A HOST–KRA $\mathbb{F}_2^\omega$-SYSTEM OF ORDER 5 THAT IS NOT ABRAMOV OF ORDER 5, AND NON-MEASURABILITY OF THE INVERSE THEOREM FOR THE $U^6(\mathbb{F}_2^n)$ NORM

ASGAR JAMNESHAN, OR SHALOM, AND TERENCE TAO

Abstract. It was conjectured by Bergelson, Tao, and Ziegler [1] that every Host–Kra $\mathbb{F}_p^\omega$-system of order k is an Abramov system of order k. This conjecture has been verified for $k \leq p + 1$. In this paper we show that the conjecture fails when $k = 5, p = 2$. We in fact establish a stronger (combinatorial) statement, in that we produce a bounded function $f : \mathbb{F}_2^n \to \mathbb{C}$ of large Gowers norm $\|f\|_{U^6(\mathbb{F}_2^n)}$ which (as per the inverse theorem for that norm) correlates with a non-classical quintic phase polynomial $e(P)$, but with the property that all such phase polynomials $e(P)$ are "non-measurable" in the sense that they cannot be well approximated by functions of a bounded number of random translates of f.

1. Introduction

Let p be a prime, and let $k \geq 1$. We consider two statements associated to these parameters: the (now-proven) inverse conjecture [9], [19] [11] for the Gowers norms in characteristic p, and the Bergelson–Tao–Ziegler conjecture [1]. We begin with the former. Given any finite abelian group $G = (G, +)$, we define the Gowers uniformity norm $\|f\|_{U^{k+1}(G)} \geq 0$ of a function $f : G \to \mathbb{C}$ by the formula

$$\|f\|_{U^{k+1}(G)}^{2^{k+1}} := \mathbb{E}_{x,h_1,\dots,h_{k+1}\in G} \prod_{\omega\in\{0,1\}^{k+1}} C^{|\omega|} f\left(x + \omega \cdot \vec{h}\right)$$

where $C : z \mapsto \bar{z}$ denotes complex conjugation, $\omega = (\omega_1, \dots, \omega_{k+1})$, $|\omega| := \omega_1 + \cdots + \omega_{k+1}$, $\vec{h} := (h_1, \dots, h_{k+1})$, $\omega \cdot \vec{h}$ denotes the dot product

$$\omega \cdot \vec{h} := \omega_1 h_1 + \cdots + \omega_{k+1} h_{k+1},$$

$\mathbb{E}_{x\in A} := \frac{1}{|A|} \sum_{x\in A}$ denotes the averaging operation, and $|A|$ denotes the cardinality of a finite set A. If $P : G \to \mathbb{T}$ is a function taking values in the

Date: March 10, 2023.

2020 *Mathematics Subject Classification.* Primary 28D15, 37A05; Secondary 37A35.

unit circle $\mathbb{T} := \mathbb{R}/\mathbb{Z}$, then we have $\|e(P)\|_{U^{k+1}(G)} \leq 1$, with equality precisely when P is a *(non-classical) polynomial of degree k*, as defined in Definition A.18 (endowing G with the degree 1 filtration); here $e\colon \mathbb{T} \to \mathbb{C}$ is the fundamental character $e(\theta) := e^{2\pi i\theta}$. The space of polynomials $P\colon G \to \mathbb{T}$ of degree at most k is an abelian group which we denote $\mathrm{Poly}^k(G)$. By convention, $\mathrm{Poly}^0(G)$ will denote the constant functions $\mathbb{T}$, and $\mathrm{Poly}^k(G) = \{0\}$ for all $k < 0$ (thus non-zero constants have degree 0, and zero has degree $-\infty$).

For each p, k, we can then form the following claim:

Conjecture 1.1 (Inverse conjecture for the Gowers norm)**.** *For every $\eta > 0$ there exists $c = c(k, p, \eta) > 0$ such that, whenever $G = \mathbb{F}_p^n$ is an elementary abelian p-group and $f\colon G \to \mathbb{D}$ is a function taking values in the unit disk $\mathbb{D} := \{z \in \mathbb{C} : |z| \leq 1\}$ and $\|f\|_{U^{k+1}(G)} \geq \eta$, there exists $P \in \mathrm{Poly}^k(G)$ such that $|\mathbb{E}_{x\in G} f(x)e(-P(x))| \geq c$.*

This conjecture has now been established for all values of k, p [23]. The case $k = 1$ is trivial, the case $k = 2$ follows from standard Fourier analytic calculations, and the case $k = 3$ was previously established in [9] (for $p > 2$) and [19] (for $p = 2$). In [22], this conjecture was shown to be a consequence of a conjecture in ergodic theory which we now pause to introduce. Define an *$\mathbb{F}_p^\omega$-system* to be a (countably generated) probability space (X, μ) equipped with a measure-preserving action $T^h\colon X \to X$, $h \in \mathbb{F}_p^\omega$ of the group $\mathbb{F}_p^\omega := \varprojlim \mathbb{F}_p^n$ (the vector space over $\mathbb{F}_p$ with a countably infinite basis). One can define analogues of the Gowers uniformity norms $\|f\|_{U^{k+1}(X)}$ (known as *Gowers–Host–Kra seminorms*) for $f \in L^\infty(X)$, and one can similarly define the group $\mathrm{Poly}^k(X)$ of polynomials $P\colon X \to \mathbb{T}$ (defined up to almost everywhere equivalence) as

$$\mathrm{Poly}^k(X) := \{P : \|e(P)\|_{U^{k+1}(X)} = 1\};$$

see [22] for details. An $\mathbb{F}_p^\omega$-system is said to be *of order at most k* if $\|f\|_{U^{k+1}(X)} > 0$ for any non-zero element f of $L^\infty(X)$ (where elements of the latter are defined up to almost everywhere equivalence). We then have

Conjecture 1.2 (Bergelson–Tao–Ziegler conjecture)**.** [1, Remark 1.25] *Let X be an ergodic $\mathbb{F}_p^\omega$-system of order at most k. Then the σ-algebra of X is generated (modulo null sets) by the polynomials in* $\mathrm{Poly}^k(X)$.

We remark that the ergodicity hypothesis on X can in fact be removed by ergodic decomposition, but we will not need to do so here.

In [23], a variant of the Furstenberg correspondence principle was used to show that Conjecture 1.2 implied Conjecture 1.1 for any given choice of p, k. In [1], Conjecture 1.2 was established in the high characteristic case $k + 1 \leq p$; combining the two results, this also gave Conjecture 1.1 in this regime. The full case of Conjecture 1.1 was subsequently established in [23] by a different method; alternate proofs of some or all of the cases of this conjecture have since been given in [7], [8], [4], [24], [18]. In particular Conjecture 1.2 was established in [4, Theorem 1.12] in the slightly larger range $k \leq p + 1$ (and an alternate proof of Conjecture 1.1 was given for all k, p). We also remark that in [1, Theorem 1.20], a weaker version of Conjecture 1.2 was established in which $\mathrm{Poly}^k(X)$ was replaced by some unspecified subalgebra of $\mathrm{Poly}^{C(p,k)}(X)$ for some constant $C(p, k)$ depending only on p, k. We also note that several other structural results on ergodic $\mathbb{F}_p^\omega$-systems are known; see in particular [4], [16].

