Commutators of Bipermutive and Affine Cellular Automata*

Ville Salo[1] and Ilkka Törmä[2]

[1] TUCS – Turku Centre for Computer Science, Finland,
University of Turku, Finland,
vosalo@utu.fi

[2] TUCS – Turku Centre for Computer Science, Finland,
University of Turku, Finland,
iatorm@utu.fi

Abstract. We discuss bipermutive cellular automata from a combinatorial and topological perspective. We prove a type of topological randomizing property for bipermutive CA, show that the commutator of a bipermutive CA is always small and that bipermutive affine CA have only affine CA in their commutator. We show the last result also in the multidimensional case, proving a conjecture of [Moore-Boykett, 97].

Keywords: cellular automata, bipermutivity, commutation, affine cellular automata

1 Introduction

Bipermutive cellular automata, that is, CA which are permutive in the left- and rightmost coordinates of their neighborhood, have been investigated in great detail in the literature. Most of the work has been in the ergodic theory of cellular automata, as this is a natural framework for studying the randomizing nature of bipermutive automata. We refer to [5] for a survey of this theory.

We take a more combinatorial approach, and study the topological dynamics of bipermutive cellular automata and their commutators in the monoid of cellular automata. On the side of topological dynamics, we obtain some basic results about orbits of one-dimensional configurations and subshifts. We prove a simple lemma stating that every pattern is self-replicating on a periodic background. We use this to show that every SFT with sufficient mixing properties becomes a full shift in the limit in the action of the CA, and we say the CA topologically randomizes such SFTs, as this is a kind of topological analogue of asymptotic randomization in ergodic theory. For bipermutive CA and a mixing SFT, topological randomization turns out to be equivalent to the existence of a transitive point. We also present a particular case of asymptotic randomization in the multidimensional setting, for a natural generalization of bipermutivity, which we call total extremal permutivity.

* Research supported by the Academy of Finland Grant 131558

Our results about orbits are purely qualitative: while we prove that certain subshifts tend to the full shift, we do not obtain any sensible bounds for when a pattern first appears. One can extract such bounds from our proofs, but they are not very good: For example, we can prove that the golden mean shift X tends to the full shift in the action of the binary XOR automaton f. However, the bounds directly obtained fall short of showing that all binary words of length n appear in $f^{a^{(n)}}(X)$ where $a^{(n)} = a^{a^{\cdot^{\cdot^{a}}}}$ denotes tetration and a is the size of the alphabet.

Interestingly, we obtain rather strong quantitative results on the commutator using the purely qualitative results on orbits: Our main result on the commutator of a totally extremally permutive CA is that for any radius, it contains only exponentially many cellular automata with that radius, while the number of cellular automata of a given radius in general is doubly exponential.

We then move on to totally extremally permutive affine self-maps of group shifts, where affine means homomorphic up to the addition of a constant. Our main result here extends the result of [4] that affine bipermutive CA have only affine CA in their commutator to all dimensions, which was conjectured in [4]. In fact, we show that the multidimensional case rather directly reduces to the one-dimensional case, so that the first proof is just an application of the result of [4]. The second proof is based directly on the lemma that all patterns self-replicate on a periodic background, as we can use this to superpose two patterns. In the case of a *homomorphic* totally extremally permutive CA on $\mathbb{Z}_p^{\mathbb{Z}^d}$, and considering only CA with 0 as a quiescent state, we give a third proof which shows that the commutator is exactly the set of all homomorphisms. This in turn is a direct consequence of our results on orbits of subshifts.

2 Definitions

Let S be a finite set, called the *alphabet.* For $d \in \mathbb{N}$, the *d-dimensional full shift* is the space $S^{\mathbb{Z}^d}$ of infinite configurations over S endowed with the product topology. For $x \in S^{\mathbb{Z}^d}$, we denote by $x_{\boldsymbol{n}}$ the symbol of x at coordinate $\boldsymbol{n}$. For any $s \in S$, when the dimension d is clear from context, we define $c(s) \in S^{\mathbb{Z}^d}$ as the configuration with $c(s)_{\boldsymbol{n}} = s$ for all $\boldsymbol{n} \in \mathbb{Z}^d$. A one-dimensional configuration $x \in S^{\mathbb{Z}}$ is *spatially periodic* if $x_{i+p} = x_i$ for some $p > 0$ and all $i \in \mathbb{Z}$.

A subset $X \subset S^{\mathbb{Z}^d}$ is called a *subshift* if it is closed in the topology and invariant under all *shift maps* $\sigma^{\boldsymbol{m}} : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ for $\boldsymbol{m} \in \mathbb{Z}^d$, defined by $\sigma^{\boldsymbol{m}}(x)_{\boldsymbol{n}} = x_{\boldsymbol{n}+\boldsymbol{m}}$. A *pattern* is a pair (N, w), where $w \in S^N$, for a finite domain $N \subset \mathbb{Z}^d$. We denote $\mathcal{B}_N(X) = \{(N, x_N) \mid x \in X\}$, and define the *language* of X as $\mathcal{B}(X) = \{(N, x_N) \mid N \subset \mathbb{Z}^d \text{ finite}, x \in X\}$. In the one-dimensional case, patterns are replaced by words in these definitions. Since a subshift is uniquely defined by its language, and every extendable and factor-closed language defines a one-dimensional subshift [3], we may write $X = \mathcal{B}^{-1}(L)$, if $\mathcal{B}(X)$ is the set of factors of the extendable language $L \subset S^*$. The *entropy* of a subshift $X \subset S^{\mathbb{Z}^d}$ is defined as $h(X) = \lim_{n\to\infty} \frac{1}{n^d} \log |\mathcal{B}_{[0,n-1]^d}(X)|$.

Alternatively, a subshift is defined by a set $F \in S$ of *forbidden patterns* as the set of configurations $\mathcal{X}_F = \{x \subset S^{\mathbb{Z}^d} \mid \forall (N, w) \in F, \boldsymbol{n} \in \mathbb{Z}^d : x_{\boldsymbol{n}+N} \neq w\}$. If F is finite, then $\mathcal{X}_F$ is *of finite type* (SFT for short). Once a finite set of forbidden patterns is chosen in the one-dimensional case, the length of the longest pattern is called the *window size* of the corresponding SFT. We say an SFT $X \subset S^{\mathbb{Z}}$ is *mixing* if there exists $n \in \mathbb{N}$, called its *mixing distance*, such that for all $u, w \in \mathcal{B}(X)$ and $m \geq n$ there exists $v \in \mathcal{B}_n(X)$ such that $uvw \in \mathcal{B}(X)$.

