

A COUNTEREXAMPLE TO THE PERIODIC TILING CONJECTURE

RACHEL GREENFELD AND TERENCE TAO

ABSTRACT. The periodic tiling conjecture asserts that any finite subset of a lattice \mathbb{Z}^d which tiles that lattice by translations, in fact tiles periodically. In this work we disprove this conjecture for sufficiently large d , which also implies a disproof of the corresponding conjecture for Euclidean spaces \mathbb{R}^d . In fact, we also obtain a counterexample in a group of the form $\mathbb{Z}^2 \times G_0$ for some finite abelian 2-group G_0 . Our methods rely on encoding a “Sudoku puzzle” whose rows and other non-horizontal lines are constrained to lie in a certain class of “2-adically structured functions”, in terms of certain functional equations that can be encoded in turn as a single tiling equation, and then demonstrating that solutions to this Sudoku puzzle exist, but are all non-periodic.

1. INTRODUCTION

In 1960, Hao Wang [W60, W75] studied the problem of tiling the plane by translated copies of finitely many squares a color attached to each side of each of them, aka *Wang squares*, where one square lies next to another only if the common edges colors match. This is a variant of Hilbert’s famous *Entscheidungsproblem*. Wang conjectured that if a set of such squares admits a tiling of the plane, then it also admits a periodic tiling. Wang’s conjecture was disproved by Berger [B66, B64], who constructed an *aperiodic* set of 20,426 Wang squares, i.e., the set of squares admits tilings but none of these tilings is periodic. Over the years, many more constructions of aperiodic translational tilings were established, with smaller tile-sets (see, e.g., [GT21, Table 1]). In this paper we establish a construction of an aperiodic translational tiling with a *single tile* in $\mathbb{Z}^2 \times G_0$, for a certain finite abelian group G_0 . As a consequence, we disprove the celebrated “periodic tiling conjecture”.

1.1. The periodic tiling conjecture. Let $G = (G, +)$ be a discrete abelian group. If A, F are subsets of G , we write $A \oplus F = G$ if the translates $a + F := \{a + f : f \in F\}$ of F by elements a of A form a partition of G . If this occurs, we say that F *tiling* G (by translations), and that A is a *tiling set* of G by F . The tiling set A is said to be *periodic* if it is the finite union of cosets of a finite index subgroup of G . We will refer to $A \oplus F = G$ as a *tiling equation*, and think of F, G as being given and $A \subset G$ as being an unknown. We say that the tiling equation $A \oplus F = G$ is *aperiodic* if there exist solutions $A \subset G$ to the tiling equation $A \oplus F = G$, but none of these solutions are periodic. A well known conjecture in the area is the periodic tiling conjecture:

Conjecture 1.1 (Discrete periodic tiling conjecture). [GS87, LW96] *Let F be a finite non-empty subset of a finitely generated discrete abelian group G . Then the tiling equation $A \oplus F = G$ is not aperiodic.*

In other words, the conjecture asserts that if F tiles G by translations, then F periodically tiles G by translations.

We also phrase the following continuous analogue of this conjecture. If Σ is a bounded measurable subset of a Euclidean space \mathbb{R}^d of positive measure, and Λ is a subset of \mathbb{R}^d , we write $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ if the translates $\lambda + \Sigma$, $\lambda \in \Lambda$, partition \mathbb{R}^d up to null sets; note from the Steinhaus lemma that this forces Λ to be discrete. If this occurs, we say that Σ (measurably) *tiles* \mathbb{R}^d *by translations*, and that Λ is a *tiling set of \mathbb{R}^d by Λ* . The tiling set Λ is said to be *periodic* if it is the finite union of cosets of a lattice (a discrete cocompact subgroup) of \mathbb{R}^d . As before, we view $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ as a tiling equation with d and Σ given, and Λ as the unknown. We say that this tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ is *aperiodic* if there exist solutions $\Lambda \subset \mathbb{R}^d$ to the tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$, but none of these solutions are periodic.

Conjecture 1.2 (Continuous periodic tiling conjecture). [GS87, LW96] *Let Σ be a bounded measurable subset of \mathbb{R}^d of positive measure. Then the tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ is not aperiodic.*

A standard argument shows that Conjecture 1.2 implies Conjecture 1.1. This implication arises from “encoding” a discrete subset F of \mathbb{Z}^d as a bounded measurable subset $F \oplus R_d$ in \mathbb{R}^d , where R_d is a “generic” fundamental domain of $\mathbb{R}^d/\mathbb{Z}^d$; we provide the details in Section 2. Conjectures 1.1 and 1.2 have been extensively studied over the years. The following partial results towards these conjectures are known:

- Conjecture 1.1 is trivial when G is a finite abelian group, since in this case all subsets of G are periodic.
- Conjectures 1.1 and 1.2 were established in $G = \mathbb{Z}$ and $G = \mathbb{R}$ [N77, LM91, LW96]. The argument in [N77] also extends to the case $G = \mathbb{Z} \times G_0$ for any finite abelian group G_0 [GT21, Section 2].
- When $G = \mathbb{Z}^2$, Conjecture 1.1 was established by Bhattacharya [B20] using ergodic theory methods. In [GT20] we gave an alternative proof of this result, and furthermore showed that every tiling in \mathbb{Z}^2 by a single tile is *weakly periodic* (a disjoint union of finitely many one-periodic sets).
- When $G = \mathbb{R}^2$, Conjecture 1.2 is known to hold for any tile which is a topological disc [BN91, G-BN91, Ken92].
- Conjecture 1.2 is known to be true for convex tiles in all dimensions [V54, M80].
- For $d > 2$, Conjecture 1.1 is known to hold when the cardinality $|F|$ of F is prime or equal to 4 [S98], but remained open in general.
- In [MSS22], it was recently shown that the discrete periodic tiling conjecture in \mathbb{Z}^d also implies the discrete periodic tiling conjecture in every quotient group \mathbb{Z}^d/Λ .
- The analogues of the above conjectures are known to fail when one has two or more translational tiles instead of just one; see [GT21] (particularly Table 1) for a summary of results in this direction. In particular, in [GT21, Theorems 1.8, 1.9] it was shown that the analogue of Conjecture 1.1 for two tiles fails¹ for $\mathbb{Z}^2 \times G_0$ for some finite group G_0 , and also for \mathbb{Z}^d for some d .

1.2. Results. In this work we construct counterexamples to Conjectures 1.1 and 1.2. Our first main result is

¹Strictly speaking, the counterexample in that paper involved tiling a periodic subset E of the group G , rather than the full group G .

Theorem 1.3 (Counterexample to Conjecture 1.1, I). *There exist a finite abelian group G_0 and a finite non-empty subset F of $\mathbb{Z}^2 \times G_0$ such that the tiling equation $A \oplus F = \mathbb{Z}^2 \times G_0$ is aperiodic. In other words, the discrete periodic tiling conjecture fails for $\mathbb{Z}^2 \times G_0$.*

Remark 1.4. Our construction will in fact make G_0 a (non-elementary) 2-group, that is to say a finite group whose order is a power of two.

The group $\mathbb{Z}^2 \times G_0$ can be viewed as a quotient \mathbb{Z}^d / Λ of a lattice \mathbb{Z}^d for sufficiently large d , so by Theorem 1.3 and the recent implication in [MSS22, Corollary 1.2]² we derive

Corollary 1.5 (Counterexample to Conjecture 1.1, II). *For sufficiently large d , there exists a finite non-empty subset F of \mathbb{Z}^d such that the tiling equation $A \oplus F = \mathbb{Z}^d$ is aperiodic. In other words, the discrete periodic tiling conjecture fails for \mathbb{Z}^d .*

The value of d produced by our arguments is in principle computable, but we have made no attempt to optimize it, and a direct examination of our proofs would produce an extremely large value for this dimension.

By a standard construction (going back to Golomb [G70]) relating discrete and continuous tiling problems, we then have a corresponding counterexample to the continuous periodic tiling conjecture:

Corollary 1.6 (Counterexample to Conjecture 1.2). *For sufficiently large d , there exists a bounded measurable subset Σ of \mathbb{R}^d of positive measure such that the tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ is aperiodic. In other words, the continuous periodic tiling conjecture fails for \mathbb{R}^d .*

We give the (straightforward) derivation of Corollary 1.6 from Corollary 1.5 in Section 2.

Our methods produce a finite group G_0 , and hence a dimension d , that is in principle explicitly computable, but we have not attempted to optimize the size of these objects. In particular the dimension d produced by our construction will be extremely large.

1.3. Previous works and constructions. Aperiodic tilings have been extensively studied and have found famous applications to many areas of mathematics and physics [AG94]. The study of the periodicity of tilings has attracted many researchers, who have introduced methods from various fields, such as geometry and topology [G-BN91, Ken92], Fourier analysis [LW96, KL96, K04], combinatorics [GT20, GT21], ergodic theory and probability [M89, L13, B20], commutative algebra [S98, B20, GT20], model theory [BJ08, GT21], and computability theory [B66, K96, L13, JR21, GT21].

We do not attempt a comprehensive survey of aperiodic constructions here, but briefly summarize the current state of knowledge as follows.

- Aperiodic tiling by multiple tiles have long known to exist. The online encyclopedia of tilings [FGH] contains many explicit examples of such tilings. In the plane, there are the famous substitution tilings constructions of Penrose and Ammann [P74, P79, DB81, G77, AGS92] (see also [GS98] and the references therein for the study of substitution tilings). Other aperiodic tiling construction methods include the finite state machine approaches of

²This is a generalization of the argument in [GT21, Section 9].

- Kari and Culik [K96, C96], and the approach of encoding arbitrary Turing machines³ into a tiling problem [B66, B64, R71, O09, GT21].
- In addition, if one allows for the tile to be rotated (and/or reflected) in addition to being translated, aperiodic non-translational tilings by a single tile were previously constructed; see, e.g., [S96, CK86, ST12]. This solves the so-called “einstein problem” which is an extension of the second part of Hilbert’s eighteenth problem.
 - Moreover, when one allows for the group to be *non-abelian*, aperiodic (and undecidable) tilings by a single tile are known to exist. For instance, in [GT21, Theorem 11.2] we give a construction in $\mathbb{Z}^2 \times H$ for a certain finite non-abelian group H . See also [GS05, SSU21] for further references to of aperiodic tilings (or subshifts of finite type) in various groups.

We were not able to adapt the previous aperiodic constructions to the setting of a *single* translational tile. Instead, our source of aperiodicity is more novel, in that our tiling of $\mathbb{Z}^2 \times G_0$ is forced to exhibit a “2-adic” structure for some large enough but fixed power of two $q = 2^s$ (say $s = 10$) in the sense that for each power q^j of q , the tiling is periodic with period $q^j \mathbb{Z}^2 \times \{0\}$ outside of a small number of cosets of that subgroup $q^j \mathbb{Z}^2 \times \{0\}$, but is unable to be genuinely periodic with respect to any of these periods. To achieve this we will set up a certain “Sudoku puzzle”, which will be rigid enough to force all solutions of this problem to exhibit a certain “self-similar” (and therefore non-periodic) behavior, yet is not so rigid that there are no solutions whatsoever. By modifying arguments from our previous paper [GT21], we are then able to encode this Sudoku-type puzzle as an instance of the original tiling problem $A \oplus F = \mathbb{Z}^2 \times G_0$.

Our encoding approach is similar in nature to previous “encoding” arguments in the tiling literature. Berger [B66, B64] encoded any Turing machine as a Wang tiling problem. Since the halting problem is known to be undecidable, Berger’s encoding implies the undecidability of the Wang domino problem. Subsequently, Wang tilings were encoded to obtain aperiodicity, strong aperiodicity, or even undecidability of various other problems; see, e.g., [ST12, S96, G70, SSU21, M89, R71, GS98, GS05]. In particular, in [GT21] we used our tiling language approach to encode any Wang tiling problem as a tiling of $\mathbb{Z}^2 \times G_0$ by two tiles, for a suitable finite abelian group G_0 (depending on the given problem). This implies the existence of an undecidable tiling problem with only two tiles. Unfortunately, in our encoding of the Wang domino puzzle, we were not able to reduce the number of the tiles from two to one. Thus, the main difficulty we address in our current work is finding another aperiodic puzzle (replacing the Wang domino puzzle) which is also *expressible* in our tiling language a tiling by a single tile.

1.4. Our argument and the organization of the paper. Our argument is a variant of the construction used in our previous paper [GT21] to produce aperiodic (and even undecidable) translational tilings with two tiles, and is summarized by the diagram in Figure 1.1. However, the fact that we are now tiling the whole group G instead of a periodic subset of G , and that we are only allowed to use one tile instead of two, creates additional technical challenges.

As in [GT21], in Section 3 we begin by replacing the single tiling equation $A \oplus F = G$ with a system $A \oplus F^{(m)} = G$, $m = 1, \dots, M$ of tiling equations for

³This method in fact allows one to construct tiling problems which are not only aperiodic, but in fact *logically undecidable*; see e.g., [GT21] for further discussion.

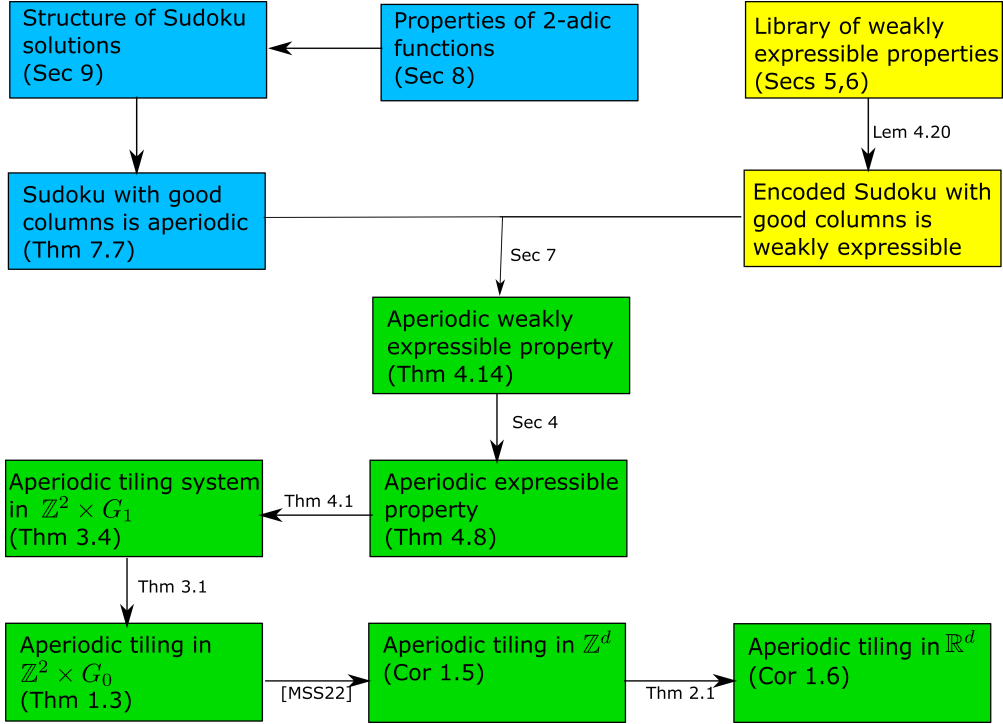


FIGURE 1.1. A high-level overview of the logical implications used in our proof. We introduce an aperiodic Sudoku puzzle (blue) and develop a tiling library to express this puzzle inside a tiling by a single tile (yellow). This, in turn, eventually leads to constructions of aperiodic translational tilings by a single tile in $\mathbb{Z}^2 \times G_0$, \mathbb{Z}^d and \mathbb{R}^d (green).

an arbitrary M , by an elementary “stacking” procedure that takes advantage of our freedom to enlarge the group G . This creates a flexible “tiling language” of constraints on the tiling set A ; the challenge is to use this language to obtain a system of constraints that is strict enough to force aperiodic behavior on this set A , while simultaneously being relaxed enough to admit at least one solution.

Next, in Section 4, we again follow [GT21] and pass from this tiling language to a more familiar language of functional equations, basically by spending one of the equations $A \oplus F^{(m)} = G$ in the system to force the tiling set A to be a graph of a function $f = (f_1, \dots, f_K)$, where $f_i: \mathbb{Z}^2 \times G_0 \rightarrow \mathbb{Z}/q\mathbb{Z}$, $1 \leq i \leq K$, and G_0 is an additional small finite abelian group which we retain for technical reasons.

One can then use one or more tiling equations $A \oplus F^{(m)} = G$ in the tiling language to create a “library” of useful functional constraints on these functions f_i , this is done in Section 5. For instance, one can ensure that a given function f_i exhibits periodicity in some direction $v_i \in \mathbb{Z}^2$, or that it encodes (the periodic extension of) a permutation of a cyclic group $\mathbb{Z}/q\mathbb{Z}$.

In Section 6 we express via functional equations the assertion that a certain subcollection of the f_i (after a routine normalization) take values in a two-element set $\{a, b\} \pmod{q}$, where a, b have different parity, thus can be viewed as boolean functions. By modifying our construction from [GT21, Section 7], we can then use tiling equations to encode arbitrary pointwise constraints

$$(f_1(x), \dots, f_K(x)) \in \Omega \tag{1.1}$$

for all $x \in \mathbb{Z}^2 \times G_0$ and arbitrary subsets Ω of $\{a, b\}^K$. This turns out to be a particularly powerful addition to our library of expressible properties.

In Section 7, by some further elementary transformations (including a change of variables that resembles the classical projective duality between lines and points), we are then able to reduce matters to demonstrating aperiodicity of a certain “Sudoku puzzle”. In this puzzle, we have an unknown function $F: \{1, \dots, N\} \times \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$ on a vertically infinite “Sudoku board” $\{1, \dots, N\} \times \mathbb{Z}$ which fills each cell (n, m) of this board with an element $F(n, m)$ of $\mathbb{Z}/q\mathbb{Z} \setminus \{0\}$ for some fixed but large $q = 2^s$. Along every row or diagonal (and more generally along any non-vertical line) of this board, the function F is required⁴ to exhibit “2-adic behavior”; the precise description of this behavior will be given in Section 7, but roughly speaking we will require that on each such non-vertical line, F behaves like a rescaled version of the function

$$f_q(n) := \frac{n}{q^{\nu_q(n)}} \pmod{q} \quad (1.2)$$

(where $\nu_q(n)$ is the number of times q divides n), that assigns to each integer n the final non-zero digit in its base q expansion (with the convention $f_q(0) := 1$). We also impose a non-degeneracy condition that the Sudoku solution function F is a periodized permutation along any of its columns.

In Section 9, for suitable choices of parameters q, N , we “solve” this Sudoku problem and show that solutions to this problem exist, but necessarily exhibit self-similar behavior (in that certain rescalings of the solution obey similar properties to the original solution), and in particular are non-periodic. By combining this aperiodicity result with the previous encodings and reductions, we are able to establish Theorem 1.3 and hence Corollary 1.6.

Remark 1.7. Our current argument also provides a solution to [GT21, Problem 12.3]. Namely, using the more advanced library we develop here (Sections 2–5), we can strengthen our previous undecidability result with two tiles by now tiling all of the group rather than just a periodic subset. We leave the details of this modification of the construction to the interested reader.

1.5. Notation. We define the disjoint union $\bigsqcup_{w \in \mathcal{W}} E_w$ of sets E_w indexed by some set \mathcal{W} to be the union $\bigcup_{w \in \mathcal{W}} E_w$ if the E_w are disjoint, and leave $\bigsqcup_{w \in \mathcal{W}} E_w$ undefined otherwise.

All groups in this paper will be written additively and be assumed to be abelian unless otherwise specified. If A, B, C are subsets of G , we use $A \oplus B = C$ to denote the assertion that the translates $a + B$, $a \in A$ partition C ; if the translates $a + B$ are not disjoint, we leave $A \oplus B$ undefined; thus $A \oplus B = C$ is equivalent to $\bigsqcup_{a \in A} (a + B) = C$. Similarly, if $\Lambda \subset \mathbb{R}^d$ and $\Sigma \subset \mathbb{R}^d$ are discrete and measurable respectively, and $E \subset \mathbb{R}^d$ is another measurable set, we write $\Lambda \oplus \Sigma =_{\text{a.e.}} E$ if the translates $\lambda + \Sigma$, $\lambda \in \Lambda$ partition E up to null sets; if the $\lambda + \Sigma$ are not disjoint up to null sets, we leave $\Lambda \oplus \Sigma$ undefined.

We use 1_E to denote the indicator of an event E , thus 1_E is 1 when E is true and 0 otherwise.

By abuse of notation, we will sometimes identify an integer $a \in \mathbb{Z}$ with its representative $a \pmod{N} \in \mathbb{Z}/N\mathbb{Z}$ in a cyclic group $\mathbb{Z}/N\mathbb{Z}$ when there is no

⁴This is analogous to how, in the most popular form of a Sudoku puzzle, the rows, columns, and 3×3 blocks of cells on a board $\{1, \dots, 9\} \times \{1, \dots, 9\}$ are required to be permutations of the digit set $\{1, \dots, 9\}$.

chance of confusion. For instance, we may refer to the multiplicative identity of $\mathbb{Z}/N\mathbb{Z}$ (viewed as a ring) as 1 rather than $1 \pmod{N}$.

If v_1, \dots, v_k are elements of a group G , we use $\langle v_1, \dots, v_k \rangle$ to denote the group that they generate. If H is a subgroup of G , then a function $f: G \rightarrow X$ on G is said to be H -periodic if $f(x+h) = f(x)$ for all $x \in G$ and $h \in H$. In particular, a function is $\langle v_1, \dots, v_k \rangle$ -periodic if and only if $f(x+v_i) = f(x)$ for all $x \in G$ and $i = 1, \dots, k$.

We use $X = O(Y)$, $X \ll Y$, or $Y \gg X$ to denote the estimate $|X| \leq CY$ for some absolute constant C (which will not depend on other parameters such as q or N). We write $X \asymp Y$ for $X \ll Y \ll X$.

We use $|E|$ to denote the cardinality of a finite set E . If $E \subset \Omega \subset \mathbb{R}^d$ with Ω non-empty, we define the *upper density of E in Ω* to be the quantity

$$\limsup_{M \rightarrow \infty} \frac{|E \cap \{-M, \dots, M\}^d|}{|\Omega \cap \{-M, \dots, M\}^d|}.$$

Thus for instance if q, N are natural numbers, the set $\{1, \dots, N\} \times q\mathbb{Z}$ has upper density $\frac{1}{q}$ in $\{1, \dots, N\} \times \mathbb{Z}$.

1.6. Acknowledgments. RG was partially supported by the AMIAS Membership and NSF grants DMS-2242871 and DMS-1926686. TT was partially supported by NSF grant DMS-1764034 and by a Simons Investigator Award. We thank Asaf Katz and Sébastien Labbé for drawing our attention to some relevant references and to Nishant Chandgotia, Rick Kenyon, Jeff Lagarias and Ralf Spatzier for helpful conversations.