Although it was not explicitly noted in [23], Conjecture 1.2 in fact gives a stronger version of Conjecture 1.1 in which the polynomial P produced by the conjecture is (approximately) "measurable" with respect to the original function f together with random shifts. More precisely, consider the following more complicated strengthening of Conjecture 1.1.

Conjecture 1.3 (Strong inverse conjecture for the Gowers norm)**.** *Let $\eta > 0$, and let $\varepsilon\colon \mathbb{N} \to \mathbb{R}^+$ be a decreasing function. Then there exists $M = M(k, p, \eta, \varepsilon())$ such that whenever $G = \mathbb{F}_p^n$ is an elementary abelian p-group and functions $f\colon G \to \mathbb{D}$ with $\|f\|_{U^{k+1}(G)} \geq \eta$, such that if $\vec{h} = (h_1, \ldots, h_M) \in G^M$ is a tuple of shifts drawn uniformly from G^M, then with probability at least $1/2$, there exist $1 \leq m \leq M$, $P \in \mathrm{Poly}^k(G)$ and a function $F\colon \mathbb{D}^{\mathbb{F}_p^M} \to \mathbb{C}$ of Lipschitz constant at most M (using say the Euclidean metric on $\mathbb{D}^{\mathbb{F}_p^M}$), such that*

$$|\mathbb{E}_{x\in G} f(x)e(-P(x))| \geq \frac{1}{m}$$

and

$$\left|\mathbb{E}_{x\in G} e(P(x)) - F\left(\left(f(x + a\cdot\vec{h})\right)_{a\in\mathbb{F}_p^M}\right)\right| \leq \varepsilon(m).$$

The numerical value of the probability $1/2$ here is inessential and could be replaced by any other constant between 0 and 1. Roughly speaking, Conjecture 1.3 is a strengthening of Conjecture 1.1 in which the polynomial P produced by that conjecture is well approximated by some combination of random shifts of f, where the degree $\varepsilon(m)$ of approximation can be guaranteed to be much better than the level $\frac{1}{m}$ of correlation between the polynomial P and the original function f. The Lipschitz property of F is unimportant, since one can easily discretize f to take on a bounded number of values, but we retain it for minor technical reasons.

Example 1.4. When $k = 1$, Conjecture 1.3 can be established by standard Fourier-analytic arguments which we now sketch here (suppressing the precise quantitative bounds needed to make precise terms such as "large" in order to simplify the exposition). If $f \colon G \to \mathbb{D}$ has large $U^2(G)$ norm, then f has a large inner product with the convolution $f*f*\tilde{f}$, where $\tilde{f}(x) := \overline{f}(-x)$. Furthermore, this convolution can be approximated in the uniform norm by a bounded linear combination of characters $e(\xi \cdot x)$. If one chooses a large number of random shifts $h_1, \dots, h_M$, then with high probability one can find a convolution filter on these shifts that isolates one of these characters, that is to say there exists a linear combination λ of the Kronecker delta functions $\delta_{h_1}, \dots, \delta_{h_M}$ such that $f * f * \tilde{f} * \lambda(x)$ is close to $e(\xi \cdot x)$. By further random sampling of the $f * \tilde{f}$ factor (and increasing the number M of shifts if necessary), one can with high probability approximate $f * f * \tilde{f} * \lambda$ (in L^1 norm) by a linear combination of shifts of f along linear combinations of $h_1, \dots, h_M$. This can then be used to establish the $k = 1$ case of Conjecture 1.3; we leave the details to the interested reader.

For $k = 2, 3$ (and $p = 2$), the strong inverse conjecture is reminiscent[1] of the quadratic Goldreich–Levin theorem from [25] (and the more recent cubic Goldreich–Levin theorem from [17]), which gives a polynomial (in n) time randomized algorithm to reconstruct the polynomial P from the function f; however strong inverse conjecture is (in principle) stronger than these Goldreich–Levin type results, in that it should (after some additional effort) yield a *bounded-time* (rather than polynomial-time) randomized algorithm to obtain an *approximation* to the polynomial P. Such algorithms

[1] We are indebted to James Leng for this observation.

are similar in spirit[2] to implicit (or "local") list decoding algorithms for Reed–Muller codes, as discussed for instance in [20], [6].

In Appendix B we will modify the arguments in [23] to show

Theorem 1.5 (Application of correspondence principle)**.** *For any given choice of k and p, Conjecture 1.2 implies Conjecture 1.3 (and hence also Conjecture 1.1).*

In particular, from the previously mentioned results of [4], Conjecture 1.3 holds in the high characteristic case $k \leq p + 1$; also, from [1, Theorem 1.20] one can establish a weaker version of Conjecture 1.3 in which the polynomial P is of degree at most $C(p, k)$ rather than k for some quantity $C(p, k)$ depending only on p, k.

However, the low characteristic case presents additional difficulties; for instance, a key "exact roots" property for polynomials in order k $\mathbb{F}_p^\omega$-systems is known to fail in low characteristic [23, Appendix E]. In fact we are able to construct the following counterexample, which is the main result of our paper.

Theorem 1.6 (Counterexample to strong inverse conjecture)**.** *Conjecture 1.3 fails when $p = 2$ and $k = 5$.*

Combining Theorem 1.6 with the contrapositive of Theorem 1.5, we conclude that Conjecture 1.2 also fails when $p = 2$ and $k = 5$; see also Remark 5.11 for how one might give a more direct construction of a counterexample to that conjecture. Our construction was located numerically, but we give a human-verifiable proof of the theorem here, taking advantage in particular of several technical simplifications available in the $p = 2$ case (in particular, we take advantage of the ability to identify the n-dimensional cube $\{0, 1\}^n$ with the n-dimensional vector space $\mathbb{F}_2^n$, for instance in (62)). It would be interesting to determine the complete range of p, k for which Conjecture 1.3 and Conjecture 1.2 holds; for instance, the case $p = 2, k = 4$ remains unresolved for both conjectures, and we have not been able to rigorously establish that these conjectures are monotone in k.

[2] We are indebted to Avi Wigderson for this remark.

Informally, Theorem 1.6 asserts that in characteristic two, there exist "pseudo-quintic" functions f which have large $U^6(\mathbb{F}_2^n)$ norm, and in fact correlate with a genuine quintic $e(P)$, but that the quintics that f correlates with will be "non-measurable" in the sense that they cannot be approximated by a combination of boundedly many translates of f. Instead, one has to use "non-measurable" operations, such as taking exact roots of polynomials as in [23], in order to locate such quintics $e(P)$.