A continuous mapping $f : X \to X$ in a subshift that commutes with all shift maps is called a *cellular automaton*. All cellular automata f are defined by *local functions* $F : S^N \to S$, where $N \subset \mathbb{Z}^d$ is the finite *neighborhood* of f, by the formula $f(x)_{\boldsymbol{n}} = F(x_{\boldsymbol{n}+N})$ for all $\boldsymbol{n} \in \mathbb{Z}^d$ [2]. A configuration x of X is called *temporally periodic (with respect to f)* if $f^p(x) = x$ for some p. If $X = S^{\mathbb{Z}^d}$, we denote by f_{loc} the local function of f with the minimal neighborhood.

A CA f with minimal neighborhood N is *permutive* in a coordinate $\boldsymbol{n} \in N$ if for all $x \in S^N$, permuting the symbol of x at $\boldsymbol{n}$ permutes the image $f_{\mathrm{loc}}(x)$. We say a CA $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ is *totally extremally permutive* if $|N| \geq 2$, and f_{loc} is permutive in the vertices of the convex hull of N (as a subset of $\mathbb{R}^d$). We define a *bipermutive* CA as a totally extremally permutive CA in dimension one. It is easy to see that our definition of bipermutivity coincides with the usual definition.

Function composition $\circ$ gives the set of all CA (on a fixed subshift) the structure of a monoid. The *commutator* of the CA $f : X \to X$ is then naturally defined as

$$C(f) = \{g : X \to X \mid g \text{ is a CA, } f \circ g = g \circ f\}.$$

Let G be a finite group. Then applying the operations of G cellwise gives rise to a natural group structure on $G^{\mathbb{Z}^d}$. A cellular automaton which is a group homomorphism of $G^{\mathbb{Z}^d}$ is said to be *homomorphic*. We avoid the commonly used terms 'linear' and 'additive' as the first can also refer to one-dimensional cellular automata, and both terms are sometimes used to refer to cellwise sums of shift maps. If $f : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ satisfies $f(x) = g(x) \cdot c(C)$ for all x, for some $C \in G$ and some homomorphic CA g, then we say f is *affine*.

We denote by $SL_d(\mathbb{Z})$ the restriction of $SL_d(\mathbb{R})$ to those functions that map $\mathbb{Z}^d$ bijectively to itself. For a configuration $x \in S^{\mathbb{Z}^d}$ and $A \in SL_d(\mathbb{Z})$, we define $A(x) \in S^{\mathbb{Z}^d}$ by $A(x)_{\boldsymbol{n}} = x_{A(\boldsymbol{n})}$ for all $\boldsymbol{n} \in \mathbb{Z}^d$, and for a subshift $X \subset S^{\mathbb{Z}^d}$, we define $A(X) = \{A(x) \mid x \in X\}$. Here, the choice of A over A^{-1} in $x_{A(\boldsymbol{n})}$ is by analogy with how shift maps are defined: we always transform the view, not the configuration. From the linearity of A it follows that $A(X)$ is also a subshift. For a cellular automaton $f : X \to X$, we define $A(f) : A(X) \to A(X)$ by $A(f)(x) = A(f(A^{-1}(x)))$ for all $x \in X$. It is easy to see that $A(f)$ is a cellular automaton, and if $N \subset \mathbb{Z}^d$ is the neighborhood of f, then $A^{-1}(N)$ is that of $A(f)$. Moreover, $A(f)$ is totally extremally permutive, homomorphic or affine if and only if f is, and if $g : X \to X$ is another CA, we have $A(f \circ g) = A(f) \circ A(g)$.

Multi-dimensional and one-dimensional full shifts have a natural connection through the following definitions. Let

$$X_p^d = \{x \in S^{\mathbb{Z}^d} \mid \forall i \in \{2, \dots, d\} : \sigma^{pe_i}(x) = x\},$$

where $(e_i)_i$ are the natural basis of $\mathbb{Z}^d$. That is, X_p^d is the d-dimensional full shift restricted to points with period $p \in \mathbb{N}$ in all but the first dimension. There is a natural bijection between X_p^d and $(S^{p^{d-1}})^{\mathbb{Z}}$, which we call ρ_p (the dimension will always be clear from context).

3 Self-replication in bipermutive CA

In this section, we study the behavior of individual configurations under the action of bipermutive CA. We give some examples, and prove Lemma 1 which states that every pattern, when surrounded by temporally and spatially periodic content, eventually self-replicates in the orbit of a bipermutive cellular automaton. All of the results of this article are, to some extent, based on this observation.

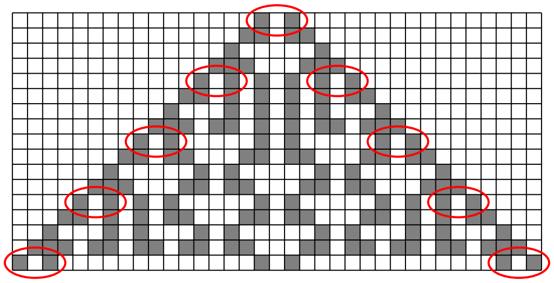

Fig. 1. An illustration of the elementary CA 150 running from the initial pattern 101 for 16 generations. The red ellipses show that the initial pattern repeats periodically at the borders.

We start with an illustration of this fundamental property of bipermutive CA for a particularly simple example: the binary CA with local rule $g_{\text{loc}}(a, b, c) = a + b + c \bmod 2$ and neighborhood $\{-1, 0, 1\}$. This is the elementary cellular automaton number 150, see Figure 1 for a sample spacetime diagram. In addition to being permutive in each coordinate, this CA exemplifies many other interesting properties (for example, it is homomorphic and totalistic). We illustrate how one can build an arbitrary pattern from restricted (sparse) input using only its bipermutivity in Figure 2.