2. BUILDING A CONTINUOUS APERIODIC TILING EQUATION FROM A DISCRETE APERIODIC TILING EQUATION

In this section we show that a counterexample to the discrete periodic tiling conjecture can be converted to a counterexample to the continuous periodic tiling conjecture. More precisely, we show

Theorem 2.1 (Lifting a discrete aperiodic tiling equation to a continuous aperiodic tiling equation). *Let $d \geq 1$. If there is an aperiodic tiling equation $A \oplus F = \mathbb{Z}^d$ for some finite non-empty subset F of \mathbb{Z}^d , then there is an aperiodic tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ for some bounded measurable subset Σ of \mathbb{R}^d of positive measure. In other words, if Conjecture 1.1 fails in \mathbb{Z}^d then Conjecture 1.2 fails in \mathbb{R}^d .*

A basic connection between the discrete lattice \mathbb{Z}^d and the continuous space \mathbb{R}^d is given by the tiling relation

$$\mathbb{Z}^d \oplus Q_d =_{\text{a.e.}} \mathbb{R}^d$$

where $Q_d := [0, 1]^d$ is the unit cube. By translation invariance one also has

$$(\mathbb{Z}^d + t) \oplus Q_d =_{\text{a.e.}} \mathbb{R}^d$$

for any $t \in \mathbb{R}^d$. However, due to the ability to “slide” cubes Q_d in various directions, there are many more tilings of \mathbb{R}^d by Q_d than these; this is evidenced for instance by the failure of Keller’s conjecture in high dimensions [LS92]. Because of this, the unit cube Q_d is not a suitable tool for establishing Theorem 2.1. Instead, we need a “rigid” version R_d of Q_d , or more precisely:

Lemma 2.2 (Existence of a rigid tile). *For any $d \geq 1$, there exists a bounded measurable subset R_d of \mathbb{R}^d such that $\mathbb{Z}^d \oplus R_d =_{\text{a.e.}} \mathbb{R}^d$, and conversely the only sets $\Lambda \subset \mathbb{R}^d$ with $\Lambda \oplus R_d =_{\text{a.e.}} \mathbb{R}^d$ are translates $\Lambda = \mathbb{Z}^d + t$ of \mathbb{Z}^d for some $t \in \mathbb{R}^d$.*

The idea of using rigid tiles to pass back and forth between discrete and continuous tiling questions goes back to the work of Golomb [G70]; see also [GT21, Lemma 9.3] for a discretized version of this lemma.

Proof. The idea is to remove and add “bumps” at the facets of Q_d to make a rigid “jigsaw puzzle piece”; see Figure 2.1. There are many constructions available. For instance, we can define R_d to be the set

$$R_d := \left(Q_d \setminus \bigcup_{k=1}^d C_k \right) \uplus \bigcup_{k=1}^d (C_k + e_k)$$

where for e_1, \dots, e_d is the standard basis for \mathbb{R}^d , and for each $k = 1, \dots, d$, $C_k \subset Q_d$ is a ϵ -subcube of Q_d , which one can for instance define as

$$C_k := \left(\prod_{j=1}^{k-1} [x_j, x_j + \epsilon] \right) \times [0, \epsilon] \times \prod_{j=k+1}^d [x_j, x_j + \epsilon]$$

where $0 < \epsilon < 1/5$ and $2\epsilon < x_j < 1 - 3\epsilon$, $j = 1, \dots, d$ are arbitrary. Because the piece C_k removed for a given k is a translate by an element of \mathbb{Z}^d of the piece $C_k + e_k$ added for a given k , we still have

$$\mathbb{Z}^d \oplus R_d =_{\text{a.e.}} \mathbb{Z}^d \oplus Q_d =_{\text{a.e.}} \mathbb{R}^d.$$

On the other hand, it is geometrically evident that if $\Lambda \oplus R_d =_{\text{a.e.}} \mathbb{R}^d$ and $t \in \Lambda$, then $t \pm e_k$ must also lie in Λ for all $k = 1, \dots, d$, as there is no other way to fit translates of R_d around the added and removed “bumps” $C_k + t$, $C_k + e_k + t$ of $R_d + t$. Thus Λ must contain a translated lattice $\mathbb{Z}^d + t$; since this lattice already is a tiling set of \mathbb{R}^d by R_d , we therefore have $\Lambda = \mathbb{Z}^d + t$, as required. \square

Using this rigid tile, it is now straightforward to establish Theorem 2.1.

Proof of Theorem 2.1. Suppose that there is a finite non-empty $F \subset \mathbb{Z}^d$ such that the tiling equation $A \oplus F = \mathbb{Z}^d$ is aperiodic.

With R_d being the rigid tile provided by Lemma 2.2, we introduce the bounded measurable subset Σ of \mathbb{R}^d by the formula

$$\Sigma := F \oplus R_d \subset \mathbb{Z}^d \oplus Q_d =_{\text{a.e.}} \mathbb{R}^d.$$

Clearly Σ has positive measure. It will suffice to show that the tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ is aperiodic. On the one hand we have

$$A \oplus \Sigma =_{\text{a.e.}} (A \oplus F) \oplus R_d =_{\text{a.e.}} \mathbb{Z}^d \oplus R_d =_{\text{a.e.}} \mathbb{R}^d$$

so there is at least one tiling of \mathbb{R}^d by Σ .

Conversely, suppose that we have a tiling $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ of \mathbb{R}^d . Then we have

$$(\Lambda \oplus F) \oplus R_d =_{\text{a.e.}} \Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$$

and hence by Lemma 2.2, we have $\Lambda \oplus F = \mathbb{Z}^d + t$ for some $t \in \mathbb{R}^d$. Then $\Lambda - t$ is a tiling set of \mathbb{Z}^d by F and is hence not periodic by hypothesis. This implies that Λ is not periodic, and so the tiling equation $\Lambda \oplus \Sigma =_{\text{a.e.}} \mathbb{R}^d$ is aperiodic as claimed. \square

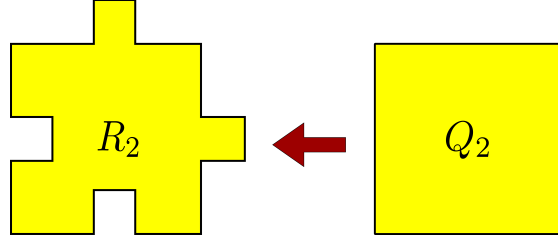


FIGURE 2.1. A “rigid” tile R_2 replacing the non rigid tile $Q_2 = [0, 1]^2$. The only tilings $\Lambda \oplus R_2 =_{\text{a.e.}} \mathbb{R}^2$ of the plane \mathbb{R}^2 by R_2 are the translated lattice tilings $(\mathbb{Z}^2 + t) \oplus R_2 =_{\text{a.e.}} \mathbb{R}^2$ for $t \in \mathbb{R}^2$.

In view of Theorem 2.1, we see that Corollary 1.5 implies Corollary 1.6. In [MSS22] it was shown that any tiling of a quotient group \mathbb{Z}^d/Λ can be identified with a tiling of \mathbb{Z}^d . This is done by a rigid pull back argument, generalizing [GT21, Section 9]. As a corollary, this gives that the discrete periodic tiling conjecture in \mathbb{Z}^d also implies the discrete periodic tiling conjecture in every quotient group \mathbb{Z}^d/Λ [MSS22, Corollary 1.2]. Thus, we have that Theorem 1.3 implies Corollary 1.6. It therefore remains to establish Theorem 1.3. This is the objective of the remaining sections of the paper.

3. BUILDING AN APERIODIC TILING EQUATION FROM AN APERIODIC SYSTEM OF TILING EQUATIONS

Theorem 1.3 asserts the construction of a single tiling equation $A \oplus F = G$ which is aperiodic. As in our previous paper [GT21], it will be more convenient to consider the significantly more flexible problem of constructing a *system*

$$A \oplus F_m = G \text{ for all } m = 1, \dots, M \quad (3.1)$$

of tiling equations which are (jointly) *aperiodic* in the sense that solutions $A \subset G$ to the system (3.1) exist, but none of them are periodic. The ability to pass to pass to this more flexible setup is provided by the following tool (compare with Theorem 2.1):

Theorem 3.1 (Concatenating an aperiodic system of tiling equations into a single aperiodic tiling equation). *Let G be a finitely generated abelian group. Suppose that there exist finite non-empty sets $F_1, \dots, F_M \subset G$ for some $M \geq 1$ such that the system (3.1) of tiling equations is aperiodic. Then there exist a 2-group of the form $\mathbb{Z}/N\mathbb{Z}$, $N = 2^r$, and a finite non-empty subset \tilde{F} of $G \times \mathbb{Z}/N\mathbb{Z}$ such that the single tiling equation*

$$\tilde{A} \oplus \tilde{F} = G \times \mathbb{Z}/N\mathbb{Z}$$

is aperiodic.

This theorem is a variant of our previous result [GT21, Theorem 1.15], in which the 2-group $\mathbb{Z}/N\mathbb{Z}$ was replaced by a proper *subset* of the cyclic group $\mathbb{Z}/(M+1)\mathbb{Z}$. In order to be able to tile the *whole* group, we will utilize a “rigid” partition of $\mathbb{Z}/N\mathbb{Z}$. More precisely, we have the following analogue of Lemma 2.2:

Lemma 3.2 (Construction of a “rigid” partition). *For every $M \geq 1$, there exist $N \geq 1$ and a partition $\mathbb{Z}/N\mathbb{Z} = E_1 \uplus \dots \uplus E_M$ of $\mathbb{Z}/N\mathbb{Z}$ into M non-empty sets E_1, \dots, E_M , such that*

$$E_i \cap (E_j + h) \neq \emptyset \quad (3.2)$$

for any $1 \leq i, j \leq M$ and $h \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$. In particular, for any $1 \leq i, j \leq M$ and $h_i, h_j \in \mathbb{Z}/N\mathbb{Z}$, we have

$$(E_i + h_i) \cap (E_j + h_j) \neq \emptyset \quad (3.3)$$

unless $h_i = h_j$ and $i \neq j$.

Proof. To construct such E_1, \dots, E_M we use the probabilistic method. Let N be a sufficiently large power of two (depending on M) to be chosen later. Let $a: \mathbb{Z}/N\mathbb{Z} \rightarrow \{1, \dots, M\}$ be a function chosen uniformly at random, thus the $a(x) \in \{1, \dots, M\}$ for $x \in \mathbb{Z}/N\mathbb{Z}$ are independent uniform random variables. We then set $E_i := \{x \in \mathbb{Z}/N\mathbb{Z} : a(x) = i\}$ to be the level sets of a . Clearly the E_1, \dots, E_M partition $\mathbb{Z}/N\mathbb{Z}$. The probability that a given E_i is empty is $(1 - 1/M)^N$. Now let $1 \leq i, j \leq M$ and $h \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$. Then the only way that (3.2) fails for this choice of parameters is if $(a(x), a(x - h)) \neq (i, j)$ for all $x \in \mathbb{Z}/N\mathbb{Z}$. As $h \neq 0$, it has even order, so one can partition $\mathbb{Z}/N\mathbb{Z}$ into $N/2$ sets of the form $\{x, x - h\}$, so the probability that (3.2) fails for this choice of parameters is at most $(1 - 1/M^2)^{N/2}$. As the total number of choices of (i, j, h) is at most $M^2 N$, the probability that this construction fails to work is thus at most

$$M(1 - 1/M)^N + M^2 N(1 - 1/M^2)^{N/2}.$$

For N sufficiently large depending on M , this failure probability is less than 1, and the claim follows. \square

Remark 3.3. An inspection of the bounds shows that one can take the 2-group $\mathbb{Z}/N\mathbb{Z}$ to be of order $N = O(M^2 \log M)$. A similar construction works with $\mathbb{Z}/N\mathbb{Z}$ replaced by other finite abelian groups of comparable order. We were able to also find deterministic constructions of the sets E_1, \dots, E_M in various such groups, but for such constructions the verification of the key property (3.3) required a longer argument than the probabilistic arguments provided here.

We are now ready to prove Theorem 3.1.

Proof of Theorem 3.1. Let G, F_1, \dots, F_M be as in that theorem. We use the partition $\mathbb{Z}/N\mathbb{Z} = E_1 \uplus \dots \uplus E_M$ provided by the above lemma to form the combined tile

$$\tilde{F} := \bigsqcup_{m=1}^M (F_m \times E_m) \subset G \times \mathbb{Z}/N\mathbb{Z}. \quad (3.4)$$

To complete the proof of Theorem 3.1, it suffices to show that the single tiling equation

$$\tilde{A} \oplus \tilde{F} = G \times \mathbb{Z}/N\mathbb{Z}. \quad (3.5)$$

is aperiodic.

To verify this claim, we first observe from hypothesis that there exists $A \subset G$ such that $A \oplus F_m = G$ for all $m = 1, \dots, M$. If we set $\tilde{A} := A \times \{0\} \subset G \times \mathbb{Z}/N\mathbb{Z}$, then we have from (3.4) that

$$\tilde{A} \oplus \tilde{F} = \bigsqcup_{m=1}^M ((A \oplus F_m) \times E_m) = G \times \bigsqcup_{m=1}^M E_m = G \times \mathbb{Z}/N\mathbb{Z}.$$

Thus the tiling equation (3.5) has at least one solution.

Conversely, suppose $\tilde{A} \subset G \times \mathbb{Z}/N\mathbb{Z}$ solves the tiling equation (3.5). We first claim that any “vertical line” $\{a\} \times \mathbb{Z}/N\mathbb{Z}$, $a \in G$ intersects \tilde{A} in at most one

point. Indeed, if $(a, h), (a, h') \in \tilde{A}$ for some $h \neq h'$, then by (3.4) $\tilde{A} \oplus \tilde{F}$ will contain both $(a + F_1) \times (h + E_1)$ and $(a + F_1) \times (h' + E_1)$ as disjoint sets. But by (3.3), $h + E_1, h' + E_1$ intersect, a contradiction.

Because each vertical line $\{a\} \times \mathbb{Z}/N\mathbb{Z}$, $a \in G$ meets A in at most one point, we can write \tilde{A} as a graph

$$\tilde{A} = \{(a, f(a)) : a \in A\}$$

for some $A \subset G$ and some function $f : A \rightarrow \mathbb{Z}/N\mathbb{Z}$. From (3.5), (3.4) we see that the sets

$$(a + F_m) \times (f(a) + E_m) \tag{3.6}$$

for $a \in A$ and $m = 1, \dots, M$ partition $G \times \mathbb{Z}/N\mathbb{Z}$.

We now claim that for any $m = 1, \dots, M$, the sets $a + F_m$, $a \in A$ are disjoint. For if we had $a + f = a' + f'$ for some distinct $a, a' \in A$ and $f, f' \in F_m$, then $\{a + f\} \times (f(a) + E_m)$ and $\{a' + f'\} \times (f(a') + E_m)$ would have to be disjoint, but this again contradicts (3.3).

By restricting the partition (3.6) of $G \times \mathbb{Z}/N\mathbb{Z}$ to a single vertical line $\{b\} \times \mathbb{Z}/N\mathbb{Z}$, we see that for any $b \in G$, we can partition $\mathbb{Z}/N\mathbb{Z}$ into $f(a_m) + E_m$, where $m = 1, \dots, M$ and a_m is the unique element of A (if it exists) such that $b \in a_m + F_m$. Since $f(a_m) + E_m$ has cardinality $|E_m| > 0$, and $|E_1| + \dots + |E_M| = N$, we conclude that a_m must exist for every $m = 1, \dots, M$. In other words, $A \oplus F_m = G$ for every $m = 1, \dots, M$. By hypothesis, this implies that A is non-periodic. Since A is the projection of \tilde{A} to G , this implies that \tilde{A} is also non-periodic. Thus the tiling equation (3.5) is aperiodic, and Theorem 3.1 follows. \square

Let us say that the *multiple periodic tiling conjecture* holds for some finitely generated abelian group G if, whenever F_1, \dots, F_M are finite non-empty subsets of G , the system (3.1) of tiling equations is not aperiodic. Obviously, the multiple periodic tiling conjecture for a given group implies the periodic tiling conjecture for that group. Applying Theorem 3.1, we conclude that the periodic tiling conjecture will hold for $\mathbb{Z}^2 \times G_0$ for all finite abelian groups G_0 if and only if the multiple periodic tiling conjecture holds for $\mathbb{Z}^2 \times G_1$ for all finite abelian groups G_1 . Thus, to establish Theorem 1.3, it now suffices to establish

Theorem 3.4 (Counterexample to multiple periodic tiling conjecture). *There exist a finite abelian group G_1 and a finite non-empty subsets F_1, \dots, F_M of $G = \mathbb{Z}^2 \times G_1$ such that the system (3.1) of tiling equations is aperiodic. In other words, the multiple periodic tiling conjecture fails for $\mathbb{Z}^2 \times G_1$.*

Our remaining task is to establish Theorem 3.4. This is the objective of the remaining sections of the paper.

4. BUILDING AN APERIODIC SYSTEM OF TILING EQUATIONS FROM AN APERIODIC PROPERTY EXPRESSIBLE IN FUNCTIONAL EQUATIONS

One can view the individual tiling equations $A \oplus F_m = G$ in (3.1) as sentences in a “tiling language” that assert various constraints on the tiling set A . Theorem 3.4 can then be thought of as asserting that this tiling language is expressive enough to describe a type of set $A \subset \mathbb{Z}^2 \times G_1$ that can exist, but is necessarily non-periodic.

In this section we show that one can replace the language of tiling equations $A \oplus F = G$ by a more familiar-looking language of *functional equations*, in which

the unknown object is now a function $\alpha: G \rightarrow H$ from a finitely generated abelian group G to a finite abelian group H , rather than a subset A of G , and then develop the further theory of this “functional equation language”. A single functional equation in this language will take the form

$$\bigoplus_{j=1}^J (\alpha(x + h_j) + E_j) = H \quad (4.1)$$

for some given shifts $h_1, \dots, h_J \in G$ and some sets $E_1, \dots, E_J \subset H$, which we may take to be non-empty. A system

$$\bigoplus_{j=1}^{J_i} (\alpha(x + h_{i,j}) + E_{i,j}) = H \text{ for all } i = 1, \dots, M \quad (4.2)$$

of such functional equations will be said to be *aperiodic* if solutions $\alpha: G \rightarrow H$ to this system exist, but that they are all non-periodic, by which we mean that there is no finite index subgroup Λ of G such that $\alpha(x + h) = \alpha(x)$ for all $x \in G$ and $h \in \Lambda$.

We then have the following tool to convert aperiodic systems of functional equations to aperiodic systems of tiling equations, in the spirit of Theorems 2.1, 3.1.

Theorem 4.1 (Converting an aperiodic system of functional equations to an aperiodic system of tiling equations). *Let G be a finitely generated abelian group, and let H be a finite abelian group. Suppose that there exists $M \geq 1$, and for each $i = 1, \dots, M$ there exist $J_i \geq 1$, shifts $h_{i,j} \in G$ and sets $E_{i,j} \subset H$ for $1 \leq j \leq J_i$, such that the system (4.2) of functional equations is aperiodic. Then there exists a system (3.1) of tiling equations in $G \times H$ which is aperiodic.*

Proof. We will consider the system of tiling equations in $G \times H$ consisting of the “vertical line test” equation

$$A \oplus (\{0\} \times H) = G \times H \quad (4.3)$$

as well as the tiling equations

$$A \oplus \bigoplus_{j=1}^{J_i} \{-h_{i,j}\} \times E_{i,j} = G \times H \quad (4.4)$$

for $i = 1, \dots, M$. It will suffice to show that this system of tiling equations is aperiodic.

On the one hand, by hypothesis there is a solution $\alpha: G \rightarrow H$ to the system (4.2). If we then form the graph

$$A := \{(x, \alpha(x)) : x \in G\} = \bigoplus_{x \in G} (\{x\} \times \{\alpha(x)\}) \subset G \times H \quad (4.5)$$

then one has

$$A \oplus (\{0\} \times H) = \bigoplus_{x \in G} \{x\} \times H = G \times H$$

and

$$\begin{aligned}
A \oplus \bigoplus_{j=1}^{J_i} \{-h_{i,j}\} \times E_{i,j} &= \bigoplus_{j=1}^{J_i} \bigoplus_{x \in G} \{x - h_j\} \times (\alpha(x) + E_{i,j}) \\
&= \bigoplus_{j=1}^{J_i} \bigoplus_{y \in G} \{y\} \times (\alpha(y + h_j) + E_{i,j}) \\
&= G \times H
\end{aligned}$$

and so A solves the system of tiling equations (4.3), (4.4).

Conversely, suppose that $A \subset G \times H$ solves the system of tiling equations (4.3), (4.4). From (4.3) we see that each vertical line $\{x\} \times H$, $x \in G$ meets A in exactly one point; in other words, A is a graph (4.5) of some function $\alpha: G \rightarrow H$. By the above calculations, we then see that each tiling equation (4.4) is equivalent to its functional counterpart (4.2), so that α is a solution to the system (4.2). By hypothesis, α is non-periodic, and hence A is non-periodic also. This establishes the theorem. \square

In order to use the above theorem, it is convenient to introduce some notation. Define a (G, H) -property to be a property P of a function $\alpha: G \rightarrow H$ (or equivalently, a subset of H^G).

Definition 4.2 (Expressible property). We say that a (G, H) -property P is *expressible in the language of functional equations*, or *expressible*⁵ for short, if there exists a system (4.2) of functional equations for some $M \geq 0$ which is obeyed by a function $\alpha: G \rightarrow H$ if and only if α obeys property P .

Definition 4.3 (Aperiodic property). We say that the property P is *aperiodic* if it is satisfiable, but only by non-periodic functions.

The following examples may help illustrate these concepts.

Example 4.4 (Empty and full property). The empty property (satisfied by no function $\alpha: G \rightarrow H$) is expressible, for instance using an empty functional equation (4.1) with $J = 0$. Similarly, the complete property (satisfied by every function $\alpha: G \rightarrow H$) is expressible, using the empty system with $M = 0$ (or alternatively by using the functional equation $\alpha(x) + H = H$). Neither property is aperiodic (the former has no solutions, and the latter includes periodic solutions).

Example 4.5 (Closure under conjunction). If P_1, \dots, P_M are a finite collection of expressible (G, H) -properties, then their conjunction $P_1 \wedge \dots \wedge P_M$ is clearly also an expressible (G, H) -property.

Example 4.6 (Expressing a clock). Let $\mathbb{Z}/N\mathbb{Z}$ be a cyclic group. Let us call a function $\alpha: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$ a *clock* if it obeys the property

$$\alpha(x + 1) = \alpha(x) + 1$$

⁵This notion is somewhat analogous to the notion of an *algebraic set* in algebraic geometry, or of a *variety* in universal algebra. For instance, the claim in Example 4.5 is analogous to the claim that the intersection of finitely many algebraic sets is again algebraic. On the other hand, unlike algebraic sets which are closed under unions thanks to the integral domain property $ab = 0 \iff a = 0 \vee b = 0$, it is not the case that the disjunction of expressible properties is again expressible, as there is no analogue of the integral domain property in our setting.

for all $x \in \mathbb{Z}$, or equivalently if it takes the form $\alpha(x) = x + a \pmod{N}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$. Then the property of being in clock is expressible by using the single functional equation

$$(\alpha(x) + \{1\}) \uplus (\alpha(x+1) + (\mathbb{Z}/N\mathbb{Z} \setminus \{0\})) = \mathbb{Z}/N\mathbb{Z}.$$

On the other hand, the property of being a clock is clearly not aperiodic.

For technical reasons we will not actually employ the clock property in our main argument, but instead rely on the following variant.

