Journal of Computer and System Sciences 157 (2026) 103749

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

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

A divide and conquer algorithm for deciding group cellular automata dynamics

Niccolò Castronuovo [a], Alberto Dennunzio [b,*], Luciano Margara [c]

[a] Liceo "A. Einstein", Rimini, 47923, Italy
[b] Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano-Bicocca, Viale Sarca 336/14, Milano, 20126, Italy
[c] Department of Computer Science and Engineering, University of Bologna, Cesena Campus, Via dell'Universita 50, Cesena, 47521, Italy

ARTICLE INFO

Article history:
Received 25 May 2025
Received in revised form 12 November 2025
Accepted 24 November 2025
Available online 9 December 2025

Keywords:
Cellular automata
Group cellular automata
Dynamical behavior
Chaos
Decidability

ABSTRACT

We prove that many dynamical properties of group cellular automata (GCA) can be decided by decomposing them into a set of much simpler GCA, provided those properties are decidable for such simpler GCA. Specifically, we provide a novel algorithmic technique that decomposes the GCA under investigation into a finite number of GCA, some defined on abelian groups, while others, if any, on products of simple non-abelian isomorphic groups. Importantly, the groups resulting from the decomposition depend only on the original group and are therefore completely independent of both the automaton and the considered property. Consequently, they do not inherit any aspect of the complexity of the automaton under investigation. We study the inheritance of the dynamical properties in the original GCA versus the same properties in the GCA obtained through decomposition. The latter turn out to be significantly easier to analyze than in the original GCA. Then, we show that injectivity, surjectivity, and equicontinuity/sensitivity to initial conditions can be decided by testing them in the smaller GCA produced by the decomposition. Moreover, we prove that the topological entropy of a GCA can be computed, provided one knows how to compute it for GCA defined on products of simple non-abelian isomorphic groups – for which we explicitly prove how to compute it in the surjective case – and on abelian groups. Finally, we prove that no strongly transitive, and therefore no positively expansive, GCA defined on non-abelian groups exist.

1. Introduction

Cellular Automata (CA) serve as formal models for complex systems and can be viewed as discrete-time dynamical systems consisting of a regular grid of variables, each taking values from a finite set. The overall state of a CA (with a little abuse of notation, we will use CA also to denote a single cellular automaton) is defined by the values of all variables at a specific time t, and it evolves in discrete time steps according to a specified local rule. This rule updates in a synchronous and homogeneous way each variable on the basis of the values at time $t-1$ of its neighboring variables (for an introduction to CA theory, see [1–3]).

* Corresponding author.
E-mail addresses: niccolo.castronuovo@studio.unibo.it (N. Castronuovo), alberto.dennunzio@unimib.it (A. Dennunzio), luciano.margara@unibo.it (L. Margara).

https://doi.org/10.1016/j.jcss.2025.103749

CA have been the subject of significant research and are applied in various fields, including computer science, physics, mathematics, biology, and chemistry, for purposes such as simulating natural phenomena, generating pseudo-random numbers, processing images, analyzing universal computation models, and cryptography (see for example [4–8]).

One of the central challenges in CA theory is describing the global behavior of a CA based on the analysis of its local rule. While the local rule has a finite representation (e.g., a finite table), the global behavior can encompass an arbitrarily large, potentially infinite, amount of information. In fact, the grid of variables representing the global state of the CA may have any size and the desired global behavior might only emerge after an arbitrarily large number of time steps.

Many properties related to the temporal evolution of general CA have been proved to be undecidable, including non-trivial properties of their limit sets and fundamental dynamical properties like sensitivity to initial conditions, equicontinuity, topological transitivity, and chaos (see for example [9–12]). Since in practical applications one needs to know if the CA used for modeling a certain system exhibits some specific property, this can be a severe issue.

Fortunately, the undecidability issue of dynamical properties of CA can be tackled by placing specific constraints on the model. In many cases, like the one we are exploring in this paper, the alphabet and the local rule are restricted to being a finite group and a homomorphism, respectively, giving rise to Group CA (GCA). It is important to note that these constraints do not at all hinder the effectiveness of such CA in practical applications. In fact, GCA can exhibit much of the complex behaviors of general CA and they are often used in various applications (see for example [8,13,6]).

During the last few decades, substantial efforts have been made to analyze the dynamical behavior of GCA on abelian finite groups, and more recently, on non-abelian (general) finite groups as well.

Many fundamental global properties of abelian GCA such as injectivity, surjectivity, sensitivity to the initial conditions, topological transitivity, ergodicity, positive expansivity, denseness of periodic orbits, and chaos have been fully characterized in terms of easy to check properties of their local rules (see [14–16] for GCA on $\mathbb{Z}/m\mathbb{Z}$ and [17–21,7] for GCA on general abelian groups). For GCA on $\mathbb{Z}/m\mathbb{Z}$, closed formulas for topological entropy and Lyapunov exponents were also provided in [22] and [23], respectively.

As to non-abelian GCA, preliminary results on injectivity and surjectivity were provided in [24] where the authors prove that, in dimensions $D > 1$, injectivity and surjectivity remain decidable. Later, the dynamical behavior of GCA was investigated across various classes of finite groups, including simple, symmetric, alternating, dihedral, quaternion, and decomposable groups, with initial findings reported in [25].

Surprisingly, the non-abelian nature of the group imposes significant restrictions on defining the local rule of GCA, resulting in a highly constrained class of GCA that is much more challenging to study.

In this paper, we introduce a novel and general algorithmic technique that simplifies the analysis of the dynamical properties of *any* GCA and the problem of deciding them, by reducing (the study of) the GCA to (the study of) a finite sequence of GCA, some of them defined on abelian groups and others on products of isomorphic simple groups.

Specifically, we show that several important properties (surjectivity, injectivity, sensitivity to initial conditions, equicontinuity) hold for a GCA $\mathcal{F}$ defined on a finite group G (not necessarily abelian) if and only if the same properties hold for a corresponding set $\{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$ of GCA, which are derived from $\mathcal{F}$ by means of our algorithmic decomposition technique and defined on much simpler finite groups $\{G_1, \ldots, G_k\}$, where each G_i is either abelian or the product of simple non-abelian isomorphic groups. Moreover, we prove a partial result concerning topological transitivity: the "if" part of the above mentioned equivalence (if and only if). Using the same technique, we also show that the topological entropy of a GCA can be computed, provided we know how to compute the topological entropy for GCA defined on products of simple isomorphic groups – for which, in the paper, we explicitly prove how to compute it in the surjective case – and on abelian groups, which are two open but much simpler problems.

As previously recalled, the dynamical properties of GCA on abelian groups have been fully characterized in terms of easy to check properties of their local rules, while, regarding GCA defined on the product of simple non-abelian isomorphic groups, we show in this paper that their dynamical behaviors are highly constrained and can be thoroughly analyzed, especially in the surjective case. Hence, the study of the dynamics of the GCA $\mathcal{F}$ on a group G can be effectively reduced to that of the GCA $\mathcal{F}_1, \ldots, \mathcal{F}_k$ some of them defined on abelian groups and others, if any, on products of isomorphic simple non-abelian groups, thus significantly simplifying the problem of studying the dynamical behavior of $\mathcal{F}$.

Indeed, in [24], the authors provide decidability results for almost the same properties dealt with in this paper, but, even though their results hold for the more general settings of D-dimensional GCA over a group subshift, "the algorithms extracted from our proofs are impractical and only serve the purpose of proving decidability", as explicitly declared by the authors themselves.

A crucial point is then how to get the set of $\{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$ of GCA defined on the finite groups $\{G_1, \ldots, G_k\}$ starting from any given GCA on G. We show that the those sets can be obtained by starting with the group G and repeatedly applying the quotient operation by any non-trivial normal and fully invariant subgroup (invariant under the action of any group endomorphism), our algorithmic decomposition technique being just the implementation of all this and based on a divide and conquer strategy (see Algorithm 1 and 2 in Section 5). At each quotienting step, we obtain two smaller groups (and correspondingly two GCA): the fully invariant normal subgroup and the quotient group. The quotienting process ends when we either obtain an abelian group or reach groups that do not admit any non-trivial normal and fully invariant subgroups. According to the theory, we know that these groups are, in fact, products of isomorphic copies of a simple group.

As overall result, our decomposition technique turns out to be an alternative way for testing the decidability of injectivity, surjectivity and, in the surjective case, sensitivity to initial conditions/equicontinuity for GCA. We stress that our method

relies on the analysis of the group on which the GCA is defined and on its local rule, independently of the dynamics produced by the time evolution of the GCA global rule. Indeed, the group decomposition is fully independent of both the GCA rule and GCA complexity. It can be performed once and reused to study many different GCA defined on the same group. In addition, we prove that there are no strongly transitive nor positively expansive GCA on non-abelian groups.

We are confident that the same decomposition technique used for one-dimensional GCA could also be successfully applied for other properties and in dimensions $D > 1$.

The rest of this paper is organized as follows.

Section 2 contains the basic group theory notions and results needed throughout the paper. In Section 3 we recall the fundamental definitions and known facts about CA and their topological and dynamical properties. Section 4 is devoted to the study of fundamental properties of GCA, such as injectivity, surjectivity, sensitivity to initial conditions, equicontinuity, topological transitivity, and topological entropy. We prove a series of results that allow us to reduce determining whether a given property holds for a GCA on a group G to checking if the same property holds for two GCA both defined on two smaller groups: a suitable normal subgroup H of G and the quotient group G/H. We also prove that a GCA on a non-abelian group can be neither strongly transitive nor positively expansive. Furthermore, we provide several results concerning the equivalence of dynamical, topological, and metric properties, which are typically distinct in the context of general CA. In Section 5, we provide our decomposition technique allowing one to exploit the results from Section 4 to reduce the study of a given property for a GCA to the analysis of a number of GCA defined on just two types of groups: abelian groups and products of isomorphic copies of simple non-abelian groups. We also provide the decidability results of the dynamical properties for GCA. Finally, Section 6 contains some concluding remarks and a list of open questions.

2. Preliminary results and notions on groups

In this section, we recall the basic notions on groups and we prove a few preliminary lemmata that will be useful in the subsequent discussion. Readers unfamiliar with group theory can refer to [26].

A *group* G is an algebraic structure consisting of a set of elements along with an operation (we will use multiplication) satisfying the following conditions: the operation is associative, it has an *identity element* $e \in G$, and every element $g \in G$ has an *inverse element* $g^{-1} \in G$. If in addition the operation is commutative then the group is said to be *abelian*.

Let G be a group. The *order* of an element $g \in G$ is the smallest positive integer n such that $g^n = e$. If no such integer exists, g is said to have infinite order, though this is irrelevant for finite groups. If G is finite, the *order* of G, denoted by $|G|$, is the number of elements in G. A set $H \subseteq G$ is a *subgroup* of G, denoted by $H \leq G$, if H forms a group with the same operation of G. The set $\{e\}$ is called the *trivial* group and is a subgroup of any group. A subgroup N of G is said to be *normal* (denoted by $N \trianglelefteq G$) if for all $g \in G$ and $n \in N$, it holds that $gng^{-1} \in N$. The *centralizer* of a subset $S \subseteq G$ is the subgroup $C_G(S) = \{x \in G : xg = gx \text{ for all } g \in S\}$, while the *center* of a group G is the set $\mathrm{Z}_G = \{g \in G : gh = hg \text{ for all } h \in G\}$. Clearly, $C_G(G) = \mathrm{Z}_G$ and it is well-known that Z_G is an abelian and normal subgroup of G.

A subset $S \subseteq G$ is called a *generating set* of G if every element of G can be written as a finite product of elements in S and their inverses. In this case, we write $G = \langle S \rangle$. The *commutator* of two elements $g, h \in G$ is $[g, h] = ghg^{-1}h^{-1}$ and the *commutator subgroup* (or derived subgroup) of G, is the subgroup $[G, G] = \langle \{[g, h] : g, h \in G\} \rangle$ generated by all commutators of elements of G. A group G is said to be *perfect* if $G = [G, G]$.

Let N be a normal subgroup of G. The *quotient group* is the set $G/N = \{gN : g \in G\}$, where each element $gN = \{gn : n \in N\}$ is called *left coset* of N in G and it is also denoted by $[g]$. The operation on G/N is the coset multiplication: $(gN)(hN) = (gh)N$ for all $g, h \in G$. The order of the quotient group G/N is given by $|G/N| = \frac{|G|}{|N|}$. It is customary to denote by π the map $\pi : G \to G/N$ associating each element g with its coset gN.

The group G is called *simple group* if it is a nontrivial group and it has no proper nontrivial normal subgroups, while G is said to be a *quasi-simple group* if it is a perfect group such that G/Z_G is a simple group.

Given two groups G and H, their *direct product* is the group $G \times H$ consisting of ordered pairs (g, h), where $g \in G$ and $h \in H$, with the group operation defined component-wise: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$. The identity element of $G \times H$ is (e_G, e_H), where e_G and e_H are the identity elements of G and H, respectively.