Let f be bipermutive, and let $a \in S$ be such that $f^p({}^\infty a^\infty) = {}^\infty a^\infty$. Then, as we outlined above, any word $w \in S^n$, when superposed on the periodic back-

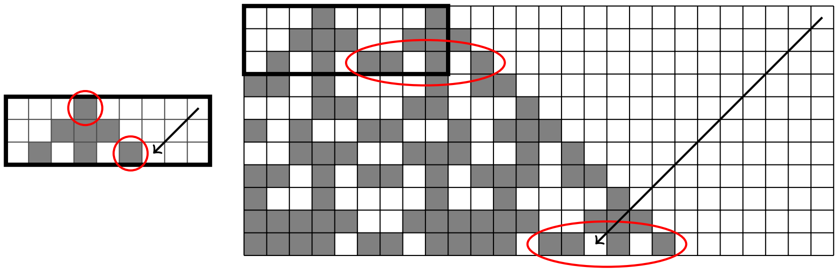

Fig. 2. We illustrate the general idea of building patterns from sparse configurations using the CA 150. We show how to systematically use its bipermutivity to build the pattern 111 while keeping the starting configuration sparse (although it 'accidentally' appears already on the first step). In the figure on the left, we show an initial part of the spacetime diagram of the configuration with a single 1, until the 1 reappears sufficiently far to the right, indicated by the red circles. The arrow indicates that by permuting the upper right coordinate, we simultaneously permute the cell it points to. In the figure on the right, we have permuted said coordinate so that the prefix 11 of 111 is obtained. We then repeat the procedure by waiting for the (arbitrary) data to the right of 11 to repeat sufficiently far away, and locating a suitable coordinate a that can be used to extend the repeated 11 into 111.

ground ${}^{\infty}a^{\infty}$, is a kind of self-replicating pattern: Copies of w periodically appear on both borders of the light cone starting from w. See Figure 1 for a concrete illustration. The precise statement is formulated in Lemma 1. The proof is straightforward.

Lemma 1. *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a left permutive CA with neighborhood $[-r, r']$, and let $y \in S^{\mathbb{Z}}$ be temporally and spatially periodic with periods t and p, respectively. Let $x \in S^{\mathbb{Z}}$ be such that $x_i = y_i$ for all $i > 0$, and let $n \in \mathbb{N}$. Then, denoting $C = pt(|S|^n)!$ and $I = [-n+1, 0]$, for all $\ell \in \mathbb{N}$, we have*

$$f^{\ell C}(x)_{I+\ell r C} = x_I.$$

The lemma states that the pattern x_I is repeated on every Cth step on the right border of the light cone. Of course, in the right (or bi-) permutive case, a symmetric result holds. We refer to both results as Lemma 1.

4 Orbits of one-dimensional subshifts in bipermutive CA

With the help of Lemma 1, we now consider the orbits of *subshifts* in bipermutive CA.

Definition 1. *Let X be a subshift, $f : X \to X$ a cellular automaton and $Y \subset X$ a subshift of X. We define the* f-orbit closure Y^f *of Y to be the set $\overline{\bigcup_{i\in\mathbb{N}} f^i(Y)}$. We also define the* asymptotic set of Y *as $\omega_f(Y) = \bigcap_{n\in\mathbb{N}} \overline{\bigcup_{i\geq n} f^i(Y)}$.*

Clearly, we always have $\omega_f(Y) \subset Y^f$, and $Y^f = Y^{\sigma^m \circ f}$ for all $m \in \mathbb{Z}$.

The first nontrivial result that follows from Lemma 1 is a generalization of the ideas in the caption of Figure 2. Namely, the property of a bipermutive cellular automaton $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ that every word is self-replicating can be used to show that every word occurs in some image $f^n(X)$ if the SFT $X \subset S^{\mathbb{Z}}$ satisfies certain mixing properties. In fact, an SFT X satisfying the assumptions of the following theorem will even contain a transitive point for f by a slightly more involved proof, but we do not need this result.

Theorem 1. *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive CA and $X \subset S^{\mathbb{Z}}$ a nontrivial mixing SFT with window size m. If there exists $v_1 \in \mathcal{B}_{m-1}(X)$ such that $v_1 s \in \mathcal{B}_m(X)$ for all $s \in S$, the $\omega_f(X) = S^{\mathbb{Z}}$.*

Proof. Suppose that such a v_1 exists. Without loss of generality we can assume that ${}^\infty v_1^\infty \in X$ (since periodic points are dense), and that m is also a mixing distance for X. Let $w \in S^*$ be arbitrary. We will show, by induction on $|w|$, that there exist arbitrarily large $n \in \mathbb{N}$ such that $w \in \mathcal{B}(f^n(X))$, from which the claim then follows. The case $|w| = 0$ is trivial.

Suppose then that the claim holds for $w \in S^*$, and let $s \in S$. We will prove the claim for the word ws. Figure 3 illustrates the proof. Let r and r' be the left and right radii of f, respectively. By the induction hypothesis, for arbitrarily large $n \in \mathbb{N}$, there exists a word $u \in \mathcal{B}_{|w|+n(r+r')}(X)$ such that $f^n(u) = w$. We can take n so large that $f^n({}^\infty v_1{}^\infty) = {}^\infty v_2{}^\infty$ has the property that $f^p({}^\infty v_2{}^\infty) = {}^\infty v_2{}^\infty$ for some $p \in \mathbb{N}$, where $|v_2| = m - 1$.

For all $k \in [m, 2m-2]$ we choose a mixing word $z_k \in \mathcal{B}_k(X)$ and an arbitrary left extension $y_k \in S^{-\mathbb{N}}$ such that $x_k = y_k.uz_k v_1^\infty \in X$. Now, $f^n(x_k)_{[rn,\infty)} = wz'_k v_2^\infty$ for some $z'_k \in \mathcal{B}_{k+n(r+r')}(X)$. Then, by Lemma 1, there exists $t_k > k + n(r + r') + |v_1|$ such that

$$f^{n+\ell t_k}(x_k)_{[r(n+\ell t_k),\infty)} = wz'_k v_2^\infty$$

for all $\ell \in \mathbb{N}$. Let $h = \mathrm{lcm}\{t_k \mid k \in [m, 2m-2]\}$, so that

$$f^{n+h}(x_k)_{[r(n+h),\infty)} = wz'_k v_2^\infty,$$

for all k.