Example 4.7 (Expressing a periodized permutation). Let $\mathbb{Z}/N\mathbb{Z}$ be a cyclic group. Let us call a function $\alpha: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$ a *periodized permutation* if it is of the form $\alpha(x) = \sigma(x \pmod{N})$ for some permutation $\sigma: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$. For instance, every clock is a periodized permutation, but the converse is not true for $N > 2$. We claim that the property of being a periodized permutation is expressible by the single functional equation

$$(\alpha(x) + \{0\}) \uplus (\alpha(x+1) + \{0\}) \uplus \cdots \uplus (\alpha(x+N-1) + \{0\}) = \mathbb{Z}/N\mathbb{Z}$$

for all $x \in \mathbb{Z}$. Indeed, this equation asserts that the N points $\alpha(x), \dots, \alpha(x+N-1)$ in $\mathbb{Z}/N\mathbb{Z}$ are all distinct, which when applied to both x and $x+1$ implies that $\alpha(x) = \alpha(x+N)$, and also that α is a permutation on any interval $\{x, \dots, x+N-1\}$, which gives the claim. Obviously, this property is not aperiodic either.

Theorem 4.1 tells us that if there is an expressible (G, H) -property P that is aperiodic, then one can use this to build an aperiodic system of tiling equations. (Note that the empty system $M = 0$ is not aperiodic, so we must have $M \geq 1$.) As a consequence, Theorem 3.4 is implied by the following statement.

Theorem 4.8 (Expressing aperiodicity). *There exist finite abelian groups G_1, H and an $(\mathbb{Z}^2 \times G_1, H)$ -property P that is both expressible and aperiodic.*

Remark 4.9 (Translation invariance). An expressible property P must necessarily be translation invariant in both the horizontal direction G and the vertical direction H . More precisely, if $\alpha: G \rightarrow H$ obeys P , then so do all the horizontal translates $x \mapsto \alpha(x+h)$ for $h \in G$, and vertical translates $x \mapsto \alpha(x) + u$ for $u \in H$. This is because each equation in (4.2) is invariant with respect to these translations. The “dilation lemma” (see e.g., [GGRT22, Theorem 1.2]) also can force some dilation invariances of expressible properties (at least if the shifts $h_{i,j}$ in (4.2) are of finite order), although we will not formalize this assertion here. These invariances are a technical complication for our applications, as they provide some limitations on what types of properties one can hope to express in the language of functional equations. For instance, one cannot hope to remove the constant a from the clock property in Example 4.6 and still retain expressibility.

It will be convenient to “coordinatize” the function $\alpha: G \rightarrow H$ by replacing it with a *tuple* $(\alpha_w)_{w \in \mathcal{W}}$ functions $\alpha_w: G \rightarrow H_w$ into various finite abelian groups H_w indexed by a finite set \mathcal{W} . Note that any such tuple $(\alpha_w)_{w \in \mathcal{W}}$ can be identified with a single function $\alpha: G \rightarrow \prod_{w \in \mathcal{W}} H_w$, defined by the formula

$$\alpha(x) := (\alpha_w(x))_{w \in \mathcal{W}}$$

for $x \in G$. Define a $(G, (H_w)_{w \in \mathcal{W}})$ -*function* to be a tuple $(\alpha_w)_{w \in \mathcal{W}}$ of functions $\alpha_w: G \rightarrow H_w$, and define a $(G, (H_w)_{w \in \mathcal{W}})$ -*property* to be a property P of a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$. We will say such a property P is *expressible*

in the language of functional equations, or *expressible* for short, if the corresponding $(G, \prod_{w \in \mathcal{W}} H_w)$ -property \tilde{P} of the combined function $\alpha: G \rightarrow \prod_{w \in \mathcal{W}} H_w$ is expressible, that is to say that there is a system of functional equations

$$\biguplus_{j=1}^{J_i} ((\alpha_w(x + h_{i,j}))_{w \in \mathcal{W}} + E_{i,j}) = \prod_{w \in \mathcal{W}} H_w \text{ for all } i = 1, \dots, M \quad (4.6)$$

for some M , some J_1, \dots, J_M , and some $h_{i,j} \in G$ and $E_{i,j} \subset \prod_{w \in \mathcal{W}} H_w$ for $1 \leq i \leq M$ and $1 \leq j \leq J_i$, which is satisfied by the tuple $(\alpha_w)_{w \in \mathcal{W}}$ if and only if the property P holds. We say that P is *aperiodic* if \tilde{P} is, or equivalently if there are tuples $(\alpha_w)_{w \in \mathcal{W}}$ obeying property P , but any such tuple has at least one of the α_w non-periodic.

Example 4.10 (Differing by a constant is expressible). Let H be a finite abelian group. The property of two functions $\alpha_1, \alpha_2: \mathbb{Z}^2 \rightarrow H$ differing by a constant (thus $\alpha_1(x) = \alpha_2(x) + c$ for all $x \in \mathbb{Z}^2$ and some $c \in H$) is an expressible $(\mathbb{Z}^2, (H, H))$ -property by using the system of functional equations

$$((\alpha_1(x), \alpha_2(x)) + \Delta) \uplus (\alpha_1(x + e_i), \alpha_2(x + e_i)) + (H^2 \setminus \Delta) = H^2 \quad (4.7)$$

for $x \in \mathbb{Z}^2$ and $i = 1, 2$, where $e_1 = (1, 0)$, $e_2 = (0, 1)$ is the standard basis of \mathbb{Z}^2 , and Δ is the diagonal group

$$\Delta := \{(a, a) : a \in H\}.$$

Indeed, the equation (4.7) can easily be seen to be equivalent to the equation

$$\alpha_1(x) - \alpha_2(x) = \alpha_1(x + e_i) - \alpha_2(x + e_i),$$

which is in turn equivalent to the constancy of $\alpha_1 - \alpha_2$ since the e_1, e_2 generate \mathbb{Z}^2 . This property is of course not aperiodic, since one can easily find a pair (α_1, α_2) of periodic functions that differ by a constant.

We are thus reduced to establishing the following claim.

Theorem 4.11 (Expressing aperiodicity for a tuple). *There exist a finite abelian group G_1 , a tuple $(H_w)_{w \in \mathcal{W}}$ of finite abelian groups indexed by a finite set \mathcal{W} , and a $(\mathbb{Z}^2 \times G_1, (H_w)_{w \in \mathcal{W}})$ -property that is both expressible and aperiodic.*

Remark 4.12. By Remark 4.9, an expressible $(G, (H_w)_{w \in \mathcal{W}})$ -property must be invariant with joint horizontal translation of a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ to $(\alpha_w(\cdot + h))_{w \in \mathcal{W}}$ by a shift $h \in G$, and also by independent vertical translations $(\alpha_w + u_w)_{w \in \mathcal{W}}$ of such functions by arbitrary shifts $u_w \in H_w$, and in some cases there are also dilation invariances. Again, these invariances present some limitations on what properties one can hope to be expressible.

To add even more flexibility to our framework, it will be convenient to relax the notion of expressibility in which we “allow existential quantifiers”.

Definition 4.13 (Weak expressibility). Let G be a finite abelian group, and let $(H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0}$ be a tuple of finite abelian groups indexed by the disjoint union of two finite sets $\mathcal{W}, \mathcal{W}_0$. Given a $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property P^* :

- (i) We define the *existential quantification* (or *projection*) P of P^* to $(G, (H_w)_{w \in \mathcal{W}})$ to be the $(G, (H_w)_{w \in \mathcal{W}})$ -property defined by requiring a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ to obey P if and only if there exists a $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -function $(\alpha_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0}$ extending the original tuple $(\alpha_w)_{w \in \mathcal{W}}$ that obeys P^* .

- (ii) A $(G, (H_w)_{w \in \mathcal{W}})$ -property P is said to be *weakly expressible* if it is the existential quantification of some expressible $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property P^* for some \mathcal{W}_0 disjoint from \mathcal{W} .

Expressible and weakly expressible properties (or more precisely, the sets of tuples obeying such properties) can be viewed as analogous⁶ to Π_0^0 and Σ_1^0 sets respectively in the arithmetic hierarchy; we will not need any analogues of higher order sets in this hierarchy.

Obviously every expressible property is weakly expressible (take $\mathcal{W}_0 = \emptyset$). It is somewhat more challenging to locate a weakly expressible property that is not obviously expressible, but we will do so in later sections. Observe that if P is an aperiodic weakly expressible $(G, (H_w)_{w \in \mathcal{W}})$ -property, then the associated expressible $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property P^* is necessarily also aperiodic, since it is satisfied by at least one tuple $(\alpha_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0}$ (formed by extending a tuple obeying P), and any such tuple must contain a non-periodic function: $\alpha_{w_0}: G \rightarrow H_{w_0}$ for at least one $w_0 \in \mathcal{W} \uplus \mathcal{W}_0$ (because the restriction $(\alpha_w)_{w \in \mathcal{W}}$ does). Hence, to prove Theorem 4.11, it suffices to show:

Theorem 4.14 (Weakly expressing aperiodicity for a tuple). *There exist a finite abelian group G_1 , a tuple $(H_w)_{w \in \mathcal{W}}$ of finite abelian groups indexed by a finite set \mathcal{W} , and an $(\mathbb{Z}^2 \times G_1, (H_w)_{w \in \mathcal{W}})$ -property that is both weakly expressible and aperiodic.*

To prove this theorem, it will be useful to observe that the class of weakly expressible properties is closed under a number of natural operations, which we now introduce.

Definition 4.15 (Lift). If G be a finitely generated abelian group, $(H_w)_{w \in \mathcal{W}}$ be a tuple of finite abelian groups indexed by a finite set \mathcal{W} , \mathcal{W}_1 be a subset of \mathcal{W} , and P_1 is a $(G, (H_w)_{w \in \mathcal{W}_1})$ -property, we define the *lift* of P_1 to $(G, (H_w)_{w \in \mathcal{W}})$ to be the $(G, (H_w)_{w \in \mathcal{W}})$ -property P , defined by requiring a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ to obey P if and only if the $(G, (H_w)_{w \in \mathcal{W}_1})$ -function $(\alpha_w)_{w \in \mathcal{W}_1}$ obeys P_1 .

One can think of this operation as that of adding “dummy functions” $\alpha_w: \mathbb{Z}^2 \times G_1 \rightarrow H_w$ for $w \in \mathcal{W} \setminus \mathcal{W}_1$ that play no actual role in the lifted property P .

Example 4.16. The $(\mathbb{Z}^2, (H, H, H))$ -property of a triple $(\alpha_1, \alpha_2, \alpha_3)$ of functions $\alpha_1, \alpha_2, \alpha_3: \mathbb{Z}^2 \rightarrow H$ such that α_2, α_3 both differ from α_1 by a constant (i.e., $\alpha_2 = \alpha_1 + c$ and $\alpha_3 = \alpha_1 + c'$ for some $c, c' \in H$) can be viewed as the conjunction of two lifts of (relabelings of) the $(\mathbb{Z}, (H, H))$ -property described in Example 4.10; one of these lifts will capture the property of α_1 and α_2 differing by a constant, and another will capture the property of α_1 and α_3 differing by a constant. If we take an existential quantification to eliminate the role of α_1 , we conclude (from Lemma 4.20 below) that the $(\mathbb{Z}^2, (H, H))$ -property of a pair $\alpha_2, \alpha_3: \mathbb{Z}^2 \rightarrow H$ differing by a constant is then weakly expressible (since this occurs if and only if we can locate $\alpha_1: \mathbb{Z}^2 \rightarrow H$ such that α_2, α_3 both differ from α_1 by a constant). Of course, from Example 4.10 we already knew that this property was in fact expressible, so this does not give an example of a weakly expressible property that is not expressible. However, in the next section we shall see several examples in which existential

⁶They are also somewhat analogous to the notions of an algebraic set and semi-algebraic set respectively in real algebraic geometry, though as before this analogy should not be taken too literally.

quantification can be used to produce weakly expressible properties that are not obviously expressible.

Example 4.17. If one lifts a $(G, (H_w)_{w \in \mathcal{W}_1})$ -property P_1 to a $(G, (H_w)_{w \in \mathcal{W}})$ -property and then takes an existential quantification back to $(G, (H_w)_{w \in \mathcal{W}_1})$, one recovers the original property P_1 (since one could simply set all the dummy functions equal to zero).

Definition 4.18 (Pullback). Let G be a finitely generated abelian group, let G' be a subgroup of G , and let $(H_w)_{w \in \mathcal{W}}$ be a tuple of finite abelian groups indexed by a finite set \mathcal{W} . If P' is a $(G', (H_w)_{w \in \mathcal{W}})$ -property, we define the *pullback* of P' to $(G, (H_w)_{w \in \mathcal{W}})$ to be the $(G, (H_w)_{w \in \mathcal{W}})$ -property P defined by requiring a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ to obey P if and only if the $(G', (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_{w, x_0})_{w \in \mathcal{W}}$ defined by $\alpha_{w, x_0}(x') := \alpha_w(x_0 + x')$ for $x' \in G'$ and $w \in \mathcal{W}$ obeys P_1 for every choice of base point $x_0 \in G$.

Example 4.19 (Pulling back the clock). Let v be a non-zero vector in \mathbb{Z}^2 , then we can identify \mathbb{Z} with the subgroup $\mathbb{Z}v = \{nv : n \in \mathbb{Z}\}$ of \mathbb{Z}^2 . If we view the clock property from Example 4.6 as a $(\mathbb{Z}v, \mathbb{Z}/N\mathbb{Z})$ -property, its pullback to $(\mathbb{Z}^2, \mathbb{Z}/N\mathbb{Z})$ is the $(\mathbb{Z}^2, \mathbb{Z}/N\mathbb{Z})$ -property of a function $\alpha: \mathbb{Z}^2 \rightarrow \mathbb{Z}/N\mathbb{Z}$ being a clock along the direction v , that is to say for every $x_0 \in \mathbb{Z}^2$ there exists $a_{x_0} \in \mathbb{Z}/N\mathbb{Z}$ such that $\alpha(x_0 + nv) = a_{x_0} + n \pmod{N}$ for every $n \in \mathbb{Z}$.

We now record the closure properties of (weak) expressibility that we will need.

Lemma 4.20 (Closure properties of (weak) expressibility).

- (i) *Any lift of an expressible (resp. weakly expressible) property is also expressible (resp. weakly expressible).*
- (ii) *Any pullback of an expressible (resp. weakly expressible) property is also expressible (resp. weakly expressible).*
- (iii) *The conjunction $P \wedge P'$ of two expressible (resp. weakly expressible) $(G, (H_w)_{w \in \mathcal{W}})$ -properties is also expressible (resp. weakly expressible).*
- (iv) *Any existential quantification of a weakly expressible property is weakly expressible.*

Proof. We begin with the expressible case of (i). Suppose that P is a $(G, (H_w)_{w \in \mathcal{W}})$ -property formed by lifting an expressible $(G, (H_w)_{w \in \mathcal{W}_1})$ -property P_1 . By definition, we can find M, J_1, \dots, J_M , and $h_{i,j} \in G$ and $E_{i,j,1} \subset \prod_{w \in \mathcal{W}_1} H_w$ for $1 \leq i \leq M$ and $1 \leq j \leq J_i$ such that a $(G, (H_w)_{w \in \mathcal{W}_1})$ -function $(\alpha_w)_{w \in \mathcal{W}_1}$ obeys P_1 if and only if it solves the system

$$\bigoplus_{j=1}^{J_i} ((\alpha_w(x + h_{i,j}))_{w \in \mathcal{W}_1} + E_{i,j,1}) = \prod_{w \in \mathcal{W}_1} H_w$$

for all $i = 1, \dots, M$ and $x \in G$. If we then define the lifted sets

$$E_{i,j} := E_{i,j,1} \times \prod_{w \in \mathcal{W} \setminus \mathcal{W}_1} H_w \subset \prod_{w \in \mathcal{W}} H_w$$

for $i = 1, \dots, M$ and $j = 1, \dots, J_i$, we see from the definitions 4.15 and 4.2 that a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ obeys P if and only if

$$\bigoplus_{j=1}^{J_i} ((\alpha_w(x + h_{i,j}))_{w \in \mathcal{W}} + E_{i,j}) = \prod_{w \in \mathcal{W}} H_w$$

for all $i = 1, \dots, M$. The claim follows.

For the weakly expressible case of (i), suppose that P is a $(G, (H_w)_{w \in \mathcal{W}})$ -property formed by lifting a weakly expressible $(G, (H_w)_{w \in \mathcal{W}_1})$ -property P_1 . By Definition 4.13, the weakly expressible $(G, (H_w)_{w \in \mathcal{W}_1})$ -property P_1 is associated to an expressible $(G, (H_w)_{w \in \mathcal{W}_1 \uplus \mathcal{W}_0})$ -property P_1^* . By relabeling, we may assume that \mathcal{W}_0 is disjoint from \mathcal{W} . The lift P^* of P_1^* to $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ is then an expressible $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property by the expressible case of (i), and can be seen to be associated to P in the sense of Definition 4.13 by expanding out the definitions. Thus P is weakly expressible as desired.

Now we establish the expressible case of (ii). Suppose that P is a $(G, (H_w)_{w \in \mathcal{W}})$ -property formed by pulling back an expressible $(G', (H_w)_{w \in \mathcal{W}})$ -property P' . By definition, we can find M, J_1, \dots, J_M , and $h_{i,j} \in G'$ and $E_{i,j} \subset \prod_{w \in \mathcal{W}} H_w$ for $1 \leq i \leq M$ and $1 \leq j \leq J_i$ such that a $(G', (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ obeys P' if and only if it solves the system

$$\biguplus_{j=1}^{J_i} ((\alpha_w(x + h_{i,j}))_{w \in \mathcal{W}} + E_{i,j}) = \prod_{w \in \mathcal{W}} H_w \quad (4.8)$$

for all $i = 1, \dots, M$ and $x \in G'$. By expanding out the definitions, we then see that a $(G, (H_w)_{w \in \mathcal{W}})$ -function $(\alpha_w)_{w \in \mathcal{W}}$ obeys P if and only if it obeys the same system of equations (4.8) for $i = 1, \dots, M$, but now with x ranging over G instead of G' . Thus P is also expressible as required.

For the weakly expressible case of (ii), suppose that P is a $(G, (H_w)_{w \in \mathcal{W}})$ -property formed by pulling back a weakly expressible $(G', (H_w)_{w \in \mathcal{W}})$ -property P' . By Definition 4.13, P' is associated to some expressible $(G', (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property $(P')^*$. If we let P^* be the pullback of $(P')^*$ to $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$, then P^* is expressible by the expressible case of (ii), and can be seen to be associated to P in the sense of Definition 4.13 by expanding out the definitions. Thus P is weakly expressible as desired.

The expressible case of (iii) is trivial (and was already noted in Remark 4.5). Now suppose that P, P' are weakly expressible $(G, (H_w)_{w \in \mathcal{W}})$ -properties. By Definition 4.13, P is associated with an expressible $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0})$ -property P^* , and P' is similarly associated with an expressible $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}'_0})$ -property $(P')^*$. By relabeling, we can assume that \mathcal{W}_0 and \mathcal{W}'_0 are disjoint. Let Q^* be the $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0 \uplus \mathcal{W}'_0})$ -property formed by lifting both P^* and $(P')^*$ to $(G, (H_w)_{w \in \mathcal{W} \uplus \mathcal{W}_0 \uplus \mathcal{W}'_0})$ and then taking their conjunction. By the previously established parts of this lemma, Q^* is expressible, and can be seen to be associated to $P \wedge P'$ in the sense of Definition 4.13 by expanding out the definitions. Thus $P \wedge P'$ is weakly expressible as desired.

Finally, (iv) is immediate from Definition 4.13, after observing that an existential quantification of an existential quantification is again an existential quantification. \square

5. A LIBRARY OF (WEAKLY) EXPRESSIBLE PROPERTIES

In view of Lemma 4.20, a natural strategy to establish Theorem 4.14 is to first build up a useful “library” of (weakly) expressible $(G, (H_w)_{w \in \mathcal{W}})$ -properties for various choices of G and $(H_w)_{w \in \mathcal{W}}$, with the aim of combining them via various applications of Lemma 4.20 to create more interesting (and ultimately, aperiodic)

examples of weakly expressible properties (analogous to how one can create a complex computer program by combining more fundamental library routines together in various ways). For instance, the clock in Example 4.6 can be regarded as one entry in this library, as can the property of being a periodized permutation as discussed in Example 4.7, or the property of differing by a constant as discussed in Example 4.10. The final objective is to then “program” such a combination of properties in the library that necessarily generates a non-periodic function. In fact we will achieve this by “programming” a certain type of “Sudoku puzzle” that can be solved, but only in a non-periodic fashion.

Example 5.1. Consider the $(\mathbb{Z}^2, \mathbb{Z}/N\mathbb{Z})$ -property P of a function $\alpha: \mathbb{Z}^2 \rightarrow \mathbb{Z}/N\mathbb{Z}$ being of the form $\alpha(x, y) = x + y + c$ for all $(x, y) \in \mathbb{Z}^2$ and some $c \in \mathbb{Z}/N\mathbb{Z}$. This is equivalent to α being a clock along the direction $e_1 = (1, 0)$ and simultaneously being a clock along the direction $e_2 = (0, 1)$, in the sense of Example 4.19. Thus this property P is the conjunction of two pullbacks of the clock property; since we know from Example 4.6 that the clock property is expressible, we conclude from several applications of Lemma 4.20 that this property P is also expressible. However, this property is not aperiodic, and so does not complete the proof of Theorem 4.14.

Example 5.2. The $(\mathbb{Z}, (\mathbb{Z}/N\mathbb{Z})_{w=1,2})$ -property of two functions $\alpha_1, \alpha_2: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$ being periodized permutations that differ by a constant is expressible, as can be seen from Lemma 4.20 after lifting Example 4.7 twice and taking conjunctions of those lifts with Example 4.10. Again, this property is not aperiodic, and so does not complete the proof of Theorem 4.14.

5.1. Expressing linear constraints. One basic property that we will add to our library is the ability to express linear constraints (up to constants) between different functions α_w , which significantly generalizes Example 4.10. The basic relation is

Proposition 5.3 (Expressing constancy modulo a subgroup). *Let G be a finitely generated abelian group, let H be a finite abelian group, and let H' be a subgroup of H . Then the (G, H) -property of a (G, H) -function α taking values in a single coset $c + H'$ of H' (i.e., there exists $c \in H$ such that $\alpha(x) \in c + H'$ for all $x \in G$) is expressible.*

Proof. Let e_1, \dots, e_d be a set of generators for G . Similarly to Example 4.10, we consider the functional equation

$$(\alpha(x) + H') \uplus (\alpha(x + e_i) + (H \setminus H')) = H$$

for all $i = 1, \dots, d$ and $x \in G$, and some unknown function $\alpha: G \rightarrow H$. This equation can be equivalently expressed as

$$\alpha(x) = \alpha(x + e_i) \pmod{H'},$$

that is to say $\alpha(x)$ and $\alpha(x + e_i)$ lie in the same coset of H' . Since the e_i generate G , this is equivalent to α lying in a single coset of H' , as claimed. \square

We isolate two useful corollaries of this proposition:

Corollary 5.4 (Expressing periodicity). *Let G be a finitely generated abelian group, let H be a finite abelian group, and let G' be a subgroup of G . Then the (G, H) -property that a (G, H) -function α is G' -periodic in the sense that $\alpha(x+h) = \alpha(x)$ for all $x \in G$ and $h \in G'$, is expressible.*

Proof. From Proposition 5.3 with G replaced by G' and H' replaced by $\{0\}$, we see that the (G', H) property of being a constant (G', H) -function is expressible. Pulling back from (G', H) to (G, H) using Lemma 4.20(ii), we obtain the claim. \square

Corollary 5.5 (Expressing linear constraints). *Let G be a finitely generated abelian group, let $\mathbb{Z}/N\mathbb{Z}$ be a cyclic group, and let $c_1, \dots, c_W \in \mathbb{Z}/N\mathbb{Z}$ be coefficients. Then the $(G, (\mathbb{Z}/N\mathbb{Z})_{w=1, \dots, W})$ -property of a tuple $\alpha_1, \dots, \alpha_W: G \rightarrow \mathbb{Z}/N\mathbb{Z}$ of functions obeying the linear relation*

$$c_1\alpha_1(x) + \dots + c_W\alpha_W(x) = c \quad (5.1)$$

for all $x \in G$ and some constant $c \in \mathbb{Z}/N\mathbb{Z}$, is expressible.