A *homomorphism* between two groups G and H is a map $\varphi : G \to H$ such that for all $a, b \in G$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. The set of all homomorphisms from G to H is denoted $\mathrm{Hom}(G, H)$. A bijective homomorphism $\varphi : G \to H$ is called *isomorphism* and G and H are said to be *isomorphic* (denoted $G \cong H$). An *endomorphism* (resp., *automorphism*) is a homomorphism (resp., isomorphism) from a group to itself. $\mathrm{End}(G)$ and $\mathrm{Aut}(G)$ stand for the sets of all the endomorphisms and automorphisms of a group G, respectively. The set $\mathrm{Aut}(G)$ forms a group under composition of functions.

The *kernel* of a homomorphism $\varphi : G \to H$ is the set $\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\}$, where e_H is the identity element of H. The kernel is a normal subgroup of G. The homomorphism φ is said to be *trivial* iff $\mathrm{Ker}(\varphi) = G$. As usual, $\mathrm{Im}(h)$ denotes the image of h.

A subgroup H of a group G is *characteristic* if $\varphi(H) \leq H$ for every $\varphi \in \mathrm{Aut}(G)$. As an example, the center of a group is a characteristic subgroup. A stronger property is fully invariance. A *fully invariant* subgroup of a group G is a subgroup H of G such that, for every $\phi \in End(G)$, $\phi(H) \leq H$. In other terms, the restriction of an endomorphism of G to a fully invariant subgroup H induces an endomorphism on H. We recall that a fully invariant subgroup is normal and the commutator subgroup of any group is a fully invariant subgroup.

Lemma 1. *Let G and G' be two groups and let $f \in \mathrm{Hom}(G, G')$. If $N' \trianglelefteq G'$ then the preimage $f^{-1}[N']$ is a normal subgroup of G. If f is surjective and $N \trianglelefteq G$, $f(N)$ is a normal subgroup of G'.*

Now we introduce a notation that will be systematically used in the following. Let e be the identity element of a group G. If $f \in \mathrm{Hom}(G^k, G)$, we will write $f = (h_1, \ldots, h_k)$ in which $h_i \in \mathrm{End}(G)$ is defined, for all $g \in G$, as $h_i(g) = f(e, \ldots, e, g, e, \ldots, e)$, where g occupies the i-th position in f and all the other entries are equal to e.

Lemma 2. *Let $f \in \mathrm{Hom}(G^k, G)$ with $f = (h_1, \ldots, h_k)$. Let $N \trianglelefteq G$. Then, for every i, $h_i(N)$ is normal in $\mathrm{Im}(f)$. In particular, if f is surjective, every $\mathrm{Im}(h_i)$ is normal in G.*

Proof. This follows by Lemma 1 and the fact that if $N \trianglelefteq G$ then the subgroup M_i of G^k consisting of the k-tuples with the i-th component in N and all the others equal to e is a normal subgroup of G^k and $h_i(N) = f(M_i)$. □

Lemma 3. *Let $f \in \mathrm{Hom}(G^k, G)$ be a surjective homomorphism. Then, $f(\mathrm{Z}_G^k) \subseteq \mathrm{Z}_G$. In particular, if $f = (h_1, \ldots, h_k)$, it holds that $h_j(\mathrm{Z}_G) \subseteq \mathrm{Z}_G$ for every j.*

Proof. Consider $(a_1, \ldots, a_k) \in \mathrm{Z}_G^k$ and $(b_1, \ldots, b_k) \in G^k$. We get

$$\begin{aligned} f(a_1, \ldots, a_k) f(b_1, \ldots, b_k) &= f(a_1 b_1, \ldots, a_k b_k) \\ &= f(b_1, \ldots, b_k) f(a_1, \ldots, a_k) \ . \end{aligned}$$

Since f is surjective this implies that $f(a_1, \ldots, a_k) \in \mathrm{Z}_G$. In particular, $f(e, \ldots, e, a_i, e, \ldots, e) = h_i(a_i) \in \mathrm{Z}_G$ for every $a_i \in \mathrm{Z}_G$. □

3. About CA and GCA

In this section, we review the fundamental definitions and key results related to CA and GCA. For additional definitions and results, we refer the reader to those introduced in [25].

3.1. CA configurations

Let G be a finite set. A CA *configuration* is any function from $\mathbb{Z}$ to G, i.e., an element of $G^{\mathbb{Z}}$. Given a configuration $c \in G^{\mathbb{Z}}$ and any integer $i \in \mathbb{Z}$, the value of c at position i is denoted by c_i, while for any $i, j \in \mathbb{Z}$ with $i \leq j$ we note $c_{[i,j]} = c_i \ldots c_j \in G^{j-i+1}$.

The set $G^{\mathbb{Z}}$ is also a topological space with the *prodiscrete topology*, i.e., the product topology when each factor G is given the discrete topology. For any $i, j \in \mathbb{Z}$ with $i \leq j$ and any $u \in G^{j-i+1}$, the *cylinder* $C([i, j], u)$ is the subset of $G^{\mathbb{Z}}$ defined as

$$C([i, j], u) := \{c \in G^{\mathbb{Z}} : c_{[i,j]} = u\}$$

The cylinders form a clopen basis for the prodiscrete topology and, when equipped with that topology, $G^{\mathbb{Z}}$ turns out to be a compact, Hausdorff, and totally disconnected topological space. Moreover, $G^{\mathbb{Z}}$ is Polish space, i.e., a separable completely metrizable topological space. Indeed, the set $G^{\mathbb{Z}}$ can be equipped with the standard Tychonoff ultrametric d defined as

$$\forall c, c' \in G^{\mathbb{Z}} : \ d(c, c') = \begin{cases} 0 & \text{if } c = c' \\ 2^{-\Delta(c,c')} & \text{otherwise} \end{cases}$$

where $\Delta(c, c') = \min\{|j| : j \in \mathbb{Z} \text{ and } c_j \neq c'_j\}$ and the topology induced by the Tychonoff metric coincides with the prodiscrete topology. Since it has no isolated points, the set $G^{\mathbb{Z}}$ is also a Cantor space.

3.2. CA

A *CA* on G is any continuous function $\mathcal{F} : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ which also shift commuting, i.e., $\mathcal{F} \circ \sigma = \sigma \circ \mathcal{F}$, where the shift map $\sigma : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is defined as follows

$$\forall c \in G^{\mathbb{Z}}, \forall i \in \mathbb{Z} : \ \sigma(c)_i = c_{i+1}.$$

Any CA can be equivalently defined by means of a *local rule* $f : G^{2\rho+1} \to G$, where $\rho \in \mathbb{N}$ (see [1]). Namely, a CA $\mathcal{F}$ with local rule f is defined as follows:

$$\forall c \in G^{\mathbb{Z}}, \ \forall i \in \mathbb{Z} : \ \mathcal{F}(c)_i = f(c_{i-\rho}, \ldots, c_{i+\rho}).$$

A CA $\mathcal{F}$ is said to be *injective* (*surjective*) if the map $\mathcal{F}$ is injective (surjective). We recall that injective CA are surjective and a CA is surjective if and only if every configuration has a finite and uniformly bounded number of pre-images [1]. A CA $\mathcal{F}$ is said to be *open* if $\mathcal{F}$ is an open map with respect to the prodiscrete topology, i.e., if it maps open sets to open sets.

A CA $\mathcal{F}$ is *topologically transitive* if for any pair of nonempty open subsets $U, V \subseteq G^{\mathbb{Z}}$ there exists a natural $t > 0$ such that $\mathcal{F}^t(U) \cap V \neq \emptyset$, while it is said to be *topologically mixing* if for any pair of nonempty open subsets $U, V \subseteq G^{\mathbb{Z}}$ there exists a natural t_0 such that the previous intersection condition holds for all $t \geq t_0$. A CA $\mathcal{F}$ is said to be *topologically weakly mixing* if the CA $\mathcal{F} \times \mathcal{F}$ is topologically transitive, while it is *totally transitive* if $\mathcal{F}^t$ is topologically transitive for all $t > 0$. A CA $\mathcal{F}$ is *strongly transitive* if for any nonempty open subset $U \subseteq G^{\mathbb{Z}}$ it holds that $\bigcup_{t\in\mathbb{N}} \mathcal{F}^t(U) = X$. Strongly transitive CA are topologically transitive and topologically transitive CA are surjective. Strongly transitive CA cannot be injective.

A CA $\mathcal{F}$ is *sensitive to initial conditions* if there exists $\epsilon > 0$ such that for any $\delta > 0$ and $c \in G^{\mathbb{Z}}$ there is a configuration $c' \in G^{\mathbb{Z}}$ with $0 < d(c', c) < \delta$ such that $d(\mathcal{F}^t(c'), \mathcal{F}^t(c)) \geq \epsilon$ for some natural t. Sensitivity to initial conditions is the well-known basic component and essence of the chaotic behavior of discrete time dynamical systems.

A CA $\mathcal{F}$ has *dense periodic orbits* (DPO) if the set of its periodic points is dense in $G^{\mathbb{Z}}$, where a periodic point for $\mathcal{F}$ is any configuration $c \in G^{\mathbb{Z}}$ such that $F^h(c) = c$ for some natural $h > 0$.

Sensitivity to initial conditions, topological transitivity and DPO are the features that together define the popular notion of *chaos* according to the Devaney definition [27].

A CA $\mathcal{F}$ is said to be *equicontinuous* if for any $\epsilon > 0$ there exists $\delta > 0$ such that for all $c, c' \in G^{\mathbb{Z}}$, $d(c, c') < \delta$ implies that $\forall k \in \mathbb{N}$, $d(\mathcal{F}^k(c'), \mathcal{F}^k(c')) < \epsilon$.

Note that there are CA that are neither sensitive to initial conditions nor equicontinuous, and these are called almost equicontinuous. As we will state in Lemma 6, this intermediate case does not exist for GCA.

A CA $\mathcal{F}$ is *positively expansive* if for some constant $\varepsilon > 0$ it holds that for any pair of distinct configurations $c, c' \in G^{\mathbb{Z}}$ there exists a natural number t such that $d(\mathcal{F}^t(c), \mathcal{F}^t(c')) \geq \varepsilon$. We emphasize that positive expansivity is a strong form of chaos. Indeed, on one hand, positive expansivity for a CA is a stronger condition than sensitivity to initial conditions. On the other hand, any positively expansive CA is also strongly transitive (due to the fact that positively expansive CA are topologically conjugated to mixing subshifts of finite type, see [28,29]), and, at the same time, it has DPO. Therefore, any positively expansive CA is chaotic according to Devaney's definition of chaos. Clearly, from the above mentioned result from [28,29] or the classical result in a more general case than CA [30,31], it follows that if a CA $\mathcal{F}$ is positively expansive, then it is surjective but not injective.

Topological entropy is one of the most studied properties of dynamical systems. Informally, the topological entropy measures the uncertainty of the forward evolution of any dynamical system in the presence of incomplete description of initial configurations. The definition of topological entropy $\mathcal{H}(F)$ of a continuous map $F : X \to X$ over a compact space X was introduced in [32]. For 1-dimensional CA $\mathcal{F}$, the definition of topological entropy is equivalent to the following [11]. Let $R(w, t)$ denote the number of distinct rectangles of width w and height t occurring in a space-time evolution diagram of $\mathcal{F}$, i.e., the cardinality of the set $\{(\mathcal{F}^i(c)_j)_{0\leq i<t,\, 0\leq j<w} \mid c \in G^{\mathbb{Z}}\}$. Then,

$$\mathcal{H}(\mathcal{F}) = \lim_{w\to+\infty} \lim_{t\to+\infty} \frac{\log R(w,t)}{t} \ .$$

In order to apply *ergodic theory* to CA we need to define the collection $\mathcal{M}$ of the measurable subsets of $G^{\mathbb{Z}}$ and a probability measure $\mu : \mathcal{M} \to [0, 1]$. We will use the (normalized) *Haar measure* μ which is defined over the σ-algebra of the cylinders of $G^{\mathbb{Z}}$. Such a measure μ is the product measure induced by the uniform probability distribution over G. In particular, for every cylinder $C([i, j], u)$ it holds that $\mu(C([i, j], u)) = \frac{1}{|G|^{j-i+1}}$.

Let $\mathcal{F}$ be a CA which is measure-preserving with respect to μ, i.e., $\mu(E) = \mu(F^{-1}(E))$ for every $E \in \mathcal{M}$. The CA $\mathcal{F}$ is said to be *ergodic* with respect to μ if for every $E \in \mathcal{M}$ it holds that $(F^{-1}(E) = E) \Rightarrow \mu(E)(1 - \mu(E)) = 0$. The CA $\mathcal{F}$ is *ergodic strong mixing* (resp., *ergodic weak mixing*) if for any pair of sets $A, B \in \mathcal{M}$, it holds that $\lim_{n\to\infty} \mu(F^{-n}(A) \cap B) = \mu(A)\mu(B)$ (resp., $\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \left|\mu\left(F^{-k}(A) \cap B\right) - \mu(A)\mu(B)\right| = 0$).