Let now k be such that

$$a = (r + r')(n + h) + |w| + 1 \equiv |u| + k \bmod (m - 1). \tag{1}$$

We can permute the coordinate a of x_k (and choose a new right tail arbitrarily), because (1) and the fact that $h > k+n(r+r')+|v_1|$ imply that it is preceded by the word v_1, and m is the window size of X. Permuting the coordinate a in x_k (point A in Figure 3) permutes the coordinate $a-r'(n+h) = r(n+h)+|w|+1$ in $f^{n+h}(x_k)$ (point B in Figure 3) without affecting any coordinate to the left of it, and thus all the words ws for $s \in S$ occur in $f^{n+h}(X)$. Since n may be chosen arbitrarily large, this concludes the induction step. $\square$

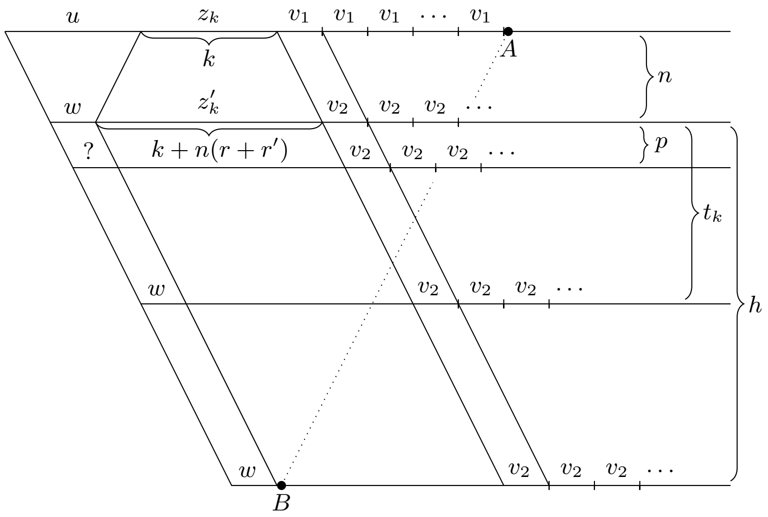

Fig. 3. A schematic diagram of the proof of Proposition 1. The coordinate A may be changed to any symbol without changing the left part, and by permuting A, we also permute B.

Note that in the proof of Proposition 1, both left and right permutivity are needed: As the CA is left permutive, Lemma 1 guarantees that w repeats on the right border of the light cone. Right permutivity on the other hand guarantees that the permutation applied to the coordinate a of x_k propagates along the left side of the light cone to a permutation of the $(n + h)$th image.

Also, we note that if X is a proper subshift of $S^{\mathbb{Z}}$, then $\bigcup_{n \in \mathbb{N}} f^n(X)$ is not actually equal to $S^{\mathbb{Z}}$. In fact, for all n, the subshift $f^n(X)$ has the same entropy as X, since a bipermutive CA is finite-to-one [3], and thus cannot contain a doubly transitive point. This means that the appearance of all words of S^k for larger and larger k in $f^n(X)$ is somehow compensated by having these words appear in only a small number of different contexts.

Example 1. Let $X \subset \{0, 1\}^{\mathbb{Z}}$ be the golden mean shift (the SFT with forbidden pattern 11), and let $f : \{0, 1\}^{\mathbb{Z}} \to \{0, 1\}^{\mathbb{Z}}$ be the binary XOR automaton, which is bipermutive. Then

$$f(X) = \mathcal{B}^{-1}((0^*(11)^*)^*).$$

Thus, $f(X)$ is conjugate to the even shift $\mathcal{B}^{-1}((1^*(00)^*)^*)$ by the CA that applies the permutation $(0\ 1)$ cellwise, and it is indeed well known that the golden mean shift and the even shift have equal entropy. However, $\mathcal{B}_2(X) = \{00, 01, 10\}$, while $\mathcal{B}_2(f(X)) = \{00, 01, 10, 11\}$.

We continue one more step:

$$f^2(X) = \mathcal{B}^{-1}((0^*10(00)^*1)^*),$$

the binary subshift where every second maximal contiguous segment of 0s is of odd length. Note that

$$\begin{aligned}\mathcal{B}_3(X) &= \{000, 001, 010, 100, 101\},\\ \mathcal{B}_3(f(X)) &= \{000, 001, 010, 011, 100, 110, 111\}, \text{and}\\ \mathcal{B}_3(f^2(X)) &= \{000, 001, 010, 011, 100, 101, 110, 111\},\end{aligned}$$

but X and $f^2(X)$ again have equal entropy.

If the entropy $h(Y)$ of a subshift $Y \subset S^{\mathbb{Z}}$ is more than $\log(|S| - 1)$, then for all $m \in \mathbb{N}$ there exists $w \in \mathcal{B}_m(Y)$ such that $ws \in \mathcal{B}(Y)$ for all $s \in S$. Similarly, in the binary case, any mixing SFT with at least two points contains such a w. Thus we have the following corollaries to Theorem 1.

Corollary 1. *If $Y \subset S^{\mathbb{Z}}$ is a mixing SFT with $h(Y) > \log(|S| - 1)$ and the CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ is bipermutive, then $\omega_f(Y) = S^{\mathbb{Z}}$.*

Corollary 2. *If $Y \subset \{0, 1\}^{\mathbb{Z}}$ is an nontrivial mixing SFT and the CA $f : \{0, 1\}^{\mathbb{Z}} \to \{0, 1\}^{\mathbb{Z}}$ is bipermutive, then $\omega_f(Y) = \{0, 1\}^{\mathbb{Z}}$.*

Proposition 1. *Let $p \in \mathbb{N}$ be a prime, let $S = \mathbb{Z}_p$, let the CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a group homomorphism with at least two neighbors, and let $Y \subset S^{\mathbb{Z}}$ be a nontrivial mixing SFT. Then $\omega_f(Y) = S^{\mathbb{Z}}$.*

We omit the proof of Proposition 1, as it is essentially the same as that of Proposition 1, except that we permute the same coordinate multiple times (f is automatically bipermutive).

Proposition 1 can be thought of as a kind of topological analogue of Theorem 5.3 in [5] (proved in [6]), which in particular states that the ergodic averages of any Markov measure with full support converge to the uniform Bernoulli measure in the weak-star topology, under the action of a bipermutive homomorphic CA on $\mathbb{Z}_p^{\mathbb{Z}}$. The automaton is said to *asymptotically randomize* such a measure. Using analogous terminology, we can say that a CA f *topologically randomizes* a subshift X if $\omega_f(X) = S^{\mathbb{Z}}$, and our result then states that a bipermutive homomorphic CA topologically randomizes every nontrivial mixing SFT $X \subset \mathbb{Z}_p^{\mathbb{Z}}$. Theorem 1 can of course also be phrased in terms of topological randomization, but the class of subshifts randomized is not quite as natural (see Question 1).