Proof. We can view $(\alpha_w)_{w=1, \dots, W}$ as a single $(G, (\mathbb{Z}/N\mathbb{Z})^W)$ -function. The linear relation (5.1) is then equivalent to this function lying in a single coset of the group

$$H' := \{(a_1, \dots, a_W) \in (\mathbb{Z}/N\mathbb{Z})^W : c_1a_1 + \dots + c_Wa_W = 0\}.$$

The claim now follows from Proposition 5.3. \square

Remark 5.6. Note that Example 4.10 is essentially the special case of Corollary 5.5 with $W = 2$, $c_1 = 1$, and $c_2 = -1$. The presence of the constant c in (5.1) is unfortunately necessary due to the translation invariance mentioned in Remark 4.9. We remark that a variant of Corollary 5.5 (in which one did not tile the whole group, and was thus able to set c to zero) was implicitly used in our previous work [GT21, §6].

Example 5.7. Let $\mathbb{Z}/N\mathbb{Z}$ be a cyclic group, and consider the $(\mathbb{Z}^2, (\mathbb{Z}/N\mathbb{Z})_{w=1,2,3})$ -property of a triple of functions $\alpha_1, \alpha_2, \alpha_3: \mathbb{Z}^2 \rightarrow \mathbb{Z}/N\mathbb{Z}$ obeying the properties

$$\begin{aligned} \alpha_1(x, y) &= \alpha_1(x+1, y) \\ \alpha_2(x, y) &= \alpha_2(x, y+1) \\ \alpha_3(x, y) &= \alpha_3(x+1, y-1) \\ \alpha_1(x, y) + \alpha_2(x, y) &= \alpha_3(x, y) \end{aligned}$$

for all $(x, y) \in \mathbb{Z}^2$, namely, $\alpha_1, \alpha_2, \alpha_3$ are periodic along the directions $(1, 0)$, $(0, 1)$, $(1, -1)$ respectively, and that $\alpha_1 + \alpha_2 = \alpha_3$. Thus, this property is expressible. It is not difficult to show that the solutions to this system of equations are given by $\alpha_1(x, y) = \phi(y) + c_1$, $\alpha_2(x, y) = \phi(x) + c_2$, $\alpha_3(x, y) = \phi(x+y) + c_3$ for some homomorphism $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$ and some constants $c_1, c_2, c_3 \in \mathbb{Z}/N\mathbb{Z}$. Thus the property of $\alpha_1, \alpha_2, \alpha_3$ taking this form is expressible. Applying existential quantification to eliminate the role of α_2, α_3 , we conclude that the $(\mathbb{Z}^2, \mathbb{Z}/N\mathbb{Z})$ -property of a function $\alpha: \mathbb{Z}^2 \rightarrow \mathbb{Z}/N\mathbb{Z}$ taking the form $\alpha(x, y) = f(y)$ for some affine function $f: \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$ (i.e., the sum of a homomorphism and a constant), is weakly expressible. This is our first example of a property which is weakly expressible, but which is not obviously expressible.

6. EXPRESSING BOOLEAN FUNCTIONS

Thus far we have been considering properties of functions $\alpha_w: G \rightarrow H_w$ which can range over the entirety of a finite abelian group H_w . In order to be able to express boolean operations (as in [GT21, §5]), we will need to start expressing properties of functions that take on only two values $\{a, b\}$ in a larger ambient group H_w (which we will take to be a cyclic 2-group $\mathbb{Z}/2^M\mathbb{Z}$). To do this, we introduce the following definition.

Definition 6.1 (Boolean function). Let G be a finitely generated abelian group, let e be an element of G of order 2, let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 1$, and let a, b be distinct elements of $\mathbb{Z}/2^M\mathbb{Z}$ of opposite parity (thus one of the a, b is even and the other is odd). A function $\alpha: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ is $(e, \{a, b\})$ -boolean if it takes values in $\{a, b\}$, and furthermore obeys the alternating property

$$\alpha(x + e) = a + b - \alpha(x) \quad (6.1)$$

for all $x \in G$; i.e., for each $x \in G$, $\alpha(x)$ takes one of the values a, b , and $\alpha(x + e)$ takes the other value. In particular, $\{a, b\}$ is equal to the image $\alpha(G)$ of α .

A $(e, \{a, b\})$ -boolean function α is said to be *compatible* with a $(e, \{a', b'\})$ -boolean function α' if $\{a', b'\}$ is a translate of $\{a, b\}$, or equivalently if the image $\alpha(G)$ of α is a translate of the image $\alpha'(G)$ of α' .

We restrict to 2-groups $\mathbb{Z}/2^M\mathbb{Z}$ here because in later arguments it will be important to exploit the fact that all odd elements of such groups are invertible (with respect to the usual ring structure on cyclic groups), and in particular have order 2^M equal to the order of the group. This will also be the main reason why we will work with “2-adic Sudoku puzzles” in later sections, as opposed to Sudoku puzzles in odd characteristic which are slightly easier to analyze.

Proposition 6.2 (Expressing a single boolean function). *Let G be a finitely generated abelian group, let e be an element of G of order two, and let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 1$. Then the $(G, \mathbb{Z}/2^M\mathbb{Z})$ -property of being $(e, \{a, b\})$ -boolean for some distinct $a, b \in \mathbb{Z}/2^M\mathbb{Z}$ of opposite parity, is expressible.*

Proof. Let e_1, \dots, e_r be a set of generators for G , and consider the $(G, \mathbb{Z}/2^M\mathbb{Z})$ -property of a function $\alpha: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ obeying the functional equation

$$(\alpha(x) + 2\mathbb{Z}/2^M\mathbb{Z}) \uplus (\alpha(x + e) + 2\mathbb{Z}/2^M\mathbb{Z}) = \mathbb{Z}/2^M\mathbb{Z} \quad (6.2)$$

for all $x \in G$, as well as the equations

$$\biguplus_{y=x, x+e} ((\alpha(y + e_i) + \{0\}) \uplus (\alpha(y) + (2\mathbb{Z}/2^M\mathbb{Z} \setminus \{0\}))) = \mathbb{Z}/2^M\mathbb{Z} \quad (6.3)$$

for all $x \in G$ and $i = 1, \dots, r$.

Suppose that α obeys this system (6.2), (6.3). Since $2\mathbb{Z}/2^M\mathbb{Z}$ is an index two subgroup of $\mathbb{Z}/2^M\mathbb{Z}$, we see that for each x , the pair $(\alpha(x), \alpha(x + e))$ must consist of an even element $a(x)$ and an odd element $b(x)$ of $\mathbb{Z}/2^M\mathbb{Z}$. On the other hand, from comparing (6.3) with (6.2) we have for each $x \in G$ and $i = 1, \dots, r$ that

$$(\alpha(x) + \{0\}) \uplus (\alpha(x + e) + \{0\}) = (\alpha(x + e_i) + \{0\}) \uplus (\alpha(x + e + e_i) + \{0\})$$

or equivalently that $a(x) = a(x + e_i)$ and $b(x) = b(x + e_i)$. Since the e_1, \dots, e_r generate G , we conclude that $a(x) = a$, $b(x) = b$ are constant in x , and α is $(e, \{a, b\})$ -boolean. Conversely, if α is $(e, \{a, b\})$ -boolean, we can reverse the above arguments and conclude the functional equations (6.2), (6.3). The claim follows. \square

Let G be a finitely generated abelian group, let e be an element G of order two, let $\mathbb{Z}/2q\mathbb{Z}$ be a cyclic group of even order, and let $W \geq 1$. By the above proposition and Lemma 4.20, one can express the $(G, (\mathbb{Z}/2q\mathbb{Z})_{w=1, \dots, W})$ -property of a tuple $\alpha_1, \dots, \alpha_W: G \rightarrow \mathbb{Z}/2q\mathbb{Z}$ of functions being such that each α_i is $(e, \{a_i, b_i\})$ -periodic for some $a_i, b_i \in \mathbb{Z}/2q\mathbb{Z}$ of different parity. However, this property does not force the boolean functions to be compatible; in other words, it does not require

that the $\{a_i, b_i\}$ are translates of each other; this is a new difficulty that was not present in our previous work [GT21], where we could enforce this compatibility by only tiling a subset of H rather than the full group H . In our context, the desired compatibility will be achieved with the assistance of the following elementary lemma.

Lemma 6.3 (An equation to force boolean compatibility). *Let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 2$, and let $\{a, b\}, \{c, d\}, \{f, g\}, \{h', k'\}, \{h'', k''\}$ be pairs of elements of $\mathbb{Z}/2^M\mathbb{Z}$ of different parity. Let $z \in \mathbb{Z}/2^M\mathbb{Z}$ be such that*

$$(a + b) + (h' + k') + (h'' + k'') = 2(c + d) + (f + g) + 2z. \quad (6.4)$$

Suppose also that for any triple $(\alpha, \tau, \tau') \in \{a, b\} \times \{h', k'\} \times \{h'', k''\}$ there exists $(\beta, \gamma) \in \{c, d\} \times \{f, g\}$ solving the equation

$$\alpha + \tau + \tau' = 2\beta + \gamma + z. \quad (6.5)$$

Then the sets $\{a, b\}, \{h', k'\}, \{h'', k''\}$ are translates of each other.

Proof. Observe that we can translate any of the pairs $\{a, b\}, \{h', k'\}, \{h'', k''\}$ by some shift in $\mathbb{Z}/2^M\mathbb{Z}$, so long as we also shift z by the same shift. So we may normalize $a = h' = h'' = 0$. By (6.5) we may then find $(\beta, \gamma) \in \{c, d\} \times \{f, g\}$ such that $0 = 2\beta + \gamma + z$. By shifting $\{c, d\}$ by $-\beta$, $\{f, g\}$ by $-\gamma$, and replacing z with 0, we may thus also normalize $\beta = \gamma = z = 0$, so without loss of generality $c = f = z = 0$. Thus we now have

$$b + k' + k'' = 2d + g \quad (6.6)$$

and for any triple $(\alpha, \tau, \tau') \in \{0, b\} \times \{0, k'\} \times \{0, k''\}$ there exists $(\beta, \gamma) \in \{0, d\} \times \{0, g\}$ such that

$$\alpha + \tau + \tau' = 2\beta + \gamma.$$

In particular

$$b, k', k'' \in \{0, 2d, g, g + 2d\}.$$

By the hypothesis of distinct parities, b, k', k'', d, g are all odd. Thus in fact we must have

$$b, k', k'' \in \{g, g + 2d\}.$$

If $b = k' = k''$ then $\{0, b\}, \{0, k'\}, \{0, k''\}$ are translates of each other as desired. There are only two remaining cases:

1. If two of the b, k', k'' are equal to g and the third is equal to $g + 2d$, then from (6.6) we have $3g + 2d = 2d + g$, which is absurd since g is odd and $M \geq 2$.
2. If one of the b, k', k'' is equal to g and the other two are equal to $g + 2d$, then from (6.6) we have $3g + 4d = 2d + g$, so in particular $g + 2d = -g$ and so $\{0, g\}$ and $\{0, g + 2d\}$ are translates of each other. Thus $\{0, b\}, \{0, k'\}, \{0, k''\}$ are translates of each other as desired.

□

Definition 6.4 (Compatible boolean property). Let G be a finitely generated abelian group, let e, e', e'' be elements of G that generate a copy of $(\mathbb{Z}/2\mathbb{Z})^3$ (so that e, e', e'' are of order 2 and linearly independent over $\mathbb{Z}/2\mathbb{Z}$), let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 2$, and let $W \geq 1$. We say that a tuple $(\alpha_w)_{w=1, \dots, W}$ of functions $\alpha_1, \dots, \alpha_W: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ obeys the *compatible boolean property* P (with parameters e, e', e'') if each α_i is $\langle e', e'' \rangle$ -periodic (thus $\alpha_i(x + e') = \alpha_i(x + e'') = \alpha_i(x)$ for all $x \in G$) and $(e, \{a_i, b_i\})$ -boolean for some $a_i, b_i \in \mathbb{Z}/2^M\mathbb{Z}$ of different

parity, and additionally that the α_i are compatible (i.e., the $\{a_i, b_i\}$ are translates of each other).

We can exploit Lemma 6.5 as follows.

Proposition 6.5 (Expressing multiple compatible boolean functions). *The compatible boolean property P is a weakly expressible $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1,\dots,W})$ -property.*

Proof. For sake of notation we just demonstrate this for $W = 2$; the general case is similar, and in any event follows from the $W = 2$ case by applying Lemma 4.20 in a similar spirit to Example 4.16.

Let $\alpha_1, \alpha_2: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ be functions. We introduce some auxiliary functions

$$\beta_1, \beta_2, \gamma_1, \gamma_2, \tau', \tau'': G \rightarrow \mathbb{Z}/2^M\mathbb{Z}.$$

Consider the $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1,\dots,8})$ -property P^* that the tuple $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \tau', \tau'')$ obeys the following properties for $i = 1, 2$:

- (i) α_i is $\langle e', e'' \rangle$ -periodic and $(e, \{a_i, b_i\})$ -boolean for some $a_i, b_i \in \mathbb{Z}/2^M\mathbb{Z}$ of different parity.
- (ii) β_i is $(e, \{c_i, d_i\})$ -boolean for some $c_i, d_i \in \mathbb{Z}/2^M\mathbb{Z}$ of different parity.
- (iii) γ_i is $(e, \{f_i, g_i\})$ -boolean for some $f_i, g_i \in \mathbb{Z}/2^M\mathbb{Z}$ of different parity.
- (iv) τ' is $\langle e + e', e'' \rangle$ -periodic and $(e, \{h', k'\})$ -boolean for some $h', k' \in \mathbb{Z}/2^M\mathbb{Z}$ of different parity.
- (v) τ'' is $\langle e', e + e'' \rangle$ -periodic and $(e, \{h'', k''\})$ -boolean for some $h'', k'' \in \mathbb{Z}/2^M\mathbb{Z}$ of different parity.
- (vi) There is a constant $z_i \in \mathbb{Z}/2^M\mathbb{Z}$ such that $\alpha_i(x) + \tau'(x) + \tau''(x) = 2\beta_i(x) + \gamma_i(x) + z_i$ for all $x \in G$.

From several applications of Corollary 5.4, Corollary 5.5, Proposition 6.2, and Lemma 4.20 we already know that P^* is expressible. To conclude the proposition, it suffices to show that the compatible boolean property P is the existential quantification of P^* .

We first show that any pair (α_1, α_2) obeying the compatible boolean property P can be lifted to a octuplet $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \tau', \tau'')$ obeying P^* . By hypothesis and Definition 6.4, each α_i is already $\langle e', e'' \rangle$ -periodic and $(e, \{a_i, b_i\})$ -boolean, where $a_i, b_i \in \mathbb{Z}/2^M\mathbb{Z}$ are of different parity and with α_1, α_2 compatible. By applying independent translations to the compatible boolean functions α_1, α_2 (which we can do by Remark 4.9), we may normalize $\{a_1, b_1\} = \{a_2, b_2\} = \{0, b\}$ for some odd $b \in \mathbb{Z}/2^M\mathbb{Z}$. Next, let τ' be an arbitrary $\langle e + e', e'' \rangle$ -periodic and $(e, \{0, b\})$ -boolean function; such a function can be constructed by arbitrarily partitioning G into cosets $x + \langle e, e', e'' \rangle$ with a marked point x and then setting

$$\tau(x + re + se' + te'') = b1_{r=s}$$

on each such coset for $r, s, t \in \mathbb{Z}/2\mathbb{Z}$. Similarly we can let τ'' be an arbitrary $\langle e', e + e'' \rangle$ -periodic and $(e, \{0, b\})$ -boolean function. For each $i = 1, 2$, the function $\alpha_i + \tau' + \tau''$ then takes values in $\{0, b, 2b, 3b\}$, and obeys the alternating property

$$(\alpha_i + \tau' + \tau'')(x + e) = 3b - (\alpha_i + \tau' + \tau'')(x)$$

for all $x \in G$. Note also that the quantities $0, b, 2b, 3b$ are all distinct since b is odd and $M \geq 2$. By binary expansion, we may thus decompose

$$(\alpha_i + \tau' + \tau'')(x) = 2\beta_i(x) + \gamma_i(x)$$

for some unique functions $\beta_i, \gamma_i: G \rightarrow \{0, b\}$. It is easy to verify that these functions are $(e, \{0, b\})$ -boolean, and so the octuplet $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \tau, \tau')$ obeys P^* as required (with $z_i = 0$ in (vi)).

Conversely, suppose that we have an octuplet $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \tau, \tau')$ obeying property P^* . Applying (vi) to x and $x + e$ and summing, we have

$$\sum_{y=x, x+e} (\alpha_i(y) + \tau'(y) + \tau''(y)) = \sum_{y=x, x+e} (2\beta_i(y) + \gamma_i(y)) + 2z_i$$

for any $x \in G$ and $i = 1, 2$. Using the boolean nature of the functions $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \tau, \tau'$ in the direction e , we conclude that

$$(a_i + b_i) + (h' + k') + (h'' + k'') = 2(c_i + d_i) + (f_i + g_i) + 2z_i$$

for $i = 1, 2$.

Let $i = 1, 2$. By (i), (iv), (v), we see that for any $x \in G$, the triple $(\alpha_i(x), \tau'(x), \tau''(x))$ takes values in the eight-element set $\{a_i, b_i\} \times \{h', k'\} \times \{h'', k''\}$. Furthermore, shifting x by e' changes the value of $\tau'(x)$ but not $\alpha(x), \tau''(x)$; shifting x by e'' changes the value of $\tau''(x)$ but not $\alpha(x), \tau'(x)$; and shifting x by $e + e' + e''$ changes the value of $\alpha_i(x)$ but not $\tau'(x), \tau''(x)$. We conclude that all eight of the elements of $\{a_i, b_i\} \times \{h', k'\} \times \{h'', k''\}$ are actually representable in the form $(\alpha_i(x), \tau'(x), \tau''(x))$ for some $x \in G$. By (vi), we conclude that every element (α_i, τ, τ') of $\{a_i, b_i\} \times \{h', k'\} \times \{h'', k''\}$ has a representation $\alpha_i + \tau + \tau' = 2\beta_i + \gamma_i + z_i$ for some $(\beta_i, \gamma_i) \in \{c_i, d_i\} \times \{f_i, g_i\}$. We can now apply Lemma 6.3 to conclude that $\{a_i, b_i\}, \{h', k'\}, \{h'', k''\}$ must be translates of each other. Thus, both α_1, α_2 are compatible with the τ', τ'' . By transitivity, this implies that α_1 is compatible with α_2 , and hence the compatible boolean property P holds as required. \square

Let G, M, e, e', e'' be as in the above proposition. If $\alpha_1, \dots, \alpha_W: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ obey the compatible boolean property, then (after permuting a_i, b_i as necessary) each α_i is $\langle e', e'' \rangle$ -invariant and is $(e, \{a_i, a_i + b\})$ -boolean for some $a_i \in \mathbb{Z}/2^M\mathbb{Z}$ and some odd b independent of i . Thus we have representations

$$\alpha_i(x) = a_i + b\tilde{\alpha}_i(x) \tag{6.7}$$

for all $x \in G$ and $i = 1, \dots, W$, where the normalized boolean functions $\tilde{\alpha}_i: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ are $\langle e', e'' \rangle$ -invariant and $(e, \{0, 1\})$ -boolean. Note that the a_i, b are only unique up to the reflection symmetry

$$(a_1, \dots, a_W, b) \mapsto (a_1 + b, \dots, a_W + b, -b)$$

which effectively replaces the normalized boolean functions $\tilde{\alpha}_i$ with their reflections $1 - \tilde{\alpha}_i$.

Let Ω be a subset of $\{0, 1\}^W$ which is symmetric with respect to the reflection

$$(y_1, \dots, y_W) \mapsto (1 - y_1, \dots, 1 - y_W).$$

We say that a $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1, \dots, W})$ -function $(\alpha_1, \dots, \alpha_W)$ obeys property P_Ω if it obeys the compatible boolean property P , and furthermore that the normalized functions $\tilde{\alpha}_1, \dots, \tilde{\alpha}_W$ obey the boolean constraint

$$(\tilde{\alpha}_1(x), \dots, \tilde{\alpha}_W(x)) \in \Omega$$

for all $x \in G$. Note that from the symmetry hypothesis, it does not matter which of the two available normalizations $\tilde{\alpha}_i$ of the α_i are used here. Importantly, such relations are weakly expressible when M is large enough:

Proposition 6.6 (Expressing symmetric boolean constraints). *Let G be a finitely generated abelian group, let e, e', e'' be elements of G that generate a copy of $(\mathbb{Z}/2\mathbb{Z})^3$, let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 2$, and let $W \geq 1$. Let Ω be a symmetric subset of $\{0, 1\}^W$. If $2^M > 2W + 4$, then the $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1, \dots, W})$ -property P_Ω is weakly expressible.*

Proof. This will be a variant of the arguments in [GT21, §6]. By increasing W by one or two if necessary (and relaxing $2^M > 2W + 4$ to $2^M > 2W$) using Lemma 4.20(iv), we may assume without loss of generality that W is odd with $W \geq 3$. The symmetric set Ω can be expressed as the intersection of a finite number of symmetric sets of the form

$$\{0, 1\}^W \setminus \{(\epsilon_1, \dots, \epsilon_W), (1 - \epsilon_1, \dots, 1 - \epsilon_W)\} \quad (6.8)$$

for some $\epsilon_1, \dots, \epsilon_W \in \{0, 1\}$. By Lemma 4.20(iii), it thus suffices to verify the claim for Ω of the form (6.8).

We introduce some auxiliary functions $\beta_1, \dots, \beta_{W-2}: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$, and let P_Ω^* be the $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1, \dots, 2W-2})$ -property that a tuple $(\alpha_1, \dots, \alpha_W, \beta_1, \dots, \beta_{W-2})$ of functions from G to $\mathbb{Z}/2^M\mathbb{Z}$ obey the following properties:

- (i) $(\alpha_1, \dots, \alpha_W, \beta_1, \dots, \beta_{W-2})$ obeys the compatible boolean property P (with W replaced by $2W - 2$);
- (ii) There is a constant $z \in \mathbb{Z}/2^M\mathbb{Z}$ such that

$$(-1)^{\epsilon_1} \alpha_1(x) + \dots + (-1)^{\epsilon_W} \alpha_W(x) = \beta_1(x) + \dots + \beta_{W-2}(x) + z$$

for all $x \in G$.

