operators. Then

$$\hat{\alpha}\hat{\beta} f(w) = \alpha\hat{\beta} f(\alpha^{-1}w) = \alpha\beta f(\beta^{-1}\alpha^{-1}w) = \widehat{\alpha\beta} f(w).$$

The operators form a group that is in general isomorphic to $S_k R$, but for $n = 1$ (or $k = 1$) the relation is only a homomorphism. Note that the reflection operator commutes with all permutation operators. If the global mapping Φ_f satisfies $\Phi_f = \hat{\alpha}\Phi_f$, the CA is said to be invariant under the operator $\hat{\alpha}$.

The meaning of the operators defined above is illustrated by the following observation. Suppose $\hat{\alpha}$ is either one of the permutation operators or the reflection operator, and consider two radius-based CAs (Definition 2) with the same state set and the same radius and respectively, with local rule f and local rule $\hat{\alpha} f$. If the initial configuration of CA A is x and the one of CA B is αx, then the same 1–1 correspondence between the configurations established by α persists for all iterations: $\alpha\Phi_f^t(x) = \Phi_{\hat{\alpha}f}^t(\alpha x)$ holds for any positive integer t (Φ^t denotes the tth iteration of Φ). Suppose now that the CAs are of the general form of Definition 1. The same relation holds, if α is a permutation, but if $\alpha = r$, it changes. Then CA A is after one step in configuration $\Phi_f(x)$, and CA B in configuration $\Phi_{\hat{r}f}(rx)$. Using $\hat{r}\Phi_f = \sigma^d\Phi_{\hat{r}f}$, we obtain $\Phi_{\hat{r}f}(rx) = \sigma^{-d}\hat{r}\Phi_f(rx) = \sigma^{-d} r\Phi_f(x)$, so $r\Phi_f(x) = \sigma^d\Phi_{\hat{r}f}(rx)$. For any number t of steps, the relation becomes $r\Phi_f^t(x) = \sigma^{dt}\Phi_{\hat{r}f}^t(rx)$.

3. Preliminaries

3.1. Groups and group actions

We assume some basic knowledge of groups as it can be found in introductory textbooks, e.g. [20,21], or [22]. However, we briefly introduce the notation that is used in the following, define group actions and related concepts and state some propositions about them, all of these to be found in more depth and more relaxed pace in the references above.

Let H be a subgroup of G, denoted by $H \leq G$. If $g \in G$, the left coset of H in G is defined by $gH = \{gh \mid h \in H\}$. The index $[G : H]$ of H in G denotes the number of left cosets of H in G. Lagrange's theorem states that $|G| = [G : H] \times |H|$. If $g \in G$, the conjugate of H by g is the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$, which is also a subgroup isomorphic to H. A subgroup N of G is called normal if $gNg^{-1} = N$ for all $g \in G$.

A group action of a group G on a set A is a map from $G \times A$ to A satisfying the following properties:

(i) $g_1(g_2 a) = (g_1 g_2)a$ for all $g_1, g_2 \in G$, $a \in A$, and
(ii) $1a = a$, for all $a \in A$.

The relation on A, defined by $a \sim b$ if and only if $a = gb$ for some $g \in G$, is an equivalence relation. The equivalence classes $[a] = \{ga \mid g \in G\}$ are called G-orbits (or just orbits), and the set of orbits forms a partition of A, denoted by A/G. The length of an orbit $[a]$ is its size $|[a]|$. An element $a \in A$ is fixed by $g \in G$ if $ga = a$. The set of all group members that fix an element $a \in A$ is called the stabilizer of a, that is the set $\mathrm{stab}(a) = \{g \in G \mid ga = a\}$, which forms a subgroup of G. If $g \in G$, the set of all fixed points of g is denoted by $\mathrm{fix}(g) = \{a \in A \mid ga = g\}$. The notation is generalized to subgroups. If $H \leq G$, then the set $\mathrm{fix}(H) = \{a \in A \mid ga = a \text{ for all } g \in H\} = \bigcap_{g\in H} \mathrm{fix}(g)$, consists of all elements of A that are fixed points for all $g \in H$.

Proposition 4 (*Orbit-Stabilizer Theorem*)**.** *If the group G acts on A and $a \in A$, then the length of the G-orbit which contains a is equal to the index of the stabilizer of a in G:*

$$|[a]| = [G : \mathrm{stab}(a)].$$

Proof. The map $ga \mapsto g\,\mathrm{stab}(a)$ that associates the element ga of the orbit with the left coset $g\,\mathrm{stab}(a)$ is well-defined and bijective. □

Every group G acts on the family of all its subgroups by conjugation. The orbits of this group action are called conjugacy classes. If $H \leq G$, then the conjugacy class of H is the set of subgroups $[H] = \{H' \leq G \mid H' = gHg^{-1} \text{ for some } g \in G\}$. The set of conjugacy classes is denoted by $\mathscr{C}(G)$. If $H \leq G$ and H is normal, then the orbit containing H is a singleton. If G is abelian, each orbit of $\mathscr{C}(G)$ is a singleton. If H_1 and H_2 are subgroups of G, the relation $H_1 \leq H_2$ is a partial order on the set of subgroups. It induces a partial order on $\mathscr{C}(G)$ by $[H_1] \leq [H_2]$ if and only if there is a $H_1' \in [H_1]$ and a $H_2' \in [H_2]$ such that $H_1' \leq H_2'$. The lattice $(\mathscr{C}(G), \leq)$ is called the reduced subgroup lattice of G.

We consider again a group G acting on an (arbitrary) set A. The orbit $O \in A/G$ is said to be of type $[H] \in \mathscr{C}(G)$ if the stabilizer of some a in O belongs to $[H]$. If two orbits O_1 and O_2 are of the same type, then there is a bijection $\varphi : O_1 \to O_2$, such that $\varphi(ga) = g\varphi(a)$ for all $g \in G$ and all $a \in O_1$. The function φ is called a G-isomorphism. Define $\mathrm{type}(A/G, H) = \{O \in A/G \mid \text{the type of } O \text{ is } [H]\}$. Note that $|A/G| = \sum_{[H] \in \mathscr{C}(G)} |\mathrm{type}(A/G, H)|$.

Having established the terminology, we consider now the family of one-dimensional CAs with k states and n neighbours. The mapping $S_k R \times L(k,n) \to L(k,n)$; $(\alpha, f) \mapsto \hat{\alpha} f$ fulfils the properties of a group action. If $f \in L(k,n)$, the orbit of f is the set $[f] = \{\hat{\alpha} f \mid \alpha \in S_k R\}$ and the set of all orbits is denoted by $L(k,n)/S_k R$. Local rules in the same orbit are connected by symmetry transformations, while orbits of the same type cannot be distinguished by symmetry transformations alone. We abbreviate $\mathrm{type}(L(k,n)/S_k R, H)$ to $\mathrm{type}(k,n,H)$. The aim of this study is to develop a method for determining $L(k,n)/S_k R$ and the sets $\mathrm{type}(k,n,H)$ where $[H] \in \mathscr{C}(S_k R)$, and in particular to derive formulas for the cardinalities of these sets.

3.2. Counting orbits

The following lemma relates the number of orbits to the number of fixed points of the group elements.

Proposition 5 (*Burnside's Lemma*). *Let G be a group acting on the set A. The number of G-orbits is*

$$|A/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)|.$$

Proof. In the sum $\sum_{g \in G} |\mathrm{fix}(g)|$, each $a \in A$ is counted $|\mathrm{stab}(a)|$ times (for $\mathrm{stab}(a)$ consists of all those $g \in G$ which fix a). If a and b lie in the same orbit, then $b = ga$ for a $g \in G$. This implies $\mathrm{stab}(b) = g\,\mathrm{stab}(a)\,g^{-1}$, and in particular $|\mathrm{stab}(b)| = |\mathrm{stab}(a)|$. So, the $[G : \mathrm{stab}(a)]$ elements constituting the orbit of a are, in the above sum, collectively counted $[G : \mathrm{stab}(a)] \times |\mathrm{stab}(a)|$ times. Each orbit thus contributes $|G|$ to the sum, and so $\sum_{g \in G} \mathrm{fix}(g) = |A/G| \times |G|$. □

The proof was adapted from [22]. Burnside's lemma gives the total number of orbits. Since we are also interested in the distribution of orbits by type, we will use the following method in Sections 4 and 5. Let $[H] \in \mathscr{C}(G)$. The set $\mathrm{stab}^{-1}([H]) = \bigcup_{H' \in [H]} \mathrm{stab}^{-1}(H')$ is the union of all orbits of type $[H]$, all having length $[G : H] = |G| / |H|$. Thus

$$|\mathrm{type}(A/G, H)| = |\mathrm{stab}^{-1}([H])| \,/\, [G : H] = |\mathrm{stab}^{-1}(H)| \times |[H]| \times |H| \,/\, |G|. \tag{1}$$