There is also a more familiar meaning to these results, as topological randomization in fact corresponds to the existence of a transitive point.

Theorem 2. *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a left permutive CA with neighborhood $[-r, r']$, where $r > 0$, and let $X \subset S^{\mathbb{Z}}$ a mixing SFT such that $\omega_f(X) = S^{\mathbb{Z}}$. Then X contains a transitive point for f.*

The next (rather trivial) example shows that the restriction to a group of prime order is necessary in Proposition 1, that just mixing does not suffice for proving Theorem 1, and that entropy $h(Y) \geq \log(|S|/2)$ is not enough for Corollary 1.

Example 2. Let f be the CA 150, $X = (\{0,1\} \times \{0\})^{\mathbb{Z}} \subset (\{0,1\}^2)^{\mathbb{Z}} = Y$ and $g = f \times f$. Then X is a mixing SFT with $h(X) = \log 2$, g is homomorphic and bipermutive, and $h(Y) = \log 4$, but $g(X) = X$.

Here, the CA g is a group homomorphism, and $\mathcal{B}_1(X)$ is a subgroup of the full group that g cannot expand. We do not know whether such cheating is the only way to guarantee that a mixing SFT does not expand to the full shift. In fact, we do not know whether a bipermutive CA randomizes every mixing SFT that uses the full alphabet.

Question 1. Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive CA, and $Y \subset S^{\mathbb{Z}}$ a nontrivial mixing SFT with $\mathcal{B}_1(Y) = S$. Do we then have $\omega_f(Y) = S^{\mathbb{Z}}$?

A positive solution to Question 1 seems plausible, and would extend Theorem 1 to a much more natural class of topologically randomized subshifts.

Definition 2. *Let $0 \in S$ and $d, k \geq 1$. The k-*sparse subshift *of dimension d is the SFT $X \subset S^{\mathbb{Z}^d}$ defined by the forbidden patterns*

$$\{P \in S^{[1,k]^d} \mid |P|_0 \leq k^d - 2\}.$$

For example, the one-dimensional binary 2-sparse subshift is just the golden mean shift. We can apply Theorem 1 to such subshifts to obtain concrete examples of simple subshifts that bipermutive automata take to the full shift in the limit, as the k-sparse subshift obviously satisfies the assumption of Theorem 1. This (and especially its generalization Proposition 2) is useful for the commutation of cellular automata, as we will see in the next section.

Corollary 3. *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive CA, $k \in \mathbb{N}$, and $X \subset S^{\mathbb{Z}}$ the k-sparse subshift. Then $\omega_f(X) = S^{\mathbb{Z}}$.*

5 Orbits of multidimensional *k*-sparse shifts in bipermutive CA

We extend Corollary 3 to higher dimensions. The proof is essentially the same as that of Proposition 1, but we use some additional tricks to make the argument cleaner. Namely, we apply a certain transformation of $SL_d(\mathbb{Z})$ to make the neighborhood shape more suitable, and then use a similar shoot-and-reperiodize technique as in [7] to partially reduce the problem to the one-dimensional case.

Definition 3. *For $\boldsymbol{n} = (x_1, \ldots, x_d) \in \mathbb{Z}^d$, denote $\pi(\boldsymbol{n}) = x_1$. A set $N \subset Z^d$ is* pointy*, if*

$$|N \cap \pi^{-1}(\min \pi(N))| = |N \cap \pi^{-1}(\max \pi(N))| = 1.$$

Lemma 2. *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a cellular automaton. Then, there exists $A \in SL_d(\mathbb{Z})$ such that $A(f)$ has a pointy neighborhood.*

The usefulness of pointy neighborhoods comes from the following observation.

Lemma 3. *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a totally extremally permutive CA with a pointy neighborhood. Then for all p, the automaton $f' = \rho_p(f) : (S^{p^{d-1}})^{\mathbb{Z}} \to (S^{p^{d-1}})^{\mathbb{Z}}$ defined by $f' = \rho_p \circ f \circ \rho_p^{-1}$ is bipermutive.*

Proposition 2. *If the CA $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ is totally extremally permutive with quiescent state 0, then $\omega_f(X) = S^{\mathbb{Z}^d}$, where X is the d-dimensional k-sparse subshift.*

Proof. We prove here the case $d = 2$. The general case follows similarly, but is notationally more complex. We first ensure that the neighborhood is pointy (the first axis is the horizontal one) and is located at the west border of the east half-plane, so that on points with a vertical period, a one-dimensional bipermutive CA with right speed of light 0 is simulated. The general idea is to successively draw larger and larger patterns at the origin as follows: As vertically periodic configurations are in a sense just one-dimensional horizontal configurations, we can apply Lemma 1 to any vertically periodic and horizontally 0-finite configuration to obtain that any finite set of columns repeats infinitely many times in the orbit. Now, as in the proof of Theorem 1, we carefully shoot a signal in the right cell at the right time, and add a huge vertical period to conclude the induction step.

Let us make this precise. We may assume without loss of generality that the lexicographically minimal element in the neighborhood of f is $(0, 0)$, and that the maximal is (m_1, m_2) with $m_1 > 0$. We may also assume that f has a pointy neighborhood by Lemma 2. Let $n \geq k$, and let $P \in S^{n \times n}$ be arbitrary. We inductively construct vertically periodic configurations $x^i \in X$ such that the lexicographical prefix of P of size i occurs in some $f^t(x^i)$ at the origin, and $x^i_{(a,b)} = 0$ for all $b \in \mathbb{Z}$ for large enough $a \in \mathbb{Z}$. For x^1, we choose $x^1_{(0,nm)} = P_{(0,0)}$ for all $m \in \mathbb{Z}$, and $x^1_{\boldsymbol{n}} = 0$ for all other $\boldsymbol{n} \in \mathbb{Z}^2$.

Suppose then that x^i has already been constructed, and let $p \in \mathbb{N}$ be its vertical period. By Lemma 3, when restricted to the set X^2_p, f simulates a bipermutive one-dimensional CA $g : (S^p)^{\mathbb{Z}} \to (S^p)^{\mathbb{Z}}$ through the bijection ρ_p. Denote $H = \{(a, b) \mid a \geq 0\} \subset \mathbb{Z}^2$. Since $\rho_p(x^i)_\ell = 0^p$ for all large enough $\ell \in \mathbb{Z}$ and the left radius of g is 0, we can use Lemma 1 to conclude that there exist arbitrarily large $t > 0$ such that $x^i|_H = f^t(x^i)|_H$.