From Proposition 6.5, Corollary 5.5, and Lemma 4.20, the property P_Ω^* is weakly expressible. By Lemma 4.20(iv), it thus suffices to show that P_Ω is the existential quantification of P_Ω^* .

We first show that any tuple $(\alpha_1, \dots, \alpha_W)$ obeying P_Ω can be extended to a tuple $(\alpha_1, \dots, \alpha_W, \beta_1, \dots, \beta_{W-2})$ obeying P_Ω^* . By hypothesis, we can write the α_i in the form (6.7) for some $a_i, b \in \mathbb{Z}/2^M\mathbb{Z}$ with b odd, and some $(e, \{0, 1\})$ -boolean and $\langle e', e'' \rangle$ -periodic functions $\tilde{\alpha}_1, \dots, \tilde{\alpha}_W: G \rightarrow \{0, 1\}$. In particular

$$(-1)^{\epsilon_1} \alpha_1 + \dots + (-1)^{\epsilon_W} \alpha_W = b(\tilde{\alpha}_{1, \epsilon_1} + \dots + \tilde{\alpha}_{W, \epsilon_W}) + z_0$$

for some constant $z_0 \in \mathbb{Z}/2^M\mathbb{Z}$, where $\tilde{\alpha}_{i, \epsilon_i}: G \rightarrow \{0, 1\}$ is the $(e, \{0, 1\})$ -boolean and $\langle e', e'' \rangle$ -periodic function $R_{\epsilon_i}(\tilde{\alpha}_i)$, where for $a = 0, 1$

$$R_a(x) := a + (-1)^a x, \quad x \in G. \quad (6.9)$$

By the choice (6.8) of Ω , we see that for every x , the tuple $(\tilde{\alpha}_{1, \epsilon_1}(x), \dots, \tilde{\alpha}_{W, \epsilon_W}(x))$ is an element of the cube $\{0, 1\}^W$ that avoids both $(0, \dots, 0)$ and $(1, \dots, 1)$. In particular, we have

$$\tilde{\alpha}_{1, \epsilon_1}(x) + \dots + \tilde{\alpha}_{W, \epsilon_W}(x) = bf(x)$$

for some $f(x) \in \{1, \dots, W - 1\}$, which is well-defined since the odd element b of $\mathbb{Z}/2^M\mathbb{Z}$ has order $2^M > 2W$; note that f is $\langle e', e'' \rangle$ -periodic and obeys the alternating property $f(x + e) = W - f(x)$ for all $x \in G$. We can therefore write

$$b(\tilde{\alpha}_{1, \epsilon_1}(x) + \dots + \tilde{\alpha}_{W, \epsilon_W}(x)) = \beta_1(x) + \dots + \beta_{W-2}(x) + b$$

for all $x \in G$, where $\beta_i(x)$ for $i = 1, \dots, W - 2$ is defined by

$$\beta_i(x) := b1_{i < f(x)}$$

if $f(x) < W/2$ and

$$\beta_i(x) := b1_{i \geq W - f(x)}$$

if $f(x) > W/2$. The reason for this rather complicated choice of β_i is so that β_i becomes a $(e, \{0, b\})$ -boolean and $\langle e', e'' \rangle$ -invariant function (in particular one has $\beta_i(x + e) = b - \beta_i(x)$ for all $x \in G$). It is then a routine matter to verify that $(\alpha_1, \dots, \alpha_W, \beta_1, \dots, \beta_{W-2})$ obeys property P_Ω as required.

Conversely, suppose that $(\alpha_1, \dots, \alpha_W, \beta_1, \dots, \beta_{W-2})$ obeys the property P_Ω^* . By property (i), we may write $\alpha_i = a_i + b\tilde{\alpha}_i$ and $\beta_i = c_i + b\tilde{\beta}_i$ for some $a_i, c_i, b \in \mathbb{Z}/2^M\mathbb{Z}$ with b odd and some $\langle e', e'' \rangle$ -invariant and $(e, \{0, 1\})$ -boolean functions $\tilde{\alpha}_1, \dots, \tilde{\alpha}_W, \tilde{\beta}_1, \dots, \tilde{\beta}_{W-2}: G \rightarrow \{0, 1\}$. Inserting these representations into (ii), we see that there exists a constant $z_0 \in \mathbb{Z}/2^M\mathbb{Z}$ such that

$$\tilde{\alpha}_{1, \epsilon_1}(x) + \dots + \tilde{\alpha}_{W, \epsilon_W}(x) = \tilde{\beta}_1(x) + \dots + \tilde{\beta}_{W-2}(x) + z_0$$

for all $x \in G$, where $\tilde{\alpha}_{i, \epsilon_i}$ is defined by $R_{\epsilon_i}(\tilde{\alpha}_i)$ and (6.9). Summing over x and $x + e$ and using the $(e, \{0, 1\})$ -boolean nature of the $\tilde{\alpha}_{i, \epsilon_i}$ and $\tilde{\beta}_i$, we conclude that

$$W = W - 2 + 2z_0$$

and hence z_0 is equal to 1 or $2^{M-1} + 1$. On the other hand, since $\tilde{\alpha}_{i, \epsilon_i}, \tilde{\beta}_i$ take values in $\{0, 1\}$, z_0 must take values in $\{-W + 2, \dots, W\}$ modulo 2^M . Since $2^{M-1} > W$, we must therefore have $z_0 = 1$. In particular, $\tilde{\alpha}_{1, \epsilon_1} + \dots + \tilde{\alpha}_{W, \epsilon_W}$ takes values in $\{1, \dots, W - 1\}$, and hence $(\tilde{\alpha}_{1, \epsilon_1}, \dots, \tilde{\alpha}_{W, \epsilon_W})$ cannot be $(0, \dots, 0)$ or $(1, \dots, 1)$. This implies that $(\alpha_1, \dots, \alpha_W)$ obeys the property P_Ω , and we are done. \square

We need a variant of the above proposition which involves a modification of Example 4.7 that is compatible⁷ with the alternating relation (6.1). We again let G, M, e, e', e'' be as in Proposition 6.5, and suppose that $\alpha_1, \dots, \alpha_W: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ obey the compatible boolean property P , so as before we have a representation (6.7), unique up to reflection symmetry.

Definition 6.7 (Boolean periodized permutation). If $v \in G$, we say that a tuple $(\alpha_1, \dots, \alpha_W)$ is a *boolean periodized permutation* along the direction v if it obeys the compatible boolean property P , and for each $x \in G$, the map

$$j \mapsto (\tilde{\alpha}_1(x + jv), \dots, \tilde{\alpha}_W(x + jv))$$

is a bijection from $\{0, \dots, 2^W - 1\}$ to $\{0, 1\}^W$

Note that the boolean periodized permutation property is preserved under reflection symmetry and is therefore well-defined. Comparing this claim with the corresponding claim with x replaced by $x + v$, we see that the boolean periodized permutation property implies in particular that

$$(\tilde{\alpha}_1(x + 2^W v), \dots, \tilde{\alpha}_W(x + 2^W v)) = (\tilde{\alpha}_1(x), \dots, \tilde{\alpha}_W(x))$$

and hence each of the $\tilde{\alpha}_i$ (or α_i) are $\langle 2^W v \rangle$ -periodic.

Proposition 6.8 (Expressing a boolean periodized permutation). *Let G be a finitely generated abelian group, let e, e', e'' be elements of G that generate a copy of $(\mathbb{Z}/2\mathbb{Z})^3$, let $\mathbb{Z}/2^M\mathbb{Z}$ be a cyclic 2-group for some $M \geq 2$, let $W \geq 1$, and let $v \in G$. Then the property of being a boolean periodized permutation along the direction v is a weakly expressible $(G, (\mathbb{Z}/2^M\mathbb{Z})_{w=1, \dots, W})$ -property.*

⁷The simpler clock property from Example 4.6 is unsuitable for this purpose due to its incompatibility with (6.1), but the reader is encouraged to think of the periodized permutation property as technical substitute for the clock property.

Proof. We can assume that v has order at least W , otherwise the property is impossible to satisfy. We claim that a tuple $(\alpha_1, \dots, \alpha_W)$ obeys the boolean periodized permutation property along v if and only if it obeys the compatible boolean property P and additionally solves the functional equation

$$\bigoplus_{j=0}^{2^W-1} (\alpha_1(x+jv), \dots, \alpha_W(x+jv)) + (2\mathbb{Z}/2^M\mathbb{Z})^W = (\mathbb{Z}/2^M\mathbb{Z})^W \quad (6.10)$$

for all x . The equation (6.10) defines an expressible property by definition (the ju are all distinct as v has order at least W), and so the proposition will follow from this claim, Proposition 6.5, and Lemma 4.20.

It remains to verify the claim. If $(\alpha_1, \dots, \alpha_W)$ is a boolean periodized permutation along v , then it obeys P , and the 2^W tuples $(\tilde{\alpha}_1(x+jv), \dots, \tilde{\alpha}_W(x+jv))$, $j = 0, \dots, 2^W - 1$ occupy distinct points in $\{0, 1\}^W$. Since $\alpha_w(x+jv) = a_i + b\tilde{\alpha}_w(x+jv)$ and b is odd, we conclude that the 2^W tuples $(\alpha_1(x+jv), \dots, \alpha_W(x+jv))$ occupy distinct cosets of $(2\mathbb{Z}/2^M\mathbb{Z})^W$. Since there are only 2^W such cosets, this gives (6.10). The converse implication follows by reversing these steps. \square

7. PROGRAMMING A SUDOKU PUZZLE

We now combine the various weakly expressible statements described in the previous section to reduce matters to demonstrating aperiodicity of a certain type of “Sudoku puzzle”. To define this puzzle we need some notation.

7.1. A 2-adically structured function. We begin the construction of the “Sudoku puzzle”. We henceforth fix a base $q = 2^{s_0}$, which will be a sufficiently large but constant power of two (for instance $s_0 = 10$, $q = 2^{10}$ would suffice). In particular, the reader should interpret any exceptional set of (upper) density $O(1/q)$ as being negligible in size. We define the *digit set* Σ to be the finite set

$$\Sigma := (\mathbb{Z}/q\mathbb{Z}) \setminus \{0\}.$$

We need a large width N depending on q ; one convenient choice to take will be

$$N := q^2,$$

although our arguments would also work *mutatis mutandis* for larger choices of N . We then define the *Sudoku board*

$$\mathbb{B} := \{1, \dots, N\} \times \mathbb{Z}.$$

Elements (n, m) of this board will be referred to as *cells*. We isolate some collections of cells of relevance to our arguments:

- A *column* is a set of cells of the form $\{n\} \times \mathbb{Z}$ for some $1 \leq n \leq N$.
- A *non-vertical line* $\ell = \ell_{i,j}$ is a set of cells of the form

$$\ell_{i,j} := \{(n, jn + i) : 1 \leq n \leq N\}$$

for some *slope* $j \in \mathbb{Z}$ and *intercept* $i \in \mathbb{Z}$.

- A *row* is a non-vertical line of slope 0, that is to say a set of cells of the form $\{1, \dots, N\} \times \{m\}$ for some $m \in \mathbb{Z}$.
- A *diagonal* is a non-vertical line of slope 1, that is to say a set of cells of the form $\{(n, n + i) : 1 \leq n \leq N\}$ for some $i \in \mathbb{Z}$.
- An *anti-diagonal* is a non-vertical line of slope -1 , that is to say a set of cells of the form $\{(n, i - n) : 1 \leq n \leq N\}$ for some $i \in \mathbb{Z}$.

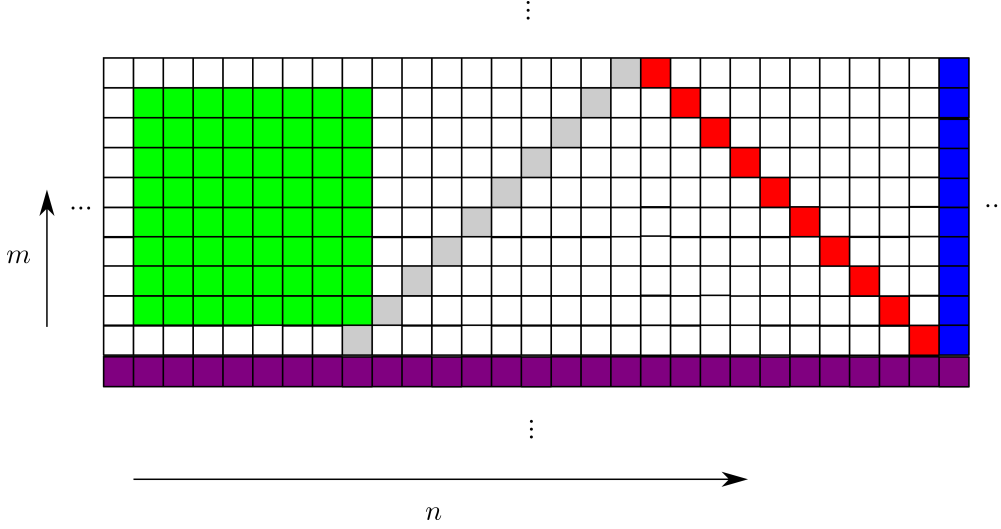


FIGURE 7.1. A portion of the Sudoku board Ω , with some selected (overlapping) objects: a column (in blue), a row (in purple), a diagonal (in gray), an antidiagonal (in red), and a square (in green).

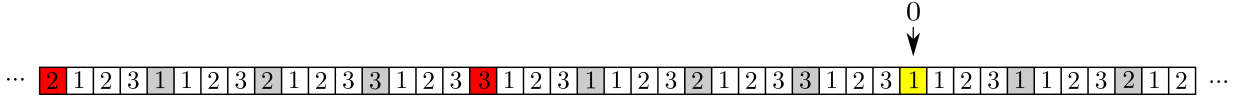


FIGURE 7.2. The function f_q for $q = 2^2$. The white cells correspond to $n \in \mathbb{Z} \setminus q\mathbb{Z}$, the gray cells are those with $n \in q\mathbb{Z} \setminus q^2\mathbb{Z}$ and , the red ones have $n \in q^2\mathbb{Z} \setminus q^3\mathbb{Z}$ and yellow indicates $n = 0$. Compare with the example of a limit-periodic pattern in [ST12, Figure 3].

- A square Q_{n_0, m_0} is a set of cells of the form

$$Q_{n_0, m_0} := \{n_0, \dots, n_0 + 7\} \times \{m_0, \dots, m_0 + 7\} \quad (7.1)$$

for some $1 \leq n_0 \leq N - 7$ and $m_0 \in \mathbb{Z}$.

See Figure 7.1.

The Sudoku puzzle that we will introduce later will be solved by filling in the cells (n, m) of the Sudoku board \mathbb{B} with digits $F(i, j)$ from Σ that obey certain permutation-like constraints along the lines of this board. This may be compared with a traditional Sudoku puzzle, in which the digit set is $\{1, \dots, 9\}$, the board is $\{1, \dots, 9\}^2$, and the constraints are that the digit assignment is a permutation on every row and column of the puzzle, as well as certain 3×3 squares in the board, and also agrees with some prescribed initial data on certain cells. We note, however, that while traditional Sudoku puzzles are designed to have a *unique* solution, the Sudoku puzzle that we will study will have a number of solutions, though all have a similar *2-adic structure* as described below.

We now introduce a “basic 2-adically structured function” $f_q: \mathbb{Z} \rightarrow \Sigma$, defined by the formula

$$f_q(q^k m) := m \pmod{q}$$

whenever $k \geq 0$ and m is an integer not divisible by q , with the (somewhat arbitrary) convention that $f_q(0) = 1$. In other words, $f_q(n)$ is the last non-zero digit in the base q expansion of n , or 1 if no such digit exists (see Figure 7.2).

3	2	1	2	3	2	1	1	3	2	1	1	3	2	1	3
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

FIGURE 7.3. An element $g(n) = f_4(12 - n)$ of $\mathcal{S}_4[16]$, depicted as a row of $N = 16$ boxes filled with digits in $\Sigma = \{1, 2, 3\}$. In the language of Lemma 8.1 below, the step is $s_g = 3 \pmod{q}$, the order ord_g is zero, the bad coset $\Gamma_g = 4\mathbb{Z}$ is the set of shaded boxes (which in this case has upper density $1/4$), and the associated affine function $\alpha_g(n) = 12 - n \pmod{4}$ vanishes on the bad coset Γ_g and agrees with g outside of that coset.

We observe the functional equations

$$f_q(qn) = f_q(n) \quad (7.2)$$

for all $n \in \mathbb{Z}$

$$f_q(n) = n \pmod{q} \quad (7.3)$$

when n is not divisible by q ; indeed, these equations specify f_q uniquely except for the value at zero. We also observe the multiplicativity property

$$f_q(an) = af_q(n) \quad (7.4)$$

whenever $a, n \in \mathbb{Z}$ with a odd and n non-zero.

Remark 7.1. The function $f_q: \mathbb{Z} \rightarrow \Sigma$ is an example of a *limit-periodic function* [G89, ST12] (so is in particular an *almost periodic function* in the sense of Besicovitch [B26]): for any natural number r , f_q agrees with a q^r -periodic function outside of a single coset $0 + q^r\mathbb{Z}$ of $q^r\mathbb{Z}$, so in particular it agrees with a periodic function outside of a set of arbitrarily small upper density in \mathbb{Z} . For s_0 large, this function is also “approximately affine” in the sense that it agrees with the affine map $n \mapsto n \pmod{q}$ outside of a single coset $0 + q\mathbb{Z}$ of $q\mathbb{Z}$, which one should view as being a relatively small (though still positive density) subset of the integers \mathbb{Z} .

Remark 7.2. One could extend f_q to a function $f_q: \mathbb{Z}_2 \rightarrow \Sigma$ on the 2-adics $\mathbb{Z}_2 := \varprojlim_{r \rightarrow \infty} \mathbb{Z}/2^r\mathbb{Z}$ (or equivalently, the q -adics $\mathbb{Z}_q := \varprojlim_{r \rightarrow \infty} \mathbb{Z}/q^r\mathbb{Z}$) which is continuous away from the origin (and has a “piecewise affine” structure). As such, we will informally think of the function f_2 (as well as various rescaled versions of this function) as having “2-adic structure”. However, we will not explicitly use the 2-adic numbers \mathbb{Z}_2 in our arguments below, as we did not find that the use of this number system gives any significant simplifications to the argument.

Our *Sudoku puzzle* is to fill the board \mathbb{B} in such a way that every non-vertical line (but not necessarily column) is a rescaled version of f_q . To make this precise we introduce the following class of finite sequences.

Definition 7.3 (A class of 2-adically structured functions). Let $\mathcal{S}[N] = \mathcal{S}_q[N]$ denote the set of all functions $g: \{1, \dots, N\} \rightarrow \Sigma$ which take the form

$$g(n) = cf_q(an + b)$$

for all $m = 1, \dots, N$ and some integers $a, b, c \in \mathbb{Z}$ with c odd.

See Figures 7.3, 7.4, 7.5, 7.6 for some examples of elements of $\mathcal{S}[N]$, where we set $q = 2^2$ (and hence $N = 16$) in order to make the figures small. The scaling factor c is of little significance and will often be normalized to 1 in our arguments.

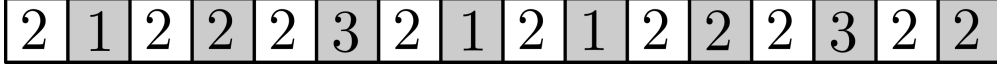


FIGURE 7.4. Another element $g(n) = f_4(2(n - 8))$ of $\mathcal{S}_4[16]$. In the language of Lemma 8.1 below, the step is $s_g = 2 \pmod{q}$, the order ord_g is one, the bad coset $\Gamma_g = 2\mathbb{Z}$ is the set of shaded boxes (which in this case has upper density $1/2$), and the associated affine function $\alpha_g(n) = 2n \pmod{4}$ vanishes on the bad coset Γ_g and agrees with g outside of that coset.

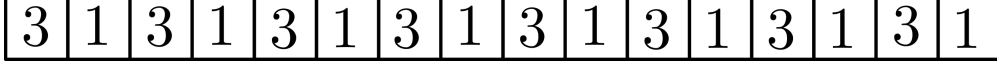


FIGURE 7.5. A third element $g(n) = f_4(2n + 1)$ of $\mathcal{S}_4[16]$. In the language of Lemma 8.1 below, the step is $s_g = 2 \pmod{q}$, the order ord_g is $-\infty$, the bad coset Γ_g is empty (so has upper density 0), and the associated affine function $\alpha_g(n) = 2n + 1 \pmod{4}$ agrees with g everywhere.

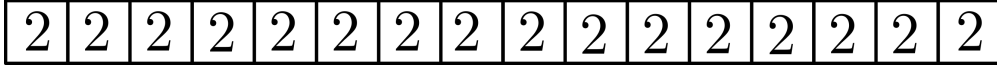


FIGURE 7.6. A constant element $g(n) = 2 \pmod{4}$ of $\mathcal{S}_4[16]$. In the language of Lemma 8.1 below, the step is 0, the order is $-\infty$, the bad coset is empty, and the associated affine function $\alpha_g(n) = 2 \pmod{4}$ agrees with g everywhere.

We will explore the properties of this class $\mathcal{S}[N]$ further in later sections. For now, we use this class to define our Sudoku puzzle.

Definition 7.4 (Sudoku puzzle). Define a *Sudoku solution* to be a function $F: \mathbb{B} \rightarrow \Sigma$ with the property that for every slope $j \in \mathbb{Z}$ and intercept $i \in \mathbb{Z}$, the function $F_{i,j}: \{1, \dots, N\} \rightarrow \Sigma$ defined by $F_{i,j}(n) := F(n, jn + i)$ lies in the class $\mathcal{S}[N]$. (See Figure 7.9.) Informally, F is a Sudoku solution if it is a rescaled copy of f_q along every non-vertical line $\ell_{i,j} = \{(n, jn + i) : 1 \leq n \leq N\}$.

A Sudoku solution is said to have *good columns* if, for every $n = 1, \dots, N$, there exists a permutation $\sigma_n: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ such that $F(n, m) = \sigma_n(m \pmod{q})$ whenever $\sigma_n(m \pmod{q})$ is non-zero.

A Sudoku solution is *periodic* if the columns $m \mapsto F(n, m)$ is periodic for all $n = 1, \dots, N$, and *non-periodic* if at least one of the columns is non-periodic.

Example 7.5 (Standard Sudoku solution). The function $F(n, m) := f_q(m)$ is a Sudoku solution with good columns (in this case, the permutations $\sigma_1, \dots, \sigma_N$ are all equal to the identity permutation. It is non-periodic. (See Figure 7.7.)

Example 7.6 (Constant Sudoku solutions). If $c \in \Sigma$, then the constant function $F(n, m) := c$ is a Sudoku solution which is periodic, but which does not have good columns.

In the remaining sections of the paper, we will prove the non-periodicity of Sudoku solutions with good columns:

⋮

2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

⋮

FIGURE 7.7. A portion of a standard Sudoku solution (with $q = 4$). Observe that it is affine outside of the shaded cells. This solution is non-periodic.

⋮

2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

⋮

FIGURE 7.8. A portion of a constant Sudoku solution (with $c = 2$). Observe that it is affine and also periodic.