3.3. GCA

Let G be a finite group with identity element e. The set $G^{\mathbb{Z}}$ is also a group, with the component-wise operation defined by the group operation of G, and we denote by $e^{\mathbb{Z}}$ the configuration taking the value e at every integer position, i.e., $e^{\mathbb{Z}}$ is the identity element of the group $G^{\mathbb{Z}}$. Clearly, when equipped with the prodiscrete topology, $G^{\mathbb{Z}}$ turns out to be both a profinite and Polish group. A configuration $c \in G^{\mathbb{Z}}$ is said to be *finite* if the number of positions $i \in \mathbb{Z}$ such that $c_i \neq e$ is finite.

If $H \leq G$, then $H^{\mathbb{Z}}$ is a closed subgroup of $G^{\mathbb{Z}}$. Moreover, $H \trianglelefteq G$ if and only if $H^{\mathbb{Z}} \trianglelefteq G^{\mathbb{Z}}$. In this case, the prodiscrete topologies on $H^{\mathbb{Z}}$ and $(G/H)^{\mathbb{Z}}$ agree with the subspace topology on $H^{\mathbb{Z}}$ and with the quotient topology on $(G/H)^{\mathbb{Z}}$, respectively.

A CA $\mathcal{F} : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is said to be a *GCA* if $\mathcal{F}$ is an endomorphism of $G^{\mathbb{Z}}$. In that case, by [33, Lemma 3], the local rule of $\mathcal{F}$ is a homomorphism $f : G^{2\rho+1} \to G$. The *kernel of a GCA* $\mathcal{F}$ is $Ker(\mathcal{F}) = \{c \in G^{\mathbb{Z}} : \mathcal{F}(c) = e^{\mathbb{Z}}\}$.

Given any function $f : G^{2\rho+1} \to G$, by [34, Lemma 8] (see also the later [25, Thm. 1]), it holds that $f \in \mathrm{Hom}(G^{2\rho+1}, G)$ if and only if there exist $2\rho + 1$ endomorphisms $h_{-\rho}, \ldots, h_\rho \in \mathrm{End}(G)$, such that $f(g_{-\rho}, \ldots, g_\rho) = h_{-\rho}(g_{-\rho}) \cdots h_\rho(g_\rho)$ for

all $g_{-\rho}, \dots, g_\rho \in G$ and $\mathrm{Im}(h_i) \subseteq C_G(\mathrm{Im}(h_j))$ for every $i \neq j$. In this case, according to the notation introduced in Section 2, we will write $f = (h_{-\rho}, \dots, h_\rho)$. Notice that some of the h_i's could be trivial but we will always assume, if not otherwise stated, that at least one between $h_{-\rho}$ and h_ρ is non-trivial. In this case ρ will be said to be *the radius* of the GCA $\mathcal{F}$ and will be indicated also with $\rho(\mathcal{F})$.

Remark 1. We stress that if H is any fully invariant subgroup of G and $\mathcal{F}$ is any GCA, then it holds that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. This is a consequence of the fact that the local rule of $\mathcal{F}$ is $f = (h_{-\rho}, \dots, h_\rho)$ for some endomorphisms $h_{-\rho}, \dots, h_\rho \in \mathrm{End}(G)$ and, since H is fully invariant, $h_i(H) \subseteq H$ for every $i \in \{-\rho, \dots, \rho\}$.

A GCA with local rule f is called *shift-like* if $\rho \geq 1$ and only one between the h_i's is non trivial, while it is called *identity-like* if $\rho = 0$. Surjective shift-like GCA are topologically transitive.

We recall here the following Theorem (which is a slight generalization of [25, Thm. 5]) that states that, for simple non-abelian and quasi-simple groups, the structure of GCA is almost trivial.

Theorem 1. *Let G be a simple non-abelian or a quasi-simple group. Then, any GCA on G is either shift-like or identity-like.*

Proof. It follows from the fact that every endomorphism of a simple or a quasi-simple group is trivial or an automorphism. □

4. Dynamical properties of GCA through group quotients

In this section, we show how to reduce the study of a number of dynamical properties of any GCA on a group G to that of two GCA defined on two smaller groups: a normal subgroup H of G and the quotient group G/H.

In the following, if G is a group and $H \trianglelefteq G$, the coset of the element $x \in G$ in G/H will be $[x] := xH$. Moreover, if $c = (\dots c_{-1}c_0c_1\dots) \in G^{\mathbb{Z}}$, then $[c]$ will denote the element of $(G/H)^{\mathbb{Z}}$ given by $(\dots[c_{-1}][c_0][c_1]\dots)$.

Definition 1. Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. Then, the maps

$$\overline{\mathcal{F}}_H : H^{\mathbb{Z}} \to H^{\mathbb{Z}} \text{ and}$$
$$\widetilde{\mathcal{F}}_H : (G/H)^{\mathbb{Z}} \to (G/H)^{\mathbb{Z}}$$

are defined as follows:

$$\forall c \in H^{\mathbb{Z}} : \overline{\mathcal{F}}_H(c) := \mathcal{F}(c) \text{ and} \tag{1}$$
$$\forall [c] \in (G/H)^{\mathbb{Z}} : \widetilde{\mathcal{F}}_H([c]) := [\mathcal{F}(c)]. \tag{2}$$

Note that, by Equations (1) and (2) and since $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$, $\overline{\mathcal{F}}_H$ and $\widetilde{\mathcal{F}}_H$ are well-defined GCA on $H^{\mathbb{Z}}$ and $(G/H)^{\mathbb{Z}}$, respectively. From now on, when the group H is clear from the context, we will simplify the notation by using $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$ in place of $\overline{\mathcal{F}}_H$ and $\widetilde{\mathcal{F}}_H$. Clearly, it holds that if $\mathcal{F}$ is a GCA on the group G with local rule $f = (h_{-\rho}, \dots, h_\rho)$ and $H \trianglelefteq G$, then $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$ if and only if $f(H^{2\rho+1}) \subseteq H$ if and only if $h_i(H) \subseteq H$ for every $-\rho \leq i \leq \rho$.

We also stress that if $f = (h_{-\rho}, \dots, h_\rho)$ is the local rule of $\mathcal{F}$, then the local rules $\overline{f}$ and $\widetilde{f}$ of $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$ are $\overline{f} = (h_{-\rho}|_H, \dots, h_\rho|_H)$ and $\widetilde{f} = (\widetilde{h}_{-\rho}, \dots, \widetilde{h}_\rho)$ where $h_i|_H$ is the restriction of h_i to H and $\widetilde{h}_i([x]) = [h_i(x)]$ for every $x \in G$.

Let us begin considering the two properties that are perhaps the most widely known and studied: surjectivity and injectivity.

Theorem 2. *Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. Then, $\mathcal{F}$ is surjective (resp., injective) if and only if both $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are surjective (resp., injective).*

Proof. It is well known [1] that a GCA $\mathcal{F}$ is surjective if and only if $\mathrm{Ker}(\mathcal{F})$ is finite and is injective if and only if $\mathrm{Ker}(\mathcal{F})$ contains only $e^{\mathbb{Z}}$. In particular, if $\mathcal{F}$ is injective it is also surjective. Clearly $\mathrm{Ker}(\overline{\mathcal{F}}) \subseteq \mathrm{Ker}(\mathcal{F})$. Thus, if $\mathcal{F}$ is surjective then $\overline{\mathcal{F}}$ is surjective and if $\mathcal{F}$ is injective then $\overline{\mathcal{F}}$ is injective. Moreover,

$$\begin{aligned}\mathrm{Ker}(\widetilde{\mathcal{F}}) &= \{[c] \in (G/H)^{\mathbb{Z}} : \widetilde{\mathcal{F}}([c]) = [e]^{\mathbb{Z}}\} \\ &= \{[c] \in (G/H)^{\mathbb{Z}} : [\mathcal{F}(c)] = [e]^{\mathbb{Z}}\} \\ &= \{[c] \in (G/H)^{\mathbb{Z}} : \exists h \in H^{\mathbb{Z}}, \mathcal{F}(c)h = e^{\mathbb{Z}}\}.\end{aligned}$$

Suppose now that $\mathcal{F}$ is surjective. Since in this case $\overline{\mathcal{F}}$ is also surjective, for every $h \in H^{\mathbb{Z}}$ there exists $h' \in H^{\mathbb{Z}}$ such that $\mathcal{F}(h') = h$. Thus, the previous set can be written as

$$\{[c] \in (G/H)^{\mathbb{Z}} : \exists h' \in H^{\mathbb{Z}}, \mathcal{F}(ch') = e^{\mathbb{Z}}\}.$$

Hence, for every $[c] \in \mathrm{Ker}(\widetilde{\mathcal{F}})$ there exists an element $ch' \in \mathrm{Ker}(\mathcal{F})$. Notice that if two elements $[c_1]$ and $[c_2]$ of $\mathrm{Ker}(\widetilde{\mathcal{F}})$ give rise to the same element $c_1 h'_1 = c_2 h'_2$ of $\mathrm{Ker}(\mathcal{F})$, then $c_1 = c_2 h'_2 (h'_1)^{-1}$ and so $[c_1] = [c_2]$. As a consequence, there exists an injective map from $\mathrm{Ker}(\widetilde{\mathcal{F}})$ to $\mathrm{Ker}(\mathcal{F})$. Since $\mathcal{F}$ is surjective, $\mathrm{Ker}(\mathcal{F})$ is finite. Thus, $\mathrm{Ker}(\widetilde{\mathcal{F}})$ is also finite and $\widetilde{\mathcal{F}}$ is surjective. If $\mathcal{F}$ is also injective, $\mathrm{Ker}(\mathcal{F}) = \{e^{\mathbb{Z}}\}$ and, hence, we get that $\mathrm{Ker}(\widetilde{\mathcal{F}}) = \{[e]^{\mathbb{Z}}\}$. Thus, $\widetilde{\mathcal{F}}$ is injective.

Assume now that $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are surjective. We want to show that $\mathcal{F}$ is surjective. Let $c \in G^{\mathbb{Z}}$. Since $\widetilde{\mathcal{F}}$ is surjective there exists $[d] \in (G/H)^{\mathbb{Z}}$ such that $\widetilde{\mathcal{F}}([d]) = [c]$. This is equivalent to state that there exists $h \in H^{\mathbb{Z}}$ with $\mathcal{F}(d)h = c$. Since $\overline{\mathcal{F}}$ is surjective, there exists $h' \in H^{\mathbb{Z}}$ such that $\mathcal{F}(h') = h$. In this way we get $\mathcal{F}(dh') = c$ and, therefore, $\mathcal{F}$ is surjective.

To complete the proof we have to show that if $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are injective then $\mathcal{F}$ is injective. Let $c \in G^{\mathbb{Z}}$ such that $\mathcal{F}(c) = e^{\mathbb{Z}}$. Then, $\widetilde{\mathcal{F}}([c]) = [e]^{\mathbb{Z}}$. Since $\widetilde{\mathcal{F}}$ is injective this implies that $[c] = [e]^{\mathbb{Z}}$, i.e., $c \in H^{\mathbb{Z}}$. Thus, $\overline{\mathcal{F}}(c) = \mathcal{F}(c) = e^{\mathbb{Z}}$ and, since $\overline{\mathcal{F}}$ is injective, $c = e^{\mathbb{Z}}$. This proves that $\mathcal{F}$ is injective. □

In the next lemma, we prove that if a GCA $\mathcal{F}$ defined on a finite group G is surjective, then the kernel of $\mathcal{F}$ is entirely contained in $\mathrm{Z}_G^{\mathbb{Z}}$.

Lemma 4. *Let $\mathcal{F}$ be a GCA on a finite group G. If $\mathcal{F}$ is surjective then* $\mathrm{Ker}(\mathcal{F}) \subseteq \mathrm{Z}_G^{\mathbb{Z}}$.

Proof. Let $\mathcal{F}$ be a GCA on a finite group G. The kernel of $\mathcal{F}$ is clearly σ-invariant, i.e., if $c \in \mathrm{Ker}(\mathcal{F})$ then $\sigma(c) \in \mathrm{Ker}(\mathcal{F})$. If $\mathcal{F}$ is surjective, then $\mathrm{Ker}(\mathcal{F})$ is a finite set. As a consequence, every element $c \in \mathrm{Ker}(\mathcal{F})$ must be σ-periodic, i.e., there exists $m \in \mathbb{Z}$ such that $\sigma^m(c) = c$. Let $c \in \mathrm{Ker}(\mathcal{F})$ and assume by contradiction that there exists $i \in \mathbb{Z}$ such that $c_i \notin \mathrm{Z}_G$. Then, there exists $g_i \in G$ such that $g_i^{-1} c_i g_i \neq c_i$. Consider the configuration $g \in G^{\mathbb{Z}}$ with g_i in position i and $g_j = e$ for every $j \neq i$. Since $\mathrm{Ker}(\mathcal{F})$ is a normal subgroup of $G^{\mathbb{Z}}$, then $g^{-1} c g \in \mathrm{Ker}(\mathcal{F})$. Since $g^{-1} c g$ is not σ-periodic, we get a contradiction. □

Notice that, if a GCA $\mathcal{F}$ is surjective, its local rule f is surjective and therefore $\mathcal{F}(\mathrm{Z}_G^{\mathbb{Z}}) \subseteq \mathrm{Z}_G^{\mathbb{Z}}$ by Lemma 3. Thus, if $\mathcal{F}$ is surjective, $\overline{\mathcal{F}}_{\mathrm{Z}_G}$ and $\widetilde{\mathcal{F}}_{\mathrm{Z}_G}$ are well-defined.