Remark 1.7. Recently, quantitative versions of Conjecture 1.1 for $p = 2$ and $k = 3, 4, 5$ have been established in [24, 18]; in particular the paper [18] covers the case $p = 2, k = 5$ of Theorem 1.6. This is however not a contradiction; a crucial step [24, Proposition 3.5] in both those papers (a special case of Theorem 2.3 below) is the ability to represent a "strongly symmetric k-linear form" as the k-fold derivative of a degree k polynomial, and this step is "non-measurable" as it requires one to expand the form into monomials using a choice of basis for $\mathbb{F}_2^n$.

1.1. **Overview of proof.** We now give an informal, high-level description of our proof of Theorem 1.6, deferring more precise details to later sections. Roughly speaking, it would suffice to exhibit, for any sufficiently large n, a function $S : \mathbb{F}_2^n \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ which was "pseudo-quintic" in the sense that the Gowers norm $\|e(S)\|_{U^6(\mathbb{F}_2^n)}$ was large, but such that $e(S)$ did not correlate in any significant fashion with $e(P)$ for any genuine quintic polynomial $P\colon \mathbb{F}_2^n \to \mathbb{T}$ which was somehow "measurable" with respect to S and related functions.

One way to ensure that the Gowers norm $\|e(S)\|_{U^6(\mathbb{F}_2^n)}$ is to enforce some structure on the sixth derivative $d^6S : \mathbb{F}_2^n \times (\mathbb{F}_2^n)^6 \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of S, defined by the formula

$$(d^6S)_{h_1,\dots,h_6}(x) := \partial_{h_1} \dots \partial_{h_6} S(x)$$

where $\partial_h S(x) := S(x + h) - S(x)$. Indeed, a routine application of the Gowers–Cauchy–Schwarz inequality and Fourier decomposition reveals that if $(d^6S)_{h_1,\dots,h_6}(x)$ can be expressed in terms of a bounded number of quintic or lower degree polynomials applied to the various vertices $x + \omega \cdot \vec{h}$ of the 6-dimensional cube $(x + \omega \cdot \vec{h})_{\omega\in\{0,1\}^6}$, then $e(S)$ will have large $U^6(\mathbb{F}_2^n)$ norm (see Lemma 5.2 for a rigorous version of this implication). As it turns out, we will be able to construct a counterexample in which $d^6 S$ is a function of a (randomly chosen) *quadratic* polynomial $Q\colon \mathbb{F}_2^n \to \mathbb{F}_2^2$ taking values in the Klein four-group $X_2 := \mathbb{F}_2^2$. That is to say, S will be chosen to obey the equation

$$(d^6 S)_{h_1,\dots,h_6}(x) = \rho\left(\left(Q(x+\omega\cdot\vec{h})\right)_{\omega\in\{0,1\}^6}\right) \tag{1}$$

for some function $\rho\colon C^6(X_2) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ whose domain $C^6(X_2) \subset X_2^{\{0,1\}^6}$ is a space of "6-cubes" in X_2 that contains all possible values of the tuple $\left(Q(x+\omega\cdot\vec{h})\right)_{\omega\in\{0,1\}^6}$. In fact, $C^6(X_2)$ can be described explicitly as the set of all tuples of the form

$$\left(x + \sum_{i=1}^{6} h_i\omega_i + \sum_{1\le i<j\le 6} h_{ij}\omega_i\omega_j\right)_{\omega\in\{0,1\}^6}$$

for $x, h_i, h_{ij} \in X_2$. (In the language of nilspaces that we will use later, we are equipping X_2 with the nilspace structure associated to the degree two filtration $\mathcal{D}_2(\mathbb{F}_2^2)$ on the Klein four-group.)

The function ρ has to obey a certain number of properties in order to be able to find a solution S to the equation (1). Firstly, ρ must be symmetric with respect to permutations of $\{1,\dots,6\}$ and must also obey a certain "cocycle equation" arising from the identity $\partial_{h+k}S = \partial_h S + T^h\partial_k S$, where $T^h S(x) := S(x+h)$ is the shift map. These properties can be formalized in the language of nilspaces by requiring ρ to be a *degree* 5 *cocycle* on X_2 taking values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$; see Definition A.6 for details. However, the property of being a degree 5 cocycle is not yet sufficient to guarantee a solution to (1); in the language of nilspaces, not all degree 5 cocycles on $\mathbb{F}_2^n$ are degree 5 coboundaries. In order to locate a solution, we will require the cocycle ρ to obey an additional property that we call "strong 2-homogeneity". This property asserts that ρ takes the form

$$\rho((x_\omega)_{\omega\in\{0,1\}^6}) = \sum_{\omega\in\{0,1\}^5} (-1)^{5-|\omega|}\psi(x_{\omega 0}, x_{\omega 1})$$

for all $(x_\omega)_{\omega\in\{0,1\}^6}$ in $C^6(X_2)$ and some function $\psi\colon C^1(X_2) \to \mathbb{T}$ on the space of pairs $C^1(X_2) = X_2 \times X_2$ on X_2, such that 2ψ is a "cubic" polynomial on $C^1(X_2)$ with respect to a certain natural nilspace structure on $C^1(X_2)$; see Definition 2.5 for a precise statement. This turns out to be sufficient to guarantee the existence of the pseudo-quintic function $S : \mathbb{F}_2^n \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$; see Theorem 2.6 and Lemma 4.1 for precise statements.

We would still like to ensure that S does not correlate with a quintic phase $e(P)$ where P can be well approximated in terms of S and its translates. An obstruction to this claim would occur if the cocycle ρ was a "degree 5 coboundary" in the sense that ρ takes the form

$$\rho((x_\omega)_{\omega\in\{0,1\}^6}) = \sum_{\omega\in\{0,1\}^6} (-1)^{6-|\omega|} F(x_\omega)$$

for all $(x_\omega)_{\omega\in\{0,1\}^6}$ in $C^6(X_2)$ and some function $F\colon X_2 \to \mathbb{T}$. Indeed, if this were the case, then one could rearrange (1) as

$$d^6(S - F(Q)) = 0$$

and thus we have $e(S) = e(P)e(F(Q))$ for some quintic polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^n)$. Morally speaking, this relation indicates that $e(P)$ correlates with $e(S)$, and that P should be well approximated by S and its translates (since from (1) we expect Q to similarly be well approximable in this fashion).

The key step in our argument is thus to locate a degree 5 cocycle $\rho\colon C^6(X_2) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ which is strongly 2-homogeneous, but not a degree 5 coboundary. This is accomplished in Section 3. We remark that this claim involves a finite system of linear equations on a finite-dimensional vector space over $\mathbb{F}_2$, and can be verified numerically by standard linear algebra packages (and in particular through calculations of certain Smith normal forms of matrices); indeed, we used such computer-assisted calculations to lead us to this particular claim. However, we were subsequently able to describe the cocycle ρ and verify its properties in a completely human-verifiable fashion; see Section 3 for details.