In calculating the numbers $|\mathrm{stab}^{-1}(H)|$ we take a detour. The mapping $\mathrm{fix}(H)$ from the set of subgroups of G into A does not create a partition of A: if H_1 is a proper subgroup of H_2 (H_1 is a subgroup of H_2 and $H_1 \neq H_2$), denoted by $H_1 < H_2$, then $\mathrm{fix}(H_2) \subset \mathrm{fix}(H_1)$. The mappings fix and stab are related

$$\mathrm{stab}^{-1}(H) = \mathrm{fix}(H) \setminus \bigcup_{H < H'} \mathrm{stab}^{-1}(H'), \tag{2}$$

where H' is also assumed to be a subgroup of G. Since the sets $\mathrm{stab}^{-1}(H)$ are disjoint, Eq. (2) implies

$$|\mathrm{stab}^{-1}(H)| = |\mathrm{fix}(H)| - \sum_{H < H'} |\mathrm{stab}^{-1}(H')|. \tag{3}$$

To calculate $|\mathrm{stab}^{-1}(H)|$ for all subgroups, we start with G, for which $\mathrm{stab}^{-1}(G) = \mathrm{fix}(G)$ holds, the calculation of the subgroups can then be done successively.

In general, the numbers $|G|$ and $|\mathrm{fix}(g)|$ are not sufficient to determine the numbers $|\mathrm{type}(A/G, H)|$. The following example describes two different group actions of the same group on the same set, so that the numbers $|\mathrm{fix}(g)|$ are the same, but the distribution of orbits by type is different. If a group G acts on a set A, it induces a homomorphism $\varphi : G \to S_A$; $g \mapsto (a \mapsto ga)$, where S_A denotes the symmetric group of A. We can therefore associate group elements of G with permutations of the set A. Let $V = \{1, a, b, c\}$ the Klein four-group and $A = \{1, 2, \ldots, 6\}$. Consider the group actions ψ_1 and ψ_2, both mappings of $V \times A$ onto A, where ψ_1 has the permutation representation

$$\sigma_1 = (), \sigma_a = (12)(34), \sigma_b = (34)(56), \sigma_c = (12)(56);$$

and ψ_2 is given by

$$\tau_1 = (), \tau_a = (12)(34), \tau_b = (13)(24), \tau_c = (14)(23).$$

It is easily verified that these representations satisfy the group axioms and are isomorphic to V. The first group action ψ_1 partitions A into the orbits $\{1,2\}$, $\{3,4\}$, and $\{5,6\}$, the second group action ψ_2 leads to the partition $\{1,2,3,4\}$, $\{5\}$, and $\{6\}$. Note that $|\mathrm{fix}(a)| = |\mathrm{fix}(b)| = |\mathrm{fix}(c)| = 2$ and $|A/V| = 3$ for both actions, while, for instance, $\mathrm{type}(A/V, V) = \emptyset$ for the first action, but $\mathrm{type}(A/V, V) = \{\{5\}, \{6\}\}$ for the second one.

3.3. Symmetry operators acting on the domain of the local rules

The domain of a local rule is the set Σ^n of all words over Σ having length n. If H is a subgroup of $S_k R$, the mapping $H \times \Sigma^n \to \Sigma^n$ defined by $(\alpha, w) \mapsto \alpha w$ satisfies the properties of a group action.

We will now study mappings that are defined on an orbit of Σ^n/H. Suppose $A \subset \Sigma^n$ is an H-orbit, and g is a mapping $A \to \Sigma$. If $\alpha \in H$ then $\alpha A = \{\alpha w | w \in A\} = A$. This shows that the domain of $\hat{\alpha} g$ is also A. Hence we can speak about functions defined on A that are invariant under H.

The set $\{A_1, \ldots, A_p\}$ of all H-orbits is a partition of Σ^n. If f is a local rule invariant under H, then the restriction $f|A_i$ is clearly also invariant under H. On the other hand, if $g_i : A_i \to \Sigma$; $i = 1 \ldots, p$, is a sequence of mappings, all invariant under H, then the local rule defined by $f(w) = g_i(w)$ if $w \in A_i$ is also invariant under H. This shows that invariant functions defined on the orbits are the building blocks of invariant functions defined on Σ^n.

Let A be again an H-orbit A and suppose $g : A \to \Sigma$ is invariant under H. Choose a word w in A, and consider a different word in A, say v. Since there is an $\alpha \in H$ such that $v = \alpha w$, the relation $g(v) = \hat{\alpha} g(v) = \alpha g(\alpha^{-1} v) = \alpha g(w)$ holds, and the value of $g(v)$ is determined by $g(w)$. This implies that there are at most k different mappings $g : A \to \Sigma$ that are invariant under H.

3.4. Examples

We will study the group action of $\langle (01)r \rangle$ on some of the orbits of two-state and three-state neighbourhoods.

1. Let $\Sigma = \{0,1\}$, and $n = 2m$ be a positive even integer. Suppose that the group $\langle (01)r \rangle$ acts on Σ^n. Consider the word $w = 0^m 1^m$ (m copies of 0 followed by m copies of 1). The group action of $(01)r$ on w results in

   $$(01)rw = (01)r(0^m 1^m) = (01)(1^m 0^m) = 0^m 1^m = w;$$

   and so the set $A = \{w\}$ represents a singleton orbit. Assume there is a function f from A to Σ that is invariant under $\langle (01)r \rangle$. Then f has to satisfy the relation $f((01)rw) = (01)rf(w)$. But since $f((01)rw) = f(w)$, we obtain the contradiction $f(w) = (01)f(w)$. This shows that there is no local rule on Σ^n that is invariant under $\langle (01)r \rangle$.

2. Let Σ be as above, let $n = 2m+1$ be a positive odd integer, and let $w \in \Sigma^n$. If we write $w = ucw$, where u and v are words of length m and c is a symbol of Σ, we see that

   $$(01)rw = (01)r(ucv) = (01)(rv)c(ru) = ((01)rv)((01)c)((01)ru).$$

   Since for all $c \in \{0,1\}$, $c \neq (01)c$, we conclude that $w \neq (01)rw$, and that $A = \{w, (01)rw\}$ is an orbit of length 2. Choose a symbol a from $\{0,1\}$ and set $f(w) = a$. If we set $f((01)rw) = (01)a$, the function f is invariant under $\langle (01)r \rangle$. Since a was arbitrary, there are two functions with domain A that are invariant under $\langle (01)r \rangle$.
3. Let $\Sigma = \{0,1,2\}$, $n = 2m$ be a positive even integer, and $w = 0^m 1^m$. The singleton $A = \{w\}$ is an orbit of $\langle (01)r \rangle$. Assume that f is invariant on A. Then $f(w) = (01)f(w)$ must hold, which is satisfiable by the choice $f(w) = 2$. Hence there exists exactly one function from A to Σ that is invariant under $\langle (01)r \rangle$.
4. Let Σ be as above, but let $n = 2m+1$ be a positive odd integer. Consider a word w of Σ^n and write it in the form $w = ucv$, where u and v are words of length m and c is a symbol. The relation $w = (01)rw$ leads to the constraints $v = (01)ru$ and $c = 2$, satisfied by 3^m words. If w is one of these words, a function f defined on the orbit $\{w\}$ that is invariant is constrained to the value $f(w) = 2$. All other orbits of Σ^n have length 2 and allow for three different invariant functions.

3.5. The degree of an orbit

We have seen in Section 3.3 that the number of invariant functions on an orbit is at most the size of the state set $k = |\Sigma|$. The examples above have shown that the number of invariant functions might also be smaller than k. Let $H \leq S_k R$ and A be an orbit of Σ^n/H. The degree of A is defined to be the number of invariant functions on A, formally

$$\deg(A) = |\{f : A \to \Sigma \mid \hat{\alpha} f = f \text{ for all } \alpha \in H\}|.$$

The procedure for calculating the orbits of a CA which we will present shortly, requires to determine the degree of a given orbit. The following two lemmas will facilitate this task. The first lemma states that to determine the degree of an orbit, it is sufficient to consider all group actions on only one word of the orbit. The second lemma says that an orbit has degree k if the length of the orbit equals the order of the group.

