Transformations of the one-dimensional cellular automata rule space

G. Cattaneo a,*, E. Formenti a, L. Margara b, G. Mauri a

a Dipartimento di Scienze dell’Informazione, 39 Via Comelico, 20135 Milano, Italy
b Dipartimento di Scienze dell’Informazione, 7 Via Mura Anteo Zamboni, Bologna, Italy

Received 15 July 1996; revised 12 December 1996

Abstract

We introduce the notion of double permutation in order to study particular classes of transformations of the one-dimensional cellular automata rule space. These classes of transformations are characterized according to different sets of metrical, language theoretic, and dynamical properties they preserve. Each set of transformations we propose induces an equivalence relation over the cellular automata rule space. We give exact results on the cardinality of the quotient sets generated by these equivalence relations. Finally, we discuss some interesting open problems.

Keywords: Transformations of cellular automata rule space; Dynamical classification; Topological conjugacy; Language complexity

1. Introduction

During the past few decades, cellular automata (CA) have received a great deal of attention in different fields of science. As an example, in Physics, CA are usually considered as a particular class of dynamical systems which are able to simulate the evolution of many natural phenomena [8,17], while in Computer Science they are often viewed as computing devices capable of universal computation [1].
The problem of grouping together CA which share the same set of properties (classification problem) is central to the theory of dynamical systems and its solution would have important consequences for all the above mentioned disciplines. As an example, in Physics, the classification of CA according to their sensitivity to initial conditions is of fundamental importance, in particular for the description of chaotic behavior.

The first empirical classification of CA according to their asymptotic behavior has been given by Wolfram [18]. He divided CA in four classes according to extensive computer simulations. Afterwards, different approaches have been developed in order to give formal and effective classifications, mainly for elementary CA, i.e. one dimensional CA with radius 1 and binary set of states. These approaches consist in grouping together CA whose local rules satisfy a certain set of properties; in this way it is induced a partition of the rule space such that all the rules in the same equivalence class have the same global dynamical behavior (see e.g., [3,4,6]). In this paper we follow a different approach. We introduce a particular group (with respect to the usual composition operation) of transformations of the rule space of one dimensional CA which we call double permutations. Any subgroup $G$ of double permutations induces an equivalence relation over the CA rule space. We investigate the properties shared by CA belonging to the same equivalence class. As an example, we show that metrical double permutations preserve injectivity, surjectivity, regularity, transitivity, sensitive dependence on initial conditions, expansiveness and Lyapunov exponent [7]. Essential double permutations preserve the complexity of languages associated to CA. We wish to emphasize that our results allow one to effectively (i.e., in finite time) group CA together according to the dynamical properties they satisfy.

Finally we introduce the notion of $G_r$ graph associated with a double permutation and we prove that the problem of finding the set of fixed points of a transformation is equivalent to the problem of counting the number of cycles of its graph. Then by the Burnside's lemma we give some exact results on the cardinality of the quotient sets of the induced equivalence relation.

The rest of this paper is organized as follows. In Sections 2 and 3 we briefly review some basic concepts about transformations and we recall the definition of homomorphisms of dynamical systems. Section 4 illustrates some well known results about one dimensional CA. In Section 5 we introduce the notion of double permutation and we study some particular classes of double permutations: metrical, essential and minimal. Each class is characterized by the properties it preserves.

2. Basic concepts on transformations

Given a set $X$, a transformation of is any bijective mapping $F: X \to X$. Transformations defined over finite sets are called permutations. Let $\mathcal{F}(X)$ be the set of all the permutations of $X$ and $\circ$ the usual operation of function composition. One can easily verify that the pair $\langle \mathcal{F}(X), \circ \rangle$ is a group (the symmetric group of $X$) and that every subset of $\mathcal{F}(X)$ closed with respect to $\circ$ is a subgroup of $\langle \mathcal{F}(X), \circ \rangle$. 
Given a permutation \( \tau \in \mathcal{F}(\mathcal{P}) \), an element \( x \in \mathcal{P} \) is moved by \( \tau \) if \( \tau(x) \neq x \), otherwise the element is fixed or is a fixed point of \( \tau \). Two permutations \( \tau_1 \) and \( \tau_2 \) are disjoint if and only if the intersection between the set of elements moved by \( \tau_1 \) and the set of elements moved by \( \tau_2 \) is empty. It is easy to verify that two disjoint transformations commute with respect to \( \circ \). This last property allows us to state the following:

**Proposition 1.** Let \( \langle \mathcal{G}, \circ \rangle \) be a subgroup of \( \langle \mathcal{F}(\mathcal{P}), \circ \rangle \). If for every \( \tau_1, \tau_2 \in \mathcal{G} \), \( \tau_1 \) and \( \tau_2 \) are disjoint, then \( \langle \mathcal{G}, \circ \rangle \) is a commutative subgroup.

Let \( \mathcal{G} \subseteq \mathcal{F}(\mathcal{P}) \) be a subgroup, we define \( \mathcal{R}_\mathcal{G} \), the relation induced by \( \mathcal{G} \) on \( \mathcal{P} \), as follows:

\[ \forall x, y \in \mathcal{P} \quad x \mathcal{R}_\mathcal{G} y \iff \exists \tau \in \mathcal{G} \text{ such that } \tau(x) = y. \]

It is easy to see that \( \mathcal{R}_\mathcal{G} \) is an equivalence relation on \( \mathcal{P} \).

Let \( F(\tau) \) be the set of fixed points of the transformation \( \tau \in \mathcal{G} \), that is:

\[ F(\tau) = \{ x \in \mathcal{P} | \tau(x) = x \}. \]

A well known combinatorial result [2] gives a relation between the number of equivalence classes of \( \mathcal{R}_\mathcal{G} \) and the number of fixed points of the transformations of \( \mathcal{G} \).