Remark 1.8. With our specific choice of ρ, we can describe the solutions to (1) more explicitly as

$$S = \frac{\binom{R}{2}Q_2}{2} + P$$

where $Q = (Q_1, Q_2)$, $R\colon \mathbb{F}_2^n \to \mathbb{Z}/4\mathbb{Z}$ is a cubic polynomial which is a "square root" of Q_1 in the sense that $2\frac{R}{4} = \frac{Q_1}{2} \mod 1$ (or equivalently $R = Q_1 \mod 2$), and $P\colon \mathbb{F}_2^n \to \mathbb{T}$ is an arbitrary quintic polynomial (we can require P to take values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if we wish S to also take values in this group). See Lemma 4.2. Heuristically, the presence of the square root in this construction prevents the quintic P (which correlates with S) from being "measurable" with respect to S and its shifts, although actually demonstrating this rigorously requires a surprisingly large amount of effort.

In order to convert this explicit cocycle ρ into an actual counterexample to Conjecture 1.3 we will rely heavily on the theory of *nilspaces*, as developed for instance in [3], although we will mostly only need to work with *finite* nilspaces, as opposed to compact or measurable nilspaces. A central role is played in particular by a certain explicit 5-step finite nilspace $X_{5,5}$. As a set, $X_{5,5}$ is given as

$$X_{5,5} = X_2 \times \frac{1}{2^5}\mathbb{Z}/\mathbb{Z} = \mathbb{F}_2^2 \times \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$$

but the cube structure on $X_{5,5}$ is somewhat non-trivial, involving the cocycle $\rho\colon C^6(X_2) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ mentioned previously. Roughly speaking, the nilspace $X_{5,5}$ is the abstraction of a pair (Q, S) of functions, in which Q is itself a pair $Q = (Q_1, Q_2)$ of classical quadratic polynomials (taking values in $\mathbb{F}_2$), and S is a "pseudo-quintic" taking values in $\frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ that obeys the identity (1). It will turn out not to be possible to correlate S with any genuine quintics that only arise from Q, S, and a bounded (and randomly selected) number of their translates. The actual verification that these translates do not actually provide any useful information for the purpose of constructing a quintic turns out to be rather tricky, requiring one to show that a certain nilspace extension "splits": see Lemma 5.7. A simpler version $X_{5,1}$ of the nilspace $X_{5,5}$, in which the cyclic group $\frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ is replaced by $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, can also be used to quickly answer a question of Candela, González-Sánchez, and Szegedy [4, Question 5.18] in the negative, thus giving a weaker version of Theorem 1.6; see Proposition 4.5.

1.2. **Acknowledgments.** OS was supported by OS was supported by NSF grant DMS-1926686 and ISF grant 3056/21. TT was supported by a Simons Investigator grant, the James and Carol Collins Chair, the Mathematical Analysis & Application Research Fund Endowment, and by NSF grant DMS-1764034.

1.3. **Notation.** We identify the field $\mathbb{F}_2$ with the cyclic group $\mathbb{Z}/2\mathbb{Z}$. If a is an element of a cyclic group $\mathbb{Z}/q\mathbb{Z}$, we use $\frac{a}{q}$ to denote the corresponding element of the finite subgroup $\frac{1}{q}\mathbb{Z}/\mathbb{Z}$ of the unit circle $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, thus

$$\frac{a+q\mathbb{Z}}{q} = \frac{a}{q} \mod 1.$$

We observe that the binomial coefficient $n \mapsto \binom{n}{2}$ is well-defined as a map from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{F}_2$; indeed, we have $\binom{n}{2} = 0 \mod 2$ when $n = 0, 1 \mod 4$ and $\binom{n}{2} = 1 \mod 2$ when $n = 2, 3 \mod 4$.

2. A characterization of coboundaries on $\mathbb{F}_2^n$

Let $G = (G, +)$ be a discrete abelian group. As discussed in Appendix A, G can be given the structure $\mathcal{D}^1(G)$ of a degree one filtered abelian group, and hence a nilspace. Given a function $F\colon G \to \mathbb{T}$ from G to the torus $\mathbb{T}$, this gives a derivative map $d^{k+1}F\colon G^{[k+1]} \to \mathbb{T}$ for every $k \geq 0$. We can describe this map more explicitly by using the identification $G \times G^{k+1} \equiv G^{[k+1]}$ given by the formula

$$(x, \vec{h}) \equiv \left(x + \omega \cdot \vec{h}\right)_{\omega \in \{0,1\}^{k+1}} \tag{2}$$

for $x \in G$ and $\vec{h} = (h_1, \dots, h_{k+1}) \in G^{k+1}$, and then writing

$$\begin{aligned}(d^{k+1}F)_{h_1,\dots,h_{k+1}}(x) &:= d^{k+1}F\left(\left(x + \omega \cdot \vec{h}\right)_{\omega \in \{0,1\}^{k+1}}\right)\\ &= \sum_{\omega \in \{0,1\}^{k+1}} (-1)^{k+1-|\omega|} F\left(x + \omega \cdot \vec{h}\right)\\ &= \partial_{h_1} \dots \partial_{h_{k+1}} F(x).\end{aligned}$$

Thus for instance we have

$$\mathrm{Poly}^k(G) = \{F\colon G \to \mathbb{T} : d^{k+1}F = 0\}$$

for any $k \geq 0$.

In a similar spirit, a degree k cocycle $\rho\colon G^{[k+1]} \to \mathbb{T}$ as defined in Definition A.6 can now be thought of as a tuple $\rho_{h_1,\dots,h_{k+1}}\colon G \to \mathbb{T}$ for each $h_1, \dots, h_{k+1} \in G$ obeying the following two axioms:

- (Symmetry) $\rho_{h_1,\dots,h_{k+1}}$ is symmetric in the parameters $h_1, \dots, h_{k+1}$.
- (Cocycle) One has the identity

$$\rho_{h_1+h_1',h_2,\dots,h_{k+1}} = \rho_{h_1,h_2,\dots,h_{k+1}} + T^{h_1}\rho_{h_1',h_2,\dots,h_{k+1}} \tag{3}$$

for all $h_1, h_1', h_2, \ldots, h_{k+1} \in G$, where (as in Appendix A) T^h denotes the translation operator

$$T^h F(x) := F(x+h).$$

We describe the cocycle property (3) in terms of the first shift h_1 only, but of course by the symmetry property, we have cocycle behavior with respect to all the other shifts as well. In the language of Definition A.6, $d^{k+1}F$ is a degree k coboundary, and thus also a degree k cocycle.

When G is an elementary abelian 2-group, there is a further constraint on degree k coboundaries $d^{k+1}F$, coming from the identity

$$0 = \partial_{2h} = 2\partial_h + \partial_h^2 \tag{4}$$

for any $h \in G$, which implies that

$$\partial_{h_1}^2 \partial_{h_2} = \partial_{h_2}^2 \partial_{h_1} \tag{5}$$

for all $h_1, h_2 \in G$. This leads to the additional "2-homogeneity" constraint

$$d^{k+1}F_{h_1,h_1,h_2,h_3,\ldots,h_k} = d^{k+1}F_{h_2,h_2,h_1,h_3,\ldots,h_k} \tag{6}$$

whenever $k \geq 2$ and $h_1, \ldots, h_k \in G$ (our choice of terminology here is inspired by [4]) . This motivates the following definition:

Definition 2.1 (2-homogeneous cocycles on elementary abelian 2-groups)**.** Let G be an elementary abelian 2-group, and let $\rho\colon G^{[k+1]} \to \mathbb{T}$ be a degree k cocycle for some $k \geq 0$. If $k \geq 2$, we say that ρ is 2-*homogeneous* if we have

$$\rho_{h_1,h_1,h_2,h_3,\ldots,h_k} = \rho_{h_2,h_2,h_1,h_3,\ldots,h_k} \tag{7}$$

whenever $h_1, \ldots, h_k \in G$. For $k < 2$, we declare all degree k cocycles to automatically be 2-homogeneous.