Lemma 6. *Let $H \leq S_k R$, A be an H-orbit, f be a function from A to Σ, and w be any word of A. If $f(\alpha w) = \alpha f(w)$ holds for all α in H, then f is invariant under H.*

Proof. By definition, f is invariant under H if $f(w) = \alpha f(\alpha^{-1} w)$ for all $w \in A$ and $\alpha \in H$. If we replace α by its inverse α^{-1}, we see that the condition becomes equivalent to $f(w) = \alpha^{-1} f(\alpha w)$ or $f(\alpha w) = \alpha f(w)$ for all $w \in A$ and $\alpha \in H$.

Let $v \in A$ and $\beta \in H$. Assuming that the condition of the lemma is fulfilled, we have to show that $f(\beta v) = \beta f(v)$. The proof is almost trivial. Since A is an H-orbit, there is a $\gamma \in H$, such that $v = \gamma w$. Then $f(\beta v) = f((\beta\gamma)w) = (\beta\gamma) f(w) = \beta(\gamma f(w)) = \beta f(\gamma w) = \beta f(v)$. □

Lemma 7. *Let $H \leq S_k R$ and A be an H-orbit. If $|A| = |H|$, then $\deg(A) = k$.*

Proof. Let w be any word of A, and a be any symbol of Σ. Define a function f from A to Σ as follows. Set $f(w) = a$ and let v be another word of A. Since $|A| = |H|$ there is exactly one $\alpha \in H$ such that $v = \alpha w$. This shows that the value $f(v) = \alpha f(w) = \alpha a$ is well defined. Lemma 6 implies that f is invariant under H. □

3.6. Outline of the complete calculation

Given a local rule space $L(k,n)$, the method to calculate the numbers $|\text{type}(k,n,H)|$, $[H] \in \mathscr{C}(S_k R)$ is as follows.

1. Construct the group $S_k R$ that is the direct product of the permutation group S_k and the reflective group $R = \{0, r\}$. Having done that, construct the sublattice of all subgroups of $S_k R$.
2. For each conjugation class $[H]$ of $\mathscr{C}(S_k R)$ choose one representative $H \in [H]$. Determine the orbits of the group action $H \times \Sigma^n \to \Sigma^n$ and their degree. Then

   $$|\text{fix}(H)| = \prod_{A \in \Sigma^n/H} \deg(A).$$

3. Beginning with $S_k R$ calculate $\text{stab}^{-1}(H)$ for all selected representatives by using Eq. (3):

   $$|\text{stab}^{-1}(H)| = |\text{fix}(H)| - \sum_{H < H'} |\text{stab}^{-1}(H')|$$

4. The number of orbits of type $[H]$ is given by Eq. (1):

   $$|\text{type}(k,n,H)| = |\text{stab}^{-1}(H)| \times |[H]| \times |H| \,/\, |G|.$$

   Sum up the numbers to obtain $|L(k,n)/S_k R|$, the total number of orbits (or apply Burnside's lemma).

3.7. Shift-equivalence

Another elementary equivalence relation was introduced in [19], which we first illustrate with an example in the domain of elementary CAs ($k = 2$, $n = 3$), using Wolfram's nomenclature to label the rules, see [11]. Set $\Sigma = \{0,1\}$ and consider the elementary CAs f_{12} and f_{34}, defined by

$$f_{12}(w) = \begin{cases} 1 & \text{if } w = 010 \text{ or } w = 011 \\ 0 & \text{otherwise} \end{cases} \quad \text{and}$$

$$f_{34}(w) = \begin{cases} 1 & \text{if } w = 001 \text{ or } w = 101 \\ 0 & \text{otherwise} \end{cases}$$

Define a function $h : \Sigma^2 \to \Sigma$ by $h(01) = 1$ and $h(w) = 0$ if $w \neq 01$. Then $f_{12}(a_0 a_1 a_2) = h(a_0 a_1)$ and $f_{34}(a_0 a_1 a_2) = h(a_1 a_2)$ for all $a_0 a_1 a_2 \in \Sigma^3$. It is easy to see that $\boldsymbol{\Phi}_{f_{34}} = \sigma \boldsymbol{\Phi}_{f_{12}}$.

Two CAs (k, N_1, f) and (k, N_2, g) are said to be shift-equivalent if $\boldsymbol{\Phi}_f^{N_1} = \sigma^j \boldsymbol{\Phi}_g^{N_2}$ for some integer j, denoted by $\boldsymbol{\Phi}_f^{N_1} \overset{\sigma}{\sim} \boldsymbol{\Phi}_g^{N_2}$. The relation $\overset{\sigma}{\sim}$ is an equivalence relation. A mapping $p : \Sigma^n \to \Sigma^m$, $m \leq n$, is called a projection if there are integers $q_0, \ldots, q_{m-1}$ such that $0 \leq q_0 < \cdots < q_{m-1} \leq n-1$ and $p(a_0 \ldots a_{n-1}) = a_{q_0} \ldots a_{q_{m-1}}$ for all $a_0 \ldots a_{n-1} \in \Sigma^n$. The set $\{q_0, \ldots, q_{m-1}\}$ is called the index set of the projection. A local rule $f : \Sigma^n \to \Sigma$ is called reducible if there exists a local rule $h : \Sigma^m \to \Sigma$ and a projection $p : \Sigma^n \to \Sigma^m$ with $m < n$, such that $f = h \circ p$, otherwise f is said to be irreducible. Let $N = \{j_0, \ldots, j_{n-1}\}$ be the neighbourhood of the CA. If f is reducible, then there is a rule h and a projection p such that $f = h \circ p$, and the index set of p is minimal. If $\{q_0, \ldots, q_{m-1}\}$ is this index set, the set $M = \{j_{q_0}, \ldots, j_{q_{m-1}}\} \subset N$ is called the support of f.

Suppose that f is reducible with support M, $f = h \circ p$, the index set of p is $\{q_0, \ldots, q_{m-1}\}$, and there is an integer t such that $M' = M + t \subset N$. Write $M' = \{j_{q'_0}, \ldots, j_{q'_{m-1}}\}$. Let p' be the projection $\Sigma^n \to \Sigma^m$ with index set $\{q'_0, \ldots, q'_{m-1}\}$ and define a local rule with the same neighbourhood N as f by $f' = h \circ p'$. From

$$\begin{aligned} \boldsymbol{\Phi}_{f'}(x)_i &= (h \circ p')(x_{i+j_0} \ldots x_{i+j_{n-1}}) = h(x_{i+j_{q'_0}} \ldots x_{i+j_{q'_{m-1}}}) \\ &= h(x_{i+j_{q_0}+t} \ldots x_{i+j_{q_{m-1}}+t}) \\ &= \sigma^t h(x_{i+j_{q_0}} \ldots x_{i+j_{q_{m-1}}}) = \sigma^t (h \circ p)(x_{i+j_0} \ldots x_{i+j_{n-1}}) = \left(\sigma^t \boldsymbol{\Phi}_f(x)\right)_i \end{aligned}$$

follows $\boldsymbol{\Phi}_{f'} = \sigma^t \boldsymbol{\Phi}_f$, so f and f' are shift-equivalent.

Let N_1 and N_2 be integer intervals. Suppose $|N_1| = n$, $|N_2| = m$, $m \leq n$, $f \in L(k,m)$, and f is irreducible. Then there are $n - m + 1$ local

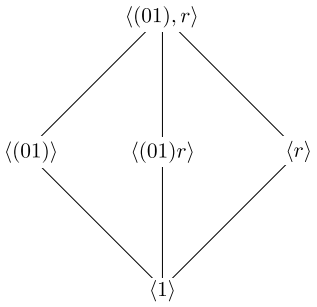

Fig. 1. The lattice of S_2R.

rules $g_i \in L(k,n)$ such that $\Phi_f^{N_1} \overset{\sigma}{\sim} \Phi^{N_2} g_i$. The reflected rules $\Phi_{\hat{r}g_i}^{N_2}$ are all different, but shift-equivalent: $\Phi_{\hat{r}f}^{N_1} \overset{\sigma}{\sim} \Phi_{\hat{r}g_i}^{N_2}$. If f is reflection-symmetric, $\hat{r}f = f$, then, if at all, only one of the g_i, is reflection-symmetric. Note also the general relation $\hat{r}\Phi_f \overset{\sigma}{\sim} \Phi_{\hat{r}f}$ from Section 2.2. There is the special case of $|N_1| = 2$, and $|N_1| = 1$. Let $f \in L(k,1)$, and consider the rules $g_0, g_1 \in L(k,2)$, such that $g_0(a_0a_1) = f(a_0)$ and $g_1(a_0a_1) = f(a_1)$. Here, equivalence by reflection and by shift coincide: $g_1 = \hat{r}g_0$ and $\Phi_{g_1} \overset{\sigma}{\sim} \Phi_{g_0}$. This shows that the orbits of $L(k,2)/S_kR$ remain unchanged if shift-equivalence is taken into account.