**Lemma 2 (Burnside).** Let \( \mathcal{G} \subseteq \mathcal{F}(\mathcal{P}) \) be a subgroup, then the number of equivalence classes with respect to \( \mathcal{R}_\mathcal{G} \) is given by:

\[ \frac{1}{|\mathcal{G}|} \sum_{\tau \in \mathcal{G}} |F(\tau)|. \]

Finally, we recall the notion of permutation cycle:

**Definition 3.** Permutation cycle. Let \( \mathcal{G} \subseteq \mathcal{F}(\mathcal{P}) \) be a subgroup and \( \tau \in \mathcal{G} \). Let \( (x_1, \ldots, x_k) \in \mathcal{P}^k \), \( k \leq |\mathcal{P}| \). Then \( (x_1, \ldots, x_k) \) is a cycle (of length \( k \)) of the permutation \( \tau \) if and only if \( \tau(x_i) = x_{i+1} \) with \( 1 \leq i < k \) and \( \tau(x_k) = x_1 \).

Every permutation can be decomposed into a finite number of disjoint cycles.

### 3. Dynamical systems homomorphisms

A (compact) discrete time dynamical system is a pair \( \langle \mathcal{X}, f \rangle \), where \( \mathcal{X} \) is a (compact) metric space and \( f \) a continuous map of \( \mathcal{X} \) on itself.

Given two metric spaces \( \mathcal{X} \) and \( \mathcal{Y} \), a function \( \mathcal{H}: \mathcal{X} \to \mathcal{Y} \) is a homeomorphism if its continuous, invertible and its inverse function is also continuous. \( \mathcal{H} \) is an isometry if and only if \( \forall a, b \in \mathcal{X} \quad d_\mathcal{X}(a, b) = d_\mathcal{Y}(\mathcal{H}(a), \mathcal{H}(b)) \), where \( d_\mathcal{X} \) and \( d_\mathcal{Y} \) are the metrics defined on \( \mathcal{X} \) and \( \mathcal{Y} \) respectively.
Given two discrete time dynamical systems \( \langle X, f \rangle \) and \( \langle Y, g \rangle \), a function \( H: X \to Y \) is a homomorphism of dynamical systems if and only if \( H \circ f = g \circ H \), that is the following diagram commutes.

\[
\begin{array}{ccc}
X & f \rightarrow & X \\
| \downarrow H | \downarrow H | \\
Y & g \rightarrow & Y \\
\end{array}
\]

The homomorphism \( H \) is said to be a factorization if it is surjective and in this case \( Y \) is said to be a factor of \( X \). Moreover, if \( H \) is a homeomorphism then it is called a topological conjugacy and the two dynamical systems are said to be topologically conjugate. If the homomorphism \( H \) is a surjective isometry then it is called a metrical conjugacy and the two systems are said to be metrically conjugate or isomorphic.

Among the properties preserved by the above ‘morphisms’ we have: surjectivity and openness for factorizations; injectivity, denseness of periodic points, transitivity, and topological mixing for topological conjugacies; sensitivity to initial conditions, expansivity, and Lyapunov exponents for isomorphisms.

We point out that in the case of compact spaces topological conjugacies preserve expansivity and sensitivity to initial conditions too. Topological conjugacy is quite important from a dynamical systems point of view since it can be proved that the relation of topological (respectively, metrical) conjugacy is an equivalence relation for dynamical system. In the sequel we are interested in the study of particular classes of transformations of the rule space of CA that induce this equivalence relation.

4. Cellular automata

A one dimensional CA is a triple \( \langle S, N, f \rangle \), where \( S = \{0, 1, \ldots, p - 1\} \) is the set of states, \( N = \{-r, \ldots, 0, \ldots, r\} \) is the neighborhood structure with rule radius \( r \), and \( f: S^{2r+1} \to S \) is the local rule. For any fixed set of states \( S \) and any rule radius \( r \) the rule space is the set, denoted by \( \mathcal{A}(S, r) \), of all the local rules \( f: S^{2r+1} \to S \). Sometimes we will say that \( f \) is a \( (S, r) \)-CA. A one dimensional CA is elementary if \( S = \{0, 1\} \) and \( r = 1 \). Each elementary rule \( f: \{0, 1\}^3 \to \{0, 1\} \) is bijectively associated with the \( \{0, 1\} \)-valued vector \( 2^3 \) components:

\[ \xi_f = (f(1, 1, 1), f(1, 1, 0), \ldots, f(0, 0, 0)) \in \{0, 1\}^{2^3} \]

called the \( \{0, 1\} \)-vector representation of \( f \). Each elementary rule \( f \) can be encoded with the integer number \( R_f \) whose base 2 representation is \( \xi_f \). This procedure can be easily extended to non elementary one dimensional CA, representing any rule \( f \in \mathcal{A}(S, r) \) by an \( S \)-valued vector (table) \( \xi_f \) of \( p^{2r+1} \) components. The global function of a given CA with local rule \( f \) is the mapping \( G_f: \mathbb{Z} \to \mathbb{Z} \) associating to any bi-infinite \( S \)-valued sequence \( c: \mathbb{Z} \to S \), \( i \mapsto c(i) \) the bi-infinite \( S \)-valued sequence \( G_f(c): \mathbb{Z} \to S \), \( i \mapsto G_f(c)(i) \) defined as follows:

\[ G_f(c)(i) = f(c(i - r), \ldots, c(i), \ldots, c(i + r)). \]
As an example, the global function of the *shift* CA, denoted by $\sigma$, with radius $r \geq 1$ and $S$ as its set of states is defined $\forall c \in S^Z, \forall i \in \mathbb{Z}$ by $\sigma(c)(i) = c(i+1)$.