Corollary 1. *Let G be a finite group and let $\mathcal{F}$ be a surjective GCA on G. It holds that $\mathcal{F}$ is injective if and only if $\overline{\mathcal{F}}_{\mathrm{Z}_G}$ is injective.*

Proof. By Lemma 4, it follows that $\mathrm{Ker}(\mathcal{F}) \subseteq Z_G^{\mathbb{Z}}$. Hence, it holds that $\mathrm{Ker}(\mathcal{F}) = \mathrm{Ker}(\overline{\mathcal{F}})$. The thesis follows from the fact that a GCA is injective if and only if its kernel contains only $e^{\mathbb{Z}}$. □

Corollary 2. *Let G be a finite group and let $\mathcal{F}$ be a surjective GCA on G. It holds that $\widetilde{\mathcal{F}}_{\mathrm{Z}_G}$ is bijective.*

Proof. Let $[c]$ be an element of $\mathrm{Ker}(\widetilde{\mathcal{F}})$, that is to say $\mathcal{F}(c) \in \mathrm{Z}_G^{\mathbb{Z}}$. Since $\mathcal{F}$ is surjective, by Theorem 2, $\overline{\mathcal{F}}_{\mathrm{Z}_G}$ is also surjective. Thus, there exists $c' \in \mathrm{Z}_G^{\mathbb{Z}}$ such that $\mathcal{F}(c') = \mathcal{F}(c)$. Hence, $c = c'z$ for some $z \in \mathrm{Ker}(\mathcal{F})$. Since, by Lemma 4, $\mathrm{Ker}(\mathcal{F}) \subseteq \mathrm{Z}_G^{\mathbb{Z}}$, it follows that $c \in \mathrm{Z}_G^{\mathbb{Z}}$ and so $[c] = [e]$. As a consequence, we get that $\mathrm{Ker}(\widetilde{\mathcal{F}}) = \{[e]\}$ and the thesis easily follows. □

If $\mathcal{F}$ is a surjective GCA on a group G, then its local rule f is clearly surjective. One may wonder whether the converse holds. The answer is negative, as the following example shows.

Example 1. Let S be a non-trivial group and consider the group $G = S \times S$. Consider the following two endomorphisms h_{-1} and h_1 of G defined by $h_{-1}(x, y) := (y, e)$ and $h_1(x, y) = (e, y)$ and let h_0 be the trivial endomorphism $h_0(x, y) = (e, e)$. Notice that the images of these endomorphisms commute element-wise so their product defines an homomorphism $f \in \mathrm{Hom}(G^3, G)$ such that $f = (h_{-1}, h_0, h_1)$. Consider a GCA $\mathcal{F}$ on G with local rule f. Notice that $\mathrm{Ker}(h_{-1}) = \mathrm{Ker}(h_1) = S \times \{e\}$. As a consequence, any configuration $c \in G^{\mathbb{Z}}$ such that $c_i = (a_i, e)$ with $a_i \in S$ belongs to the kernel of $\mathcal{F}$. Thus $\mathcal{F}$ is not surjective. On the other hand, the homomorphism f is clearly surjective since $f((a_{-1}, b_{-1}), (a_0, b_0), (a_1, b_1)) = (b_{-1}, b_1)$.

The following proposition ensures that for GCA surjectivity is equivalent to both openness and DPO.

Proposition 1. *Let $\mathcal{F}$ be a GCA on a finite group G. Then, the following statements are equivalent:*

(1) *$\mathcal{F}$ is surjective;*
(2) *$\mathcal{F}$ is open;*
(3) *$\mathcal{F}$ has DPO.*

Proof. It is well known that a surjective homomorphism of Polish group is open [35, Thm. 1.5] and a CA is open iff it is constant-to-one [1]. Hence, (1) and (2) are equivalent. While (3) ⇒ (1) holds for any discrete dynamical system on a compact space, the implication (1) ⇒ (3) comes from [36, Prop. 3.2] which in turn is a special case of a theorem in [37]. □

We now turn our attention to several other dynamical properties of GCA. As in the case of injectivity and surjectivity, our goal is to reduce their study to that of GCA defined on smaller groups.

Before proceeding, however, we prove the equivalence of various forms of chaotic behavior of a dynamical system in the particular case of GCA.

Theorem 3. *Let $\mathcal{F}$ be a GCA on a finite group G. The following statements are equivalent:*

(1) *$\mathcal{F}$ is topologically transitive;*
(2) *$\mathcal{F}$ is totally transitive;*
(3) *$\mathcal{F}$ is topologically weakly mixing;*
(4) *$\mathcal{F}$ is topologically mixing;*
(5) *$\mathcal{F}$ is ergodic weak mixing;*
(6) *$\mathcal{F}$ is ergodic strong mixing;*
(7) *$\mathcal{F}$ is ergodic.*

Proof. The following chains of implications are true:
(1) $\iff$ (2) $\iff$ (3): holds for general CA [38, Prop. 9.2].
(6) $\implies$ (4) $\implies$ (1): the first implication holds for endomorphisms of compact groups and measures with full support [39], while the second one is trivial.
(5) $\iff$ (6) $\iff$ (7): follows from the fact that they are equivalent for continuous endomorphisms of compact groups [40, Thm. 2] and the fact that a global rule of any GCA on G is a continuous endomorphism of the compact group $G^{\mathbb{Z}}$ (equipped with the prodiscrete topology).
(1) $\iff$ (7): follows from the fact that a surjective endomorphism (and more generally an affine transformation) of a compact metric group is ergodic (with respect to the Haar measure) if and only if it is topologically transitive [41, Cor. 5.5]. □

Theorem 3 allows us, in what follows, to consider only topological transitivity, as the other properties listed above are equivalent to it.

Theorem 4. *Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. If $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are topologically transitive, then $\mathcal{F}$ is topologically transitive. Moreover, if $\mathcal{F}$ is topologically transitive, then $\widetilde{\mathcal{F}}$ is topologically transitive.*

Proof. Let $Cyl(G)$ be the clopen basis of cylinders for $G^{\mathbb{Z}}$. The corresponding clopen basis for $H^{\mathbb{Z}}$ is $Cyl(H) = Cyl(G) \cap H^{\mathbb{Z}}$. Let π be the projection map $\pi : G \to G/H$ defined by $\pi(g) = gH = [g]$. With slight abuse of notation we will use π to denote also the corresponding projection from $G^{\mathbb{Z}}$ to $(G/H)^{\mathbb{Z}}$.

First, we show that if $\mathcal{F}$ is topologically transitive, then $\widetilde{\mathcal{F}}$ is also topologically transitive. Let $\widetilde{U}$ and $\widetilde{V}$ be two nonempty open sets in $(G/H)^{\mathbb{Z}}$. Consider the open sets $\pi^{-1}(\widetilde{U})$ and $\pi^{-1}(\widetilde{V})$. There exists $n \geq 0$ and $x \in \pi^{-1}(\widetilde{U})$ such that $\mathcal{F}^n(x) \in \pi^{-1}(\widetilde{V})$. Hence, $\widetilde{\mathcal{F}}^n([x]) = [\mathcal{F}^n(x)] \in V$ with $[x] \in U$ and the map $\widetilde{\mathcal{F}}$ is topologically transitive.

Now we prove that, if $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are topologically transitive, then $\mathcal{F}$ is topologically transitive as well. We exploit the following well-known result by Moothathu [38]: if F and G are any two topologically transitive CA over the alphabets A and B, respectively, then the product CA $F \times G$ over the alphabet $A \times B$ is also topologically transitive. We also use the following fact: if a CA F over the alphabet A is topologically transitive, then for every $k > 0$ and for every pair of integers i, j, there exists n_k such that, for every $X, Y \in A^k$ the condition $F^{n_k}(C([i, i+k-1], X)) \cap C([j, j+k-1], Y) \neq \emptyset$ holds. Hence, by Moothathu's result, if F and G are two topologically transitive CA over the alphabets A and B, for every $k > 0$ and for every pair of integers i, j, there exists n_k such that, for every $X, Y \in A^k$ and $Z, W \in B^k$, both the conditions $F^{n_k}(C([i, i+k-1], X)) \cap C([j, j+k-1], Y) \neq \emptyset$ and $G^{n_k}(C([i, i+k-1], Z)) \cap C([j, j+k-1], W) \neq \emptyset$ hold.

Now consider the case $F = \overline{\mathcal{F}}$ and $G = \widetilde{\mathcal{F}}$. Assume that both these GCA are topologically transitive. We are going to show that $\mathcal{F}$ is also topologically transitive.

Let i, j, k be any three integers, with $k > 0$. Consider any two words $u = g_1 g_2 \cdots g_k, u' = g'_1 \cdots g'_k \in G^k$ and let $[u] = [g_1] \cdots [g_k]$ and $[u'] = [g'_1] \cdots [g'_k]$ be the corresponding words in $(G/H)^k$. Let n_k be the positive integer from Moothathu's result above mentioned. Thus, it holds that $\widetilde{\mathcal{F}}^{n_k}(C([i, i+k-1], [u])) \cap C([j, j+k-1], [u']) \neq \emptyset$, where both $C([i, i+k-1], [u])$ and $C([j, j+k-1], [u'])$ are cylinders in $(G/H)^{\mathbb{Z}}$. This means that there exists a configuration c in $(G/H)^{\mathbb{Z}}$ with $c \in C([i, i+k-1], [u])$ such that $\widetilde{\mathcal{F}}^{n_k}(c) = c'$ where $c' \in C([j, j+k-1], [u'])$.

Equivalently, if g and g' are any two configurations in $G^{\mathbb{Z}}$ such that $g \in C([i, i+k-1], u)$, $g' \in C([j, j+k-1], u')$, $[g] = c$, and $[g'] = c'$, we get $\mathcal{F}^{n_k}(g) = g'h'$ for some $h' \in H^{\mathbb{Z}}$. Denote by h'_i the i-th element of h'. Now consider the words e^k and ${h'_1}^{-1} \cdots {h'_k}^{-1}$ in H^k. Again by Moothathu's result, $\overline{\mathcal{F}}^{n_k}(C([i, i+k-1], e^k)) \cap C([j, j+k-1], h'_1 \cdots h'_k) \neq \emptyset$, where the two are cylinders appearing in this intersection condition are subsets of $H^{\mathbb{Z}}$. This means that there exists a configuration $h \in C([i, i+k-1], e^k)$ such that $\overline{\mathcal{F}}^{n_k}(h) = h''$ for some $h'' \in C([j, j+k-1], {h'_1}^{-1} \cdots {h'_k}^{-1})$. Now consider $\mathcal{F}^{n_k}(gh)$. It holds that $\mathcal{F}^{n_k}(gh) = \mathcal{F}^{n_k}(g)\mathcal{F}^{n_k}(h) = g'h'h''$. This shows that

$$\mathcal{F}^{n_k}(C([i, i+k-1], u)) \cap C([j, j+k-1], u') \neq \emptyset \ ,$$

and therefore $\mathcal{F}$ is topologically transitive. □

We leave the following question open, as we have not been able to answer it.

Question 1. Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a topologically transitive GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. Is $\overline{\mathcal{F}}$ topologically transitive?

A positive answer to Question 1 would allow us to conclude that $\mathcal{F}$ is topologically transitive if and only if $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$ are topologically transitive.

In what follows, we consider two widely studied dynamical properties that are more restrictive than topological transitivity—namely, strong transitivity and positive expansivity—and prove that no GCA on a finite non-abelian group satisfies these properties.

Theorem 5. *Let $\mathcal{F}$ be a GCA on a finite non-abelian group G. It holds that $\mathcal{F}$ is neither strongly transitive nor positively expansive.*

Proof. Assume that there exists a strongly transitive GCA $\mathcal{F}$ on a finite non-abelian group G. Since $\mathcal{F}$ is strongly transitive, $\mathcal{F}^m$ is surjective for every $m \in \mathbb{N}$. By Lemma 4, we have that $\mathrm{Ker}(\mathcal{F}^m) \subseteq \mathrm{Z}_G^{\mathbb{Z}}$ for every $m \in \mathbb{N}$.

Now consider a cylinder U containing only elements of $G^{\mathbb{Z}} \setminus \mathrm{Z}_G^{\mathbb{Z}}$ as, for example, the cylinder containing all the configurations c such that c_0 is a fixed element which does not belong to Z_G. Since $\mathrm{Ker}(\mathcal{F}^m) \subseteq \mathrm{Z}_G^{\mathbb{Z}}$, we get $e^{\mathbb{Z}} \notin \bigcup_{m\in\mathbb{N}} \mathcal{F}^m(U)$. This contradicts the assumption that $\mathcal{F}$ is strongly transitive. The second assertion follows from the fact that any positively expansive CA is strongly transitive. □

The previous theorem does not come as a surprise. In fact, similar results hold in other contexts. As an example, it is known that if a compact connected topological group admits a positively expansive endomorphism, it must be abelian [42].