Remark 2.2. Not all cocycles on elementary abelian 2-groups obey the 2-homogeneity condition (7). For instance, if $G = \mathbb{F}_2^2$ is generated by $e_1 = (1,0), e_2 = (0,1)$, then by letting $\rho\colon G^{[3]} \to \mathbb{T}$ be the symmetric trilinear form

$$\rho_{h_1,h_2,h_3}(x) := \frac{h_1^{(2)}h_2^{(1)}h_3^{(1)} + h_1^{(1)}h_2^{(2)}h_3^{(1)} + h_1^{(1)}h_2^{(1)}h_3^{(2)}}{2} \mod 1,$$

where $h_i = (h_i^{(1)}, h_i^{(2)}) \in G$, one can verify that ρ is a degree 2 cocycle on the elementary abelian 2-group G that does not obey (7). This degree 2 cocycle will be related to a non-trivial (but now 2-homogeneous) degree 5 cocycle on the degree 2 filtered abelian group $\mathcal{D}^2(\mathbb{F}_2^2)$ that we will construct in the next section.

We have just established that every degree k coboundary on an elementary abelian 2-group is 2-homogeneous. We now provide a converse to this above observation when $G = \mathbb{F}_2^n$.

Theorem 2.3 (All 2-homogeneous $\mathbb{T}$-cocycles are coboundaries for elementary abelian 2-groups)**.** *Let $G = \mathbb{F}_2^n$ be an elementary abelian 2-group, and let $k \geq 0$. Then every 2-homogeneous degree k cocycle $\rho\colon G^{[k+1]} \to \mathbb{T}$ is a degree k coboundary.*

Informally, this theorem asserts that the equation $d^kF = \rho$ can be solved for some $F\colon G \to \mathbb{T}$ if and only if ρ is a 2-homogeneous degree k cocycle. This fact will be useful to us when the time comes to solve the equation (1), as discussed in the introduction.

Remark 2.4. A notable special case of this theorem occurs when $\rho_{h_1,\dots,h_k}$ is constant for each $h_1, \dots, h_k$, then the 2-homogeneous degree k cocycle ρ is what is referred to as a *non-classical symmetric multilinear form* in [24] and a *strongly symmetric multilinear form* in [8], and the potential F produced by this theorem is then a (non-classical) polynomial of degree k. This special case of Theorem 2.3 was previously established in [24, Proposition 3.5].

Proof. We first consider the base case $k = 0$. From the cocycle identity we have

$$\rho_{x+h}(0) = \rho_x(0) + \rho_h(x)$$

for all $x, h \in G$. Hence we have $\rho = dF$ where $F(x) \coloneqq \rho_x(0)$.

Now suppose inductively that $k > 0$ and the claim has already been proven for $k - 1$. For each $h_1 \in G$, the function $\rho_{h_1}\colon G^{[k]} \to \mathbb{T}$ defined by $(\rho_{h_1})_{h_2,\dots,h_{k+1}}(x) \coloneqq \rho_{h_1,\dots,h_{k+1}}(x)$ can be easily verified to be a 2-homogeneous degree $k-1$ cocycle. Hence by induction hypothesis, there exists $F_{h_1}\colon G \to \mathbb{T}$ such that

$$\rho_{h_1} = d^kF_{h_1}. \tag{8}$$

Since ρ_{h_1} is a cocycle in h_1, we have

$$d^k F_{h_1+h_1'} = d^k F_{h_1} + T^{h_1} d^k F_{h_1'}$$

for all $h_1, h_1' \in G$. In other words, we have the quasi-cocycle condition

$$F_{h_1+h_1'} - F_{h_1} - T^{h_1} F_{h_1'} \in \mathrm{Poly}^{k-1}(G). \tag{9}$$

Also, from the symmetry between h_1, h_2 of $(\rho_{h_1})_{h_2,\dots,h_{k+1}}$, we have that

$$\partial_{h_3,\dots,h_{k+1}}(\partial_{h_2} F_{h_1} - \partial_{h_1} F_{h_2}) = 0$$

for all $h_1, \dots, h_{k+1} \in G$, or in other words we have the quasi-curlfree condition

$$\partial_{h_2} F_{h_1} - \partial_{h_1} F_{h_2} \in \mathrm{Poly}^{k-2}(G) \tag{10}$$

for all $h_1, h_2 \in G$. Finally, when $k \geq 2$, we have from (6) that

$$\partial_{h_3} \dots \partial_{h_k}(\partial_{h_1}^2 F_{h_2} - \partial_{h_2}^2 F_{h_1}) = 0$$

for all $h_1, \dots, h_k \in G$, or equivalently

$$\partial_{h_1}^2 F_{h_2} - \partial_{h_2}^2 F_{h_1} \in \mathrm{Poly}^{k-3}(G)$$

and hence (by (4))

$$2(\partial_{h_2} F_{h_1} - \partial_{h_1} F_{h_2}) \in \mathrm{Poly}^{k-3}(G). \tag{11}$$

This constraint is implied by (10) when $k > 2$ thanks to (61), but is not redundant for $k = 2$.

We will show that the properties (9), (10), (11) imply that there exists $\phi\colon G \to \mathbb{T}$ such that

$$F_h - \partial_h \phi \in \mathrm{Poly}^{k-1}(G) \tag{12}$$

for all $h \in G$. If (12) holds, then by applying d^k and using (8) we conclude that $\rho - d^{k+1}\phi = 0$, giving the claim.

It remains to establish (12). We prove this by a further induction on the dimension n. The case $n = 0$ is trivial, so suppose $n \geq 1$ and that the claim has already been proven for $n-1$. Now split $G = \mathbb{F}_2^{n-1} \times \mathbb{F}_2$ and let $e = (0, 1)$ be the generator for the $\mathbb{F}_2$ factor. The operator ∂_e is annihilated by $1 + T^e$ since $(1 + T^e)\partial_e = \partial_{2e} = 0$. Also, for $k > 2$, the operator $1 + T^e = 2 + \partial_e$ maps $\mathrm{Poly}^{k-2}(G)$ to $\mathrm{Poly}^{k-3}(G)$ thanks to (61), hence from (10)

$$\partial_h(1 + T^e)F_e \in \mathrm{Poly}^{k-3}(G)$$

for all $h \in G$, hence

$$(1 + T^e)F_e \in \mathrm{Poly}^{k-2}(G). \tag{13}$$

The same argument works when $k = 2$, where we use (11) instead of (10) to handle the 2 component of $1 + T^e = 2 + \partial_e$ applied to $\partial_h F_e - \partial_e F_h$. The conclusion (13) also holds when $k = 1$, since in this case the expression (10) vanishes.