The collection $S^Z$ of all bi-infinite $S$-valued sequences is the *phase space* of the discrete time dynamics generated by iterations of the global function $G_f$; the elements of are said to be *configurations*. The mapping $d: S^Z \times S^Z \to \mathbb{R}^+$ defined by:

$$\forall x, y \in S^Z d(x, y) = \sum_{i=-\infty}^{+\infty} \frac{\delta(x_i, y_i)}{2|\delta|}$$

(where $\forall a, b \in S, \delta(a, b) = 1$ if $a \neq b$, 0 otherwise) is a metric on the phase space $S^Z$, whose corresponding topology coincides with the product topology induced by the discrete topology of $S$. With this topology $S^Z$ is a Cantor space, i.e. a compact, totally disconnected, and perfect space. A subbase of clopen (i.e., closed and open) sets for $S^Z$ consists of all the sets of the form $S_i(s) = \{c \in S^Z | c(i) = s\}$ with $s \in S$. Then every element of the base is a finite intersection of elements of the subbase. Let us recall that with respect to this topology any global function $G_f$ generated by a local rule $f$ is a continuous mapping.

Hedlund ([9], Thm. 3.4)) proved that the following two statements are equivalent.

1. $F: S^Z \to S^Z$ is continuous and commutes with the shift map (i.e. $F \circ \sigma = \sigma \circ F$).
2. $F: S^Z \to S^Z$ is a global function of a suitable local rule $f$, i.e., $F = G_f$.

A CA is injective (surjective or open, respectively) if and only if its global function is injective (surjective or open, respectively). The above properties are not independent. In [13] it is proved that surjectivity is a necessary condition for both injectivity and openness. There are many ways to decide if a rule is surjective or not. In [11, 12] it is shown that surjectivity is equivalent to the property of being balanced. A one dimensional rule is balanced if it is $k$-balanced for all $k \in \mathbb{N}$, that is if all the words in $S^*$ of length $k$ have equal multiplicity in the semi-automaton associated with the rule itself (see [11, 12] for another definition of $k$-balance). In particular a rule is 1-balanced if and only if

$$\forall s \in S\{x \in S^{2r+1} | f(x) = s\} = p^{2r},$$

where $r$ is the rule radius.

A second result is related to the notion of permutivity. Consider a CA $f \in \mathcal{R}(S, r)$. Let $(y_1, \ldots, y_{2r})$ be a fixed $2r$-tuple over $S$ then it follows that $g(x_{-r}) = f(x_{-r}, y_1, \ldots, y_{2r})$ is a mapping from $S$ to $S$. If $g(x_{-r})$ is a permutation of $S$ for every choice of $y_1, \ldots, y_{2r}$ then $f$ is *permutive* in $x_{-r}$. In an analogous way we can define permutivity in $x_r$. Hedlund in [9] proves that permutivity in $x_{-r}, (x_r)$ is a sufficient condition for the surjectivity of a CA global map.

In this paper we study a particular subgroup of transformations of the rule space that preserve injectivity, surjectivity and openness.

5. Transformations of CA rule spaces

In this section we will specialize the concept of transformation (i.e. permutuation) to the case of arbitrary (any radius and any finite set of states) CA rule spaces.
Definition 4. **Transformation of CA local rules.** Let $S$ be a finite set of states and $r$ a local radius, then a transformation of the space of $(S, r) - CA$ local rules is a one-to-one transformation from $\mathcal{R}(S, r)$ onto $\mathcal{R}(S, r)$.

The set of all transformations of the CA rule space $\mathcal{R}(S, r)$ will be denoted by $\mathcal{F}(\mathcal{R}(S, r))$. Let $h: S \rightarrow S$ be a self-inverse permutation of $S$, then we can introduce the rule space transformation $h: \mathcal{R}(S, r) \rightarrow \mathcal{R}(S, r)$ defined by the law $h(f) = (h \circ f): S^{2r+1} \rightarrow S$. We say that $h$ is the transformation of the rule space induced by the self-inverse permutation $h$. Let $\mathcal{X}$ be the set of all the transformations of the rule space induced by self-permutations of $S$.

In this paper we are particularly interested in the identical transformation $h_i: \mathcal{R}(S, r) \rightarrow \mathcal{R}(S, r)$ where $h_i(f) = f$, and the complement transformation $h_c: \mathcal{R}(S, r) \rightarrow \mathcal{R}(S, r)$, where $h_c(f): S^{2r+1} \rightarrow S$ is defined by the law $h_c(f)(x) = f(x)$ where $\forall x \in S^{2r+1}$.

Definition 5. **Double permutation of CA.** A transformation $\tau$ of CA rule space $\mathcal{R}(S, r)$ is a double permutation if and only if it is the composition of two permutations $g \in \mathcal{G}$ and $h \in \mathcal{X}$, associating to the CA rule $f: S^{2r+1} \rightarrow S$ the transformation $\tau(f) = (g \circ h)(f)$.

For instance, Table 1 contains a permutation $g$ of $(0, 1)^3$, the elementary rule $f = (0, 0, 1, 0, 1, 1, 0, 0)$, and the corresponding elementary rule obtained by applying the double permutation $\tau(g, h)(f) = h_c(f \circ g)$.

A transformation $\tau \in \mathcal{F}(\mathcal{R}(S, r))$ preserves a property $P$ if and only if every CA $f$ that satisfies $P$ is such that $\tau(f)$ satisfies $P$ too.

**Proposition 6. The class of double permutations preserves the property of being 1-balanced.**

**Proof.** Suppose that $\tau$ is $\tau(g, h)$ with $g \in \mathcal{G}$ and $h \in \mathcal{X}$. Then if $f$ is a 1-balanced rule, $\tau(f)$ is 1-balanced too since its outputs are a permutation of those of $f$, hence the cardinality of the counterimage of $s \in S$ does not change. □

| Table 1 |
| Example of double permutation of $\mathcal{R}(S, r)$ |
|---|---|---|---|
| $x$ | $g$ | $f$ | $f \circ g$ | $h_c(f \circ g)$ |
| 000 | 000 | 0 | 0 | 1 |
| 001 | 010 | 0 | 1 | 0 |
| 010 | 001 | 1 | 0 | 1 |
| 011 | 011 | 0 | 0 | 1 |
| 100 | 100 | 1 | 1 | 0 |
| 101 | 110 | 1 | 0 | 1 |
| 110 | 101 | 0 | 1 | 0 |
| 111 | 111 | 0 | 0 | 1 |
We specialize the concept of fixed point of a permutation to the case of double permutations as follows. The CA rule $f \in \mathcal{R}(S, r)$ is a fixed point of the double permutation $\tau(g, h)$ if and only if $\tau(g, h)(f) = f$, i.e. if and only if the following component-wise identity holds:

$$\forall x \in S^{2r+1} \quad f(x) = [h(f \circ g)](x).$$

A double permutation of CA can be conveniently represented by means of a graph defined as follows.