We now proceed to consider another well-studied dynamical property that is less restrictive than topological transitivity, namely sensitivity to initial conditions.

First of all, we prove a technical result about the structure of the local rule of the power of a given GCA. It will be useful in the sequel.

Lemma 5. *Let $\mathcal{F}$ be a GCA over a group G. For every $n \geq 1$, let ρ_n be the radius of the GCA $\mathcal{F}^n$ and let $f^{(n)} = (h^{(n)}_{-\rho_n}, \ldots, h^{(n)}_{\rho_n})$ be its local rule. It holds that $\rho_n \leq n\rho_1$ and*

$$h^{(n)}_j(x) = \prod_{\substack{(i_1,i_2,\ldots,i_n)\in\{-\rho_1,\ldots,\rho_1\}^n:\\ i_1+i_2+\cdots+i_n=j}} h^{(1)}_{i_n}(h^{(1)}_{i_{n-1}}(\cdots h^{(1)}_{i_1}(x)\cdots))$$

for every $x \in G$ and for every $-\rho_n \leq j \leq \rho_n$.

Proof. The proof immediately follows by the definition of GCA. Notice that the radius of $\mathcal{F}^n$ can be smaller than $n\rho_1$, where ρ_1 is the radius of $\mathcal{F}$, since the endomorphisms $h^{(n)}_{-n\rho_1}$ and $h^{(n)}_{n\rho_1}$ could be trivial. □

The following lemma (proved also in [24] in a different setting and using a different technique) guarantees that a GCA is either equicontinuous or sensitive to initial conditions.

Lemma 6. *Let $\mathcal{F}$ a GCA over a finite group G. Then, $\mathcal{F}$ is either equicontinuous or sensitive to initial conditions.*

Proof. The assertion is true for continuous endomorphisms of completely metrizable groups [43, Thm. 3.11]. □

The following result establishes a condition equivalent to sensitivity to initial conditions over metric groups.

Lemma 7. *Let $\mathcal{G}$ be a metric group and ϕ an endomorphism of $\mathcal{G}$. Then, ϕ is sensitive to initial conditions if and only if there exists $\epsilon > 0$ such that, for any $\delta > 0$ there is an element $g \in \mathcal{G}$ and an integer $t \geq 0$ such that $0 < d(g, e) < \delta$ and $d(\phi^t(g), e) \geq \epsilon$.*

Proof. If ϕ is sensitive to initial conditions the asserted condition is trivially satisfied. Suppose now that the condition holds. We want to prove that ϕ is sensitive, i.e., that there exists $\epsilon > 0$ such that, for any $\delta > 0$ and any configuration $g' \in \mathcal{G}$, there is a configuration $g'' \in \mathcal{G}$ and an integer $t \geq 0$ such that $0 < d(g'', g') < \delta$ and $d(\phi^t(g''), \phi^t(g')) \geq \epsilon$.

Fix $\epsilon > 0$. Since the condition holds, for every $\delta > 0$ there exist $g \in \mathcal{G}$ and an integer $t \geq 0$ with $0 < d(g, e) < \delta$ and $d(\phi^t(g), e) \geq \epsilon$.

Given any element g' we get $d(gg', g') = d(g, e)$ and $d(\phi^t(gg'), \phi^t(g')) = d(\phi^t(g)\phi^t(g'), \phi^t(g')) = d(\phi^t(g), \phi^t(e))$. Thus we can take $g'' = gg'$. □

We now prove that sensitivity to initial conditions for arbitrary GCA $\mathcal{F}$ can be characterized in terms of the radius of the iterates $\mathcal{F}^n$ of $\mathcal{F}$. This generalizes the case of GCA over $\mathbb{Z}_m$ [16, Lemma 4.1].

Lemma 8. *Let $\mathcal{F}$ be a GCA on the group G. It holds that $\mathcal{F}$ is sensitive to initial conditions if and only if $\limsup_{n\to\infty} \rho(\mathcal{F}^n) = \infty$. Equivalently, $\mathcal{F}$ is equicontinuous if and only if $\limsup_{n\to\infty} \rho(\mathcal{F}^n) < \infty$.*

Proof. If $\limsup_{n\to\infty} \rho(\mathcal{F}^n)$ is finite then there exists $k > 0$ such that $\rho(\mathcal{F}^n) < k$ for every n. Then, for every $\epsilon > 0$, if $g \in G^{\mathbb{Z}}$ is any configuration sufficiently close to $e^{\mathbb{Z}}$, it holds that $d(\mathcal{F}^n(g), e^{\mathbb{Z}}) < \epsilon$ and, hence, by Lemma 7, $\mathcal{F}$ is not sensitive to initial conditions.

Suppose now that $\limsup_{n\to\infty} \rho(\mathcal{F}^n) = \infty$, i.e., for every k we can find n such that $\rho(\mathcal{F}^n) > k$. Set $\rho(\mathcal{F}^n) = \rho_n$ and let $f^{(n)} = (h^{(n)}_{-\rho_n}, \dots, h^{(n)}_{\rho_n})$ be the local rule of $\mathcal{F}^n$. Without loss of generality we can assume that $h^{(n)}_{-\rho_n}$ is a non-trivial endomorphism. Consider a configuration $g \in G^{\mathbb{Z}}$ such that $g_{-\rho_n} \notin \mathrm{Ker}(h^{(n)}_{-\rho_n})$ and $g_i = e$ for every $i \neq -\rho_n$. Clearly $d(g, e^{\mathbb{Z}}) = \frac{1}{2^{\rho_n}}$ and $\mathcal{F}^n(g)(0) = h^{(n)}_{-\rho_n}(g_{-\rho_n}) \neq e$. Hence, $d(\mathcal{F}^n(g), e^{\mathbb{Z}}) = 1$. By Lemma 7, this shows that $\mathcal{F}$ is sensitive to initial conditions with $\epsilon = 1$. □

Remark 2. A trivial consequence of Lemma 8 is the following. With the same notations used in Lemma 5, we can state that a GCA $\mathcal{F}$ is equicontinuous if and only if there exists a positive constant K such that the endomorphisms $h^{(n)}_j$ are trivial for every $n \geq 1$ and for every j such that $|j| > K$.

Theorem 6. *Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. It holds that $\mathcal{F}$ is equicontinuous if and only if both $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are equicontinuous. Equivalently, $\mathcal{F}$ is sensitive to initial conditions if and only if either $\widetilde{\mathcal{F}}$ or $\overline{\mathcal{F}}$ is sensitive to initial conditions.*

Proof. Denote by $f^{(n)} = (h^{(n)}_{-\rho_n}, \dots, h^{(n)}_{\rho_n})$, $\widetilde{f}^{(n)} = (\widetilde{h}^{(n)}_{-\rho_n}, \dots, \widetilde{h}^{(n)}_{\rho_n})$ and $\overline{f}^{(n)} = (\overline{h}^{(n)}_{-\rho_n}, \dots, \overline{h}^{(n)}_{\rho_n})$ the local rules of $\mathcal{F}^n$, $\widetilde{\mathcal{F}}^n$ and $\overline{\mathcal{F}}^n$, respectively. We assume, as usual, that, for every $n \geq 1$, at least one between the endomorphisms $h^{(n)}_{-\rho_n}$ and $h^{(n)}_{\rho_n}$ is non-trivial. However, the radius of $\overline{\mathcal{F}}^n$ ($\widetilde{\mathcal{F}}^n$, respectively) could be smaller than ρ_n since $\overline{h}^{(n)}_{-\rho_n}$ and $\overline{h}^{(n)}_{\rho_n}$ ($\widetilde{h}^{(n)}_{-\rho_n}$ and $\widetilde{h}^{(n)}_{\rho_n}$, respectively) could be both trivial.

Hence, we get that $\rho(\widetilde{\mathcal{F}}^n) \leq \rho(\mathcal{F}^n)$ and $\rho(\overline{\mathcal{F}}^n) \leq \rho(\mathcal{F}^n)$ for every n. Thus, by Lemma 8, if at least one between $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ is sensitive to initial conditions, $\mathcal{F}$ is also sensitive to initial conditions. Equivalently, if $\mathcal{F}$ is equicontinuous, $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are also equicontinuous.

We now prove the converse implication: if both $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$ are equicontinuous, then $\mathcal{F}$ is, too. So, assume that $\widetilde{\mathcal{F}}$ and $\overline{\mathcal{F}}$ are equicontinuous. By Remark 2, there exist

- a constant $\widetilde{K}$ such that every G/H-endomorphism $\widetilde{h}^{(n)}_j$ is trivial for every $n \geq 1$ and every j such that $|j| > \widetilde{K}$, and
- a constant $\overline{K}$ such that every H-endomorphism $\overline{h}^{(n)}_j$ is trivial for every $n \geq 1$ and every j such that $|j| > \overline{K}$.

Set $K = \widetilde{K} + \overline{K} + 2\rho_1$.

We want to show that every endomorphism $h^{(n)}_j$ is trivial for every $n \geq 1$ and every j such that $|j| > K$. To this aim recall that, by Lemma 5,

$$h^{(n)}_j(x) = \prod_{\substack{(i_1,i_2,\dots,i_n)\in\{-\rho_1,\dots,\rho_1\}^n \\ i_1+i_2+\cdots+i_n=j}} h^{(1)}_{i_n}(h^{(1)}_{i_{n-1}}(\cdots h^{(1)}_{i_1}(x)\cdots))$$

for every $x \in G$ and for every $-\rho_n \leq j \leq \rho_n$.

Assume that $|j| > K$. Note that, given our definition of K, if $(i_1, \dots, i_n) \in \{-\rho_1, \dots, \rho_1\}^n$ is such $i_1 + \cdots + i_n = j$, then the set

$$A_{(i_1,\dots,i_n)} := \{(s, \ell) \in \mathbb{Z}_+ \times \mathbb{Z} : \\ i_1 + \cdots + i_s = \ell,\ |\ell| > \widetilde{K} \text{ and } |j - \ell| > \overline{K}\}$$

is non-empty and there exists an element (s, ℓ) in this set with minimal value of s. Denote by $\widehat{(s, \ell)}_{i_1,\dots,i_n}$ such an element.

Consider now the following set of pairs $\widehat{(s, \ell)}_{(i_1,\dots,i_n)}$ when $(i_1, \dots, i_n)$ varies among the n-tuples in $\{-\rho_1, \dots, \rho_1\}$ such that $i_1 + \cdots + i_n = j$:

$$\mathcal{S}_{j,n} := \{(\widehat{s}, \widehat{\ell})_{(i_1,\cdots,i_n)} : (i_1, \ldots, i_n) \in \{-\rho_1, \ldots, \rho_1\}^n \text{ s.t. } i_1 + \cdots + i_n = j\} \ .$$

Thus, we can write $h_j^{(n)}$ as

$$h_j^{(n)}(x) = \prod_{(\widehat{s},\widehat{\ell})\in\mathcal{S}_{j,n}} \prod_{\mathcal{B}_{\widehat{s},\widehat{\ell}}} \prod_{\mathcal{C}_{\widehat{s},\widehat{\ell}}} h_{i_n}^{(1)}(h_{i_{n-1}}^{(1)}(\cdots h_{i_1}^{(1)}(x)\cdots)) \ ,$$

where the second product is over the set

$$\mathcal{B}_{\widehat{s},\widehat{\ell}} := \{(i_1, i_2, \ldots, i_{\widehat{s}}) \in \{-\rho_1, \ldots, \rho_1\}^{\widehat{s}} : i_1 + i_2 + \cdots + i_{\widehat{s}} = \widehat{\ell}\}$$

and the third is over the set

$$\mathcal{C}_{\widehat{s},\widehat{\ell}} := \{(i_{\widehat{s}+1}, \ldots, i_n) \in \{-\rho_1, \ldots, \rho_1\}^{n-\widehat{s}} : i_{\widehat{s}+1} + \cdots + i_n = j - \widehat{\ell}\} \ .$$

The last expression for $h_j^{(n)}$ can be in turn rewritten as

$$h_j^{(n)}(x) = \prod_{(\widehat{s},\widehat{\ell})\in\mathcal{S}_{j,n}} h_m^{(n-\widehat{s})}(h_{\widehat{\ell}}^{(\widehat{s})}(x)) \ ,$$

where $m = j - \widehat{\ell}$.

Note that, by our previous assumptions, the endomorphisms $\widetilde{h}_{\widehat{\ell}}^{(\widehat{s})}$ and $\overline{h}_m^{(n-\widehat{s})}$ are trivial. Hence, $h_{\widehat{\ell}}^{(\widehat{s})}(x) \in H$ for every $x \in G$ and $h_m^{(n-\widehat{s})}(h_{\widehat{\ell}}^{(\widehat{s})}(x)) = e$ for every $x \in G$. Therefore, we get that $h_j^{(n)}$ is trivial and this concludes the proof. □

We end this section by considering the topological entropy of a GCA.