Let $N_1 = [-r_1, r_1]$, and $N_2 = [-r_2, r_2]$ with $r_2 < r_1$. If $f \in L(k, 2r_2+1)$, $p(a_{-r_1} \dots a_{r_1}) = a_{-r_2} \dots a_{r_2}$, and $g = f \circ p \in L(k, 2r_1+1)$, then $\Phi_g = \Phi_f$. In this case, $\Phi_{\hat{r}g} = \Phi_{\hat{r}f}$ holds.

A local rule defined on a smaller neighbourhood might reappear in multiple copies that are shift-equivalent when considering larger neighbourhoods. We conclude that shift-equivalence is another important elementary equivalence relation. However, it is of a different nature since it concerns only local rules that can be defined on a proper subset of the neighbourhood. The consideration of shift-equivalence into the presented framework, which is based on the group of permutations and reflection, goes beyond the scope of this study. Results for the number of equivalence classes, obtained with a computer program that also considered shift-equivalence, can be found in [19] for small families of CAs ($k = 2$, $n = 2, 3, 4$ and $k = 3$, $n = 2$).

4. Two states

This section deals with the orbits of one-dimensional two-state CAs, that is $\Sigma = \{0, 1\}$.

4.1. The group S_2R

S_2, the symmetric group of degree 2, contains as its elements the identity 1 and the transposition (01). The direct product S_2R is given by

$$S_2R = \langle(01)\rangle\langle r\rangle = \{1,(01)\}\{1,r\} = \{1,(01),r,(01)r\} = \langle(01),r\rangle.$$

The notation $\langle\alpha,\beta,\dots\rangle$ is called a generator, and denotes the group with the property that every element of the group can be written as finite product of the elements of the generator and their inverses. Since S_2 is abelian and r commutes with 1 and (01), S_2R is abelian too. It is isomorphic to the Klein four-group. The lattice of subgroups is depicted in Fig. 1.

4.2. Odd number of neighbours

Suppose the number of neighbours is odd, $n = 2\,m+1$, $m = 0, 1, 2, \dots$. For each subgroup H of S_2R, we will calculate the number of orbits of H acting on Σ^n. For the next paragraphs w denotes a word of Σ^n.

1. The group $\langle 1\rangle$. All orbits are of length 1, and so Σ^n partitions into 2^{2m+1} singletons.
2. The group $\langle r\rangle$. The relation $w = rw$ is satisfied if and only if the word w is of the form $ua(ru)$ where $|u| = m$ and a is a symbol. This relation is fulfilled by 2^{m+1} words. The set of these words divides into 2^{m+1} orbits of length 1. The remaining $2^{2m+1} - 2^{m+1}$ words of Σ^n are all in orbits of length 2. The total number of orbits is therefore $(2^{2m+1} - 2^{m+1})/2 + 2^{m+1} = 2^m(2^m + 1)$.
3. The group $\langle(01)\rangle$. Consider any word w of Σ^n and let a denote the symbol in the centre of the word. Then $(01)a$ is the symbol in the centre of the word $(01)w$. This shows that the words w and $(01)w$ are always different. Hence Σ^n partitions into 2^{2m} orbits of length 2.
4. The group $\langle(01)r\rangle$. As before, the words w and $(01)rw$ are always different. Hence the number of orbits is again 2^{2m}.
5. The group S_2R. If $w = rw$ holds, then also $r(01)w = (01)w$ holds. We have seen that there are 2^{m+1} words satisfying the relation $w = rw$, and so there are 2^m orbits of length 2 consisting of the words w and $(01)w$. The remaining $2^{2m+1} - 2^{m+1}$ words divide into orbits of length 4. Thus the total number of orbits is $(2^{2m+1} - 2^{m+1})/4 + 2^m = 2^{m-1}(2^m + 1)$.

All the orbits of the groups have degree 2. Put $H_1 = S_2R$, $H_2 = \langle(01)\rangle$, $H_3 = \langle(01)r\rangle$, $H_4 = \langle r\rangle$ and $H_5 = \langle 1\rangle$. Set $a_i = |\mathrm{fix}(H_i)|$, $b_i = |\mathrm{stab}^{-1}(H_i)|$, and $c_i = |\mathrm{type}(2, n, H_i)|$, for $i = 1, \dots, 5$. If p_i is the number of orbits (of degree 2) of the group H_i, then $a_i = 2^{p_i}$. We get

$$b_1 = a_1 = c_1;$$
$$b_2 = a_2 - a_1, c_2 = b_2/2;$$
$$b_3 = a_3 - a_1, c_3 = b_3/2;$$
$$b_4 = a_4 - a_1, c_4 = b_4/2;$$
$$b_5 = a_5 - a_1 - b_2 - b_3 - b_4 = a_5 + 2a_1 - a_2 - a_3 - a_4, c_5 = b_5/4.$$

The total number of orbits is given by $\sum_i c_i$. Expressing the c_i's by the p_i's leads to the following result.

Proposition 8. *Let m be a nonnegative integer.*

(i) The set of rules $L(2, 2m+1)$ partitions into $\frac{1}{4}\left(2 \times 2^{2^{2m}} + 2^{2^m(2^m+1)} + 2^{2^{2m+1}}\right)$ orbits.

(ii) The number of orbits of $L(2, 2m+1)$ by type are

$$\begin{aligned}
|\mathrm{type}(2, 2m+1, S_2R)| &= 2^{2^{m-1}(2^m+1)};\\
|\mathrm{type}(2, 2m+1, \langle(01)\rangle)| &= \tfrac{1}{2}\left(2^{2^{2m}} - 2^{2^{m-1}(2^m+1)}\right);\\
|\mathrm{type}(2, 2m+1, \langle(01)r\rangle)| &= \tfrac{1}{2}\left(2^{2^{2m}} - 2^{2^{m-1}(2^m+1)}\right);\\
|\mathrm{type}(2, 2m+1, \langle r\rangle)| &= \tfrac{1}{2}\left(2^{2^m(2^m+1)} - 2^{2^{m-1}(2^m+1)}\right);\\
|\mathrm{type}(2, 2m+1, \langle 1\rangle)| &= \tfrac{1}{4}\left(2^{2^{2m+1}} + 2 \times 2^{2^{m-1}(2^m+1)}\right.\\
&\quad \left. -2 \times 2^{2^{2m}} - 2^{2^m(2^m+1)}\right).
\end{aligned}$$

Part (i) is a particular case of Proposition 21 in [8].

4.3. Even number of neighbours

Suppose the number of neighbours is even, $n = 2m$, $m = 1, 2, \dots$. For the next paragraphs w denotes a word of Σ^n. Example 1 has shown that there is no local rule invariant under $\langle(01)r\rangle$, and by implication no local rule invariant under S_2R. Thus, in calculating the number of orbits, we therefore only have to consider the remaining subgroups.

1. The group $\langle 1\rangle$. The set Σ^n partitions into 2^{2m} orbits of length 1.
2. The group $\langle(01)\rangle$. The set Σ^n partitions into 2^{2m-1} orbits of length 2.
3. The group $\langle r\rangle$. The set Σ^n partitions into $2^{m-1}(2^m + 1)$ orbits.

Table 1
Count of two-state orbits by type.

H	$\lvert\text{type}(2,n,H)\rvert$				
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
$\langle(01),r\rangle$	2	0	8	0	1 024
$\langle(01)r\rangle$	0	0	4	0	32 256
$\langle(01)\rangle$	0	2	4	128	32 256
$\langle r\rangle$	1	4	28	512	523 776
$\langle 1\rangle$	0	1	44	16 064	1 073 447 424
	3	7	88	16 704	1 074 036 736

All the orbits of the three groups above are of degree 2. Put $H_1=\langle r\rangle$, $H_2=\langle(01)\rangle$, and $H_3=\langle 1\rangle$. Set $a_i=|\text{fix}(H_i)|$, $b_i=|\text{stab}^{-1}(H_i)|$, and $c_i=|\text{type}(2,n,H_i)|$, for $i=1,2,3$. If p_i is the number of orbits (of degree 2) of the group H_i, then $a_i=2^{p_i}$. We get

$b_1=a_1, c_1=b_1/2;$

$b_2=a_2, c_2=b_2/2;$

$b_3=a_3-b_1-b_2, c_3=b_3/4.$

The total number of orbits is given by $\sum_i c_i$. Expressing the c_i's by the p_i's leads to the following result.

Proposition 9. *Let m be a positive integer.*

(i) The set $L(2,2\ m)$ of local rules partitions into $\frac{1}{4}\left(2^{2^{m-1}(2^m+1)}+2^{2^{2m-1}}+2^{2^{2m}}\right)$ orbits.