**Definition 7.** Graph of a double permutation of CA ($\mathcal{G}_\tau$). Let $\tau$ be a transformation of $(S, r) - CA$, with $\tau = \tau(g, h)$ for suitable $h, g$. The graph of $\tau$ is a structure $\mathcal{G}_\tau = \langle V, E \rangle$ where:

$$V = S^{2r+1}, \quad E = \{ (x, y) \in V \times V | y = g(x) \}.$$ 

The edges of the graph are labeled according to the mapping $\rho: E \rightarrow S$ defined in the following way:

$$\forall (x, y) \in E \quad \rho((x, y)) = [h(f \circ g)](x).$$

The labeling of the $\mathcal{G}_\tau$ graph is important since allows us to transform the problem of verifying if a rule is a fixed point of $\tau$ into a problem of existence of a labeling with certain properties. Following lemma will be useful later.

**Lemma 8.** Let $\tau = \tau(g, h_c)$ be a double permutation of CA. A CA rule $f$ is a fixed point of $\tau$ if and only if all the edges in the same cycle of $\mathcal{G}_\tau$ have the same label.

**Remark 9.** We wish to emphasize that not all double permutations can have fixed points. In fact, take $\tau(g, h, h)$ for some $g \in \mathcal{G}$. It is easy to see that $\tau$ has fixed point if and only if the cycles of $g$ have even length, except at most a cycle of period 1 in the case of $p$ odd.

**Lemma 10.** Let $\tau = \tau(g, h_c)$ be a double permutation of CA that can have fixed points. A CA rule $f$ is a fixed point of $\tau$ if and only if for all pairs of adjacent edges $(a, b)$, $(b, c)$ in the same cycle it holds that $|\rho(a, b) - \rho(b, c)| = p - 1$.

Theorem 11 put into relation the number of fixed points of some special double permutations with the number of cycles of its graph.

**Theorem 11.** Let $\tau = \tau(h_s, g)$, with $s \in \{i, c\}$ be a double permutation of CA that can have fixed points and let $k$ be the number of cycles of the $\mathcal{G}_\tau$ graph; then $|F(\tau)| = p^k$.

**Proof.** We have to distinguish two cases: $\tau(g, h_i)$ and $\tau(g, h_c)$. We prove the latter, the former is trivial. Let $x_1, \ldots, x_s \ (s > 1)$ be a cycle of $\mathcal{G}_\tau$, then it is obviously a
cycle of \( g \) and, by Remark 9, it has even length. Because of Lemma 10 we have the following set of equalities:

\[
\begin{align*}
    f(x_1) &= f(x_2) \\
    f(x_2) &= f(x_3) \\
    &\vdots \\
    f(x_s) &= f(x_1).
\end{align*}
\]

This chain of equalities has \( p \) possible solutions:

\[
\begin{align*}
    f(x_1) &= f(x_3) = \ldots = f(x_{2t-1}) = u, \\
    f(x_2) &= f(x_4) = \ldots = f(x_{2t}) = u
\end{align*}
\]

where \( s = 2t \) and \( u \in S \). The number of fixed points of \( \tau \) is given by the number of all the possible combinations of \( p \) objects out of \( k \), that is \( p^k \). \( \square \)

**Example 12.** Consider the following transformation of a given CA:

\[
\forall x, y, z \in \{0, 1\} \quad \tau(f)(x, y, z) = f(x, z, y).
\]

Fig. 1 shows the \( \mathcal{G}_\tau \) graph of \( \tau \) suitably labeled for the elementary rule of code 155. By Lemma 10, it is easy to see that this rule is not a fixed point of \( \tau \) since \( f(0, 0, 1) \neq f(0, 1, 0) \) even if the tuples \((0, 0, 1)\) and \((0, 1, 0)\) belong to the same cycle of the \( \mathcal{G}_\tau \) graph.

A double permutation \( \tau(g, h) \) is self-inverse if and only if \( g \) is self-inverse. If \( \tau \) is self inverse we have the following result which gives an upper bound for the number of fixed points of \( \tau \).
Proposition 13. Let \( \tau \) be a self inverse double permutation and \( k = p^{2^r + 1} \), then

\[
|F(\tau)| = 0 \quad \text{or} \quad |F(\tau)| \geq \begin{cases} 
2^k/2 & \text{if } p \text{ is even} \\
2^{(k+1)/2} & \text{otherwise}.
\end{cases}
\]

Proof. First of all note that a self-inverse permutation has cycles of length at most 2. Then the first part of the proposition immediately follows from Theorem 11, Lemma 8 and Lemma 10. The rest of the proof trivially follows from the observation that \( \tau \) has at least a period 1 cycle. \( \square \)

5.1. Metrical transformations

In this section we consider a particular class of transformations which preserve very important properties such as sensitivity, regularity, transitivity and even the global dynamical behavior of the CA.

The following theorems explain why we choose \( \mathcal{R} \) that way in the definition of double permutation. In fact we prove that any permutation in \( \mathcal{R} \) induces a metrical conjugacy between CA.