Theorem 7. *Let G be a finite group and $H \trianglelefteq G$. Let $\mathcal{F}$ be a GCA on G such that $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. Then,*

$$\mathcal{H}(\mathcal{F}) = \mathcal{H}(\widetilde{\mathcal{F}}) + \mathcal{H}(\overline{\mathcal{F}}).$$

Proof. The proposition holds for endomorphisms of compact groups (see [44, Thm. 2] and [45]). □

5. Algorithmic decomposition technique: iterated quotienting

In Section 4 we have shown that the study of a number of dynamical properties of a GCA $\mathcal{F}$ can be reduced to that of the same properties of two GCA, namely $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$, defined on smaller groups. However, these smaller groups do not guarantee that the analysis of the dynamical properties of $\overline{\mathcal{F}}$ and $\widetilde{\mathcal{F}}$ will be simpler than that of the original GCA $\mathcal{F}$.

In this section, we show that by iterating the decomposition of the original group a finite number of times, and using suitable quotient groups at each step, we eventually obtain a collection of GCA for which the analysis of the relevant properties becomes significantly simpler, if not immediate. To this end, we begin with some definitions and preliminary results.

Let G be a finite group. A group word is a formal expression in terms of variables and group operations (multiplication, inverses, and identity). A *verbal subgroup* of a group G is defined as the subgroup generated by all elements obtained by substituting elements of G into the variables of a given set of group words. As an example, the verbal subgroup of a group G generated by the group word $xyx^{-1}y^{-1}$ is the commutator of G.

A finite group G will be called *invariantly simple* (*characteristically simple*, *verbally simple*, respectively) if the only fully invariant (characteristic, verbal, respectively) subgroups of G are the trivial subgroup and G itself.

Theorem 8. *For any finite group G, the following statements are equivalent:*

(1) *G is characteristically simple;*
(2) *G is invariantly simple;*
(3) *G is verbally simple;*
(4) *G is the direct product of isomorphic simple groups.*

Proof. By definition, it immediately follows that if G is characteristically simple then it is invariantly simple, and that if G is invariantly simple then it is verbally simple. It is also well-known that a finite characteristically simple group is the direct product of isomorphic simple groups [46, Thm. 1.4]. Moreover, a finite verbally simple group is characteristically simple [47, Cor. 53.57]. On the contrary, it is easy to see that the direct product of isomorphic simple groups is characteristically simple. □

We now introduce a recursive procedure, namely, a divide and conquer one, called `Decomposition` that, given a GCA $\mathcal{F}$ on a finite group G, produces a finite set $\{(\mathcal{F}_1, G_1), \ldots, (\mathcal{F}_k, G_k)\}$ of GCA $\mathcal{F}_i$ on invariantly simple groups G_i such that $\mathcal{F}$ on G is surjective, injective, equicontinuous (and maybe topologically transitive) if and only if all the $\mathcal{F}_i$ on G_i satisfy the same property. Moreover, the topological entropy of $\mathcal{F}$ on G is the sum of the topological entropies of all the $\mathcal{F}_i$ on G_i. Note that the output of the procedure `Decomposition` depends on the sequence of fully invariant subgroups H's chosen

Algorithm 1: Decomposition.

Input: A GCA $(\mathcal{F}, G)$
Output: A finite set $\{(\mathcal{F}_1, G_1), \ldots, (\mathcal{F}_k, G_k)\}$ of GCA, where each G_i is an invariantly simple group.
Function `Decomposition(`$\mathcal{F}$`,`G`)`**:**
  if *G is invariantly simple* **then**
    return $\{(\mathcal{F}, G)\}$
  Let H be any non-trivial proper fully invariant subgroup of G;
  a $\leftarrow$ `Decomposition(`$\widetilde{\mathcal{F}}, G/H$`)`;
  b $\leftarrow$ `Decomposition(`$\overline{\mathcal{F}}, H$`)`;
  return $a \cup b$

at step 4 (in all the recursive calls). However, any of the possible outputs of `Decomposition` will work for our purposes. The following result is a trivial consequence of Remark 1 and Theorems 2, 4, 6 and 7.

Theorem 9. *Let $\mathcal{F}$ be a GCA over a finite group G. The following statements hold.*

(1) *$\mathcal{F}$ is injective (resp., surjective) (resp., equicontinuous) if and only if all the GCA in the set* `Decomposition(`$\mathcal{F}, G$`)` *are injective (resp., surjective) (resp, equicontinuous), while $\mathcal{F}$ is sensitive to initial conditions if and only if at least one GCA in that set is sensitive to initial conditions, too.*
(2) *If all of the GCA in the set* `Decomposition(`$\mathcal{F}, G$`)` *are topologically transitive, then $\mathcal{F}$ is topologically transitive.*
(3) *The topological entropy of $\mathcal{F}$ is equal to the sum of the topological entropies of the GCA in the set* `Decomposition(`$\mathcal{F}, G$`)`*.*

We now give an explicit strategy for selecting the subgroups H's that will allow us to simplify the problem of deciding a number of dynamical properties of the GCA under consideration.

Let G be a finite group. Set $G^{(0)} := G$ and, for every $i \geq 0$, $G^{(i+1)} := [G^{(i)}, G^{(i)}]$. The series $\{G^{(i)}\}$ is called *the derived series* of G. The derived series of G eventually reaches a perfect group. Denote such a group by $\widehat{G}$. The group G is said to be *solvable* if $\widehat{G} = \{e\}$. Solvable groups are a central topic in algebra and includes the widely studied class of *nilpotent* groups [26]. Moreover, every finite group of odd order is solvable by the celebrated Feit-Thompson theorem. We recall that the commutator subgroup $[G, G]$ of a group G is fully invariant and thus normal in G. Moreover, the quotient of $G/[G, G]$ is abelian. It is not hard to verify that, if G is a solvable finite group, then all the GCA produced by `Explicit-`

Algorithm 2: Explicit Decomposition.

Input: A GCA $(\mathcal{F}, G)$
Output: A finite set $\{(\mathcal{F}_1, G_1), \ldots, (\mathcal{F}_k, G_k)\}$ of GCA where G_i's are either abelian or non-abelian invariantly simple groups. If G is solvable then all G_i's are abelian
Function `Explicit-Decomposition(`$\mathcal{F}$`,`G`)`**:**
  if $[G, G] = \{e\}$ **then**
    return $\{(\mathcal{F}, G)\}$
  if $[G, G] = G$ **then**
    return `Decomposition(`$\mathcal{F}, G$`)`
  $H \leftarrow [G, G]$;
  a $\leftarrow$ `Explicit-Decomposition(`$\widetilde{\mathcal{F}}, G/H$`)`;
  b $\leftarrow$ `Explicit-Decomposition(`$\overline{\mathcal{F}}, H$`)`;
  return $a \cup b$

`Decomposition(`$\mathcal{F}, G$`)` are abelian. Since a complete characterization of surjectivity, injectivity, and sensitivity to initial conditions for GCA over abelian groups exists [18,7], we also have a characterization of these properties in the case of solvable groups.

We now consider the case of non-solvable groups. In this case, the set `Explicit-Decomposition(`$\mathcal{F}, G$`)` also contains GCA on products of isomorphic, non-abelian simple groups.

Let S be a finite non-abelian simple group and let G be the product of m copies of S, i.e., $G = S_1 \times \cdots \times S_m$, where $S_i \cong S$ for every i. In the following we will identify the subgroup $\{g \in G : g_i \in G \text{ and } g_j = e \; \forall j \neq i\}$ of G with S_i.

Since the kernel of every endomorphism h of G is a normal subgroup and a normal subgroup of a direct product of non-abelian simple groups is the direct product of some of them (see, for instance, [48, p. 174]), it follows that $\mathrm{Ker}(h) = \prod_{t\in I} S_t$, where I is a nonempty proper subset of $\{1, \ldots, m\}$.

Consider now a *surjective* GCA $\mathcal{F}$ over G. Thus the local rule $f = (h_{-\rho}, \ldots, h_\rho)$ of $\mathcal{F}$ is also surjective.

By Lemma 2, $\mathrm{Im}(h_i)$ is also a normal subgroup of G and, hence, it holds that $\mathrm{Im}(h_i) = \prod_{t\in J} S_t$, where J is a nonempty proper subset of $\{1, \ldots, m\}$.

If $i \neq j$, $\mathrm{Im}(h_j) \subseteq C_G(\mathrm{Im}(h_i))$. Since S_t is non-abelian, this implies that the factors S_t appearing in $\mathrm{Im}(h_j)$ are distinct from the factors S_t appearing in $\mathrm{Im}(h_i)$. Since f is surjective, the $\mathrm{Im}(h_i)$'s form a partition of the factors S_t's.

If the endomorphism h_i has r_i factors in the image it must have $m - r_i$ factors in the kernel.

Suppose that there exists a simple group S_r among the factors of G which belongs to the factors of $\mathrm{Ker}(h_i)$ for every i. In that case the restriction of f to S_r^k induces a GCA over S_r whose local rule is trivial, but this contradicts the fact that $\mathcal{F}$ is surjective (see Example 1).

In particular, the following fact holds.

Remark 3. If G is a finite group which is the product of simple isomorphic non-abelian groups, then any GCA $\mathcal{F}$ with local rule $f = (h_{-\rho}, \ldots, h_\rho)$ on G is surjective if and only if

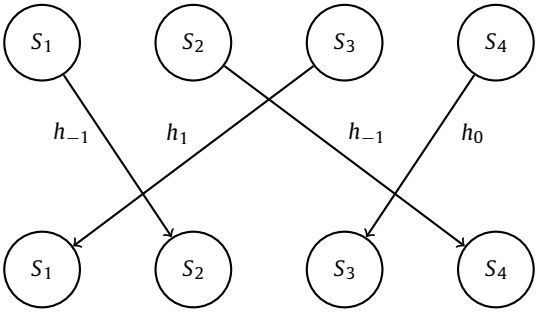
$$\bigcap_{-\rho \le j \le \rho} \mathrm{Ker}(h_j) = \{e\} \ .$$

We can conclude that every factor S_t appearing in G is a factor of exactly one of the images of the h_i's and there are no factors S_t which are factors of every kernel of the h_i's. Thus, for every S_t, there exists precisely an i such that S_t is not a factor of $\mathrm{Ker}(h_i)$.

Definition 2. Let us define π_f as *the action of the family of endomorphisms h_i's thought as a* permutation over the set of the factors S_t *of* G and denote by o its *order*.

We illustrate these facts by an example.

Example 2. Consider a local rule of the form $f = (h_{-1}, h_0, h_1)$ and a group $G = S_1 \times S_2 \times S_3 \times S_4$. Suppose that $\mathrm{Im}(h_{-1}) = S_2 \times S_4$, $\mathrm{Im}(h_0) = S_3$, $\mathrm{Im}(h_1) = S_1$, $\mathrm{Ker}(h_{-1}) = S_3 \times S_4$, $\mathrm{Ker}(h_0) = S_1 \times S_2 \times S_3$, and $\mathrm{Ker}(h_1) = S_1 \times S_2 \times S_4$. We can represent the situation as follows.



In this case the permutation π_f is the permutation whose only cycle is $(1, 2, 4, 3)$ and its order is $o = 4$.

In the following, with a slight abuse of notation, we will identify the endomorphism h_i with the restriction of h_i to those factors of G on which h_i acts non-trivially. This restriction is clearly an automorphism of those factors.

For any $1 \le i \le m$, consider S_i, the i-th factor of G. Then, there exists exactly one h_j acting non-trivially on S_i whose image is another $S_{i^{(1)}}$. Over the factor $S_{i^{(1)}}$ there exists exactly one $h_{j^{(1)}}$ acting non-trivially and so on. After o steps we will return on the initial factor S_i applying the endomorphism $h_{j^{(o-1)}}$ to the factor $S_{i^{(o-1)}}$.

Definition 3. Define the automorphism $\hat{h}_i$ of S_i in the following way:

$$\hat{h}_i := h_{j^{(o-1)}} \circ \ldots \circ h_{j^{(1)}} \circ h_j \ ,$$

Table 1
The dynamical behavior of the GCA $\mathcal{F}$ from Example 4.

c	$\cdots$	$\cdots$	$a_1^{(i)}a_2^{(i)}a_3^{(i)}a_4^{(i)}$	$\cdots$	$\cdots$
$\mathcal{F}(c)$	$\cdots$	$\cdots$	$h_1(a_3^{(i+1)})h_{-1}(a_1^{(i-1)})h_0(a_4^{(i)})h_{-1}(a_2^{(i-1)})$	$\cdots$	$\cdots$
$\mathcal{F}^2(c)$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\mathcal{F}^3(c)$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\mathcal{F}^4(c)$	$\cdots$	$\cdots$	$\hat{h}_1(a_1^{(i-1)})\hat{h}_2(a_2^{(i-1)})\hat{h}_3(a_3^{(i-1)})\hat{h}_4(a_4^{(i-1)})$	$\cdots$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathcal{F}^n(c)$	$\cdots$	$\cdots$	$a_1^{(i-n')}a_2^{(i-n')}a_3^{(i-n')}a_4^{(i-n')}$	$\cdots$	$\cdots$

and denote by o_i the order of $\hat{h}_i$ as an automorphism (i.e., o_i is the smallest positive number such that the composition of $\hat{h}_i$ with itself o_i times is the identity map on S_i).