(ii) The number of orbits of $L(2,2\ m)$ by type are

$$\begin{aligned}|\text{type}(2,2\ m,\langle(01)\rangle)| &= \tfrac{1}{2}2^{2^{2m-1}};\\ |\text{type}(2,2\ m,\langle r\rangle)| &= \tfrac{1}{2}2^{2^{m-1}(2^m+1)};\\ |\text{type}(2,2\ m,\langle 1\rangle)| &= \tfrac{1}{4}\left(2^{2^{2m}}-2^{2^{2m-1}}-2^{2^{m-1}(2^m+1)}\right).\end{aligned}$$

Table 1 depicts the number of orbits of two-state CAs for a neighbourhood size $n=1,\ldots,5$. For each n and each subgroup H of S_2R the table gives the number of orbits of $\text{stab}^{-1}(H)$. The last row lists the total number of orbits for a given n.

5. Three states

After calculating the orbits of one-dimensional two-state CAs in Section 4 this section deals with one-dimensional three-state CAs, that is $\Sigma=\{0,1,2\}$.

5.1. The group S_3R

The group S_3R, which is the direct product of the symmetric group S_3 and the reflection group R, contains all the symmetry operators of one-dimensional three-state CAs.

Some remarks:

1. S_3 is not abelian, and neither is S_3R, for instance $(01)(02)=(021)$, but $(02)(01)=(012)$.
2. The depiction of the lattice of subgroups, Fig. 2, arranges groups of equal order in the same row. From bottom to top the orders are 1, 2, 3, 4, 6, and 12.
3. The dashed rectangles demarcate conjugacy classes of subgroups. The other subgroups are normal and form singleton classes with respect to conjugation. Collapsing the conjugacy classes into single nodes result in the reduced subgroup lattice.
4. Groups are specified by generators, e.g. $S_3=\langle(01),(12)\rangle$.
5. From $[(012)r]^3=r$ follows $\langle(012)r\rangle=\langle(012),r\rangle$.
6. The group $\langle(01)r,(012)\rangle$ consists of the elements $1,(01)r,(12)r,(20)r,(012)$, and (021).

5.2. The orbits of the subgroups of S_3R acting on Σ^n

The following lemma facilitates the calculation of orbits of subgroups that contain the permutation (012).

Lemma 10. *Suppose H is a subgroup of S_3R that contains the permutation (012), and suppose that A is an orbit of H acting on Σ^n. Then the number 3 divides the length of A.*

Proof. There is no word in Σ^n that is invariant under (012). This is equivalent to saying that for all words w in Σ^n, the permutation (012) is not an element of the subgroup $\text{stab}(w)$, and hence that the group $\langle(012)\rangle$ is not a subgroup of $\text{stab}(w)$. Since (012) and (210) are the only elements of order 3 in H, the subgroup $\text{stab}(w)$ is not divisible by 3. From $|\text{stab}(w)|\ |A|=|H|$ follows the proposition. □

The next simple lemma will help us in classifying orbits of degree 1.

Lemma 11. *Suppose H is a subgroup of S_3R and A is an orbit of H acting on Σ^n. Then* $\deg(A)\le 1$

(i) if $(01)\in H$ and there is a $w\in A$ such that $w=(01)w$; or
(ii) if $(01)r\in H$ and there is a $w\in A$ such that $w=(01)rw$.

Proof. Let α be (01) or $(01)r$ and suppose that f is an invariant function from A to Σ. Then the relation $f(w)=\alpha^{-1}f(\alpha w)=\alpha f(w)$ implies $f(w)=2$. □

All words below are understood to be words over Σ. The word w always denotes a word of Σ^n. Sometimes we will write w as a concatenation of two words, that is $w=uv$, if $n=2m$ is even, and as a concatenation of a word, a symbol, and a further word, that is $w=uav$, if $n=2m+1$ is odd. If we do so, we assume that $|u|=|v|=m$. For each subgroup H of S_3R the number of free orbits of H acting on Σ^n is calculated as follows. In the calculations themselves we will make frequent use of Lemma 7 and Lemma 11, without explicitly referencing them.

1. The group $\langle 1\rangle$. Σ^n splits up into 3^n orbits of length 1.
2. The group $\langle r\rangle$. A calculation similar to the state set of size 2 yields $(3^{2m}+3^m)/2$ orbits of degree 3 if $n=2m$ is even, and $(3^{2m+1}+3^{m+1})/2$ orbits of degree 3 if $n=2m+1$ is odd.
3. The groups $\langle(01)\rangle$, $\langle(12)\rangle$, $\langle(20)\rangle$. We study $\langle(01)\rangle$. Only the word $w=2^n$ (n copies of 2) satisfies the equation $(01)w=w$. Hence the orbit $\{2^n\}$ is of degree 1. The remaining words split up into $(3^n-1)/2$ orbits of length 2 and degree 3.
4. The groups $\langle(01)r\rangle$, $\langle(12)r\rangle$, $\langle(20)r\rangle$. We study $\langle(01)r\rangle$.
   Suppose $n=2m$ is even and $w=uv$. The relation $uv=(01)r(uv)=((01)rv)((01)ru)$ implies $v=(01)ru$ and so is satisfied by 3^m words which form 3^m orbits of length 1 and degree 1. The remaining words split up into $(3^{2m}-3^m)/2$ orbits of degree 3.
   Suppose $n=2m+1$ is odd and $w=uav$. The relation $uav=(01)r(uav)=((01)rv)((01)a)((01)ru)$ implies $v=(01)ru$ and $a=2$, which is satisfied by 3^m words resulting in 3^m orbits of length 1 and degree 1. The remaining words split up into $(3^{2m+1}-3^m)/2$ orbits of degree 3.
5. The group $\langle(012)\rangle$. All orbits are of the form $\{w,(012)w,(210)w\}$ with pairwise different elements. This shows that Σ^n partitions into 3^{n-1} orbits of degree 3.
6. The group $S_3=\langle(01),(12)\rangle$. The orbit $\{0^n,1^n,2^n\}$ is of degree 1 because $(01)2^n=2^n$. The remaining words split up into $(3^{n-1}-1)/2$ orbits of length 6 and degree 3.
7. The groups $\langle(01),r\rangle$, $\langle(12),r\rangle$, $\langle(20),r\rangle$. We study $\langle(01),r\rangle$. Only the word 2^n satisfies the relation $w=rw=(01)w=(01)rw$. The corresponding orbit $\{2^n\}$ is of degree 1.
   Suppose $n=2m$ is even. There are two ways that the orbit $\{w, rw, (01)w, (01)rw\}$ can fold up into orbits of length 2.

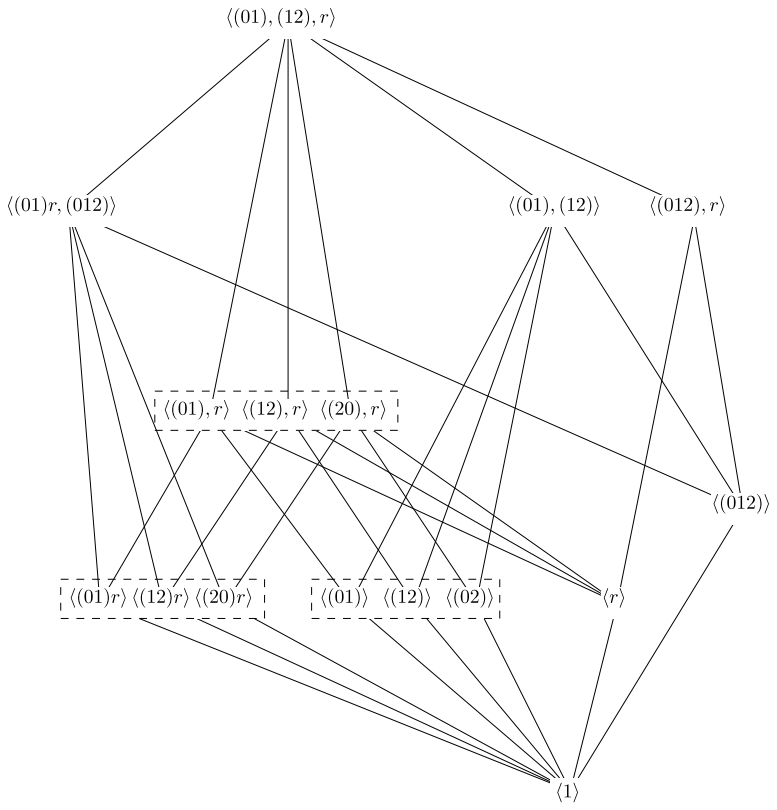

Fig. 2. The lattice of S_3R.