Theorem 14. [9] Let \( f : S \rightarrow S \) be the local rule of a radius zero CA and let \( G_f \) be its induced global function. Then the following statements are equivalent:

1. \( f \) is a permutation of \( S \)
2. \( G_f \) is a homeomorphism on \( S^Z \).

The previous theorem is due to Hedlund and may be further strengthened by the following:

Theorem 15. Let \( f : S \rightarrow S \) be the local rule of a radius zero CA and let \( G_f \) be its induced global function. Then the following statements are equivalent:

1. \( f \) is a permutation of \( S \)
2. \( G_f \) is an isometry.

Proof. Assume (i). From the definition of \( \delta \) and the fact that \( f \) is injective we have:

\[
\forall x, y \in S^Z \quad d(G_f(x), G_f(y)) = \sum_{i=-\infty}^{+\infty} \frac{\delta(f(x_i), f(y_i))}{2^{|i|}} = \sum_{i=-\infty}^{+\infty} \frac{\delta(x_i, y_i)}{2^{|i|}} = d(x, y).
\]

\( G_f \) is thus an isometry, which is trivially onto. Let us recall that any surjective isometry is necessarily continuous, invertible, and with continuous inverse.

Assume that \( f \) is not injective. Then there exists \( s, t \in S \) such that \( s \neq t \) and \( f(s) = f(t) \). We conclude that \( G_f \) is not an isometry since \( d(G_f(s), G_f(t)) = 0 \neq d(s, t) \), where \( s = (\ldots, s, s, s, \ldots) \) and \( t = (\ldots, t, t, t, \ldots) \) are the configurations which are homogeneous with respect to \( s \) and \( t \), respectively. \( \square \)
For any self-inverse permutation $h$ of $S$ let $\phi_h: S^2 \to S^2$ be the mapping defined as follows:

$$\forall c \in S^2, \forall i \in \mathbb{Z} \quad \phi_h(c)(i) = h(c(i)).$$

For any such $h$ let $\tau_h: \mathcal{R}(S, r) \to \mathcal{R}(S, r)$ be the double permutation $\tau(h, g_h)$ of the CA rule space induced by $h$, where $g_h: S^{2r+1} \to S^{2r+1}$ is the permutation defined as follows:

$$\forall(x_{-r}, \ldots, x_r), g_h(x_{-r}, \ldots, x_r) = (h(x_{-r}), \ldots, h(x_r)).$$

This double permutation induced from $h$ is then explicitly given by the law:

$$\forall(x_{-r}, \ldots, x_r), \tau_h(f)(x_{-r}, \ldots, x_r) = h(f(h(x_{-r}), \ldots, h(x_r))).$$

**Lemma 16.** Let $h$ be a self-inverse permutation of $S$, then $\phi_h$ is a surjective isometry.

**Proof.** The mapping $\phi_h$ is trivially surjective. Let us prove that $\phi_h$ is an isometry:

$$d(\phi_h(x), \phi_h(y)) = \sum_{i = -\infty}^{+\infty} \frac{1}{2^{|i|}} = \sum_{i = -\infty}^{+\infty} \frac{d(x, y)}{2^{|i|}} = d(x, y).$$

The above equalities follow from the injectivity of $h$. Since every surjective isometry is continuous, invertible with inverse continuous, we have that $\phi_h$ is a homeomorphism.

**Theorem 17.** Let $h$ be a self-inverse permutation of $S$ then the induced double permutation $\tau_h$ is an isomorphism of CA rule space $\mathcal{R}(S, r)$, in the sense that for any CA local rule $f$, the two discrete time dynamical systems $\mathcal{A} = \langle S^2, G_f \rangle$ and $\tau_h(\mathcal{A}) = \langle S^2, G_{\tau_h(f)} \rangle$ are conjugate through the surjective isometry $\phi_h$.

**Proof.** Indeed, for all $c \in S^2$:

$$G_{\tau_h(f)} \circ \phi_h)(c)(i) = G_{\tau_h(f)}(\ldots \phi_h(c) \ldots)(i) = G_{\tau_h(f)}(\ldots h(c) \ldots)(i) = h(h(f(c_{i-\tau}), \ldots, h^2(c_{i+\tau}))(i)) = h(h(f(c_{i-\tau}, \ldots, c_{i+\tau}))(i) = \phi_h \circ G_f)(c)(i) = \phi_h(\ldots f(c_{i-\tau}, \ldots, c_{i+\tau}) \ldots)(i) = \phi_h(\ldots f(c_{i-\tau}, \ldots, c_{i+\tau}) \ldots)(i).$$

Then $\phi_h \circ G_f = G_{\tau_h(f)} \circ \phi_h$. □

**Note 1.** Along the lines of Theorem 17, in the sequel, properties of the dynamical systems $\mathcal{A} = \langle S, r, f \rangle$ and $\tau(\mathcal{A}) = \langle S, r, \tau(f) \rangle$ are, for abuse of terminology, referred to the CA rules $f$ and $\tau(f)$. For instance, if $\mathcal{A}$ and $\tau_h(\mathcal{A})$ are isomorphic (i.e. metrically conjugate) then we say that $f$ and $\tau_h(f)$ are isomorphic.
In literature the following metrical transformations of CA rule space have received a big deal of attention. They associate to any rule \( f \in \mathcal{R}(S, r) \) the transformed rule defined as follows:

\[
\forall (x_{-r}, \ldots, x_0, \ldots, x_r) \in S^{2r+1} \\
\tau_i(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(x_{-r}, \ldots, x_0, \ldots, x_r) \\
\tau_n(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(x_{-1}, \ldots, x_0, \ldots, x_r) \\
\tau_r(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(x_{r}, \ldots, x_0, \ldots, x_{-r}) \\
\tau_{rn}(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(x_{r}, \ldots, x_0, \ldots, x_{-r}).
\]

It is clear that all the above transformations are double permutations, and in particular \( \tau_i, \tau_n \in \mathcal{R} \).