Applying Lemma A.24, we may find $F'_e \in \mathrm{Poly}^{k-1}(G)$ such that

$$(1 + T^e)F_e = (1 + T^e)F'_e$$

Since $F_e - F'_e$ is annihilated by $1 + T_e$, we may write

$$F_e - F'_e = \partial_e \phi$$

for some $\phi\colon G \to \mathbb{T}$. If we then write

$$F''_h := F_h - F'_e - \partial_h \phi$$

we see that F''_h obeys the same axioms (9), (10), (11) as F_h, but with the additional property that $F''_e = 0$. In particular from (10) we have

$$\partial_e F''_{(h,0)} \in \mathrm{Poly}^{k-2}(G)$$

for all $h \in \mathbb{F}_2^{n-1}$. Since $\partial_e F''_{(h,0)}(x, 1) = -\partial_e F''_{(h,0)}(x, 0)$, we thus have

$$\partial_e F''_{(h,0)}(x, x_n) = (-1)^{x_n} G_h(x)$$

for all $x \in \mathbb{F}_2^{n-1}$ and some $G_h \in \mathrm{Poly}^{k-2}(\mathbb{F}_2^{n-1})$. If we set $H_h\colon G \to \mathbb{T}$ be the function

$$H_h(x, x_n) := 1_{x_n=1} G_h(x),$$

then

$$\partial_e H_h = \partial_e F''_{(h,0)} \tag{14}$$

is a polynomial of degree $k - 2$ on G, while

$$\partial_{h_1} \dots \partial_{h_{k-1}} H_h = 0$$

whenever $h_1, \dots, h_{k-1} \in \mathbb{F}_2^{n-1}$. From this (and Lemma A.17) we conclude that $H_h \in \mathrm{Poly}^{k-1}(G)$. By (14), $F''_{(h,0)} - H_h$ is e-invariant and can be thus viewed as a function on $\mathbb{F}_2^{n-1}$. One then verifies that the functions $F''_{(h,0)} - H_h$ obey the same axioms (9), (10), (11) as F_h, but on $\mathbb{F}_2^{n-1}$ rather than $\mathbb{F}_2^n$.

Applying the inner induction hypothesis and lifting back to G, we can find an e-invariant $\phi'' \colon G \to \mathbb{T}$ such that

$$F''_{(h,0)} - H_h - \partial_{(h,0)}\phi'' \in \mathrm{Poly}^{k-1}(G)$$

for all $h \in \mathbb{F}_2^{n-1}$, thus

$$F''_h - \partial_h \phi'' \in \mathrm{Poly}^{k-1}(G) \tag{15}$$

for all $h \in \mathbb{F}_2^{n-1} \times \{0\}$. On the other hand, from (9), the vanishing of F''_e, and the e-invariance of ϕ'' we see that

$$(F''_{h+e} - \partial_{h+e}\phi'') - (F''_h - \partial_h\phi'') \in \mathrm{Poly}^{k-1}(G)$$

and hence the property (15) holds for all $h \in \mathbb{F}_2^n$, not just $h \in \mathbb{F}_2^{n-1} \times \{0\}$. In particular,

$$F_h - \partial_h(\phi + \phi'') \in \mathrm{Poly}^{k-1}(G)$$

for all h, thus closing the induction. □

The above theorem applies to cocycles taking values in $\mathbb{T}$. For our application (and in particular, to solve the equation (1)) we will need a variant of this theorem that applies to cocycles taking values in the smaller group $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, which is an elementary abelian 2-group. For this, we will need a stronger version of the 2-homogeneity condition, which we only define for $k \geq 3$, but which we will define on more general nilspaces than elementary abelian 2-groups with the degree 1 filtration.

Definition 2.5 (Strongly 2-homogeneous cocycles)**.** Let X be a finite nilspace, let $k \geq 3$, and let $\rho \colon C^{k+1}(X) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ be a degree k cocycle taking values in the elementary abelian 2-group $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. We say that ρ is *strongly* 2-*homogeneous* if we have $\rho = d^k\psi$ for some function $\psi \colon C^1(X) \to \mathbb{T}$ with $2\psi \in \mathrm{Poly}^{k-2}(C^1(X))$, where the nilspace structure on $C^1(X)$ is defined in Remark A.3.

We first observe that strongly 2-homogeneous cocycles on $\mathcal{D}^1(\mathbb{F}_2^n)$ are 2-homogeneous (viewed as cocycles in $\mathbb{T}$). Indeed, since $\rho = d^k\psi$ and $k \geq 3$, we have

$$\rho_{h_1,h_1,h_2,h_3,\dots,h_k} = \partial_{h_1}^2 \partial_{h_2} (d^{k-3}\psi)_{h_3,\dots,h_k}$$

and

$$\rho_{h_1,h_2,h_2,h_3,\dots,h_k} = \partial_{h_2}^2 \partial_{h_1} (d^{k-3}\psi)_{h_3,\dots,h_k}$$

and the condition (7) follows from (5). Now we obtain a variant of Theorem 2.3.

Theorem 2.6 (All strongly 2-homogeneous cocycles are $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-coboundaries for elementary abelian 2-groups)**.** *Let $G = \mathbb{F}_2^n$ for some natural number n (endowed with the degree one filtration $\mathcal{D}^1(G)$), and let $k \geq 3$. Then a degree k cocycle $\rho\colon G^{[k+1]} \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is a degree k coboundary (in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ rather than in $\mathbb{T}$) if and only if it is strongly 2-homogeneous.*

Proof. First suppose that ρ is a degree k coboundary in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, thus $\rho = d^k F$ for some $F\colon G \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Then we can write $\rho = d^{k-1}\psi$ with $\psi := dF$; since $2F = 0$, we have $2\psi = 0$, and so ρ is certainly strongly 2-homogeneous.