First, if $w = rw$ and $w \neq (01)w$ holds. From the set of 3^m words that satisfy $w = rw$ we remove 2^n. The remaining words in this set split up into $(3^m - 1)/2$ orbits of length 2 and degree 3.

Second, if $rw = (01)w$ and $rw \neq w$ holds. If $w = uv$ the relation $rw = (01)w$ implies $v = (01)ru$. As above, we remove from the set of 3^m words that satisfy this relation the word 2^n to obtain $(3^m - 1)/2$ orbits of length 2 and degree 1.

The remaining $3^{2m} - 2(3^m - 1) - 1$ words in Σ^n split up into orbits of length 4 and degree 3. Summing up the orbits of degree 3, we obtain for their number $(3^{2m} - 2(3^m - 1) - 1)/4 + (3^m - 1)/2 = (3^{2m} - 1)/4$.

Suppose $n = 2m + 1$ is odd. We consider again the two different types of orbits of length 2.

The first occurs, if $w = rw$ and $w \neq (01)w$ holds. A similar calculation as above obtains $(3^{m+1} - 1)/2$ orbits of length 2 and degree 3.

The second occurs, if $rw = (01)w$ and $rw \neq w$. If w is written as uav, the relation becomes $(rv)a(ru) = ((01)u)((01)a)((01)v)$, yielding the constraints $v = (01)ru$ and $a = 2$ which are satisfied by 3^m words. Removing the word 2^n from this set results in $(3^m - 1)/2$ orbits of length 2 and degree 1.

The remaining $3^{2m+1} - (3^{m+1} - 1) - (3^m - 1) - 1 = (3^{m+1} - 1)(3^m - 1)$ words in Σ^n split up into free orbits of length 4. Hence the total number of orbits of degree 3 is $(3^{m+1} - 1)(3^m - 1)/4 + (3^{m+1} - 1)/2 = (3^{m+1} - 1)(3^m + 1)/4$.

8. The group $\langle (012)r \rangle$. If $w = rw$, then $\{w, (012)w, (210)w\}$ is an orbit of length 3. If $w \neq rw$, the orbit containing w is of length 6. The calculation is similar to the one of the group $\langle r \rangle$. If $n = 2m$ is even, Σ^n partitions into $(3^{2m-1} + 3^{m-1})/2$ orbits of degree 3, if $n = 2m + 1$ is odd, Σ^n partitions into $(3^{2m} + 3^m)/2$ orbits of degree 3.
9. The group $\langle (01)r, (012) \rangle$. An orbit is of length 3 if and only if the orbit contains a word w that satisfies the relation $w = (01)rw$.

Suppose $n = 2m$ is even and write $w = uv$. Then $w = (01)rw$ holds if and only if $v = (01)ru$ holds. Each of these 3^m words is in a different orbit. This shows that there are 3^m orbits of length 3. All of them have degree 1. The remaining words split up into $(3^{2m-1} - 3^m)/2$ orbits of length 6 and degree 3.

Suppose $n = 2m + 1$ is odd and write $w = uav$. Then $w = (01)rw$ holds if and only if $v = (01)ru$ holds and $a = 2$. Again, this shows that there are 3^m orbits of length 3 and degree 1. The remaining words split up into $(3^{2m} - 3^m)/2$ orbits of length 6 and degree 3.

10. The group S_3R. The set $\{0^n, 1^n, 2^n\}$ is the only orbit of length 3. The degree is 1. If $n = 1$ it is the only orbit.

Suppose $n = 2m$ is even. By Lemma 10 the next possible length of an orbit is 6. If w is a word in an orbit of length 6, either $w = rw$ or $w = \alpha w$, where α denotes a transposition. There are 3^m words for which $w = rw$. If we subtract the 3 words of the orbit of length 3, we obtain $3(3^{m-1} - 1)$ words that split up into $(3^{m-1} - 1)/2$ orbits of degree 3. There are also 3^m words for which $w = (01)rw$, or 3×3^m words for which $w = \alpha rw$, where α denotes any of the three transpositions $(01), (12), (20)$. If we subtract the 3 words of the orbit of length 3, we obtain $3(3^m - 1)$ words that split up into $(3^m - 1)/2$ orbits of degree 1.

The remaining words of Σ^n partition into orbits of length 12. The number of remaining words is $3^{2m} - 3(3^{m-1} - 1) - 3(3^m - 1) - 3$, splitting up into $(3^m - 1)(3^{m-1} - 1)/4$ orbits of length 12 and degree 3. The total number of orbits of degree 3 then is $(3^m - 1)(3^{m-1} - 1)/4 + (3^{m-1} - 1)/2 = (3^m + 1)(3^{m-1} - 1)/4$.

Suppose $n > 1$ and $n = 2m + 1$ is odd. There are 3^{m+1} words that satisfy $w = rw$. Similar to the calculation above, we obtain $3^{m+1} - 3$ words that split up into $(3^m - 1)/2$ orbits of degree 3. The relation $ucv = (01)r(ucv)$ implies $v = (01)r$ and $c = 2$. As above, we see that $3^{m+1} - 3$ words satisfying $w = \alpha rw$ split up into $(3^m - 1)/2$ orbits of degree 1.

The remaining words of Σ^n partition into orbits of length 12. The number of remaining words is $3^{2m+1} - 6(3^m - 1) - 3$, splitting

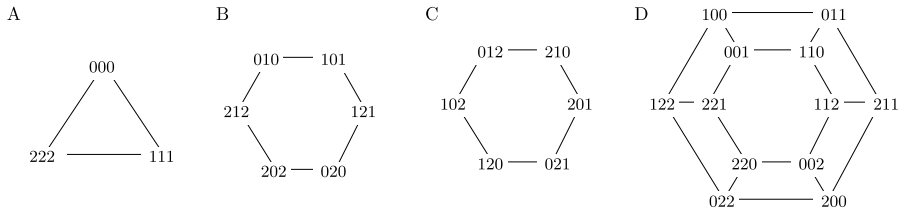

Fig. 3. The orbits of S_3R acting on $\{0,1,2\}^3$.

up into $(3^m-1)^2/4$ orbits of length 12 and degree 3. The total number of orbits of degree 3 then is $(3^m-1)^2/4+(3^m-1)/2 = (3^{2m}-1)/4$. Fig. 3 depicts the orbits of Σ^3/S_3R. The graphs are informal, highlighting certain symmetries of the orbits.

5.3. Counting the orbits of $L(3,n)/S_3R$ by type

Too shorten the notation, we enumerate the representatives of the conjugation classes: $H_1 = S_3R$, $H_2 = \langle (01)r,(012)\rangle$, $H_3 = \langle (01),(12)\rangle$, $H_4 = \langle (012)r\rangle$, $H_5 = \langle (01),r\rangle$, $H_6 = \langle (012)\rangle$, $H_7 = \langle (01)r\rangle$, $H_8 = \langle (01)\rangle$, $H_9 = \langle r\rangle$, and $H_{10} = \langle 1\rangle$. We set $a_i = |\mathrm{fix}(H_i)|$, $b_i = |\mathrm{stab}^{-1}(H_i)|$, and $c_i = |\mathrm{type}(3,n,H_i)|$. In the previous subsection we determined the degree of orbits for one representative H_i of the conjugation classes $[H_i]$. If p_i is the number of orbits of H_i of degree 3, then $a_i = 3^{p_i}$. We express now b_i and c_i in terms of a_i. Then

$$b_1 = a_1 = c_1;$$
$$b_2 = a_2 - a_1, c_2 = b_2/2;$$
$$b_3 = a_3 - a_1, c_3 = b_3/2;$$
$$b_4 = a_4 - a_1, c_4 = b_4/2;$$
$$b_5 = a_5 - a_1, c_5 = 3b_5/3 = b_5;$$
$$b_6 = a_6 - a_1 - b_2 - b_3 - b_4 = a_6 + 2a_1 - a_2 - a_3 - a_4, c_6 = b_6/4;$$
$$b_7 = a_7 - a_1 - b_2 - b_5 = a_7 + a_1 - a_2 - a_5, c_7 = 3b_7/6 = b_7/2;$$
$$b_8 = a_8 - a_1 - b_3 - b_5 = a_8 + a_1 - a_3 - a_5, c_8 = 3b_8/6 = b_8/2;$$
$$b_9 = a_9 - a_1 - b_4 - 3b_5 = a_9 + 3a_1 - a_4 - 3a_5, c_9 = b_9/6;$$
$$b_{10} = a_{10} - a_1 - b_2 - b_3 - b_4 - 3b_5 - b_6 - 3b_7 - 3b_8 - b_9$$
$$= a_{10} - 6a_1 + 3a_2 + 3a_3 + a_4 + 6a_5 - a_6 - 3a_7 - 3a_8 - a_9, c_{10} = b_{10}/12.$$

The equations for c_5, c_7, and c_8 contain an additional factor 3 due to the size of the conjugation classes, see Eq. (1) and Fig. 2. The total number of orbits is therefore

$$\sum_{i=1}^{10} c_i = \frac{1}{12}\left(a_9 + a_{10}\right) + \frac{1}{6}\left(a_4 + a_6\right) + \frac{1}{4}\left(a_7 + a_8\right). \tag{4}$$

Proposition 12. *Let m be a nonnegative integer. The set $L(3,2m+1)$ of local rules partitions into*

$$\frac{1}{12}\left(3^{(3^{2m+1}+3^{m+1})/2} + 3^{3^{2m+1}}\right) + \frac{1}{6}\left(3^{(3^{2m}+3^m)/2} + 3^{3^{2m}}\right)$$
$$+ \frac{1}{4}\left(3^{(3^{2m+1}-3^m)/2} + 3^{(3^{2m+1}-1)/2}\right)$$

orbits.