Theorem 7.7 (Non-periodicity of Sudoku solutions with good columns). *Let $q = 2^{s_0}$ be sufficiently large. Then every Sudoku solution with good columns is non-periodic.*

Remark 7.8. A remarkable feature of this result is that while the property of being a Sudoku solution with good columns is “local” in the sense that it can

⋮

3	2	1	3	3	2	1	2	3	2	1	1	3	2	1	2
2	1	3	3	2	1	2	3	2	1	1	3	2	1	1	3
1	3	3	2	1	2	3	2	1	1	3	2	1	1	3	2
3	3	2	1	2	3	2	1	1	3	2	1	3	3	2	1
3	2	1	2	3	2	1	1	3	2	1	2	3	2	1	3
2	1	2	3	2	1	1	3	2	1	1	3	2	1	3	3

⋮

FIGURE 7.9. A portion of a Sudoku solution with good columns. Observe that it is affine outside of the shaded cells, and is also non-periodic.

be verified by considering a bounded number of cells of the solution at a time, the conclusion is “global” in that it genuinely involves an infinite number of cells, and is not obviously verifiable in a bounded complexity fashion. Namely, Sudoku puzzles have enough rigidity in them to achieve non-trivial constraints on the solutions, but are not so rigid that they cannot be solved. An analogous claim can be proven for odd primes q as well, and is in fact slightly simpler (for instance, the pseudo-affine functions appearing in Section 9 can be replaced by genuinely affine functions), but we will not be able to use that variant of the above theorem for our purposes, and so leave the details of this variant to the interested reader.

We assume this theorem for now and show how it implies Theorem 4.14 (and thus Theorem 1.3 and Corollary 1.6).

Proof of Theorem 4.14 assuming Theorem 7.7. We will show that Sudoku solutions with good columns can be encoded as a weakly expressible property. Assuming Theorem 7.7, this will give an aperiodic weakly expressible property, proving Theorem 4.14. Let s_0, N be such that Theorem 7.7 holds. We introduce the binary encoding map $B: \{0, 1\}^{s_0} \rightarrow \mathbb{Z}/q\mathbb{Z}$ defined by

$$B(\epsilon_0, \dots, \epsilon_{s_0-1}) := \epsilon_0 + 2\epsilon_1 + \dots + 2^{s_0-1}\epsilon_{s_0-1};$$

this is of course a bijection. In the space $\{0, 1\}^{2s_0N}$ of tuples

$$(\omega_{a,b,n})_{(a,b,n) \in \mathcal{W}}$$

of boolean variables $\omega_{a,b,n} \in \{0, 1\}$ indexed by the $2s_0N$ -element set

$$\mathcal{W} := \{0, 1\} \times \{0, \dots, s_0 - 1\} \times \{1, \dots, N\},$$

we define the subset Ω of those tuples in $\{0, 1\}^{2s_0N}$ obeying the following axioms:

- (i) (Encoded Sudoku solution) The sequence $n \mapsto B(\omega_{1,0,n}, \dots, \omega_{1,s_0-1,n})$ lies in $\mathcal{S}[N]$.

- (ii) (Encoded good columns) If $n = 1, \dots, N$ is such that $B(\omega_{0,0,n}, \dots, \omega_{0,s_0-1,n}) \neq (0, \dots, 0)$, then $B(\omega_{1,0,n}, \dots, \omega_{1,s_0-1,n}) = B(\omega_{0,0,n}, \dots, \omega_{0,s_0-1,n})$ (or equivalently that $\omega_{0,b,n} = \omega_{1,b,n}$ for $b = 0, \dots, s_0 - 1$).

This set is not symmetric, so we also introduce the symmetrized counterpart $\tilde{\Omega} \subset \{0, 1\}^{1+2s_0N}$ in $\{0, 1\}^{1+2s_0N}$ consisting of those tuples $(\omega_*, (\omega_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ such that

$$(R_{\omega_*}(\omega_{a,b,n}))_{(a,b,n) \in \mathcal{W}} \in \Omega$$

where R_a , $a = 0, 1$ is as in (6.9).

We consider the group $G := \mathbb{Z}^2 \times (\mathbb{Z}/2\mathbb{Z})^3$, which contains in particular the three elements $e := ((0, 0), (1, 0, 0))$, $e' := ((0, 0), (0, 1, 0))$, $e'' := ((0, 0), (0, 0, 1))$ which generate a copy of $(\mathbb{Z}/2\mathbb{Z})^3$. We now introduce a property S , which aims to encode Sudoku solutions with good columns. Let M be a natural number that is sufficiently large depending on s_0, N , and let S denote the $(G, (\mathbb{Z}/2^M\mathbb{Z})^{1+2s_0N})$ -property that a tuple $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ of functions $\alpha_*, \alpha_{a,b,n}: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ obey the following axioms.

- (a) $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ obeys property $P_{\tilde{\Omega}}$.
- (b) For each $a = 0, 1$; $b = 0, \dots, s_0 - 1$; $n = 1, \dots, N$, the function $\alpha_{a,b,n}$ is $\langle(-n, 1), (0, 0, 0)\rangle$ -periodic.
- (c) For each $n = 1, \dots, N$, the tuple $(\alpha_{0,0,n}, \dots, \alpha_{0,s_0-1,n})$ is a boolean periodized permutation in the direction $((1, 0), (0, 0, 0))$.

By Proposition 6.6, Corollary 5.4, Proposition 6.8, and Lemma 4.20, S is a weakly expressible property. It will thus suffice to show that S is aperiodic.

We first show that there is at least one tuple $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ obeying S . Let $F(n, m)$ be a Sudoku solution with good columns (for instance, one can take the standard Sudoku solution from Example 7.5), and let $\sigma_1, \dots, \sigma_N: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ be the associated permutations. We represent this data via the boolean functions $\beta_{a,b,n}: \mathbb{Z}^2 \rightarrow \{0, 1\}$ for $(a, b, n) \in \mathcal{W}$, defined by the binary encodings

$$B(\beta_{0,0,n}(i, j), \dots, \beta_{0,s_0-1,n}(i, j)) = \sigma_n(jn + i \pmod{q})$$

and

$$B(\beta_{1,0,n}(i, j), \dots, \beta_{1,s_0-1,n}(i, j)) = F(n, jn + i) \quad (7.5)$$

for $n = 1, \dots, N$ and $(i, j) \in \mathbb{Z}^2$. By construction, the $\beta_{a,b,n}$ are $\langle(-n, 1)\rangle$ -periodic; as σ_n is a permutation, the tuple $(\beta_{0,0,n}, \dots, \beta_{0,s_0-1,n})$ obeys the permutation property in the direction $(1, 0)$ for each $n = 1, \dots, N$. Finally, since F is a Sudoku solution with good columns, we see that the tuple $(\beta_{a,b,n}(i, j))_{(a,b,n) \in \mathcal{W}}$ lies in Ω for each $(i, j) \in \mathbb{Z}^2$. If we now define the tuple $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ of functions $\alpha_*, \alpha_{a,b,n}: G \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ by the formulae

$$\alpha_*(x, (\epsilon, \epsilon', \epsilon'')) := \epsilon$$

and

$$\alpha_{a,b,n}(x, (\epsilon, \epsilon', \epsilon'')) := R_\epsilon(\beta_{a,b,n}(x))$$

for all $x \in \mathbb{Z}^2$, $a = 0, 1$, $b = 0, \dots, s_0 - 1$, $n = 1, \dots, N$, $\epsilon, \epsilon', \epsilon'' \in \{0, 1\}$ (where R_ϵ is as in (6.9)), it is a routine matter to verify that this tuple obeys property S .

Conversely, suppose that $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ obeys S . By (a), we can write $\alpha_* = a'_* + b'\tilde{\alpha}_*$ and $\alpha_{a,b,n} = a'_{a,b,n} + b'\tilde{\alpha}_{a,b,n}$ for some $a'_*, a'_{a,b,n}, b' \in \mathbb{Z}/2^M\mathbb{Z}$ with b' odd, and some $\langle e', e'' \rangle$ -periodic $(e, \{0, 1\})$ -boolean functions $\tilde{\alpha}_*, \tilde{\alpha}_{a,b,n}: G \rightarrow \{0, 1\}$ such that

$$(\tilde{\alpha}_*(\tilde{x}), (\tilde{\alpha}_{a,b,n}(\tilde{x}))_{(a,b,n) \in \mathcal{W}}) \in \tilde{\Omega} \quad (7.6)$$

for all $\tilde{x} \in G$. If we define the functions $\beta_{a,b,n}: \mathbb{Z}^2 \rightarrow \{0,1\}$ by the formula

$$\beta_{a,b,n}(x) := R_{\tilde{\alpha}_*(x,(0,0,0))}(\tilde{\alpha}_{a,b,n}(x,(0,0,0)))$$

for all $(a,b,n) \in \mathcal{W}$, $x \in \mathbb{Z}^2$, we have

$$(\beta_{a,b,n}(x))_{(a,b,n) \in \mathcal{W}} \in \Omega \quad (7.7)$$

for all $x \in \mathbb{Z}^2$. From axiom (b) we see that each $\beta_{a,b,n}$ is $(-n,1)$ -periodic, and from axiom (c) we see that for each $n = 1, \dots, N$, the tuple $(\beta_{0,0,n}, \dots, \beta_{0,s_0-1,n})$ is a boolean periodized permutation in the direction $(1,0)$. From the $(-n,1)$ -periodicity of the $\beta_{a,b,n}$, we may define functions $F_a: \mathbb{B} \rightarrow \mathbb{Z}/2^M\mathbb{Z}$ for $a = 0, 1$ by requiring that

$$B(\beta_{a,0,n}(i,j), \dots, \beta_{a,s_0-1,n}(i,j)) = F_a(n, jn + i)$$

for all $n = 1, \dots, N$ and $(i,j) \in \mathbb{Z}^2$. From (7.7) we see that F_1 is a Sudoku solution (in particular, it avoids zero and takes values in Σ), and also that $F_1(n,m) = F_0(n,m)$ whenever $F_0(n,m)$ is non-zero. Since $(\beta_{0,0,n}, \dots, \beta_{0,s_0-1,n})$ is a boolean periodized permutation in the direction $(1,0)$, we see that for all $(n,m) \in \mathbb{B}$, the q points $F_0(n,m), \dots, F_0(n, m+q-1)$ take on distinct values of $\mathbb{Z}/q\mathbb{Z}$, and thus we must have $F_0(n,m) = \sigma_n(m \pmod q)$ for some permutation $\sigma_n: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ (cf. Example 4.7). Thus F_1 has good columns, and is thus non-periodic thanks to Theorem 7.7. If $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ were periodic, F_1 would be periodic. We then conclude that $(\alpha_*, (\alpha_{a,b,n})_{(a,b,n) \in \mathcal{W}})$ is non-periodic. Thus, property S is aperiodic as required. \square

Remark 7.9. The encoding (7.5) resembles the classical projective duality between points and lines in the plane. Indeed, a non-vertical line $\ell_{i,j} = \{(n, jn + i) : n = 1, \dots, N\}$ in the Sudoku board \mathbb{B} corresponds to a point (i,j) in the lattice \mathbb{Z}^2 .

It remains to prove Theorem 7.7. This is the objective of the remaining sections of the paper.

8. BASIC PROPERTIES OF 2-ADIC STRUCTURED FUNCTIONS AND SUDOKU SOLUTIONS

We begin by analyzing the class $\mathcal{S}[N]$ defined in Definition 7.3. We can largely describe the behavior of an element g of $\mathcal{S}[N]$ by some statistics which we call the “order”, “step”, “bad coset”, and “associated affine function” of g .

Lemma 8.1 (Statistics of a 2-adic function). *To every $g \in \mathcal{S}[N]$ one can find an order $\text{ord}_g \in \{-\infty, 0, \dots, s_0 - 1\}$, a step $s_g \in \mathbb{Z}/q\mathbb{Z}$, a bad coset $\Gamma_g \subset \mathbb{Z}$, and an associated affine function $\alpha_g: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$, obeying the following axioms:*

- (i) $\alpha_g: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ is not identically zero, and is a function of the form $\alpha_g(n) = s_g n + c_g$ for some $c_g \in \mathbb{Z}/q\mathbb{Z}$, for all $n \in \mathbb{Z}$, thus the step s_g is the slope of the affine function α_g .
- (ii) The bad coset $\Gamma_g \subsetneq \mathbb{Z}$ is the zero set $\{n \in \mathbb{Z} : \alpha_g(n) = 0\}$ of α_g ; it is empty if $\text{ord}_g = -\infty$, and is a coset of $2^{-\text{ord}_g}q\mathbb{Z}$ otherwise. (In particular, the upper density of Γ_g is equal to $2^{\text{ord}_g}/q$, and if $\text{ord}_g \geq 0$, then s_g is an odd multiple of 2^{ord_g} .)
- (iii) One has $g(n) = \alpha_g(n)$ whenever $\alpha_g(n) \neq 0$; in other words, g agrees with the affine function α_g outside of the bad coset Γ_g .

- (iv) One can find integers $a, b \in \mathbb{Z}$ such that $\alpha_g(n) = an + b \pmod{q}$ and $g(n) = f_q(an + b)$ for all $n \in \mathbb{Z}$. (In particular, this implies that $a = s_g \pmod{q}$, so if $\text{ord}_g \geq 0$, a is an odd multiple of 2^{ord_g} and b is divisible by 2^{ord_g} .)

See Figures 7.3, 7.4, 7.5, 7.6 for some illustrations of these statistics. We remark that the elements of $\mathcal{S}[N]$ of very high order (close to s_0) will be problematic for our analysis, because the bad coset has large upper density in those cases; fortunately, we will be able to show that this case occurs quite rarely for our applications.

Proof. If $g \in \mathcal{S}[N]$, then by definition there exist integers a, b, c with c odd such that $g(n) = cf_q(an + b)$. Since $f_q(0n + 0) = f_q(0n + 1) = 1$, we may assume without loss of generality that a, b do not both vanish. Noting that $f_q(an + b) = f_q(a(n + q^r) + b)$ for all $n = 1, \dots, N$ if r is large enough, we may assume without loss of generality that $an + b$ is non-vanishing on $\{1, \dots, N\}$. By (7.4), we may replace a, b, c by $ca, cb, 1$ and assume without loss of generality that $c = 1$. By (7.2) we may assume that a, b are not simultaneously divisible by q .

We then set $\alpha_g(n) := an + b \pmod{q}$, $s_g := a \pmod{q}$, $\Gamma_g := \{n \in \mathbb{Z} : \alpha_g(n) = 0\}$. If Γ_g is empty we set $\text{ord}_g = -\infty$, otherwise we set ord_g equal to the largest number of powers of two that divide a . (This order cannot exceed $s_0 - 1$, otherwise α_g would be constant and non-zero, and so Γ_g would be empty). The verification of the axioms (i)-(iv) is then routine. \square

In principle, it is possible that the order ord_g , step s_g , bad coset Γ_g , or associated affine function α_g produced by this lemma are not unique, because there are multiple ways to express g in the form $f_q(an + b)$. For instance, for $n = 1, \dots, N$, the function $f_q(n)$ can also be written as $f_q(n + q^m)$ for any m with $q^m > N$, or as $f_q(q^r n)$ for any $r \geq 1$. We will be able to exclude this scenario, thanks to (a modification of) the following useful proposition.

Proposition 8.2 (Rigidity outside of a bad coset). *Let $\{n_0, \dots, n_0 + 7\}$ be an interval of length 8 in $\{1, \dots, N\}$, and let $\alpha: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ be an affine function. Suppose that $g(n) = f_q(an + b)$ is an element of $\mathcal{S}[N]$ such that $g(n) = \alpha(n)$ whenever $n \in \{n_0, \dots, n_0 + 7\}$ is such that $\alpha(n) \neq 0$. Then in fact we have $g(n) = \alpha(n)$ whenever $n \in \{1, \dots, N\}$ and $\alpha(n) \neq 0$.*

We caution that while the conclusion of this proposition strongly suggests that $\alpha_g = \alpha$, and the proof below will support this claim in most cases, there are a few cases in which this is not actually true. For instance, if $g(n) = f_q(0n + \frac{q}{2}) = \frac{q}{2}$, then g agrees with the affine function $\alpha(n) := \frac{q}{2}n \pmod{q}$ whenever $\alpha(n) \neq 0$, but $\alpha_g(n) = \frac{q}{2}$ is not the same function as α .

Proof. By definition, we can write (possibly non-uniquely)

$$g(n) = f_q(an + b)$$

and $\alpha_g(n) = an + b \pmod{q}$ for some $a, b \in \mathbb{Z}$, for all $n \in \mathbb{Z}$.

We may assume that α does not vanish identically, as the claim is vacuously true otherwise. We set $\Gamma := \{n \in \mathbb{Z} : \alpha(n) = 0\}$ to be the zero set of α ; this is either empty, or a coset of $2^j\mathbb{Z}$ for some $1 \leq j \leq s_0$.

First suppose that we can find elements $n, m \in \{n_0, \dots, n_0 + 7\}$ of different parity that lie outside $\Gamma \cup \Gamma_g$. Then the affine functions α and α_g both agree at n, m ; since the odd number $m - n$ is invertible in $\mathbb{Z}/q\mathbb{Z}$, this implies that $\alpha = \alpha_g$, and hence $g(n) = \alpha_g(n) = \alpha(n)$ whenever $n \in \{1, \dots, N\}$ lies outside $\Gamma_g = \Gamma$, giving the claim in this case.

Thus the only remaining cases are when $\Gamma \cup \Gamma_g$ occupies at least one full coset of $2\mathbb{Z}$. There are three ways this can happen: either Γ is a coset of $2\mathbb{Z}$, Γ_g is a coset of $2\mathbb{Z}$, or $\Gamma_g = 4\mathbb{Z} + c$ and $\Gamma = 4\mathbb{Z} + c + 2$ for some c .

We first exclude the latter case. Without loss of generality we may place $c \in \{n_0, \dots, n_0 + 3\}$. By hypothesis, we have $g(c) = \alpha(c)$ and $g(c + 4) = \alpha(c + 4)$; since α vanishes on $4\mathbb{Z} + c + 2$, we conclude that $g(c) = g(c + 4) = \frac{q}{2} \pmod{q}$. On the other hand, as $c \in \Gamma_g$, by Lemma 8.1 (iv), we have that $\text{ord}_g = s_0 - 2$ (as Γ_g to be a coset of $4\mathbb{Z}$), $a = \frac{q}{4}a'$ is an odd multiple of $\frac{q}{4}$ and we can write $ac + b = qm$ for some integer m with $g(c) = f_q(m)$ and $g(c + 4) = f_q(m + a')$. As a' is odd, by (7.3) we conclude that at least one of $g(c), g(c + 4)$ is odd, a contradiction. Hence this case cannot occur.

Now suppose that $\Gamma = 2\mathbb{Z} + c$ is a coset of $2\mathbb{Z}$. We divide into two subcases:

- If $\Gamma_g \setminus \Gamma$ is empty or contained in a coset of $8\mathbb{Z}$, then $g(n) = \alpha(n) = \alpha_g(n)$ for at least three of the four points in $n \in \{n_0, \dots, n_0 + 7\} \cap (2\mathbb{Z} + c + 1)$. But $\alpha(n) = \frac{q}{2} \pmod{q}$ on these points, hence α_g equals $\frac{q}{2} \pmod{q}$ on these points also. As α_g is affine, we conclude that α_g equals $\frac{q}{2} \pmod{q}$ on all of $2\mathbb{Z} + c + 1$, and the claim follows.
- If Γ_g is a coset $2^i\mathbb{Z} + c'$ disjoint from $\Gamma = 2\mathbb{Z} + c$ for some $i = 1, 2$, then $\text{ord}_g = s_0 - i$, $a = 2^{\text{ord}_g}a'$ is an odd multiple of $2^{\text{ord}_g} = q/2^i$, and we may normalize $c' \in \{n_0, n_0 + 1, n_0 + 2, n_0 + 3\}$, hence by hypothesis

$$g(c') = \alpha(c'); \quad g(c' + 2^i) = \alpha(c' + 2^i).$$

As $c' \in \Gamma_g$, we may write

$$\frac{q}{2^i}a'c' + b = ac' + b = qm$$

for some integer m and odd a' , with $g(c') = f_q(m) = \alpha(c')$ and $g(c' + 2^i) = f_q(m + a') = \alpha(c' + 2^i)$. Since a' is odd, by (7.3) at least one of $f_q(m), f_q(m + a')$ is odd; on the other hand, α is equal to $\frac{q}{2} \pmod{q}$ on $2\mathbb{Z} + c + 1$, and hence at $c', c' + 2^i$, giving a contradiction.

Finally, suppose that Γ is not a coset of $2\mathbb{Z}$, but $\Gamma_g = 2\mathbb{Z} + c$ is. We again divide into two subcases:

- If $\Gamma \setminus \Gamma_g$ is empty or contained in a coset of $8\mathbb{Z}$, then by arguing as before we see that the affine function α equals $\frac{q}{2} \pmod{q}$ on at least three of the four points in $n \in \{n_0, \dots, n_0 + 7\} \cap (2\mathbb{Z} + c + 1)$, and hence on all of $2\mathbb{Z} + c + 1$. Since Γ is not a coset of $2\mathbb{Z}$, this forces α to be the constant function $\frac{q}{2} \pmod{q}$, and hence g is equal to $\frac{q}{2} \pmod{q}$ on all of $\{n_0, \dots, n_0 + 7\}$. In particular, g is even on $\{n_0, \dots, n_0 + 7\} \cap (2\mathbb{Z} + c)$. However, if we normalize $c \in \{n_0, n_0 + 1\}$, we observe that $\text{ord}_g = s_0 - 1$, $a = \frac{q}{2}a'$ is an odd multiple of $\frac{q}{2}$, and $ac + b = qm$ for some integer m , with $g(c) = f_q(m)$ and $g(c + 2) = f_q(m + a')$. Thus at least one of $g(c), g(c + 2)$ is odd, a contradiction.
- If Γ is a coset $4\mathbb{Z} + c'$ disjoint from $\Gamma_g = 2\mathbb{Z} + c$, then α is always a multiple of $\frac{q}{4}$, so in particular g is even on $\{n_0, \dots, n_0 + 7\} \cap (2\mathbb{Z} + c)$. Now we can argue as in the previous case to obtain a contradiction.

□

A variant of the argument gives

Proposition 8.3. *If $N \geq 8$, then an element g of $\mathcal{S}[N]$ has a well-defined order, step, affine function, and bad coset.*

Proof. Suppose $g \in \mathcal{S}[N]$ has two representations $g = f_q(a_1n + b_1) = f_q(a_2n + b_2)$ with associated orders $\text{ord}_1, \text{ord}_2$, steps s_1, s_2 , affine functions α_1, α_2 , and bad cosets Γ_1, Γ_2 . Our task is to show that $\text{ord}_1 = \text{ord}_2$, $s_1 = s_2$, $\alpha_1 = \alpha_2$, and $\Gamma_1 = \Gamma_2$.

First suppose that we can find elements $n, m \in \{1, \dots, N\}$ of different parity that lie outside $\Gamma_1 \cup \Gamma_2$. The arguments in the proof of Proposition 8.2 (with α_1, α_2 playing the roles of α, α_g respectively, and similarly for Γ_1, Γ_2 and Γ, Γ_g) imply that $\alpha_1 = \alpha_2$, which implies that the steps $s_1 = s_2$ agree, and that the bad cosets $\Gamma_1 = \Gamma_2$ (which are the zero sets of $\alpha_1 = \alpha_2$) agree. Since the upper density of Γ_i is $2^{\text{ord}_i}/q$, we then conclude that $\text{ord}_1 = \text{ord}_2$, as claimed.