**Theorem 18.** Every CA \( f \) is isomorphic to \( \tau_i(f) \).

**Proof.** Let \( \phi_r : S^Z \to S^Z \) defined in this way:

\[
\forall c \in S^Z \forall i \in \mathbb{Z} \quad \phi_r(c)_i = c_{-i}.
\]

Let us prove that \( \phi_r \) is an isometry. For all \( x, y \in S^Z \) we have:

\[
d(\phi_r(x), \phi_r(y)) = \sum_{i=-\infty}^{+\infty} \frac{\delta(\phi_r(x)_i, \phi_r(y)_i)}{2^{|i|}} = \sum_{i=-\infty}^{+\infty} \frac{\delta(x_{-i}, y_{-i})}{2^{|i|}} = \sum_{j=-\infty}^{+\infty} \frac{\delta(x_j, y_j)}{2^{|j|}} = d(x, y).
\]

It is easy to see that \( \phi_r \) is surjective and therefore it is a (space) homeomorphism. Let us prove that two given CA \( f \) and \( \tau_i(f) \) are homomorphic by the homomorphism \( \phi_r \). Let \( c \in S^Z \):

\[
(\phi_r \circ G_f)(c)_i = \phi_r(\ldots, f_j(c_{-r}, \ldots c_i \cdots c_{i+r}), \ldots)_i \\
= f_j(c_{-r}, \ldots c_i \cdots c_{i+r})(G_{\tau_i(f)} \circ \phi_r(c)_i) \\
= G_{\tau_i(f)}(\ldots \phi_r(c)_{i-r} \ldots \phi_r(c)_i \ldots \phi_r(c)_{i+r}) \\
= f(\phi_r(c)_{i-r} \ldots \phi_r(c)_i \ldots \phi_r(c)_{i+r}) = f(c_{-r} \ldots c_{-i} \ldots c_{i+r}). \quad \Box
\]

Since all double permutations in \( \mathcal{T}_r = \{ \tau_i, \tau_r, \tau_n, \tau_{rn} \} \) are self-inverse, then \( \mathcal{T}_r \) is closed under \( \circ \) therefore it is a subgroup of \( \mathcal{R} \). As a consequence the induced relation \( \mathcal{R}_r \) is an equivalence relation.

**Lemma 19.** \( \tau_i, \tau_r \) have \( p^k \), \( p^{(k+1)/2} \) fixed points, respectively, where \( k = p^{2r+1} \).
Proof. To prove this lemma we use the notion of $S_{\tau}$ graph and Theorem 11. The $S_{\tau}$ graph of $\tau_i$ has only self-loops. By Theorem 11, $\tau_i$ has $p^k$ fixed points. In the $S_{\tau}$ graph of $\tau_r$, the only possible self-loops are those tuples that have symmetrical values with respect to the central element of the tuple itself. Their number is given by the permutations of $p$ objects over $r + 1$ places, that is $p^{r+1}$. The remaining tuples are forcefully cycles of order 2. Then $\tau_r$ has $p^{r+1} + (k - p^{r+1})/2 = (k + p^{r+1})/2$ cycles and, by Theorem 11, $p^{(k+p^{r+1})/2}$ fixed points. □

Lemma 20. $\tau_n$, $\tau_{rn}$ both have $p^{k/2}$ fixed points. If $p$ is even the number of fixed points is $p^{(k+1)/2}$, where $k = 2^r + 1$.

Proof. We prove the lemma only for $\tau_n$ the proof for $\tau_{rn}$ is similar.

Assume $p$ even. Since the $S_{\tau}$ graph of $\tau_n$ only contains cycles of length 2, then, by theorem 11, $\tau_n$ has $p^{k/2}$ fixed points.

Assume $p$ odd. Then $\tau_n$ has a unique loop, all the other cycles have length 2. We may conclude that the number of cycles is $(k - 1)/2 + 1 = (k + 1)/2$. Then $|F(\tau_n)| = p^{(k+1)/2}$. □

Proposition 21. Let $k = p^{2^r + 1}$ and $l = p^{r+1}$ then:

$$|F(\mathcal{R}(\mathcal{S}, r))/\mathcal{R}| = \begin{cases} \frac{p^k + p^{(k+1)/2} + 2 \cdot p^{k/2}}{4} & \text{if } p \text{ is even} \\ \frac{p^k + p^{(k+1)/2} + 2 \cdot p^{(k+1)/2}}{4} & \text{otherwise.} \end{cases}$$

Proof. The proof immediately follows from Lemma 2 and Lemma 20. □

Remark 22. As a trivial consequence of Proposition 18 and Theorem 17 we have that all the elements of the same equivalence class $\{f, \tau_2, f \tau_2, f\}$ are pairwise isomorphic.

Fig. 2 shows an example of the equivalence class of the elementary CA 154. We stress that even the space-time patterns are similar to each other.

![Fig. 2. Example of space-time patterns for the class of rule 154.](image-url)
5.2. Essential transformations

Essential transformations have been introduced by Sutner [15]. In this section we show that essential transformations preserve the language complexity of a CA. Moreover we prove that two CA in the same equivalence class (with respect to essential transformations) are not necessarily metrically conjugate. On the other hand two metrically conjugate CA have not necessarily the same language complexity.

Consider the following transformations of CA, for all $f \in \mathcal{A}(S, r)$, let $\tau_f$, $\tau_e$, $\tau_c$ and $\tau_{ce}$ be defined as follows:

\[ \forall (x_{-r}, \ldots, x_0, \ldots, x_r) \in S^{2r+1} \]

\[ \tau_c(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = \overline{f(x_{-r}, \ldots, x_0, \ldots, x_r)} \]

\[ \tau_e(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = \overline{f(x_{-r}, \ldots, x_0, \ldots, x_r)} \]

\[ \tau_{ce}(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = \overline{f(x_{-r}, \ldots, x_0, \ldots, x_r)} \]

All the above transformations are double permutations. It is easy to show that $\tau_e$ and $\tau_c$ are pairwise disjoint and that the class $\mathcal{T}_e = \{\tau_f, \tau_e, \tau_c, \tau_{ce}\}$ is closed with respect to $\circ$.