Let m be a positive integer. The set $L(3,2\,m)$ of local rules partitions into

$$\frac{1}{12}\left(3^{(3^{2m}+3^m)/2} + 3^{3^{2m}}\right) + \frac{1}{6}\left(3^{(3^{2m-1}+3^{m-1})/2} + 3^{3^{2m-1}}\right)$$
$$+ \frac{1}{4}\left(3^{(3^{2m}-3^m)/2} + 3^{(3^{2m}-1)/2}\right)$$

orbits.

The total number of orbits can be derived more simply from Burnside's Lemma:

$$|L(3,n)/S_3R| = \frac{1}{|S_3R|}\sum_{\alpha\in S_3R}|\mathrm{fix}(\alpha)| =$$

Table 2
Count of three-state orbits by type.

H	$\lvert\mathrm{type}(3,1,H)\rvert$	$\lvert\mathrm{type}(3,2,H)\rvert$	$\lvert\mathrm{type}(3,3,H)\rvert$
$\langle (01),(12),r\rangle$	1	1	9
$\langle (01)r,(012)\rangle$	0	0	9
$\langle (01),(12)\rangle$	0	1	36
$\langle (012)r\rangle$	1	4	360
$\langle (01),r\rangle$	2	8	6 552
$\langle (012)\rangle$	0	4	4 716
$\langle (01)r\rangle$	0	9	262 431
$\langle (01)\rangle$	0	35	793 845
$\langle r\rangle$	3	116	64 566 684
$\langle 1\rangle$	0	1 556	635 433 642 324
	7	1 734	635 499 276 966

$$\frac{1}{12}\left(|\mathrm{fix}(1)| + |\mathrm{fix}(r)| + 3|\mathrm{fix}((01))| + 3|\mathrm{fix}((01)r)|\right.$$
$$\left.+2|\mathrm{fix}((012))| + 2|\mathrm{fix}((012)r)|\right),$$

where we have used the relation $|\mathrm{fix}(\alpha)| = |\mathrm{fix}(\beta\alpha\beta^{-1})|$. If we note that $\mathrm{fix}(\alpha) = \mathrm{fix}(\langle\alpha\rangle)$, we obtain Eq. (4). Since the calculation depends only on the cyclic subgroups, Burnside's lemma is preferable, if only the total number of orbits is required.

Table 2 lists the cardinalities of orbits by type, i.e. $|\mathrm{type}(3,n,H)|$, $[H]\in\mathscr{C}(S_3R)$, for a neighbourhood size of one, two, and three. The last row gives the total number of orbits, that is $|L(3,n)/S_3R|$. In contrast to two-state CAs, we have refrained from giving explicit formulas for $c_i = |\mathrm{type}(3,n,H_i)|$ in the above proposition. These formulas become lengthy, but can be easily derived by expressing the c_i's in terms of the p_i's above.

5.4. Constructing local rules that are invariant

The focus of this study so far has been on deriving formulas for the cardinalities of the orbits of CA rules by type as well as for their total number. We point out that an analogous method to the one described in Section 3.6 can be used to actually construct the local rules that are invariant. We will not treat this subject systematically, but give an example. Let $\Sigma = \{0,1,2\}$ and $n = 3$. The orbits of S_3R acting on Σ^3 and their degrees were derived in Section 5.2 and depicted in Fig. 3. We have also seen that the degree of orbit A and C is 1 and the degree of orbit B and D is 3. According to Section 3.3, we form the set of local rules $\{f\}$ on Σ^3 by considering the restriction of f on the partitions $A,\ldots,D$, denoted by $f_A,\ldots,f_D$. Since the degree of A is 1, we need to determine the value of f_A for a given word w, for instance 000. The relation $(12)f_A(000) = f_A((12)000) = f_A(000)$ implies $f_A(000) = 0$. The other values follow from $f_A(\alpha 000) = \alpha f_A(000) = \alpha 0$, $\alpha\in S_3R$. Similarly, $(02)rf_C(012) = f_C((02)r012) = f_C(012)$ implies $f_C(012) = 1$, the other values follow as above. Thus there is only one function f_A on A and only one function f_C on C invariant under S_3R:

$$f_A = \begin{pmatrix} 000 & 111 & 222 \\ 0 & 1 & 2 \end{pmatrix},\quad f_C = \begin{pmatrix} 012 & 210 & 201 & 102 & 120 & 021 \\ 1 & 1 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

The orbit B is of degree 3, so we can pick a word in B, say 010, define $f_B(010) = a$ with $a\in\Sigma$ arbitrary, and derive the other function values

$$f_D = \begin{pmatrix} 001 & 100 & 011 & 110 & 112 & 211 & 002 & 200 & 022 & 220 & 122 & 221 \\ b & b & (01)b & (01)b & (012)b & (012)b & (12)b & (12)b & (021)b & (021)b & (02)b & (02)b \end{pmatrix}.$$

Box I.

Table 3
Python 3 program that calculates the number of orbits.

```
import itertools as it
k = 3; n = 2                    # number of states; neighbourhood size
s = tuple(range(k))             # state set (0,1,..,k-1)
def enc(w) :                    # encodes a word
    v = 0
    for a in w : v = k*v+a
    return v                    # returns  w[0]*k^(n-1)+..+w[n-1]
rfl_pairs = [(enc(w),enc(w[::-1])) for w in it.product(s, repeat=n)
    if w != w[::-1]]            # pairs (i,j), w_j = rw_i != w_i
def reflectRule(f) :            # returns reflected rule
    g = list(f)                 # copy f
    for (i,j) in rfl_pairs : g[i] = f[j]
    return tuple(g)
def permutateRule(f, perm) :    # returns permutated rule
    g = [0] * k**n
    for w in it.product(s, repeat=n) :
        g[enc([perm[a] for a in w])] = perm[f[enc(w)]]
    return tuple(g)
def orbit(f) :                  # returns the orbit of f
    orb = set()
    for perm in it.permutations(s) :
        pf = permutateRule(f,perm)
        orb.update({pf, reflectRule(pf)})
    return tuple(orb)
def countOrbits() :             # counts all orbits
    processed = set()           # keep track of processed rules
    count = 0
    for f in it.product(s,repeat=k**n) :
        if f not in processed :
            count += 1
            processed.update(orbit(f))
    return count
print(countOrbits())            # prints number of orbits
```

as above. So

$$f_B = \begin{pmatrix} 010 & 101 & 121 & 212 & 020 & 202 \\ a & (01)a & (012)a & (02)a & (12)a & (021)a \end{pmatrix}.$$

We proceed with orbit D in the same way and set $f_D(001) = b$, $b \in \Sigma$, see the unnumbered equation given in Box I. We set $f(w) = f_X(w)$ if $w \in X$. Since a and b were arbitrary symbols of Σ, there are 9 orbits of length 1 of type S_3R, in accordance with the entry $|\text{type}(3, 3, S_3R)|$ in Table 2.

6. Validation

In the previous sections the exact numbers of orbits for one-dimensional two-state and three-state CAs were calculated. This section takes another approach and describes an algorithmic brute-force approach to determine these numbers for small k and n. The algorithm is implemented in Python 3 and depicted in Table 3.