Example 3. Consider the same local rule of the previous example. In this case $\hat{h}_1 = h_1 \circ h_0 \circ h_{-1} \circ h_{-1}$, $\hat{h}_2 = h_{-1} \circ h_1 \circ h_0 \circ h_{-1}$, $\hat{h}_3 = h_0 \circ h_{-1} \circ h_{-1} \circ h_1$, and $\hat{h}_4 = h_{-1} \circ h_{-1} \circ h_1 \circ h_0$.

Definition 4. A group G which is the product $S_1 \times \ldots \times S_m$ of finite, non-abelian, isomorphic simple groups S_i is said to be *minimal* with respect to the action of a given GCA $\mathcal{F}$ over G if there are no two non-empty, disjoint sets I, J with $I \cup J = \{1, 2, \ldots, m\}$, such that $\mathcal{F}((\prod_{i\in I} S_i)^{\mathbb{Z}}) \subseteq (\prod_{i\in I} S_i)^{\mathbb{Z}}$ and $\mathcal{F}((\prod_{i\in J} S_i)^{\mathbb{Z}}) \subseteq (\prod_{i\in J} S_i)^{\mathbb{Z}}$.

When $\mathcal{F}$ is surjective, the group G is minimal with respect to the action of $\mathcal{F}$ if and only if the corresponding permutation π_f above defined is a single cycle. Notice that if G is not minimal with respect to $\mathcal{F}$ it is possible to decompose the dynamics of $\mathcal{F}$ into the product of the dynamics of $\mathcal{F}$ restricted to its minimal components. In fact each minimal component H satisfies $\mathcal{F}(H^{\mathbb{Z}}) \subseteq H^{\mathbb{Z}}$. So, in this case we can continue the decomposition previously illustrated one step further.

Lemma 9. *Let $G = S_1 \times \ldots \times S_m$ be a product of finite, non-abelian, isomorphic simple groups. Let $\mathcal{F}$ be a surjective GCA on G with local rule $f = (h_{-\rho}, \ldots, h_\rho)$. Let $\mathrm{Im}(h_i) = \prod_{t\in J_i} S_t$, where J_i is a proper subset of $\{1, \ldots, m\}$ and let $r_i = |J_i|$. Let o and o_i, $1 \le i \le m$, be the permutation orders introduced in Definitions 2 and 3. If G is minimal with respect to $\mathcal{F}$, then it holds that*

$$\mathcal{F}^{o\,\mathrm{lcm}(o_1,\ldots,o_m)} = \sigma^{-\mathrm{lcm}(o_1,\ldots,o_m)\sum_i i r_i}.$$

Proof. Let $c \in G^{\mathbb{Z}}$ be any configuration. Thus, we can write $c_i = (a_1^{(i)}, \ldots, a_m^{(i)})$ with $a_j^{(i)} \in S_j$. Consider the configuration $\mathcal{F}^o(c)$. The element $\mathcal{F}^o(c)_i$ is

$$(\hat{h}_1(a_1^{(i+\sum j r_j)}), \ldots, \hat{h}_m(a_m^{(i+\sum j r_j)})).$$

Therefore, the element $\mathcal{F}^{o\,\mathrm{lcm}(o_1,\ldots,o_m)}(c)_i$ is

$$(a_1^{(i+\mathrm{lcm}(o_1,\ldots,o_m)\sum j r_j)}, \ldots, a_m^{(i+\mathrm{lcm}(o_1,\ldots,o_m)\sum j r_j)}). \quad \square$$

We illustrate the previous proof by an example.

Example 4. Consider the same local rule f of the previous examples. Notice that $r_1 = 2$, $r_2 = 1$ and $r_3 = 1$ (because $\mathrm{Im}(h_{-1})$ has two factors, while $\mathrm{Im}(h_0)$ and $\mathrm{Im}(h_1)$ have one factor each). Consider the GCA $\mathcal{F}$ having f as local rule. In this case $\sum_i i r_i = -1$, $n' = \mathrm{lcm}(o_1, o_2, o_3, o_4)$, and $n = on' = 4n'$. Table 1 represents the behavior of $\mathcal{F}$.

The following example shows that the condition about the minimality of G with respect to $\mathcal{F}$ in Lemma 9 is necessary.

Example 5. Let S be a simple, non-abelian group and consider the group $G = S \times S$. Consider the two endomorphisms h_{-1} and h_1 of G defined by $h_{-1}(x, y) := (x, 1)$, and $h_1(x, y) = (1, y)$. Notice that the images of these two endomorphisms commute element-wise so their product defines an homomorphism $f \in \mathrm{Hom}(G^3, G)$ such that $f = (h_{-1}, h_0, h_1)$, where h_0 is the trivial endomorphism. Consider the GCA $\mathcal{F}$ over G with local rule f.

Notice that $\mathcal{F}$ is nothing but the product of two shift-like GCA, namely, the shift σ and its inverse σ^{-1}. Indeed, $f((x, y), (x', y')) = (x, y')$ and, hence, if $c \in G^{\mathbb{Z}}$ is the configuration such that the element in position i is $c_i = (x_i, y_i)$, then $\mathcal{F}(c)$ is the configuration such that $\mathcal{F}(c)_i = (x_{i-1}, y_{i+1})$.

It is clear that, in this case, Lemma 9 fails. In fact, there are no powers of $\mathcal{F}$ that are shifts. We stress that this fact does not constitute a contradiction since G is not minimal with respect to $\mathcal{F}$. The two factors $S \times \{e\}$ and $\{e\} \times S$ are actually invariant under $\mathcal{F}$.

As a consequence of Lemma 9 we have the following result.

Theorem 10. *Let G be a product of m finite, non-abelian, isomorphic simple groups. Let $\mathcal{F}$ be a GCA on G with local rule $f = (h_{-\rho}, \dots, h_\rho)$. Suppose that G is minimal with respect to $\mathcal{F}$. The following facts hold:*

(1) *$\mathcal{F}$ is injective if and only if $\mathcal{F}$ is surjective if and only if*

$$\bigcap_{-\rho \le i \le \rho} \mathrm{Ker}(h_i) = \{e\};$$

(2) *$\mathcal{F}$ is topologically transitive if and only if it is surjective and $\sum_i i r_i \neq 0$, where the r_i's are defined as in Lemma 9;*
(3) *if $\mathcal{F}$ is surjective, $\mathcal{F}$ is sensitive to initial conditions if and only if it is topologically transitive;*
(4) *if $\mathcal{F}$ is surjective, the topological entropy of $\mathcal{F}$ is*

$$\mathcal{H}(\mathcal{F}) = \frac{\left|\sum_i i r_i\right| \log(|G|)}{o},$$

where o and the o_i's are defined as in Lemma 9;
(5) *$\mathcal{F}$ is neither strongly transitive nor positively expansive.*

Proof.

(1) Any injective CA is also surjective. If $\mathcal{F}$ is surjective, since Z_G is the trivial group, $\mathcal{F}$ is also injective according to Lemma 4. As to the equivalence between the surjectivity of $\mathcal{F}$ and the fact that the intersection of all the kernels of the h_i's is trivial, see Remark 3.
(2) Assume that $\mathcal{F}$ is topologically transitive. Clearly, $\mathcal{F}$ is also surjective. If, for a sake of argument, the equality $\sum_i i r_i = 0$ holds, by Lemma 9 it would follow that there exists n such that $\mathcal{F}^n$ is the identity. But this is impossible since $\mathcal{F}$ is topologically transitive. Hence, $\sum_i i r_i \neq 0$. As to the converse implication, if $\mathcal{F}$ is surjective and $\sum_i i r_i \neq 0$, there exists n such that $\mathcal{F}^n$ is a shift-like GCA. Therefore, $\mathcal{F}$ is topologically transitive.
(3) It is well known that any topologically transitive CA is also sensitive to initial conditions. Assume now that $\mathcal{F}$ is a surjective GCA which is not topologically transitive. By item (2), $\sum_i i r_i = 0$ and there exists n such that $\mathcal{F}^n$ is the identity. Therefore, $\mathcal{F}$ is not sensitive to initial conditions by Lemma 8.
(4) It is well known [49, Thm. 1.2, p. 335] that, if F is any continuous map over a compact topological space, it holds that

$$\mathcal{H}(F^k) = k\mathcal{H}(F)$$

for every $k \in \mathbb{N}$. Moreover, it is also know that the topological entropy of the shift σ^r on the alphabet G is $|r| \log(|G|)$. In our case, by Lemma 9, we get

$$\begin{aligned} o \,\mathrm{lcm}(o_1, \dots, o_m)\mathcal{H}(\mathcal{F}) &= \mathcal{H}(\mathcal{F}^{o\,\mathrm{lcm}(o_1,\dots,o_m)}) \\ &= \mathcal{H}(\sigma^{-\mathrm{lcm}(o_1,\dots,o_m)\sum_i i r_i}) \\ &= \mathrm{lcm}(o_1, \dots, o_m) \left|\sum_i i r_i\right| \log(|G|). \end{aligned}$$

Thus,

$$\mathcal{H}(\mathcal{F}) = \frac{\left|\sum_i i r_i\right| \log(|G|)}{o}.$$

(5) It directly follows by Theorem 5. □

5.1. Decidability of dynamical properties

Let C be a possibly infinite set of CA, such as the set of GCA. Let P be a property that a CA may or may not satisfy, such as surjectivity or topological transitivity. P is decidable for C if and only if there exists an algorithm that, given a CA $F \in C$, returns "Yes" if F satisfies P, and "No" otherwise. If, instead of a property P, we consider a numerical function $N : C \to \mathbb{R}$, such as topological entropy or Lyapunov exponents, N is computable for C if and only if there exists an algorithm that, given a CA $F \in C$, computes $N(F)$. Deciding a property (or computing a function) involves a computational cost that the notion of

decidability (or computability) does not take into account. We will therefore say that a property is efficiently decidable (or a function is efficiently computable) if the algorithm that decides whether the property holds (or computes the function) is efficient, where efficient usually means polynomial-time. As for CA, efficient algorithms typically analyze the structure of the local rule, which is a finite object, whereas inefficient algorithms usually operate on the space-time dynamics of the CA, which is potentially infinite in size.

The literature contains a number of results related to the decidability and computability of properties and functions, respectively, across various classes of CA. Below, we list some of the most significant ones. In what follows, we will denote by D-CA the class of D-dimensional CA. The same notation will also be used for GCA.

- Every non-trivial property of limit sets of general 1-CA is undecidable [12].
- Surjectivity and injectivity are decidable for general 1-CA [50] and undecidable for general 2-CA [51]. Surjectivity and injectivity are decidable for D-GCA with $D \geq 1$ [24].
- Topological entropy for general 1-CA is uncomputable [11]. It is computable for 1-GCA on $\mathbb{Z}/m\mathbb{Z}$ and for general positively expansive 1-CA [22]. We strongly believe that the topological entropy is also efficiently computable for 1-GCA on abelian groups.
- Strong transitivity is efficiently decidable for D-GCA on $\mathbb{Z}/m\mathbb{Z}$ with $D \geq 1$ [16]. We strongly believe that strong transitivity is also efficiently decidable for D-GCA on abelian groups with $D \geq 1$.
- Lyapunov exponents are efficiently computable for 1-GCA on $\mathbb{Z}/m\mathbb{Z}$ [23].
- Sensitivity to the initial conditions and topological transitivity are undecidable for general 1-CA (even when restricting to the case of reversible 1-CA) [52].
- Sensitivity to the initial conditions, equicontinuity, topological transitivity, ergodicity, positive expansivity, and DPO are efficiently decidable for 1-GCA on abelian groups [17–21,7].
- Sensitivity to the initial conditions and equicontinuity are decidable for D-GCA with $D \geq 1$ [24].
- Non-transitivity is semi-decidable for D-GCA with $D \geq 1$ [24].

The fact that many dynamical properties can be decided by our algorithmic method is based on the following fundamental remark.

Remark 4. Since G is a finite group, the set of GCA produced by the function `Explicit-Decomposition` defined in Section 5 are computable.

As a consequence of our decomposition method, Remark 4 and the other results presented in this paper, the following statements are true.
(1) If Question 1 had a positive answer, *topological transitivity, totally transitivity, ergodicity, weakly and strongly mixing are decidable properties for 1-GCA.* By Theorem 3, all these properties are equivalent for 1-GCA. Hence, if Question 1 had an affirmative answer, by Theorems 4 and 10, topological transitivity would turn out to be decidable for 1-GCA.
(2) *If topological entropy is computable for surjective 1-GCA on abelian groups, then it is computable for all surjective 1-GCA.* It follows by Theorems 7 and 10. In other words, the topological entropy of a 1-GCA can be computed, provided we know how to compute the topological entropy for 1-GCA defined on products of simple non-abelian isomorphic groups – for which we explicitly proved how to compute it in the surjective case – and on abelian groups.
(3) *If strong transitivity is decidable for 1-GCA on abelian groups then it is decidable for all 1-GCA.* Indeed, since strongly transitive 1-GCA do not exist unless the underlying group is abelian (Theorem 5), the decidability of strong transitivity for 1-GCA reduces to its decidability for GCA on abelian groups.
(4) *Positive expansivity is decidable for 1-GCA.* This follows by the same reasoning as in (3). Note that positively expansive CA do not exist in dimensions greater than 1.
(5) *DPO is a decidable property for 1-GCA.* It follows by Proposition 1.
(6) *Sensitivity to initial conditions* and *equicontinuity* are decidable for surjective 1-GCA (Lemma 6, Theorems 6, and 10).