Then the induced relation $\mathcal{R}_e$ is an equivalence relation.

**Lemma 23.** $\tau_e$ has no fixed points.

**Proof.** See Remark 9.

The proof of the following lemma is very similar to the one of Lemma 19.

**Lemma 24.** Let $k = p^{2r+1}$,

\[ |F(\tau_f)| = |F(\tau_{ce})| = \begin{cases} p^{k/2} & \text{if } p \text{ is even} \\ p^{(k+1)/2} & \text{otherwise}. \end{cases} \]

**Proposition 25.** Let $k = p^{2r+1}$ then:

\[ |\mathcal{F}(\mathcal{A}(S, r))/\mathcal{R}_e| = \begin{cases} \frac{p^k + 2 \cdot p^{k/2}}{4} & \text{if } p \text{ is even} \\ \frac{p^k + 2 \cdot p^{(k+1)/2}}{4} & \text{otherwise}. \end{cases} \]

**Proof.** The proof immediately follows from the Lemma 2 and Lemma 23.

As for essential transformations the approach of topological (metrical) conjugacy in order to transfer relevant properties from a system to another is no more feasible. This is well proved in the following example:
Example 26. Consider the elementary rule 128. The transformed rule under $\tau_c$ has code 127. Suppose that there exist a $H: \{0,1\}^Z \to \{0,1\}^Z$ such that $H \circ G_{128} = G_{127} \circ H$. Let us consider the quiescent configuration $0$, then:

$$H(0) = G_{127}(H(0)).$$

that is $H(0)$ is a fixed point of $G_{127}$. A contradiction, since $G_{127}$ has no fixed points! (The claim can be proved by using the methods explained in [5]). Hence the rules 128 and 127 are not topologically conjugate.

Fig. 3 underlines the results in Example 26. Here the space-time patterns of rule 89 and 154 are completely different.

Remark 27. Example 26 underlines that there is no 'morphism' that connects two essential rules. In order to prove that essential rules preserve injectivity and surjectivity we have to follow a completely different approach. We use De Bruijn graphs. They are particular graphs associated with every CA rule and are used to describe properties of the CA themselves. For a good introduction about De Bruijn graphs and CA see [5,16]. Here we consider the product graph of De Bruijn graphs, since in [14] Sutner restates the problem of surjectivity and injectivity in terms of properties of those peculiar graphs. We denote them by $\mathcal{DB}^2$. We use the fact that if a CA has its $\mathcal{DB}^2$ isomorphic to the one of a surjective CA, then it is itself surjective. In this way we prove that $\tau_e$ and $\tau_c$ preserve injectivity and surjectivity. As for $\tau_n$, the property is trivial since $\tau_n = \tau_{re}$ is a metrical transformation.

Lemma 28. The product graph $\mathcal{DB}^2$ of the De Bruijn graphs associated with the CA $f$ and $\tau_c(f)$ are isomorphic and the isomorphism is the identity.

Proof. Let $E_f$ and $E_{f_c}$ be the edges set of $\mathcal{DB}_f^2$ and $\mathcal{DB}_{f_c}^2$, respectively. It follows that $((xy, ab), (yz, bc)) \in E_f$ if and only if $f(xyz) = f(abc)$, that is if and only if $f(xyz) = f(abc)$. The latter equality holds if and only if $((xy, ab), (yz, bc)) \in E_f$. Therefore the two graphs are isomorphic and the isomorphism is the identity. $\square$
In a similar way it can be shown that the property stated in Lemma 28 holds for \( \tau_e \) too. From Remark 27 and Lemma 28 we can state the following proposition.

**Proposition 29.** Essential transformations preserve injectivity, surjectivity and openness.

Essential transformations are also characterized by another important property: they preserve language complexity. Before proving this claim we need to explain what we mean by language associated with a CA and what we mean by its complexity.

**Definition 30.** Language associated with a configuration \( c \in S^k \) \( L(c) := \{ w = w_1 \ldots w_k \in S^* : \exists i \in \mathbb{Z}, c(i) = w_1, \ldots, c(i+k-1) = w_k \} \).

Sometimes \( L(c) \) is called the cover of \( c \).

**Definition 31.** Language associated with a CA \( f \)

\[
L(f) := \bigcup_{c \in G_f(S^k)} L(c).
\]

We denote by \( L'(f) \) the language defined as follows:

\[
L'(f) = \{ w \in S^* | w = w_1 \ldots w_n \in L(f) \}.
\]

It is a matter of thought to see that if the language associated with a CA \( f \) is \( L(f) \) then the one associated with \( \tau_e(f) \) is \( L'(f) \). Similarly, the language associated with \( \tau_e(f) \) is the same as \( L(f) \). It should be noted that, as for the minimal deterministic automaton, when we pass from \( L(f) \) to \( L'(f) \) we only relabel the edges of the transition graph. In the latter case the transition graphs of the two minimal automaton are isomorphic. Then, if we take as language complexity the size of the minimal automaton which recognizes it, by the above remarks we have proved the following:

**Proposition 32.** Essential transformations preserve language complexity.

Let \( \mu_{\mathcal{A}} \) denote the number of states of the minimal deterministic automaton recognizing the language associated with a CA. The following example shows that, in general, \( \mu_{\mathcal{A}}(f) \neq \mu_{\mathcal{A}}(\tau_e(f)) \).

**Example 33.** Consider the elementary CA of code 26, \( \tau_e(26) = 82 \). The minimal deterministic automaton for Rule 26 and 83 are shown in Figs. 4 and 5, respectively. Note that \( \mu_{\mathcal{A}}(82) \neq \mu_{\mathcal{A}}(26) \). Moreover, the two transition graphs are not isomorphic. It follows that the transformation \( \tau_e \) can not be essential.