On repeating the rest of the analysis in the proof of Proposition 8.2, we see that the only other case that does not lead to a contradiction is if Γ_1 is a coset $2\mathbb{Z} + c$ of $2\mathbb{Z}$ and $\alpha_2 = \frac{q}{2} \pmod{q}$ on the complementary coset $2\mathbb{Z} + c + 1$. Thus α_2 is either equal to α_1 , or the constant $\frac{q}{2}$. In the former case we are done as before. In the latter case, Γ_2 is empty, and now we can obtain a contradiction by interchanging the roles of Γ_1 and Γ_2 and appealing again to the analysis in the proof of Proposition 8.2. \square

We remark that the statistics $s_g, \text{ord}_g, \Gamma_g, \alpha_g$ of an element g of $\mathcal{S}[N]$ does not uniquely determine g , because there is still some variability of g within the bad coset Γ_g . For instance, the elements $n \mapsto f_q(n)$ and $n \mapsto f_q(n + q)$ of $\mathcal{S}[N]$ are both of step 1 and order 0 with bad coset $q\mathbb{Z}$ and associated affine function $n \mapsto n \pmod{q}$, but disagree inside of the bad coset. Nevertheless, the statistics $s_g, \text{ord}_g, \Gamma_g, \alpha_g$ still give some partial constraints on the behavior of g on the bad coset Γ_g ; for instance, all elements $g \in \mathcal{S}[N]$ with step 1, order 0, bad coset $q\mathbb{Z}$ and associated affine function $n \mapsto n \pmod{q}$ must take the form $g(n) = \frac{n}{q} - c \pmod{q}$ for all n in the bad coset $\{1, \dots, N\} \cap q\mathbb{Z}$ except at a single point $n = cq$ for some $c = 1, \dots, q$. It is this partial control inside the bad coset which will ultimately allow us to conclude the aperiodicity required in Theorem 7.7.

We close this section by recording some simple invariances of Sudoku solutions.

Proposition 8.4 (Sudoku invariances).

- (i) (*Affine invariance*) If $F: \mathbb{B} \rightarrow \Sigma$ is a Sudoku solution, then for any integers a, b, c , the function $(n, m) \mapsto F(n, am + bn + c)$ is also a Sudoku solution.
- (ii) (*Reflection symmetry*) If $F: \mathbb{B} \rightarrow \Sigma$ is a Sudoku solution, then so is the reflection $(n, m) \mapsto F(N + 1 - n, m)$.
- (iii) (*Homogeneity*) If $F: \mathbb{B} \rightarrow \Sigma$ is a Sudoku solution, then so is cF for any odd $c \in \mathbb{Z}/q\mathbb{Z}$.

Proof. Claims (i), (ii) are immediate from Definition 7.4, while claim (iii) follows from this definition together with Definition 7.3 and (7.4). \square

9. THE STRUCTURE OF SUDOKU SOLUTIONS

We are now ready to prove Theorem 7.7. The logical structure of the argument is summarized in Figure 9.1.

To use the property of having good columns, we begin with the following lemma. By definition, if the digits of a Sudoku solution $F: \mathbb{B} \rightarrow \Sigma$ were perfectly equidistributed, then each digit would occur on a set of density $\frac{1}{q-1}$ (as defined in Section 1.5). It will be convenient to work with a weaker variant of this property. We say

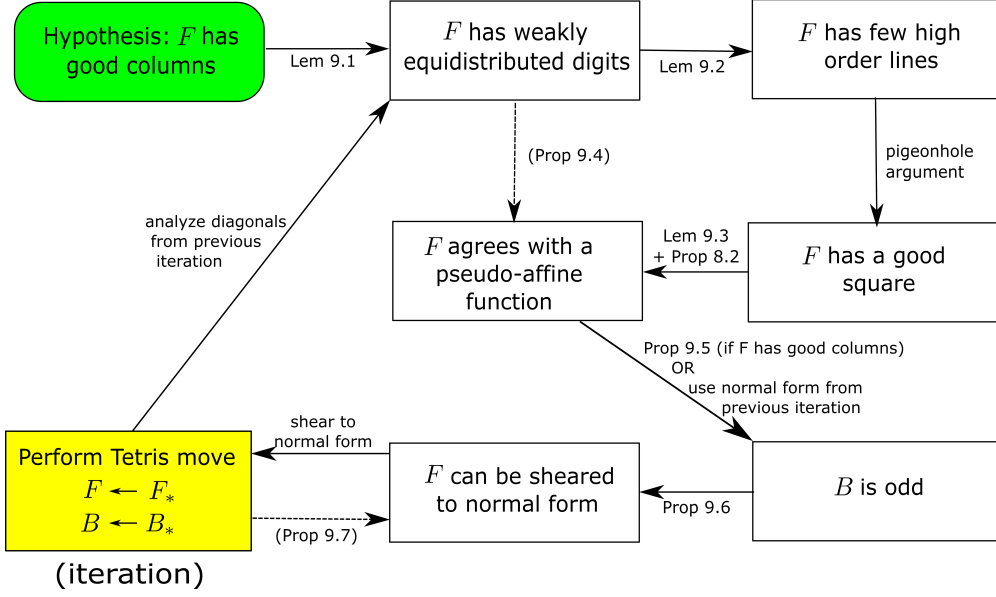


FIGURE 9.1. A schematic description of how enough structure is obtained on a Sudoku solution F with good columns that one can eventually conclude that solutions are aperiodic and prove Theorem 7.7. Dashed arrows indicate implications that are essentially compositions of other arrows in the diagram. At a key step in the argument (depicted by the yellow box) the analysis shifts from a Sudoku solution F to its “post-Tetris move” version F_* (after first shearing to normal form). Among other things, this move reduces any putative period in the solution by a factor of q .

that F has *weak digit equidistribution* if each digit $\sigma \in \Sigma$ occurs in the solution with upper density at most $\frac{2}{q}$ in \mathbb{B} .

Lemma 9.1 (Good columns implies weak digit equidistribution). *Every Sudoku solution with good columns has weak digit equidistribution.*

Proof. Let $F: \mathbb{B} \rightarrow \Sigma$ be a Sudoku solution with good columns. By the triangle inequality, it suffices to verify the claim for each separate column $\{n\} \times \mathbb{Z}$, that is to say to show that

$$\limsup_{M \rightarrow \infty} \frac{1}{2M+1} |\{m \in \{-M, \dots, M\} : F(n, m) = \gamma\}| \leq \frac{2}{q}$$

for each $n = 1, \dots, N$. By the good column property, there is a permutation $\sigma_n: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ such that $F(n, m) = \sigma_n(m \pmod{q})$ whenever $\sigma_n(m \pmod{q}) \neq 0$. Thus the property $F(n, m) = \gamma$ can only occur in two cosets of $\mathbb{Z}/q\mathbb{Z}$, the coset $\sigma_n^{-1}(\{\gamma\})$ and the coset $\sigma_n^{-1}(\{0\})$, and the claim follows. \square

For each line $\ell_{i,j} = \{(n, jn + i) : 1 \leq n \leq N\}$ in the Sudoku board, we have the associated element $F_{i,j}$ of $\mathcal{S}[N]$ defined by

$$F_{i,j}(n) := F(n, jn + i).$$

In particular we have an associated order $\text{ord}_{F_{i,j}} \in \{-\infty, 0, 1, \dots, s_0 - 1\}$ of a line to be the order of the associated sequence $n \mapsto F(n, jn + i)$. We have the following bound on the density of lines of high order:

Lemma 9.2 (Weak digit equidistribution implies high-order lines are rare). *Suppose that $F: \mathbb{B} \rightarrow \Sigma$ be a Sudoku solution with weak digit equidistribution. Then, for non-negative order $0 \leq o \leq s_0 - 1$, and any slope j , the set $\{i \in \mathbb{Z} : \text{ord}_{F_{i,j}} = o\}$ has upper density at most 2^{-o+1} in \mathbb{Z} .*

Proof. If i is such that $\text{ord}_{F_{i,j}} = o$, then there is an affine function $n \mapsto 2^o(an + b)$ with $a, b \in \mathbb{Z}/q\mathbb{Z}$ and a odd, such that $F_{i,j}(n) = 2^o(an + b)$ whenever $2^o(an + b) \neq 0$. In particular, $F(n, jn + i)$ attains the value $q/2 \pmod{q}$ at least $2^o N/q = 2^o q$. On the other hand, weak digit equidistribution, the triangle inequality the set of $(n, i) \in \{1, \dots, N\} \times \mathbb{Z}$ for which $F_{i,j}(n) = q/2 \pmod{q}$ has upper density at most $2/q$ in $\{1, \dots, N\} \times \mathbb{Z}$. The claim then follows from a standard double counting argument. \square

Once one knows that high-order lines are rare, the function F becomes mostly affine along horizontal lines, diagonals, and anti-diagonals. One can then expect to “concatenate” this information together (in the spirit of [TZ16]) to conclude that F is in fact mostly a two-dimensional affine function $F(n, m) = An + Bm + C$. This is almost correct, but in our 2-adic setting there is an additional technicality, in that a small amount of quadratic behavior is also permitted. More precisely, define a *pseudo-affine function* on \mathbb{Z}^2 to be a function $\Psi: \mathbb{Z}^2 \rightarrow \mathbb{Z}/q\mathbb{Z}$ that is of the form

$$\Psi(n, m) = An + Bm + C + D\frac{q}{4}m(m - n) \quad (9.1)$$

for some coefficients $A, B, C, D \in \mathbb{Z}/q\mathbb{Z}$; see Figure 9.2. Observe that such functions are affine along infinite non-vertical lines $\bar{\ell}_{i,j} := \{(n, jn + i) : n \in \mathbb{Z}\}$, since

$$\Psi(n, jn + i) = An + Bjn + Bi + C + D\frac{q}{4}(2nij - in + i^2) + D\frac{q}{2}n\binom{j}{2}$$

thanks to the identity

$$\frac{q}{2}n^2 - \frac{q}{2}n = q\binom{n}{2} = 0 \pmod{q}.$$

The quadratic term $D\frac{q}{4}m(m - n)$ in the definition of a pseudo-affine function is unfortunately necessary, but plays only a minor technical role in the analysis (for q large enough) and we recommend that the reader ignore these terms at a first reading. The most important coefficient of a pseudo-affine function Ψ will be the vertical coefficient B ; in particular, the behavior is particularly tractable when B is odd.

It is clear that the class of pseudo-affine functions forms an additive group. Note that this group is closed under translations in \mathbb{Z}^2 , if $\Psi(x)$, $x \in \mathbb{Z}^2$ is a pseudo-affine function and $t \in \mathbb{Z}^2$, then $\Psi(x + t)$, $x \in \mathbb{Z}^2$ is a pseudo-affine function. We have the following concatenation result:

Lemma 9.3 (Concatenation lemma). *Let $F: Q \rightarrow \mathbb{Z}/q\mathbb{Z}$ be a function defined on an 8×8 square Q such that for any (infinite) line $\bar{\ell}_{i,j} = \{(n, jn + i) : n \in \mathbb{Z}\}$ with $j = -1, 0, 1$ (i.e., an infinite anti-diagonal, horizontal line, or diagonal) intersecting Q , the function $n \mapsto F(n, jn + i)$ is affine on $\{n : (n, jn + i) \in Q\}$. Then there exists a pseudo-affine function $\Psi: \mathbb{Z}^2 \rightarrow \mathbb{Z}/q\mathbb{Z}$ which agrees with F on Q .*

Proof. By translation invariance we may normalize $Q = \{0, \dots, 7\} \times \{0, \dots, 7\}$. The functions $n \mapsto F(n, 0)$ and $n \mapsto F(n, n)$ are affine on $\{0, \dots, 7\}$, thus there

⋮

	3	5	7	1	3	5	7	1	3	5	7	1	3	5	7	1	
	2	6	2	6	2	6	2	6	2	6	2	6	2	6	2	6	
	5	3	1	7	5	3	1	7	5	3	1	7	5	3	1	7	
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	7	1	3	5	7	1	3	5	7	1	3	5	7	1	3	5	
	6	2	6	2	6	2	6	2	6	2	6	2	6	2	6	2	
	1	7	5	3	1	7	5	3	1	7	5	3	1	7	5	3	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
...	3	5	7	1	3	5	7	1	3	5	7	1	3	5	7	1	...
	2	6	2	6	2	6	2	6	2	6	2	6	2	6	2	6	
	5	3	1	7	5	3	1	7	5	3	1	7	5	3	1	7	
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	7	1	3	5	7	1	3	5	7	1	3	5	7	1	3	5	
	6	2	6	2	6	2	6	2	6	2	6	2	6	2	6	2	
	1	7	5	3	1	7	5	3	1	7	5	3	1	7	5	3	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

⋮

FIGURE 9.2. The pseudo-affine function $\Psi(n, m) = m + \frac{q}{4}m(m - n) \pmod{q}$ with $q = 8$. Observe that while Ψ is not affine in a two-dimensional sense, it is affine along all non-vertical lines. Also, the zero set of Ψ (shaded in grey) remains well-behaved, being equal to $\mathbb{Z} \times q\mathbb{Z}$. A Sudoku solution that agreed with this pseudo-affine function outside of the grey cells would be in normal form in the sense of Proposition 9.6 below, and suitable for applying a “Tetris” move to for further analysis.

exist coefficients $A, B, C \in \mathbb{Z}/q\mathbb{Z}$ such that $F(n, m) = An + Bm + C$ for

$$(n, m) \in \{(n, 0) : 0 \leq n \leq 7\} \cup \{(n, n) : 0 \leq n \leq 7\}. \quad (9.2)$$

By subtracting the pseudo-affine function $An + Bm + C$ from $F(n, m)$ we may normalize $A = B = C = 0$, thus F now vanishes on the set (9.2).

The function $n \mapsto F(n, 6 - n)$ is affine on $\{0, \dots, 6\}$ and vanishes at $n = 3, 6$, hence vanishes on all of $\{0, \dots, 6\}$. In particular F now vanishes at both $(1, 1)$ and $(5, 1)$. Since $n \mapsto F(n, 1)$ is affine on $\{0, \dots, 7\}$, we conclude that $F(n, 1) = D \frac{q}{2}(1 - n)$ for some $D \in \mathbb{Z}/q\mathbb{Z}$. By subtracting the pseudo-affine function $D \frac{q}{4}m(m - n)$ from F (which vanishes on (9.2)) we may normalize $D = 0$. Thus F now vanishes on $\{(n, 1) : 0 \leq n \leq 7\}$.

For $i = 1, \dots, 7$, the function $n \mapsto F(n, i - n)$ is affine on $\{0, \dots, i\}$ and vanishes at $n = i - 1, i$, hence vanishes on all of $\{0, \dots, i\}$. In particular, $F(0, m) = F(1, m) = 0$ for all $m = 0, \dots, 6$. As $n \mapsto F(n, m)$ is affine on $\{0, \dots, 7\}$, we conclude that F now vanishes on $\{0, \dots, 7\} \times \{0, \dots, 6\}$. By inspecting F on diagonal and anti-diagonal lines that meet the top row $\{0, \dots, 7\} \times \{7\}$ of the

square, one can then check that F vanishes here also. Thus F is identically zero on Q , and the claim follows. \square

We utilize this lemma as follows.

Proposition 9.4 (Weak digit equidistribution implies pseudo-affine structure). *Suppose that $F: \mathbb{B} \rightarrow \Sigma$ be a Sudoku solution with weak digit equidistribution. Suppose that q is sufficiently large. Then there exists a pseudo-affine function $\Psi: \mathbb{Z}^2 \rightarrow \mathbb{Z}/q\mathbb{Z}$, which does not vanish on at least one square $\{n_0, \dots, n_0 + 7\} \times \{m_0, \dots, m_0 + 7\}$, such that $F(n, m) = \Psi(n, m)$ whenever $(n, m) \in \mathbb{B}$ is a cell with $\Psi(n, m) \neq 0$.*

Proof. Let $M > 100N$ be a sufficiently large parameter (that can depend on q) to be chosen later. The first step is to locate a square $Q = \{n_0, \dots, n_0 + 7\} \times \{m_0, \dots, m_0 + 7\}$ in $\{1, \dots, N\} \times \{1, \dots, M\}$ with good properties. The number of possible such squares Q is $(N - 7)(M - 7)$; we select one at random.

To each non-vertical line $\ell_{i,j} = \{(n, jn + i) : 1 \leq n \leq N\}$, one can form the bad set $\Gamma_{i,j} := \{(n, jn + i) : n \in \Gamma_{F_{i,j}} \cap \{1, \dots, N\}\}$ associated to the bad coset $\Gamma_{F_{i,j}}$ of $F_{i,j}$. If the $\text{ord}_{F_{i,j}} = o$, this bad set has spacing $q/2^o$, and thus has cardinality $O(2^o N/q) = O(2^o q)$. Thus, there are at most $O(2^o q)$ squares Q with the property that Q contains one of the elements of this bad set. On the other hand, for $j = -1, 0, 1$ (i.e., horizontal lines, diagonals, and anti-diagonals), we see from Lemma 9.2 that the set of intercepts i with $\text{ord}_{F_{i,j}} = o$ have upper density $O(2^{-o})$. Summing in o and over the $O(M)$ possible lines $\ell_{i,j}$ of slope $j = -1, 0, 1$ intersecting $\{1, \dots, N\} \times \{1, \dots, M\}$, we conclude from double counting (for M large enough) that the probability that Q contains a bad point from a horizontal line, diagonal, or anti-diagonal intersecting Q is $O(\frac{\sum_{o=0}^{s_0-1} 2^{-o} q \times M}{(N-7)(M-7)}) = O(\log q/q)$. Thus, assuming q is large enough, we can find a square

$$Q = \{n_0, \dots, n_0 + 7\} \times \{m_0, \dots, m_0 + 7\}$$

in $\{1, \dots, N\} \times \{1, \dots, M\}$ with the property that all horizontal lines, diagonals, and anti-diagonals $\ell_{i,j}$ passing through Q are such that $Q \cap \Gamma_{i,j} = \emptyset$. In particular, on every such line ℓ , F agrees on $Q \cap \ell$ with a (one-dimensional) affine function. Applying Lemma 9.3, we may find a pseudo-affine function $\Psi: \mathbb{Z}^2 \rightarrow \mathbb{Z}/q\mathbb{Z}$ such that F agrees with Ψ on Q . In particular, Ψ is non-vanishing on Q .

Call a cell (n, m) *good* if either $\Psi(n, m) = 0$, or if $\Psi(n, m) = F(n, m)$. Then all elements of Q are good. Also, from Proposition 8.2 we see that if a line $\ell_{i,j}$ contains eight good consecutive cells, then all the cells in the line are good. Applying this fact to the eight horizontal lines $\ell_{m,0} = \{(n, m) : 1 \leq n \leq N\}$ for $m \in \{m_0, \dots, m_0 + 7\}$, we conclude that all the cells in the rectangular region $\{1, \dots, N\} \times \{m_0, \dots, m_0 + 7\}$ are good. Applying the fact again to the diagonal lines $\ell_{m,1} = \{(n, n + m) : 1 \leq n \leq M\}$ for $m_0 - 1 \leq m \leq m_0 + 8 - N$, we conclude that all the cells in the partial horizontal line $\{8, \dots, N\} \times \{m_0 + 8\}$ are good; applying the fact again to the horizontal line $\ell_{m_0+8,0} = \{(n, m_0 + 8) : 1 \leq n \leq N\}$, we conclude that in fact all the cells in $\ell_{m_0+8,0}$ are good. A reflected version of the same argument shows that all the cells in $\ell_{m_0-1,0}$ are good. Thus we have extended the rectangle of good cells by one row in both directions. Iterating this argument to fill out the remaining rows of the Sudoku board, we conclude that all the cells in \mathbb{B} are good, giving the claim. \square

Assuming good columns, we can obtain an important control on a key coefficient B of the pseudo-affine function Ψ .

Proposition 9.5 (Odd vertical coefficient). *Let F be a Sudoku solution with good columns. Let $\Psi(n, m) = An + Bm + C + D\frac{q}{4}m(m - n)$ be the pseudo-affine function produced by Proposition 9.4. Then B is odd.*

Proof. By Lemma 9.1, F has weak digit equidistribution. Hence, from applying Proposition 9.4 we obtain that there exists $1 \leq n \leq N$ such that the function $m \mapsto \Psi(n, m)$ is not identically zero. This function is affine on every coset of $4\mathbb{Z}$, and hence is non-vanishing on at least one coset $8\mathbb{Z} + c$ of $8\mathbb{Z}$. Suppose for contradiction that B was even. Then the function $m \mapsto \Psi(n, m)$ is $\langle \frac{q}{2} \rangle$ -periodic on $8\mathbb{Z} + c$, thus $m \mapsto F(n, m)$ is also. But as F has good columns, we also have $F(n, m) = \sigma_n(m)$ whenever $\sigma_n(m \pmod{q}) \neq 0$, for some permutation $\sigma_n: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$. This implies that σ_n has a zero in every coset $\{m \pmod{q}, m + \frac{q}{2} \pmod{q}\}$ of $\frac{q}{2}\mathbb{Z}/q\mathbb{Z}$ with $m \in 8\mathbb{Z} + c$, which is absurd. \square

This gives us a normal form as follows. Given a Sudoku solution F , define a *shearing* of F to be any map $F': \mathbb{B} \rightarrow \Sigma$ of the form

$$F'(n, m) := BF(n, m + An + C)$$

for some integers A, B, C with B odd. Note from Proposition 8.4 that F' is also a Sudoku solution; furthermore, F has good columns if and only if F' does, and F is periodic if and only if F' is. The property of one Sudoku solution being a shearing of another can also be easily verified to be an equivalence relation. In view of Remark 7.9, the shear-invariance of Sudoku solutions is closely related to the translation invariance of tiling equations $A \oplus F = G$.

Proposition 9.6 (Normal form). *Let $F(n, m)$ be a Sudoku solution which agrees with a pseudo-affine function $\Psi(n, m) = An + Bm + C + D\frac{q}{4}m(m - n)$ with $B \in \mathbb{Z}/q\mathbb{Z}$ odd when $\Psi(n, m)$ is non-zero. Then there exists a shearing F' of F which is in normal form in the sense that*

$$F'(n, m) = m + D\frac{q}{4}m(m - n) \tag{9.3}$$

for some $D \in \mathbb{Z}/q\mathbb{Z}$, all $n \in \{1, \dots, N\}$, and all $m \in \mathbb{Z} \setminus q\mathbb{Z}$.