Now, there are arbitrarily large $t \in \mathbb{N}$ such that $f^t(x^i)$ contains the lexicographical prefix of P of size i at the origin. Let thus t be larger than the maximal $a \in \mathbb{Z}$ with $x^i_{(a-k,b)} \neq 0$ for some $b \in \mathbb{Z}$. Let (c, d) be the lexicographically $(i + 1)$th coordinate of P. We let $y(s)^i \in X$ be as x^i, but with the coordinate $(tm_1 + c, tm_2 + d)$ containing $s \in S$. Now, permuting s in $y(s)^i$ permutes $f^t(y(s)^i_{(c,d)})$, so we can choose s so that $f^t(y(s)^i_{(c,d)}) = P_{(c,d)}$, and denote $y^i = y(s)^i$.

Since (m_1, m_2) is the lexicographically maximal vector in the neighborhood of f, (c, d) is the lexicographically minimal coordinate which can change in $f^t(y(s)^i)$, when we permute s. Thus, $f^t(y^i)$ contains the lexicographical prefix of P of size $i+1$ at the origin. We obtain x^{i+1} from y^i by adding any sufficiently large vertical period. □

Similarly to how Theorem 1 could be generalized to Proposition 1, we can generalize Proposition 2 to Proposition 3.

Proposition 3. *Let $p \in \mathbb{N}$ be a prime, let $S = \mathbb{Z}_p$, let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a group homomorphism with at least two neighbors, and let $Y \subset S^{\mathbb{Z}}$ be a the k-sparse shift. Then $\omega_f(\{0,1\}^{\mathbb{Z}^d} \cap Y) = S^{\mathbb{Z}}$.*

6 Commutation

In this section, we discuss the commutator of a totally extremally permutive cellular automaton. First, we consider the size of such a commutator, and then look at what happens when the totally extremally permutive CA is also an affine map on a full shift with cellwise defined group structure.

6.1 Size of the commutator of a totally extremally permutive CA

In this section, we prove a strong upper bound on the number of commuting cellular automata of any radius. This result is based on the following lemma, which relates the commutator of a given CA f to the f-closures of subshifts.

Lemma 4. *Let $X \subset S^{\mathbb{Z}^d}$ be a subshift, let $f : X \to X$ be a CA and let $Y \subset X$ with $Y^f = X$. Then the map $\phi : C(f) \to X^Y$ defined by $\phi(g) = g|_Y$ is injective.*

Proof. Let $g, h \in C(f)$ be such that $g|_Y = h|_Y$, and let $x \in X$ be arbitrary. Let $r \in \mathbb{N}$ be a common radius for g and h, and let $y \in Y$ and $i \in \mathbb{N}$ be such that $f^i(y)_{[-r,r]^d} = x_{[-r,r]^d}$. Then, since $g, h \in C(f)$, we have

$$g(x)_0 = g(f^i(y))_0 = f^i(g(y))_0 = f^i(h(y))_0 = h(f^i(y))_0 = h(x)_0.$$

Since x was arbitrary, we have $g = h$. □

Proposition 4. *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a totally extremally permutive CA with a quiescent state $0 \in S$. For all $n \in \mathbb{N}$, define*

$$C_n(f) = \left\{ g \in C(f) \mid [0, n-1]^d \text{ is a neighborhood for } g \right\}.$$

Then $|C_n(f)| \leq |S|^{1+n^d(|S|-1)}$.

Proof. Let $X \subset S^{\mathbb{Z}^d}$ be the n-sparse shift. Proposition 2 and Lemma 4 together imply that $|C_n(f)|$ is at most the number of local maps $\mathcal{B}_{[0,n-1]^d}(X) \to S$. Since we have $|\mathcal{B}_{[0,n-1]^d}(X)| = 1 + n^d(|S| - 1)$, the number of such maps is $|S|^{1+n^d(|S|-1)}$. □

The upper bound, reached for example by the identity CA, is $|C_n(f)| = |S|^{|S|^{n^d}}$ for all $n \in \mathbb{N}$. In [1], a concept called 'symmetry' is defined for one-dimensional subshifts: the symmetry of an SFT $X \subset S^{\mathbb{Z}}$ is defined as the limit superior of $\frac{1}{n} \log \log A(n)$, where $A(n)$ is the number of bijective CA on X which have neighborhood $[0, n-1]$. For $X = S^{\mathbb{Z}}$, this is 1 if logarithms are taken in base $|S|$, see [1]. We give a more general definition in the same vein, by taking the same limit for an arbitrary set of CA.

Definition 4. *Fix an alphabet S, and let F be a set of cellular automata on the full shift $S^{\mathbb{Z}^d}$ such that $f \in F$ implies $\sigma^{\boldsymbol{v}} \circ f \in F$ for all $\boldsymbol{v} \in \mathbb{Z}^d$. The* density *of F is defined as*

$$d(F) = \limsup_n \frac{1}{n^d} \log\log A([0, n-1]^d),$$

where $A(N)$ is the number of cellular automata in F with minimal neighborhood contained in N, and logarithms are taken in base $|S|$. If F is a set of cellular automata on a subshift $X \subset S^{\mathbb{Z}}$, we define F' by mapping illegal configurations to a fixed symbol, and let $d(F) = d(F')$.

It is easy to see that the density of the set of automorphisms of a one-dimensional SFT is equal to its symmetry (which in turn is equal to its entropy [1]), and that the density of the commutator of the identity map is 1. We summarize Proposition 4 by noting that the density of the commutator of any totally extremally permutive CA is 0. In [4], it was proved that if $f, g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ are commuting radius-$\frac{1}{2}$ cellular automata and f is bipermutive, then there exist functions $\phi, \psi : S \to S$ such that $g_{\text{loc}}(a, b) = f_{\text{loc}}(\phi(a), \psi(b))$ (g is an *isotope* of f). From this one can compute the weaker upper bound of $\frac{1}{2}$ for the density of the commutator of a bipermutive CA.

6.2 Commutator of an affine totally extremally permutive CA

Next, we turn to affine totally extremally permutive cellular automata on $G^{\mathbb{Z}^d}$, where G is a finite group. By the next lemma, no generality is lost if we assume G to be abelian.