Some of the results presented in this paper are related to those proven in [24]. We believe it is useful to clarify analogies and differences between the two.

First of all, it is important to emphasize that the results obtained in [24] are based on the analysis of the space-time dynamics of the GCA under consideration. This entails an unsustainable computational cost, even for very simple GCA. In this work, we propose a completely different approach, which relies on the analysis of the structure of the group on which the GCA is defined and on its local rule. This analysis is completely independent of the dynamical evolution of the GCA. Indeed, the group decomposition, which is the most time-consuming part of our method, is fully independent of the GCA rule and can be considered a task which is prodromal to the analysis of many GCA: it can be performed once and reused to study all different GCA defined on the same group. These decompositions can therefore be computed without depending on the complexity of the GCA. Furthermore, in principle, our technique could be applied to any dynamical property we desire to investigate.

On the other hand, the result obtained in [24] are in a sense more general than ours since apply to D-dimensional GCA defined on any subshift of $G^{\mathbb{Z}}$. As for the computational cost of our algorithmic method, it is significantly lower than that of the algorithms proposed in [24].

It is rather remarkable that two such distant approaches have led to a surprisingly strong convergence of results.

6. Conclusion and further work

This paper establishes that several fundamental set-theoretic and dynamical properties of a GCA hold if and only if the same properties are satisfied by a corresponding set of GCA defined on significantly easier to study finite groups (abelian groups or products of simple non-abelian isomorphic groups). The set of such GCA is obtained by means of a novel algorithmic technique provided in this paper and based on the group decomposition, where the latter is fully independent of the GCA rule and the GCA complexity. In our opinion, our results are not only interesting in themselves, but also pave the way for tackling and solving a number of open questions related to the dynamical behavior of GCA.

Unfortunately, our results do not help to solve the problem of explicitly establishing the relationship between the local rule defining the cellular automaton and its global dynamical behavior. One of the reasons why this problem is so challenging is that the local rule of a GCA cannot be expressed using an easy-to-manage algebraic formulation. In the case of abelian GCA, their study can be reduced to that of Linear CA where the local rule can be represented by a square matrix whose elements are Laurent polynomials. This allows characterizing the dynamical properties of the GCA in terms of specific properties of the characteristic polynomial of the matrix representing the local rule of the Linear CA associated with the GCA. As far as we know, in the case of non-abelian groups, the only practical way to represent a local rule is by describing the behavior of its associated endomorphisms, e.g., by assigning their values when applied to the generators of the group. A method to overcome this limitation would be a significant step toward an easy-to-check characterization of dynamical properties.

CRediT authorship contribution statement

Niccolò Castronuovo: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Alberto Dennunzio:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Luciano Margara:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, 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.

Acknowledgments

This work was partially supported by the PRIN 2022 PNRR project “Cellular Automata Synthesis for Cryptography Applications (CASCA)” (P2022MPFRT) funded by the European Union – Next Generation EU, and by the HORIZON-MSCA-2022-SE-01 project 101131549 “Application-driven Challenges for Automata Networks and Complex Systems (ACANCOS)”.

Data availability

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

References

[1] G.A. Hedlund, Endomorphisms and automorphisms of the shift dynamical system, Math. Syst. Theory 3 (1969) 320–375.
[2] K.-P. Hadeler, J. Müller, Cellular Automata: Analysis and Applications, Springer Monographs in Mathematics, Springer, 2017.
[3] T. Ceccherini-Silberstein, M. Coornaert, Cellular Automata and Groups, Springer Monographs in Mathematics, Springer, 2010.
[4] A.M. del Rey, J.P. Mateus, G.R. Sánchez, A secret sharing scheme based on cellular automata, Appl. Math. Comput. 170 (2) (2005) 1356–1364.
[5] P. Anghelescu, S. Ionita, E. Sofron, Block encryption using hybrid additive cellular automata, in: A. König, M. Köppen, N.K. Kasabov, A. Abraham (Eds.), 7th International Conference on Hybrid Intelligent Systems, HIS 2007, Kaiserslautern, Germany, September 17–19, 2007, IEEE Computer Society, 2007, pp. 132–137.
[6] C.F. Rubio, L.H. Encinas, S.H. White, Á.M. del Rey, G.R. Sánchez, The use of linear hybrid cellular automata as pseudo random bit generators in cryptography, Neural Parallel Sci. Comput. 12 (2) (2004) 175–192.
[7] J. Kari, Linear cellular automata with multiple state variables, in: H. Reichel, S. Tison (Eds.), STACS 2000, in: LNCS, vol. 1770, Springer-Verlag, 2000, pp. 110–121.
[8] A. Dennunzio, E. Formenti, D. Grinberg, L. Margara, Decidable characterizations of dynamical properties for additive cellular automata over a finite abelian group with applications to data encryption, Inf. Sci. 563 (2021) 183–195.
[9] K. Culik II, J. Pachl, S. Yu, On the limit sets of cellular automata, SIAM J. Comput. 18 (4) (1989) 831–842.
[10] K. Culik II, S. Yu, Undecidability of ca classification schemes, Complex Syst. 2 (1988) 177–190.
[11] L.P. Hurd, J. Kari, K. Culik, The topological entropy of cellular automata is uncomputable, Ergod. Theory Dyn. Syst. 12 (2) (1992) 255–265.
[12] J. Kari, Rice's theorem for the limit sets of cellular automata, Theor. Comput. Sci. 127 (2) (1994) 229–254.
[13] S. Nandi, B.K. Kar, P.P. Chaudhuri, Theory and applications of cellular automata in cryptography, IEEE Trans. Comput. 43 (12) (1994) 1346–1357.
[14] G. Cattaneo, E. Formenti, G. Manzini, L. Margara, Ergodicity, transitivity, and regularity for linear cellular automata over $\mathbb{Z}_m$, Theor. Comput. Sci. 233 (1–2) (2000) 147–164.

[15] G. Manzini, L. Margara, Attractors of linear cellular automata, J. Comput. Syst. Sci. 58 (3) (1999) 597–610.
[16] G. Manzini, L. Margara, A complete and efficiently computable topological classification of d-dimensional linear cellular automata over $\mathbb{Z}_m$, Theor. Comput. Sci. 221 (1–2) (1999) 157–177.
[17] A. Dennunzio, E. Formenti, D. Grinberg, L. Margara, Dynamical behavior of additive cellular automata over finite abelian groups, Theor. Comput. Sci. 843 (2020) 45–56.
[18] A. Dennunzio, E. Formenti, D. Grinberg, L. Margara, An efficiently computable characterization of stability and instability for linear cellular automata, J. Comput. Syst. Sci. 122 (2021) 63–71.
[19] A. Dennunzio, E. Formenti, L. Manzoni, L. Margara, A.E. Porreca, On the dynamical behaviour of linear higher-order cellular automata and its decidability, Inf. Sci. 486 (2019) 73–87.
[20] A. Dennunzio, E. Formenti, L. Margara, An easy to check characterization of positive expansivity for additive cellular automata over a finite abelian group, IEEE Access 11 (2023) 121246–121255.
[21] A. Dennunzio, E. Formenti, L. Margara, An efficient algorithm deciding chaos for linear cellular automata over $(\mathbb{Z}/m\mathbb{Z})^n$ with applications to data encryption, Inf. Sci. 657 (2024) 119942.
[22] M. d'Amico, G. Manzini, L. Margara, On computing the entropy of cellular automata, Theor. Comput. Sci. 290 (3) (2003) 1629–1646.
[23] M. Finelli, G. Manzini, L. Margara, Lyapunov exponents versus expansivity and sensitivity in cellular automata, J. Complex. 14 (2) (1998) 210–233.
[24] P. Béaur, J. Kari, Effective projections on group shifts to decide properties of group cellular automata, Int. J. Found. Comput. Sci. 35 (1&2) (2024) 77–100.
[25] A. Dennunzio, E. Formenti, L. Margara, On the dynamical behavior of cellular automata on finite groups, IEEE Access 12 (2024) 122061–122077.
[26] J.J. Rotman, Introduction to the Theory of Groups, 4th edition, Graduate Texts in Mathematics, Springer, New York, 1995.
[27] R.L. Devaney, An Introduction to Chaotic Dynamical Systems, Addison-Wesley Advanced Book Program, Addison-Wesley, 1989.
[28] M. Nasu, Textile systems for endomorphisms and automorphisms of the shift, in: Memoirs of the American Mathematical Society, American Mathematical Society, 1995.
[29] P. Kůrka, Languages, equicontinuity and attractors in cellular automata, Ergod. Theory Dyn. Syst. 17 (2) (1997) 417–433.
[30] S. Schwartzman, On transformation groups, Ph.D. thesis, Yale University, 1952.
[31] E.M. Coven, M. Keane, Every compact metric space that supports a positively expansive homeomorphism is finite, in: Dynamics & Stochastics, in: IMS Lecture Notes – Monograph Series, vol. 48, Institute of Mathematical Statistics, Beachwood, OH, 2006, pp. 304–305.
[32] R.L. Adler, A.G. Konheim, M.H. McAndrew, Topological entropy, Trans. Am. Math. Soc. 114 (2) (1965) 309–319.
[33] V. Salo, I. Törmä, On shift spaces with algebraic structure, in: S.B. Cooper, A. Dawar, B. Löwe (Eds.), How the World Computes - Turing Centenary Conference and 8th Conference on Computability in Europe, CiE 2012, Proceedings, Cambridge, UK, June 18–23, 2012, in: Lecture Notes in Computer Science, vol. 7318, Springer, 2012, pp. 636–645.
[34] V. Salo, I. Törmä, Color blind cellular automata, J. Cell. Autom. 9 (5–6) (2014) 477–509.
[35] K.H. Hofmann, S.A. Morris, Open mapping theorem for topological groups, in: Topology Proc., vol. 31, 2007, pp. 533–551.
[36] M. Boyle, B. Kitchens, Periodic points for onto cellular automata, Indag. Math. 10 (4) (1999) 483–493.
[37] B. Kitchens, K. Schmidt, Automorphisms of compact groups, Ergod. Theory Dyn. Syst. 9 (4) (1989) 691–735.
[38] T.S. Moothathu, Homogeneity of surjective cellular automata, Discrete Contin. Dyn. Syst. 13 (1) (2005) 195–202.
[39] M. Denker, C. Grillenberger, K. Sigmund, Ergodic Theory on Compact Spaces, Lecture Notes in Mathematics, vol. 27, Springer-Verlag, Berlin, 1976.
[40] H. Chu, Some results on affine transformations of compact groups, Invent. Math. 28 (2) (1975) 161–183.
[41] P. Walters, Ergodic Theory: Introductory Lectures, Lecture Notes in Computer Science, Springer-Verlag, 1975.
[42] P.-F. Lam, On expansive transformation groups, Trans. Am. Math. Soc. 150 (1) (1970) 131–138.
[43] Z. Jiang, J. Li, Chaos for endomorphisms of completely metrizable groups and linear operators on Fréchet spaces, J. Math. Anal. Appl. 543 (2, Part 3) (2025) 129033.
[44] S.A. Juzvinskiĭ, Metric properties of endomorphisms on homogeneous spaces of compact groups, Math. USSR, Izv. 5 (1) (1971) 80.
[45] A. Giordano Bruno, S. Virili, Topological entropy in totally disconnected locally compact groups, Ergod. Theory Dyn. Syst. 37 (7) (2017) 2163–2186.
[46] D. Gorenstein, Finite Groups, AMS Chelsea Publishing Series, American Mathematical Society, 2007.
[47] H. Neumann, Varieties of Groups, Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge, Springer Berlin Heidelberg, 2012.
[48] D. Dummit, R. Foote, Abstract Algebra, 3rd edition, Wiley, 2003.
[49] C. Robinson, Dynamical Systems: Stability, Symbolic Dynamics and Chaos, Studies in Advanced Mathematics, CRC-Press, 1995.
[50] S. Amoroso, Y. Patt, A decision procedure for surjectivity and injectivity of parallel maps for tessellation structures, J. Comput. Syst. Sci. 6 (5) (1972) 448–464.
[51] J. Kari, Reversibility and surjectivity of cellular automata in dimension d $\geq$ 2, Inf. Comput. 118 (1) (1994) 192–210.
[52] V. Lukkarila, Sensitivity and topological mixing are undecidable for reversible one-dimensional cellular automata, J. Cell. Autom. 5 (3) (2010) 241–272.