Proof. We claim that the zero set of Ψ takes the form

$$\{(n, m) \in \mathbb{Z}^2 : \Psi(n, m) = 0\} = \{(n, m) \in \mathbb{Z}^2 : m = A'n + C' \pmod{q}\} \tag{9.4}$$

for some coefficients $A', C' \in \mathbb{Z}/q\mathbb{Z}$. To see this, we temporarily divide out by the invertible element B to normalize $B = 1$. If $\Psi(n, m) = 0$, then $An + m + C = 0 \pmod{4}$, hence

$$0 = \Psi(n, m) = An + m + C + D\frac{q}{4}(-An - C)(-An - C - n) \pmod{q}$$

which one can write (using $\frac{q}{2}n^2 = \frac{q}{2}n \pmod{q}$) as

$$0 = An + m + C + DC^2\frac{q}{4} + (2A + 1)DC\frac{q}{4}n + D\frac{q}{2}\binom{A + 1}{2}n \pmod{q}$$

and thus

$$m = A'n + C' \pmod{q}$$

where $A' := -A - (2A + 1)DC\frac{q}{4} - D\frac{q}{2}\binom{A+1}{2}$ and $C' := -C - DC^2\frac{q}{4}$. Conversely, if $m = A'n + C' \pmod{q}$ then $An + m + C = 0 \pmod{4}$ and $\Psi(n, m) = 0$. This gives (9.4).

Let F'' denote the shearing

$$F''(n, m) := F(n, m + A'n + C')$$

of F , and similarly define $\Psi''(n, m) := \Psi(n, m + A'n + C')$. From direct computation, Ψ'' is of the form $\Psi''(n, m) = A''n + B''m + C'' + D''\frac{q}{4}m(m - n)$ for some $A'', B'', C'', D'' \in \mathbb{Z}/q\mathbb{Z}$ with B'' odd (and thus invertible), and $\Psi''(n, m)$ vanishes when $m = 0 \pmod{q}$. Substituting $m = 0$ we conclude that $A'' = C'' = 0$. If we then set $F'(n, m) := F''(n, m)/B''$ we obtain the desired shearing F' in normal form. \square

In view of Propositions 9.5, 9.6, we see that to conclude the proof of Theorem 7.7, it suffices to show that all Sudoku solutions F in normal form are non-periodic. Suppose for contradiction that we had a periodic Sudoku solution F in normal form, thus F is $\langle(0, M)\rangle$ -periodic for some period M (i.e., $F(n, m) = F(n, m + M)$ for all $(n, m) \in \mathbb{B}$). From the normal form condition (9.3) we see that M must be divisible by q . The key proposition we will establish to conclude the argument is:

Proposition 9.7 (Tetris iteration). *Let F be a Sudoku solution in normal form. We consider the Tetris move of replacing F with the function*

$$F_*(n, m) := F(n, qm)$$

which is also a Sudoku solution thanks to Proposition 8.4. Then there exists a shearing of F_ that is in normal form.*

Indeed, if F is an $\langle(0, M)\rangle$ -periodic Sudoku solution in normal form, the post-Tetris move solution F_* will be a $\langle(0, M/q)\rangle$ -periodic Sudoku solution, and its shearing will be a $\langle(0, M/q)\rangle$ -periodic Sudoku solution in normal form. Iterating this gives an infinite descent of periods M , which is absurd.

Remark 9.8. In the computer game “Tetris”, every time a row is completely filled with blocks, it is deleted. Analogously to this, a Sudoku solution F in normal form has its values completely specified on all rows $\ell_{m,0} = \{(n, m) : 1 \leq n \leq N\}$ with $m \not\equiv 0 \pmod{q}$; deleting all these rows yields the post-Tetris move solution F_* . This may help explain our terminology of a “Tetris move”.

9.1. Analyzing the Tetris move. It remains to establish Proposition 9.7. In order to deploy tools such as Proposition 9.4, we will need to control upper digits of densities of the post-Tetris solution F_* . To do this, we first analyze the diagonal lines $F_{i,1}(n) = F(n, n + i)$ of the original solution F . From (9.3) we have

$$F_{i,1}(n) = n + i + D\frac{q}{4}(n + i)i \pmod{q}$$

whenever $n + i \not\equiv 0 \pmod{q}$. We can simplify this to

$$F_{i,1}(n) = a_{i,1}n + b_{i,1}$$

whenever $n + i \not\equiv 0 \pmod{q}$, where the coefficients $a_{i,1}, b_{i,1} \in \mathbb{Z}/q\mathbb{Z}$ are given by the formulae

$$a_{i,1} := 1 + D\frac{q}{4}i \pmod{q} \tag{9.5}$$

and

$$b_{i,1} := i + D\frac{q}{4}i^2 \pmod{q}.$$

Observe that $a_{i,1}$ is odd, and $F_{i,1}(n)$ is equal to $a_{i,1}n + b_{i,1}$ for $n \in \{1, \dots, N\}$ outside of the coset $\Gamma_{F_{i,1}} := \{n \in \mathbb{Z} : n + i = 0 \pmod{q}\}$ of $q\mathbb{Z}$. By Proposition 8.3 (applied to some interval $\{n_0, \dots, n_0 + 7\}$ in $\{1, \dots, N\}$ avoiding $\Gamma_{F_{i,1}}$), this forces the step $s_{F_{i,1}}$ of $F_{i,1}$ to equal $a_{i,1}$, and the order $\text{ord}_{F_{i,1}}$ to equal 0.

Thus, by Lemma 8.1 (iv), we may write

$$F_{i,1}(n) = f_q(\tilde{a}_{i,1}n + \tilde{b}_{i,1})$$

for some integers $\tilde{a}_{i,1}, \tilde{b}_{i,1}$ with $\tilde{a}_{i,1} = a_{i,1} \pmod{q}$ and $\tilde{b}_{i,1} = b_{i,1} \pmod{q}$. If we now let $n_i \in \{1, \dots, q\}$ be such that $n_i + i = 0 \pmod{q}$, we conclude in particular that $\tilde{a}_{i,1}n_i + \tilde{b}_{i,1} = q\tilde{c}_{i,1}$ for some integer $\tilde{c}_{i,1}$, and

$$\begin{aligned} F_*\left(n_i + qj, \frac{n_i + i}{q} + j\right) &= F_{i,1}(n_i + qj) \\ &= f_q(q\tilde{c}_{i,1} + \tilde{a}_{i,1}qj) \\ &= f_q(\tilde{a}_{i,1}j + \tilde{c}_{i,1}). \end{aligned} \tag{9.6}$$

for $j = 0, \dots, q-1$. Since $\tilde{a}_{i,1}$ is odd, this implies that $F_*(n_i + qj, \frac{n_i + i}{q} + j) = \tilde{a}_{i,1}j + \tilde{c}_{i,1} \pmod{q}$ for all but one value of j . In particular each digit γ of Σ is attained by $F_*(n_i + qj, \frac{n_i + i}{q} + j)$ at most twice. Averaging over all i and double counting using $N = q^2$, we conclude that the upper density of $\{(n, m) \in \mathbb{B} : F_*(n, m) = \gamma\}$ in \mathbb{B} does not exceed the upper density of E by more than $2/q$. In other words, F_* has weak digit equidistribution.

We may now invoke Proposition 9.4 and conclude that there exists a pseudo-affine function

$$\Psi_*(n, m) = A_*n + B_*m + C_* + D_*\frac{q}{4}m(m - n)$$

which is not identically zero in \mathbb{B} , and such that $F_*(n, m) = \Psi_*(n, m)$ whenever $\Psi_*(n, m)$ is non-zero.

Since \mathbb{B} can be covered by sets of the form $\{(n_0 + qj, m_0 + j) : j = 0, \dots, q-1\}$ for $n_0 = 1, \dots, q$ and $m_0 \in \mathbb{Z}$, we can find $n_0 = 1, \dots, q$ and $m_0 \in \mathbb{Z}$ such that Ψ_* does not vanish identically on this set. By repeating the calculation (9.6) (with $i = qm_0 - n_0$) we see that

$$F_*(n_0 + qj, m_0 + j) = f_q(\tilde{a}j + \tilde{c})$$

for some integers \tilde{a}, \tilde{c} (depending on n_0, m_0) with \tilde{a} odd. In particular,

$$f_q(\tilde{a}j + \tilde{c}) = \Psi_*(n_0 + qj, m_0 + j) \tag{9.7}$$

whenever $j = 0, \dots, q-1$ is such that the right-hand side is non-zero.

As \tilde{a} is odd, the left-hand side of (9.7) attains the value $\frac{q}{2} \pmod{q}$ at most twice for $j = 0, \dots, q-1$. On the other hand, at the midpoint between consecutive values of j in which the (not identically zero) affine function $\Psi_*(n_0 + qj, m_0 + j)$ vanishes, this affine function will attain the value of $\frac{q}{2} \pmod{q}$. We conclude that $\Psi_*(n_0 + qj, m_0 + j)$ vanishes for at most three values of $j = 0, \dots, q-1$; meanwhile $\tilde{a}j + \tilde{c} \pmod{q}$ vanishes for one value of j . Hence by the pigeonhole principle, and the assumption that q is large, the identity

$$\tilde{a}l + \tilde{c} = \Psi_*(n_0 + ql, m_0 + l) \pmod{q}; \quad l = j, j+1$$

holds for two consecutive values $l = j, j+1$ of l . Subtracting these two identities and reducing modulo 2, we conclude that B_* has the same parity as \tilde{a} and is thus odd. Applying Proposition 9.6, we conclude that there exists a shearing of F_*

that is in normal form. This concludes the proof of Proposition 9.7, and hence of Theorem 7.7, Theorem 1.3, and Corollary 1.6.

10. OPEN PROBLEMS

We close by posing some problems left open by our work.

10.1. Explicit bound on dimension. The dimension d produced by our proof of Corollary 1.5 is explicit but extremely large and probably not optimal. This is for a number of reasons, the most significant being that we need an enormous number of functional equations in order to encode the property $P_{\tilde{\Omega}}$ appearing in Section 7. Thus, a natural question is

Question 10.1. *What is the smallest value of d for which Corollary 1.5 (resp. Corollary 1.6) is true?*

The fact that our construction originates in the virtually two-dimensional space $\mathbb{Z}^2 \times G_0$ hints that Conjectures 1.1 and 1.2 might fail in a “reasonably small” dimension.

On the other hand, there may be hope to extend the known positive results on the periodic tiling conjecture beyond the known cases.

Question 10.2. *Is the Conjecture 1.1 true in \mathbb{Z}^3 ? Is the Conjecture 1.2 true in \mathbb{R}^2 ?*

10.2. Connected tiles. An inspection of our proof of Corollary 1.6 reveals that the tile $\Sigma \subset \mathbb{R}^d$ constructed by the argument is a finite union of cubes; however, this union need not be connected. Given the positive results available for connected tiles (and in particular for topological disks [Ken92]), it is natural to ask

Question 10.3. *Is it possible in Corollary 1.6 to choose Σ to be an open connected set?*

Of course the question can be trivially answered without the requirement that Σ is open, simply by adding suitable measure zero line segments to the tile Σ constructed by our arguments.

10.3. Cardinality of aperiodic tiles. In view of the results in [S98], it might be interesting to compute the size of our tile F in Corollary 1.5.

Question 10.4. *Suppose that a finite $F \subset \mathbb{Z}^d$ admits an aperiodic tiling. What is the fewest number of prime factors that the cardinality of F can have?*

10.4. Decidability of tilings. A famous application of the study of the periodicity of tiling is to the problem of determining whether tilings are *decidable*. Namely, the question⁸ whether there exists an algorithm that, upon any input of a finite set F in a finitely generated abelian group G , computes (in finite time) if this set is a tile of G or not. A well known argument of H. Wang [W75] shows that if any tile admits a periodic tiling then any tiling problem is decidable.

In this work we prove that there are tiles of finitely generated abelian groups which tile aperiodically. However, the decidability of tilings by a single tile remains open.

⁸One can also ask, for an individual tile F , whether the existence of a tiling $A \oplus F = G$ is logically decidable (i.e., provable or disprovable) in a first-order theory such as ZFC. The two questions are closely related; see [GT21] for further discussion.

Question 10.5. *Does there exist any undecidable tiling problem with a single tile?*

In a previous paper [GT21] we proved the undecidability of tilings of *periodic* sets by *two* tiles. This implies, in particular, the existence of aperiodic tilings by two tiles. Our proof consists of encoding any Wang tiling as a tiling of a periodic set with two tiles; then, the undecidability of Wang tilings [B66, B64] implies the existence of an undecidable tiling problem with only two tiles.

10.5. Weak periodicity. Let d and $F \subset \mathbb{Z}^d$ be as in Corollary 1.5. Observe that by our construction, all the sets in $\text{Tile}(F; \mathbb{Z}^d) := \{A \subset \mathbb{Z}^d : A \oplus F = \mathbb{Z}^d\}$ are $(d-2)$ -periodic in the sense that for every $A \in \text{Tile}(F; \mathbb{Z}^d)$ there exist $d-2$ linearly independent vectors v_1, \dots, v_{d-2} in \mathbb{Z}^d such that A is invariant under translations by v_j for every $j = 1, \dots, d-2$.

Definition 10.6. A set $S \subset \mathbb{Z}^d$ is called *k-weakly periodic* if it can be partitioned into finitely many sets, each of which is *k*-periodic.

It is not difficult to show that if a tile in \mathbb{Z}^d admits a tiling of \mathbb{Z}^d which is $(d-1)$ -weakly periodic then it also admits a tiling which is periodic. Thus, our aperiodic construction contains the largest possible amount of periodicity.

In [GT20] we showed that for every $F \subset \mathbb{Z}^2$ all the sets in $\text{Tile}(F; \mathbb{Z}^2)$ are 1-weakly periodic. This, in particular, implies Conjecture 1.1 in \mathbb{Z}^2 .

The following question remains open.

Question 10.7. *Let $d \geq 3$ and $F \subset \mathbb{Z}^3$ be finite. Are there any $A \in \text{Tile}(F; \mathbb{Z}^d)$ which are not 1-weakly periodic?*

10.6. The structure of our construction. We believe that with additional effort, our analysis should give a complete classification of the space of Sudoku solutions with good columns, and hence also the set of tilings by the tile F in Theorem 1.3, however the answer appears to be somewhat complicated⁹ and we do not give it here.

Problem 10.8. *Find a complete classification of the space $\text{Tile}(F; \mathbb{Z}^2 \times G_0)$, where F and G_0 are as in Theorem 1.3. What is the dynamical structure of this space (viewed as a topological dynamical system with the translation action of $\mathbb{Z}^2 \times G_0$)?*

Following [L21], it would be of interest to study the tilings in $\text{Tile}(F; \mathbb{Z}^2 \times G_0)$ that have a substitution structure.

Question 10.9. *Can any of the tilings by our aperiodic tile be interpreted as a substitution tiling?*

The 2-adic nature of the Sudoku solutions suggests a positive answer.

REFERENCES

- [AGS92] R. Amman, B. Grünbaum and G.C. Shephard, *Aperiodic tiles*, Disc. Comp. Geom., **8** (1992), 1–25.
- [AG94] Beyond quasicrystals. Papers from the Winter School held in Les Houches, March 7–18, 1994. Edited by Françoise Axel and Denis Gratias.
- [BJ08] A. Ballier, E. Jeandel, *Tilings and model theory*, JAC 2008, Uzès, France, 29–39.
- [B66] R. Berger, *The undecidability of the domino problem*, Memoirs of the American Mathematical Society, **66** (1966) 72.

⁹In particular, the D coefficient in the pseudo-affine functions (9.1) is somewhat difficult to control.

- [B64] R. Berger. The Undecidability of the Domino Problem. PhD thesis, Harvard University, 1964.
- [B26] A.S. Besicovitch, *On generalized almost periodic functions*, Proc. London Math. Soc., **25** (1926), 495–512.
- [BN91] D. Beauquier, M. Nivat, *On translating one polyomino to tile the plane*, Discrete Comput. Geom. **6** (1991), no. 6, 575–592.
- [B20] S. Bhattacharya, *Periodicity and Decidability of Tilings of \mathbb{Z}^2* , Amer. J. Math., **142**, (2020), 255–266.
- [BLR93] M. Blum, M. Luby, R. Rubinfeld, *Self-testing/correcting with applications to numerical problems*, Journal of Computer and System Sciences **47** (1993), 549–595.
- [CK86] J. H. Conway and K. M. Knowles, *Quasiperiodic tiling in two and three dimensions*, J. Phys. A, ((19)17):3645–3653, 1986.
- [C96] K. Culik II., *An aperiodic set of 13 Wang tiles*, Discrete Math., **160** (1996), 245–251.
- [DB81] N. G. De Bruijn, *Algebraic theory of Penrose’s non-periodic tilings of the plane*, Kon. Nederl. Akad. Wetensch. Proc. Ser. A **43.84** (1981): 1–7.
- [FGH] D. Frettlöh, F. Gähler, E. Harriss: Tilings encyclopedia, <https://tilings.math.uni-bielefeld.de/>
- [F74] B. Fuglede, *Commuting self-adjoint partial differential operators and a group theoretic problem*, Journal of Functional Analysis, Volume 16, Issue 1, (1974), 101–121.
- [G77] M. Gardner, Scientific American January 1977, pp. 110–121.
- [G-BN91] D. Girault-Beauquier, M. Nivat, *Tiling the plane with one tile*, Topology and category theory in computer science (Oxford, 1989), 291–333, Oxford Sci. Publ., Oxford Univ. Press, New York, 1991.
- [G89] C. Godreche, *The sphinx: a limit-periodic tiling of the plane*, 1989 J. Phys. A: Math. Gen. **22** L1163.
- [G70] S. W. Golomb, *Tiling with sets of polyominoes*, J. Comb. Thy. **9** (1970), 60–71.
- [GS98] C. Goodman-Strauss *Matching rules and substitution tilings*, Ann. of Math. (2), **147**(1):181–223, 1998.
- [GS05] C. Goodman-Strauss, *A strongly aperiodic set of tiles in the hyperbolic plane* Invent. Math., **159**(1):119–132, 2005.
- [GGRT22] J. Grebík, R. Greenfeld, V. Rozhoň, T. Tao, *Measurable tilings by abelian group actions*, preprint, [arXiv:2203.01511](https://arxiv.org/abs/2203.01511)
- [GT20] R. Greenfeld, T. Tao, *The structure of translational tilings in \mathbb{Z}^d* , Discrete Analysis (2021):16, 28 pp.
- [GT21] R. Greenfeld, T. Tao, *Undecidable translational tilings with only two tiles, or one non-abelian tile*, [arXiv:2108.07902](https://arxiv.org/abs/2108.07902).
- [GT22] R. Greenfeld, T. Tao, *A counterexample to the periodic tiling conjecture (announcement)*, [arXiv:2209.08451](https://arxiv.org/abs/2209.08451).
- [GS87] B. Grünbaum, G.C. Shephard, Tilings and Patterns. W.H. Freeman, 1987.
- [JR21] W. Jeandel, M. Rao, *An aperiodic set of 11 Wang tiles*, Adv. Comb. 2021, Paper No. 1, 37 pp.
- [K96] J. Kari, *A small aperiodic set of Wang tiles*, Discrete Math., **160** (1996), 259–264.
- [Ken92] R. Kenyon, *Rigidity of planar tilings*, Invent. Math., **107** (1992), 637–651.
- [K04] M.N. Kolountzakis, *The Study of Translational Tiling with Fourier Analysis*, In: Brاندolini, L., Colzani, L., Travaglini, G., Iosevich, A. (eds) Fourier Analysis and Convexity. Applied and Numerical Harmonic Analysis. Birkhäuser, Boston, MA (2004).
- [KL96] M. N. Kolountzakis, J. C. Lagarias, *Structure of tilings of the line by a function*, Duke Math. J. **82** (1996), 653–678.
- [L21] S. Labbé, *Substitutive Structure of Jeandel–Rao Aperiodic Tilings*, Discrete Comput Geom **65**, 800–855 (2021).
- [L95] J. C. Lagarias, *Meyer’s Concept of Quasicrystal and Quasiregular Sets*, Commun Math Phys **179**, 365–376 (1996).
- [LS92] J. Lagarias, P. Shor, *Keller’s cube-tiling conjecture is false in high dimensions*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), no. 2, 279–283.
- [LW96] J. C. Lagarias, Y. Wang, *Tiling the line with translates of one tile*, Invent. Math. **124** (1996), no. 1–3, 341–365.

- [LM91] H. Leptin, D. Müller, *Uniform partitions of unity on locally compact groups*, Adv. Math. **90** (1991), no. 1, 1–14.
- [L13] L.A. Levin, *Forbidden information*, Journal of the ACM, **60**, no. 2, (2013) 1–9.
- [M80] P. McMullen, *Convex bodies which tile space by translations*, Mathematika **27** (1980), 113–121.
- [M70] Y. Meyer, *Nombres de Pisot, nombres de Salem et analyse harmonique*, Lecture Notes in Mathematics **117** (1970), Springer-Verlag.
- [M95] Y. Meyer, *Quasicrystals, diophantine approximation and algebraic numbers*, Axel, F., Gratias, D. (eds) Beyond Quasicrystals. Centre de Physique des Houches, vol 3. Springer, Berlin, Heidelberg (1995).
- [MSS22] T. Meyerovitch, S. Sanadhya, Y. Solomon, *A note on reduction of tiling problems*, arXiv:2211.07140.
- [M89] S. Mozes, *Tilings, substitution systems and dynamical systems generated by them*, J. Anal. Math. **53**, 139–186 (1989).
- [N77] D. J. Newman, *Tesselation of integers*, J. Number Theory **9** (1977), no. 1, 107–111.
- [O09] N. Ollinger, *Tiling the plane with a fixed number of polyominoes*, Lecture Notes in Comput. Sci., 5457, Springer, Berlin, 2009.
- [P74] R. Penrose, *The role of aesthetics in pure and applied mathematical research*, Bull.Inst.Math.Appl. **10** 266–271, 1974.
- [P79] R. Penrose, *Pentaplexity a class of non-periodic tilings of the plane*, The mathematical intelligencer 2.1 (1979): 32–37.
- [R71] R. M. Robinson, *Undecidability and nonperiodicity for tilings of the plane*, Inventiones Mathematicae, (1971), **12** (3), 177–209.
- [SSU21] A. Şahin, M. Schraudner, I. Ugarcovici, *A strongly aperiodic shift of finite type on the discrete Heisenberg group using Robinson tilings*, Illinois J. Math. **65** (3) 655 – 686, September 2021.
- [S96] M. Senechal, *7.2 The SCD (Schmitt–Conway–Danzon) tile*, Quasicrystals and Geometry, Cambridge University Press (1996), pp. 209–213.
- [ST12] J.E.S. Socolar, J.M. Taylor, *Forcing Nonperiodicity with a Single Tile*, Math Intelligencer **34**, 18–28 (2012).
- [S98] M. Szegedy, *Algorithms to tile the infinite grid with finite clusters*, Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS '98), IEEE Computer Society, Los Alamitos, CA, (1998), 137–145.
- [TZ16] T. Tao, T. Ziegler, *Concatenation theorems for anti-Gowers-uniform functions and Host-Kra characteristic factors*, Discrete Anal. (2016), Paper No. 13, 60 pp.
- [V54] B. A. Venkov, *On a class of Euclidean polyhedra*, Vestnik Leningrad Univ. Ser. Math. Fiz. Him. **9** (1954), 11–31.
- [W60] H. Wang, *Proving theorems by pattern recognition i*, Communications of the ACM, **3**(4):220–234, 1960.
- [W75] H. Wang, *Notes on a class of tiling problems*, Fundamenta Mathematicae, **82** (1975), 295–305.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NJ 08540.

Email address: greenfeld.math@gmail.com

UCLA DEPARTMENT OF MATHEMATICS, LOS ANGELES, CA 90095-1555.

Email address: tao@math.ucla.edu