Lemma 5. *Let G be a finite group, and suppose there exists a totally extremally permutive and affine cellular automaton on $G^{\mathbb{Z}^d}$ with minimal neighborhood of size at least 2. Then, G is abelian.*

Lemma 6. *Let G, H be abelian groups, and let $g : G \to H$ be such that $g(a + b - c) = g(a) + g(b) - d$ holds for some $c \in G$ and $d \in H$, and all $a, b \in G$. Then, $g(a) = h(a) - g(2c) + 2d$ for a homomorphism $h : G \to H$. In particular, g is affine.*

In [4] it was proved, using algebraic methods, that among CA with radius 1/2, affine and bipermutive CA can only commute with affine CA. We show the small step required to generalize this result for our definition of commutator in one dimension:

Theorem 3. *Let $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ be bipermutive and affine (so that G is abelian), and let $g : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ commute with f. Then g is affine.*

Proof (Based on the results of [4]). By composing with shifts, we may assume f has neighborhood $[0, m_f]$ and g has neighborhood $[0, m_g]$. Then, since g commutes with f, it also commutes with f^k. Let k be large enough that $m_f \cdot k \geq m_g$. Then, the $m_f \cdot k$ blocking of f^k is bipermutive and affine with radius 1/2, and the corresponding blocking h of g has radius $1/2$. Thus, the result of [4] applies, and h is an affine self-map of $(G^{m_f \cdot k})^{\mathbb{Z}}$. But clearly g must then have been affine for $G^{\mathbb{Z}}$, because the blocking operation is a group isomorphism.

We can also prove this directly, using Lemma 1:

Proof (Using Lemma 1). First, we can assume that f has a unary fixed point $c(a)$ by taking powers of f, and we denote $g(c(a)) = c(b)$. Now, f also fixes $c(b)$. Without loss of generality, assume f has neighborhood $[0, m]$ and g has neighborhood $[0, n]$. Let $w \in G^{2n+1}$ and $e \in \{a, b\}$, and let $x \in G^{\mathbb{Z}}$ be the configuration with $x_{[-n,n]} = w$ and $x_i = e$ for $i \notin [-n, n]$. Denote $M = (|G|^{2n+1})!$ and apply Lemma 1, so that

$$f^M(x)_j = f^M(x)_{j-mM} = w_j \tag{2}$$

for all $j \in [-n, n]$.

Let then $w^1, w^2 \in G^{n+1}$, let by $x \in G^{\mathbb{Z}}$ be the configuration with $x_j = w^1_j$ and $x_{j+mM} = w^2_j$ for all $j \in [0, n]$, and a everywhere else. By the affinity of f and (2), we have

$$f^M(x)_j = w^1_j + w^2_j - C$$

for all $j \in [0, n]$ and some constant $C \in G$. Thus we have $g(f^M(x))_{\mathbf{0}} = g_{\text{loc}}(w^1 + w^2 - \underbrace{(C, \ldots, C)}_{n+1})$. On the other hand, we have $g(x)_j \neq b$ only when $j \in [-n, n]$ or $j - mM \in [-n, n]$, so using the affinity of f and (2), we see that $f^M(g(x))_{\mathbf{0}} = g_{\text{loc}}(w^1) + g_{\text{loc}}(w^2) - C$. Since f and g commute, these values are equal, and thus g is affine by Lemma 6 (setting $c = (C, \ldots, C)$ and $d = C$). □

Now, let us reduce the multidimensional case to the one-dimensional case.

Theorem 4. *Let $f : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ be totally extremally permutive and affine (so that G is abelian), and let $g : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ commute with f. Then g is affine.*

Proof (Using Lemma 1). We only present a proof for $d = 2$. We first modify the neighborhoods of f and g. First, we compose with a shift so that the lexicographically minimal element in the neighborhood of f is $(0, 0)$. Then, we ensure that for the maximal element (m_1, m_2) of the neighborhood, we have $m_1 > 0$ by considering $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)(f)$ instead in the case $m_1 = 0$. We also make sure f has a pointy neighborhood by applying Lemma 2. These transformations amount to mapping $f \mapsto \sigma^{\boldsymbol{v}}(A(f))$ for some $A \in SL_2(\mathbb{Z})$ and $\boldsymbol{v} \in \mathbb{Z}^2$. Note that $f' = \sigma^{\boldsymbol{v}} \circ A(f)$ and $g' = \sigma^{\boldsymbol{v}'} \circ A(g)$ commute for all $\boldsymbol{v}' \in \mathbb{Z}^2$, and f' is affine and totally extremally permutive.

Now, let the neighborhood of g' be contained in $[0, p-1]^2$ (by choosing $\boldsymbol{v}'$ appropriately), and consider the vertically periodic subshift X_p. The restrictions $f'|_{X_p}$ and $g'|_{X_p}$ simulate one-dimensional cellular automata on $(G^p)^{\mathbb{Z}}$ through the bijection ρ_p. By Lemma 3, the one-dimensional CA corresponding to $f'|_{X_p}$ is bipermutive, and it is clearly affine. Then, by Theorem 3, $g'|_{X_p}$ is affine. This implies that g' is affine as well, since g' has neighborhood $[0, p-1]^2$. Finally, also g is affine since transformations of $SL_d(\mathbb{Z})$ are group isomorphisms. □

For the special case of totally extremally permutive *homomorphic* CA on a group of prime order, there is a very nice characterization for the commutator restricted to CA with quiescent state 0. This can be seen as a corollary of the previous results, but we present a very short direct proof based on Proposition 3 and Lemma 4.

Proposition 5. *Let $G = \mathbb{Z}_p$, let $f : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ be a totally extremally permutive homomorphism. Then $g : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ with $g(c(0)) = c(0)$ commutes with f if and only if g is homomorphic.*

Proof. Let g have radius r. Then $X^f = S^{\mathbb{Z}}$, where $X = \{0,1\}^{\mathbb{Z}^d} \cap Y$ and Y is the r-sparse shift, by Proposition 3. As $G = \mathbb{Z}_p$, all homomorphic automata commute, so in particular $h \circ f = f \circ h$ for the unique homomorphic automaton defined by $h|_X = g|_X$. Thus, $g = h$ by Lemma 4. □

References

1. Mike Boyle, Douglas Lind, and Daniel Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):pp. 71–114, 1988.
2. G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.
3. Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge, 1995.
4. Cristopher Moore and Timothy Boykett. Commuting cellular automata. *Complex Systems*, 11(1):55–64, 1997.
5. Marcus Pivato. The ergodic theory of cellular automata. *Int. J. General Systems*, 41(6):583–594, 2012.
6. Marcus Pivato and Reem Yassawi. Limit measures for affine cellular automata ii. *Ergodic Theory and Dynamical Systems*, 24:1961–1980, 11 2004.
7. V. Salo. On Nilpotency and Asymptotic Nilpotency of Cellular Automata. *ArXiv e-prints*, May 2012.