Conversely, suppose that ρ is strongly 2-homogeneous. Applying Theorem 2.3 (viewing ρ as a cocycle in the larger group $\mathbb{T}$), we already have

$$\rho = d^{k+1}F$$

for some $F\colon G \to \mathbb{T}$. However, we are not done yet, because this function F does not necessarily lie in the smaller group $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. To address this issue, we exploit the further properties of the strongly 2-homogeneous cocycle ψ. Writing $\rho = d^k\psi$, we have

$$d^k(dF - \psi) = 0$$

or equivalently

$$dF - \psi \in \mathrm{Poly}^{k-1}(C^1(G)).$$

Multiplying by 2 using Proposition A.22, we conclude that

$$d(2F) - 2\psi \in \mathrm{Poly}^{k-2}(C^1(G));$$

since 2ψ also lies in $\mathrm{Poly}^{k-2}(C^1(G))$ by hypothesis, we conclude

$$d(2F) \in \mathrm{Poly}^{k-2}(C^1(G))$$

or equivalently

$$2F \in \mathrm{Poly}^{k-1}(G).$$

By (61), we may thus write $2F = 2F'$ for some $F' \in \mathrm{Poly}^k(G)$. Then $F - F'$ takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and

$$\rho = d^{k+1}F = d^{k+1}(F - F'),$$

giving the claim. □

3. A non-trivial cocycle

Henceforth we take $k = 5$ and $p = 2$. Theorem 2.6 asserts, roughly speaking, there are no "non-trivial" order k cocycles on degree one filtrations $\mathcal{D}^1(\mathbb{F}_2^n)$, where by "non-trivial" we mean an order k cocycle which is strongly 2-homogeneous but not an order k-coboundary. However, it turns out that this claim breaks down as soon as $n = 2$ if one instead considers the degree two filtration $\mathcal{D}^1(\mathbb{F}_2^n)$. More precisely, the main result of this section is as follows. For the remainder of the paper, we take X_2 to be the 2-step nilspace

$$X_2 \coloneqq \mathcal{D}^2(\mathbb{F}_2^2), \tag{16}$$

which is also 2-homogeneous thanks to Proposition A.29.

Theorem 3.1 (A non-trivial cocycle)**.** *There exists a strongly* 2*-homogeneous degree* 5 *cocycle* $\rho\colon C^6(X_2) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ *on* X_2 *taking values in* $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$*, which is not a degree* 5 *coboundary (when viewed as a cocycle in* $\mathbb{T}$*).*

In the remainder of this section we establish this theorem; our original discovery of this cocycle was computer-assisted, and indeed one could easily verify the claims in this theorem from standard linear algebra packages, but we provide a human-verifiable proof of this theorem below.

It will be convenient to adopt the following notation from [23, Definitions 6.1, 6.3].

Definition 3.2 (Concatenation and symmetric square)**.** [23] If V is a vector space over a field $\mathbb{F}$, and $S : V^k \to \mathbb{F}$ and $T\colon V^l \to \mathbb{F}$ are symmetric multilinear forms, we define the *concatenation* $S * T\colon V^{k+l} \to \mathbb{F}$ to be the symmetric multilinear form

$$S * T(h_1, \dots, h_{k+l}) \coloneqq \sum_{\{1,\dots,k+l\}=\{i_1,\dots,i_k\}\cup\{j_1,\dots,j_l\}} S(h_{i_1}, \dots, h_{i_k})T(h_{j_1}, \dots, h_{j_l})$$

and similarly define the symmetric square $\mathrm{Sym}^2(S)\colon V^{2k} \to \mathbb{F}$ to be the symmetric multilinear form

$$\begin{aligned}&\mathrm{Sym}^2(S)(h_1, \dots, h_{2k})\\ &\quad\coloneqq \sum_{\{\{i_1,\dots,i_k\},\{j_1,\dots,j_k\}\}:\{1,\dots,2k\}=\{i_1,\dots,i_k\}\cup\{j_1,\dots,j_k\}} S(h_{i_1}, \dots, h_{i_k})S(h_{j_1}, \dots, h_{j_l}).\end{aligned}$$

One can similarly define higher symmetric powers $\mathrm{Sym}^m(S)\colon V^{mk} \to \mathbb{F}$, but we will only need the $m = 2$ case here.

Examples 3.3. If $B\colon V^2 \to \mathbb{F}$ is a symmetric bilinear form, then $\mathrm{Sym}^2(B)\colon V^4 \to \mathbb{F}$ is the symmetric quartilinear form

$$\mathrm{Sym}^2(B)(a,b,c,d) := B(a,b)B(c,d) + B(a,c)B(b,d) + B(a,d)B(b,c),$$

while if $L\colon V \to F$ is a linear form, then $L * B\colon V^3 \to \mathbb{F}$ is the trilinear form

$$L * B(a,b,c) := L(a)B(b,c) + L(b)B(a,c) + L(c)B(a,b)$$

and $B*B = 2\mathrm{Sym}^2(B)$; in particular, in characteristic two we have $B*B = 0$. The trilinear form in Remark 2.2 can be written as

$$\rho_{h_1,h_2,h_3}(x) = (\mathrm{Sym}^2(L_1) * L_2)(h_1,h_2,h_3) \tag{17}$$

where $L_1, L_2\colon \mathbb{F}_2^2 \to \mathbb{F}_2$ are the coordinate functions $L_i(x_1,x_2) := x_i$.

A 6-cube in $X_2 = \mathcal{D}^2(\mathbb{F}_2^2)$ can be viewed as a pair $(Q^{(1)}, Q^{(2)})$, where $Q^{(1)}, Q^{(2)}\colon \mathbb{F}_2^6 \to \mathbb{F}_2$ are quadratic polynomials, so in particular their second derivatives can be viewed as symmetric bilinear forms $d^2Q^{(i)}\colon \mathbb{F}_2^6 \times \mathbb{F}_2^6 \to \mathbb{F}_2$, defined for $i = 1,2$ by the formula

$$d^2Q^{(i)}(h,k) := \partial_h\partial_k Q^{(i)}$$

(note that the right-hand side is a constant and thus identifiable with an element of $\mathbb{F}_2$). We then define the cocycle ρ by

$$\rho(Q^{(1)}, Q^{(2)}) := \frac{\mathrm{Sym}^2(d^2Q^{(1)}) * (d^2Q^{(2)})(e_1,\dots,e_6)}{2} \mod 1 \tag{18}$$

with $e_1,\dots,e_6$ the standard basis of $\mathbb{F}_2^6$; compare with (17).

One can describe ρ more explicitly as follows. Instead of using the pair $(Q^{(1)}, Q^{(2)})$, one can alternatively parameterize a 6-cube in X_2 as a tuple

$$\left(x + \sum_{i=1}^{6} h_i\omega_i + \sum_{1\le i<j\le 6} h_{ij}\omega_i\omega_j\right)_{\omega\in\{0,1\}^6} \tag{19}$$

for some $x, h_i, h_{ij} \in X_2$. We write x in coordinates as $x = (x^{(1)}, x^{(2)})$ for $x^{(1)}, x^{(2)} \in \mathbb{F}_2$, and similarly write $h_i = (h_i^{(1)}, h_i^{(2)})$ and $h_{ij} = (h_{ij}^{(1)}, h_{ij}^{(2)})$; the polynomials $Q^{(k)}$, $k = 1, 2$ in the previous description of a 6-cube in X_2 then take the form

$$Q^{(k)}(\omega_1, \dots, \omega_6) = x^{(k)} + \sum_{i=1}^{6} h_i^{(k)} \omega_i + \sum_{1 \leq i < j \leq 6} h_{ij}^{(k)} \omega_i \omega_j,$$

so in particular

$$d^2 Q^{(k)}(\omega, \omega') = \sum_{1 \leq i < j \leq 6} h_{ij}^{(k)} (\omega_i \omega'_j + \omega'_i \omega_j)$$