This example illustrates the phenomenon of exponential blow-up \[15\]. In fact, rules 26 and 82 are only one bit variant from rule 90 (a surjective rule).

From Example 33 it follows that \( G_f \) and \( G_{\mathcal{A}} \) belong to distinct classes of \( \mathcal{R}_t \), while they are in the same class according to \( \mathcal{R}_s \). This proves that \( \mathcal{R}_s \) is not refinement of \( \mathcal{R}_t \).
5.3. Minimal transformations

In Sections 5.1 and 5.2 we have shown that essential and metrical transformations preserve injectivity, surjectivity and openness of the global CA rule. In this section we take the basic transformations of the two sets and create a new class of transformation which enjoy the same set of properties. In this way $\mathcal{R}_t$ and $\mathcal{R}_e$ are refinements of this new equivalence relation. A double permutation is basic iff it cannot be obtained as the composition of two other double permutations. Note, for example, that since $\tau_n = \tau_c \circ \tau_e$, 

![Diagram](image-url)
consider the following transformations of CA, let \( \tau_{rc}, \tau_{re}, \tau_{rce} \) be defined as follows:

\[
\forall (x_{-r}, \ldots, x_0, \ldots, x_r) \in \mathbb{Z}^{2r+1}
\]

\[
\tau_{rc}(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(x_r, \ldots, x_0, \ldots, x_{-r})
\]

\[
\tau_{re}(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(\overline{x}_r, \ldots, \overline{x}_0, \ldots, \overline{x}_{-r})
\]

\[
\tau_{rce}(f)(x_{-r}, \ldots, x_0, \ldots, x_r) = f(\overline{x}_r, \ldots, \overline{x}_0, \ldots, \overline{x}_{-r}).
\]

\( \tau_{rc}, \tau_{re}, \tau_{rce} \) are double permutations. Since all of them are self-inverse, and

\[
\mathcal{T}_m = \{ \tau_i, \tau_c, \tau_e, \tau_r, \tau_{ce}, \tau_{re}, \tau_{rce}, \tau_{rest}\}
\]

is closed with respect to \( \circ \), we conclude that \( \mathcal{T}_m \) is a subgroup of \( \mathcal{T}(\mathbb{Z}) \). Then the induced relation \( \mathcal{R}_m \) is an equivalence relation. We can state the following:

**Lemma 34.** \( \tau_{rc} \) has no fixed points.

**Lemma 35.** Let \( k = p^{2r+1} \) then:

\[
|F(\tau_{rc})| = |F(\tau_{ce})| = |F(\tau_{rce})| = \begin{cases} 
p^{k/2} & \text{if } p \text{ is even} \\
p^{(k+1)/2} & \text{otherwise.}
\end{cases}
\]

**Proposition 36.** Let \( k = p^{2r+1} \) and \( l = p^{r+1} \) then:

\[
|\mathcal{R}(\mathcal{T}, r)|/\mathcal{R}_m| = \begin{cases} 
p^k + p^{(k+1)/2} + 4 \cdot p^{k/2} \\8 & \text{if } p \text{ is even} \\
p^k + p^{(k+1)/2} + 4 \cdot p^{(k+1)/2} \\8 & \text{otherwise.}
\end{cases}
\]

**Proof.** The proof follows from Lemma 34, Lemma 35 and Lemma 2.

It can be easily shown that the equivalence relations \( \mathcal{R}_t \) and \( \mathcal{R}_e \) are refinements of \( \mathcal{R}_m \). Unfortunately the class \( \mathcal{T}_m \) does not preserve the properties preserved by \( \mathcal{R}_t \) and \( \mathcal{R}_e \). The properties preserved by the \( \mathcal{T}_m \) class are, as we mentioned before, injectivity, surjectivity and openness. Moreover this class has the very important property of minimizing the cardinality of the quotient set with respect to \( \mathcal{R}_m \).

6. Conclusions and open problems

In this paper we have studied transformations defined over the one dimensional CA rule space. In particular we have distinguished a particular set of transformations which we called double permutations. Representing double permutations by means of suitable
graphs we have obtained exact results about the cardinality of the quotient set of the induced equivalence relation. Then we have investigated some interesting classes of double permutations: metrical, essential and minimal ones. We characterized each class according to the set of properties it preserves. In particular we have shown that all of them preserve surjectivity. This latter property is quite significant when exploring the rule space. For example, if we consider the classification of Culik and Yu [6], all surjective CA are class one. Notwithstanding this apparent simplicity they are important because it has been shown [10] that many elementary rules that exhibit a very complex dynamics mimic surjective rules on localized subsets of their phase space. From the point of view of language complexity we have already said that those CA whose rule is one bit mutant from a surjective one show an exponential growth in the complexity of the associated language. Finally surjectivity is a necessary condition for reversibility [13]. All these examples show the importance of having transformations that preserve surjectivity when exploring the rule space.

All the surjectivity preserving double permutations we have studied are self-inverse. But being self-inverse is neither necessary nor sufficient to preserve surjectivity. In fact, consider \( \tau = \tau(g, h_l) \), where \( g \) is given in Table 2. Then \( \tau \) is a double permutation and has period 4, moreover it is easy to see that \( \tau \) preserves surjectivity. Being self-inverse in also not sufficient. Consider the double permutation described in the Example 1. We have that \( \tau(54) = 86 \) but while the rule 86 is surjective, 54 is not!

There are still many open problems about this subject, below we discuss the most interesting ones. As we have already said all the double permutations we have studied preserve surjectivity but there are some double permutations that do not have this property, so we propose the following:

**Open Problem 1.** Is the class of surjectivity preserving transformations a proper subclass of the class of double permutations?

**Open Problem 2.** Are the class of essential or topological transformations maximal with respect to language complexity or topological conjugacy?
Acknowledgements

We want to thank Klaus Sutner for many useful discussions that were at the origin of this paper.

References