Appendix

Proof of Lemma 1:

Proof. We begin with an auxiliary observation. Let $A = (Q, \Sigma, \delta)$ be a reversible DFA, and let $q \in Q$ and $w \in \Sigma^*$ be arbitrary. Then $\delta(q, w^{\ell \cdot |Q|!}) = q$ for all $\ell \in \mathbb{N}$, which follows from the fact that the function $\delta(\cdot, w)$ is a bijection from Q to itself.

Then, let $Q = S^n$ and $\Sigma = S^{r+r'}$, and let $\delta : (Q \times \Sigma) \to Q$ be defined by $\delta(q, w) = f(qw)$. We claim that $A = (Q, \Sigma, \delta)$ is a reversible DFA. That it is a DFA is trivial, so let $q, q' \in Q$ and $w \in \Sigma$ with $q_i \neq q'_i$, where $i \in [0, n-1]$ is maximal. Since f is left permutive, we have $\delta(q, w)_i \neq \delta(q', w)_i$, and thus A is reversible.

Consider the words $q_i = f^i(x)_{I+ri} \in Q$ and $w_i = f^i(x)_{[1,r+r']+ri} \in \Sigma$ for $i \in \mathbb{N}$. Since r is the right 'speed of light' for f, we actually have $w_i = f^i(y)_{[1,r+r']+ri}$ for all $i \in \mathbb{N}$, and thus the sequence $(w_i)_{i \in \mathbb{N}}$ is periodic with period pt. Furthermore, we see that $\delta(q_i, w_i) = q_{i+1}$ holds for all i. Denoting $w = w_0, \ldots, w_{pt-1} \in \Sigma^{pt}$, we have $\delta(q_0, w^{\ell \cdot |Q|!}) = q_0$ for all $\ell \in \mathbb{N}$ by the above discussion on reversible DFAs, and expanding the definitions gives the claim. □

Proof of Theorem 2:

Proof. We show that given any $w \in \mathcal{B}_p(X)$ and $v \in S^p$, there exist $x \in X$ and $N \in \mathbb{N}$ such that $x_{[0,p-1]} = w$ and $f^N(x)_{[0,p-1]} = v$. We may assume without loss of generality that ${}^\infty w.w^\infty \in X$, and then there exist $m, t \in \mathbb{N}$ such that $f^m({}^\infty w.w^\infty) = f^{t+m}({}^\infty w.w^\infty) = {}^\infty u.u^\infty$ for some $u \in \mathcal{B}(X)$. Since $\omega_f(X) = S^{\mathbb{Z}}$, there exists $M \geq m$ and $v_1, v_2 \in \mathcal{B}(X)$ such that $f^M(v_1 v_2) = v$ and $|v_1| = rM$. Define $y = z v_1.v_2 w' w^\infty$, where $z \in S^{-\mathbb{N}}$ and $w' \in \mathcal{B}(X)$ are chosen such that $y \in X$ and p divides $|v_2 w'|$. Now, $f^M(y) = z'.v w'' u'^\infty$ for some $z' \in S^{-\mathbb{N}}$, $w'' \in (S^p)^*$ and $u' \in S^p$. Lemma 1 now implies that for $C = pt(|S|^p)!$ and all $\ell \in \mathbb{N}$, we have $f^{M+\ell C}(y)_{\ell r C + [0,p-1]} = v$. Since $y_{\ell r C + [0,p-1]} = w$ for large enough ℓ, some translate of y can be chosen as x. □

Proof of Lemma 2:

Proof. For all $n \in \mathbb{N}$, define the *shear map* $A_n \in SL_d(\mathbb{Z})$ by

$$A_n(x_1, x_2, \ldots, x_d) = (x_1 + n \sum_{i=2}^{d} x_i, x_2, \ldots, x_d).$$

Let $N \subset \mathbb{Z}^d$ be the neighborhood of f. Then for $n = \max \pi(N) - \min \pi(N)$, the image $A_n(N)$ is pointy, so $A_n(f)$ has a pointy neighborhood. □

Proof of Lemma 5:

Proof. If there exists such an affine cellular automaton, then there must in particular exist a *homomorphism* f with minimal neighborhood of size at least 2. So, let $f : G^{\mathbb{Z}^d} \to G^{\mathbb{Z}^d}$ be such a homomorphism, and order the arguments of its local rule $f_{\mathrm{loc}} : G^n \to G$ so that it is permutive in its first two arguments. Let $g, h \in G$, and let $g', h' \in G$ such that $f_{\mathrm{loc}}(g', 1, 1, \ldots, 1) = g$ and $f_{\mathrm{loc}}(1, h', 1, \ldots, 1) = h$. Since f_{loc} is a homomorphism, we have

$$\begin{aligned} g \cdot h &= f_{\mathrm{loc}}(g', 1, 1, \ldots, 1) \cdot f_{\mathrm{loc}}(1, h', 1, \ldots, 1) = f_{\mathrm{loc}}(g', h', 1, \ldots, 1) \\ &= f_{\mathrm{loc}}(1, h', 1, \ldots, 1) \cdot f_{\mathrm{loc}}(g', 1, 1, \ldots, 1) = h \cdot g. \end{aligned}$$

□

Proof of Lemma 6:

Proof. We have

$$\begin{aligned} g(a+b) &= g(a + (b+c) - c) \\ &= g(a) + g(b+c) - d \\ &= g(a) + g(b + 2c - c) - d \\ &= g(a) + g(b) + g(2c) - 2d. \end{aligned}$$

Denote $e = g(2c) - 2d$, and let $h(a) = g(a) + e$. Then

$$\begin{aligned} h(a+b) &= g(a+b) + e \\ &= g(a) + g(b) + 2e \\ &= h(a) + h(b), \end{aligned}$$

so h is a homomorphism and g is affine. □