We start with some general considerations applicable to any programming language that supports arrays (referred to as sequences in Python). The state set $\Sigma = \{0, 1, \ldots, k-1\}$ is ordered, and so is the set Σ^n if we adopt the lexicographical order. We write the set Σ^n as an increasing sequence (w_i); $0 \le i < k^n$. This arrangement allows for the representation of a local rule f by the sequence (b_i), $0 \le i < k^n$, where $b_i = f(w_i)$. We define an encoding function, denoted by enc, which maps a word to an integer. The function returns the index i of the word w within the sequence (w_i) such that $w = w_i$, or equivalently, the numerical value when w is read as a number in base k: if $w = a_{n-1} \ldots a_0$, then $\text{enc}(w) = a_{n-1}k^{n-1} + \cdots + a_0$. Given a local rule f represented by the sequence $b = (b_i)$ and a word w, to find $f(w)$ compute $j = \text{enc}(w)$, and then access the jth element in the sequence b: $f(w) = b_j$.

The program listed in Table 3 implements local rules and words as sequences. The symmetry operators are implemented in a manner closely aligned with their theoretical definitions.

We first discuss the reflection operator. The variable `rfl_pairs` refers to a sequence of integer pairs (i, j) satisfying the relations $w_j = rw_i$ and $w_i \neq rw_i$ (`w[::-1]` is a Python idiom used to reverse a sequence). The function `reflectRule` takes a sequence `f` that represents a rule, and returns its reflected version `g`. Initially, the rule provided as argument is copied into the variable `g`. Then, a `for` loop iterates over `refl_pairs`, modifying the values of `g` accordingly to the pairs of `reflectRule`.

We now shift focus to the implementation of the permutation operator. Permutations of the state set are represented as sequences of length `k`. The function `permutateRule` accepts a local rule `f` and a permutation `perm`, and returns the permutated rule `g`. It begins with initializing the variable `g` with a sequence of length k^n. A `for` loop then iterates all words in the domain, and for each word `w`, `g` is changed, according to the equation $g(\sigma(a_0 \ldots a_{n-1})) = g\left((\sigma a_0) \ldots (\sigma a_{n-1})\right) = \sigma f(a_0 \ldots a_n)$.

The function `orbit` determines the orbit of the input function `f`. It iterates all permutations of Σ, and adds the permutated rule and the permutated and reflected rule to the orbit. If f is invariant under a certain operation then f will not be changed. Since the underlying data structure of the equivalence class is a `set`, subsequent additions of the same element have no effect.

Lastly `countOrbits` iterates the set of local rules: `it.product(s,repeat=k**n)` creates the cartesian product of Σ with itself, k^n times, representing the set of local rules. If a rule belongs to an orbit of an already processed rule, the body of the `for` loop is skipped. Otherwise a new orbit is created, the counter is incremented, and the members of the class are stored in a set referenced by the variable `processed`.

On a typical PC, the program prints the result within a few seconds for the input parameters $k = 2$ and $n \leq 4$ as well as for $k = 3$ and $n \leq 2$. With an optimized implementation and improved hardware, it might be possible to achieve results for a few additional combinations, such as $k = 2$, and $n = 5$. However, the algorithm's runtime complexity prevents calculations for larger input parameters.

The presented implementation is minimalistic. We briefly explore two kinds of improvements.

1. By incorporating minor changes, more detailed insights about the orbits can be obtained. As an example, adding a hashtable to the function body of `countEquiClasses` allows tracking the number of equivalence classes based on their size.
2. Although traversing the entire domain might be unfeasible, exploring only parts of it might still be instructive. For instance, if the main loop is adjusted to iterate only the set $\mathrm{fix}(\langle(012)\rangle)$, it is feasible to obtain the results for the upper lattice of S_3R, which consists of groups that encompass the group $\langle(012)\rangle$.

7. Summary

This work investigates the classification of one-dimensional cellular automata (CAs) into orbits (also called equivalence classes) using a group-theoretical approach. A cellular automaton operates on a bi-infinite lattice of cells, each existing in one of a finite number of states, and evolves according to local rules that depend on a fixed-size neighbourhood of cells.

The study defines equivalence through transformations such as reflection, permutation of states, and their combinations. The key contributions include:

- Formalizing orbits by systematically incorporating symmetry operations, including reflection and state permutations, to identify and group equivalent rules within the set of local rules;
- Deriving orbits for two-state and three-state cellular automata with arbitrary neighbourhood, which generalizes previous results and corroborates existing findings, such as the well-established 88 equivalence classes for elementary cellular automata (two states, three neighbours);
- Exploring group actions and symmetries acting on the set of local rules, developing a comprehensive methodological framework for calculating orbits of the set of local rules across varying numbers of states and neighbourhood sizes;
- Classifying orbits by their isomorphism type with respect to the symmetry operations and giving results for the number of orbits per type;
- Implementing an algorithmic validation through a brute-force approach in Python, empirically verifying the theoretical results for families of CAs with a small set of local rules.

The study concludes by highlighting the significance of symmetry-based classification in substantially reducing the number of unique CA rules. This approach provides a rigorous foundation for future investigations into cellular automata dynamics and computational properties, potentially opening new avenues for understanding discrete complex systems and computational mechanisms.

CRediT authorship contribution statement

Martin Schaller: Writing – original draft, Visualization, Software, Investigation, Formal analysis, Conceptualization. **Karl Svozil:** Methodology, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to express their sincere thanks to the anonymous referees for their valuable comments and suggestions.

This research was funded in whole or in part by the Austrian Science Fund (FWF) [Grant DOI:10.55776/PIN5424624]. The authors acknowledge TU Wien Bibliothek for financial support through its Open Access Funding Programme.

Data availability

No data was used for the research described in the article.

References

[1] K. Zuse, Rechnender Raum, Friedrich Vieweg & Sohn, Braunschweig, 1969.
[2] K. Zuse, Calculating space, in: MIT Technical Translation AZT-70-164-GEMIT, MIT (Proj. MAC), Cambridge, MA, 1970.
[3] K. Zuse, Discrete mathematics and Rechnender Raum, 1994.
[4] J. von Neumann, in: A.W. Burks (Ed.), Theory of Self-Reproducing Automata, University of Illinois Press, Champaign, Illinois, USA, 1966.
[5] S. Wolfram, Statistical mechanics of cellular automata, Rev. Modern Phys. 55 (1983) 601.
[6] S. Wolfram, Theory and Applications of Cellular Automata: Including Selected Papers, 1983-1986, in: Advanced Series on Complex Systems, World Scientific, 1986.
[7] W. Li, N.H. Packard, The structure of the elementary cellular automata rule space, Complex Systems 4 (1990).
[8] G. Cattaneo, E. Formenti, L. Margara, G. Mauri, Transformations of the one-dimensional cellular automata rule space, Parallel Comput. 23 (1997) 1593, cellular automata.
[9] A. Castillo-Ramirez, M. Gadouleau, Elementary, finite and linear vn-regular cellular automata, Inform. and Comput. 274 (2020) 104533, aUTOMATA 2017.
[10] A. Castillo-Ramirez, M. Sanchez-Alvarez, A. Vazquez-Aceves, A. Z.-C., A generalization of cellular automata over groups, Comm. Algebra 51 (2023) 3114, http://dx.doi.org/10.1080/00927872.2023.2177663.
[11] S. Wolfram, Universality and complexity in cellular automata, Phys. D: Nonlinear Phenom. 10 (1984) 1.
[12] K. Culik, S. Yu, Undecidability of ca classification schemes, Complex Systems 2 (1988) 177–190.
[13] M. Vispoel, A.J. Daly, J.M. Baetens, Progress, gaps and obstacles in the classification of cellular automata, Phys. D: Nonlinear Phenom. 432 (2022) 133074.
[14] A. Castillo-Ramirez, M.G. Magaña-Chavez, A study on the composition of elementary cellular automata, 2023, arXiv:2305.02947 [nlin.CG].
[15] K. Culik, L. Hurd, S. Yu, Computation theoretic aspects of cellular automata, Phys. D: Nonlinear Phenom. 45 (1990) 357.
[16] J. Kari, Theory of cellular automata: A survey, Theoret. Comput. Sci. 334 (2005) 3.
[17] G.A. Hedlund, Endomorphisms and automorphisms of the shift dynamical systems, Math. Syst. Theory 3 (1969) 320.
[18] E. Jen, Aperiodicity in one-dimensional cellular automata, Phys. D: Nonlinear Phenom. 45 (1990) 3.
[19] E.L. Ruivo, P.P. de Oliveira, F. Lobos, E. Goles, Shift-equivalence of k-ary, one-dimensional cellular automata rules, Commun. Nonlinear Sci. Numer. Simul. 63 (2018) 280.
[20] D. Dummit, R. Foote, Abstract Algebra, Wiley, 2003.
[21] J.S. Milne, Group theory (v4.00), 2021, available at www.jmilne.org/math/.
[22] J. Rotman, An Introduction to the Theory of Groups, in: Graduate Texts in Mathematics, Springer New York, 2012.