for $\omega = (\omega_1, \dots, \omega_6)$, $\omega' = (\omega'_1, \dots, \omega'_6)$ in $\mathbb{F}_2^6$. From (18) we conclude that the cocycle ρ applied to the 6-cube (19) is then given by the formula

$$\begin{aligned} &\rho\left(\left(x + \sum_{i=1}^{6} h_i \omega_i + \sum_{1 \leq i < j \leq 6} h_{ij} \omega_i \omega_j\right)_{\omega \in \{0,1\}^6}\right) \\ &:= \frac{\sum_{\{\{a,b\},\{c,d\}\},\{e,f\} : \{1,\dots,6\} = \{a,b\} \cup \{c,d\} \cup \{e,f\}} h_{ab}^{(1)} h_{cd}^{(1)} h_{ef}^{(2)}}{2} \mod 1 \end{aligned} \tag{20}$$

where the sum is over the $\frac{1}{2!} \frac{6!}{2!2!2!} = 45$ different ways one can partition $\{1, \dots, 6\}$ into three doubleton sets $\{a, b\}, \{c, d\}, \{e, f\}$, where we only sum once for each choice of $\{\{a, b\}, \{c, d\}\}$ and $\{e, f\}$ (so that each monomial $h_{ab}^{(1)} h_{cd}^{(1)} h_{ef}^{(2)}$ occurs at most once).

The function ρ is clearly symmetric with respect to permutations of the indices $1, \dots, 6$. If we fix the h_{ij} for $1 < i < j \leq 6$, then this function is linear in the remaining variables h_{1i}, $1 < i < 6$, from which it is easy to verify that ρ obeys the cocycle property in Definition A.6(ii). Thus ρ is a degree 5 cocycle.

Suppose for contradiction that ρ is a degree 5 coboundary, thus there is a function $F \colon X_2 \to \mathbb{T}$ such that

$$\begin{aligned} &\rho\left(\left(x + \sum_{i=1}^{6} h_i \omega_i + \sum_{1 \leq i < j \leq 6} h_{ij} \omega_i \omega_j\right)_{\omega \in \{0,1\}^6}\right) \\ &= \sum_{\omega \in \{0,1\}^6} (-1)^{|\omega|} F\left(x + \sum_{i=1}^{6} h_i \omega_i + \sum_{1 \leq i < j \leq 6} h_{ij} \omega_i \omega_j\right) \end{aligned} \tag{21}$$

whenever $x, h_i, h_{ij} \in X_2$. We now descend from this sixth order equation on $X_2 = \mathcal{D}^2(\mathbb{F}_2^2)$ to a third order equation on $\mathcal{D}^1(\mathbb{F}_2^2)$ as follows. We restrict to those cubes in which all the h_i and h_{ij} vanish except for h_{12}, h_{34}, h_{56}, which we relabel as k_1, k_2, k_3 respectively. Then the right-hand side of (21) cancels down to

$$\sum_{\omega\in\{0,1\}^3} (-1)^{3-|\omega|} F\left(x + \sum_{i=1}^{3} k_i\omega_i\right)$$

while the right-hand side of (20) simplifies to

$$\frac{k_1^{(1)}k_2^{(1)}k_3^{(2)} + k_1^{(1)}k_2^{(2)}k_3^{(1)} + k_1^{(2)}k_2^{(1)}k_3^{(1)}}{2} \mod 1$$

and hence on $\mathcal{D}^1(\mathbb{F}_2^2)$ we have

$$(d^3F)_{k_1,k_2,k_3} = \frac{k_1^{(1)}k_2^{(1)}k_3^{(2)} + k_1^{(1)}k_2^{(2)}k_3^{(1)} + k_1^{(2)}k_2^{(1)}k_3^{(1)}}{2} \mod 1$$

for all $k_1, k_2, k_3 \in \mathbb{F}_2^2$. However, as observed in Remark 2.2, the right-hand side does not obey the 2-homogeneity condition (7) and so cannot be a coboundary on $\mathcal{D}^1(\mathbb{F}_2^2)$, giving the desired contradiction.

Finally, we need to show that $\rho = d^5\psi$ for some $\psi\colon X_2^{[1]} \to \mathbb{T}$ with 2ψ a cubic polynomial. We let $[]\colon \mathbb{F}_2 \to \mathbb{Z}/4\mathbb{Z}$ be any left inverse of the projection map $\mod 2\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2$; in particular one has $[0]^2 = 0 \mod 4$ and $[1]^2 = 1 \mod 4$ regardless of the choice of left inverse. An element of $C^1(X_2)$ takes the form $(x, x+h)$ with $x, h \in \mathbb{F}_2^2$, We write $x = (x^{(1)}, x^{(2)})$, $h = (h^{(1)}, h^{(2)})$ and define ψ by the formula

$$\psi(x, x+h) := \frac{[x^{(1)}]^2[h^{(2)}]^2}{4} + \frac{x^{(1)}h^{(1)}x^{(2)}}{2} \mod 1.$$

We first verify that 2ψ is a cubic polynomial. Since $[x]^2 = x^2 = x \mod 2$, We have

$$2\psi(x, x+h) = \frac{x^{(1)}h^{(2)}}{2} \mod 1$$

and a 4-cube in $C^1(X_2)$ takes the form

$$\left(\left(x + \sum_{i=1}^{4} h_i\omega_i + \sum_{1\le i<j\le 4} h_{ij}\omega_i\omega_j, x + \sum_{i=1}^{4} h_i\omega_i + \sum_{1\le i<j\le 4} h_{ij}\omega_i\omega_j + h_0 + \sum_{i=1}^{4} h_{0i}\omega_i\right)\right)_{\omega\in\{0,1\}^4}$$

for some $x, h_0, h_i, h_{0i}, h_{ij} \in X_2$. The function $d^4(2\psi)$ applied to this cube is then equal to

$$\sum_{\omega\in\{0,1\}^4} (-1)^{|\omega|} \frac{(x^{(1)} + \sum_{i=1}^4 h_i^{(1)}\omega_i + \sum_{1\le i<j\le 4} h_{ij}^{(1)}\omega_i\omega_j)(h_0^{(2)} + \sum_{i=1}^4 h_{0i}^{(2)}\omega_i)}{2} \mod 1.$$

But the numerator is cubic in the ω_i and thus does not contain any monomials of the form $\omega_1\omega_2\omega_3\omega_4$. This expression therefore vanishes, and so 2ψ is cubic as required.

It remains to show that $\rho = d^5\psi$. A 5-cube in $X_2^{[1]}$ takes the form

$$\left(\left(x + \sum_{i=1}^5 h_i\omega_i + \sum_{1\leq i<j\leq 4} h_{ij}\omega_i\omega_j, x + \sum_{i=1}^5 h_i\omega_i + \sum_{1\leq i<j\leq 5} h_{ij}\omega_i\omega_j + h_0 + \sum_{i=1}^5 h_{0i}\omega_i\right)\right)_{\omega\in\{0,1\}^5}$$

for some $x, h_0, h_i, h_{0i}, h_{ij} \in X_2$. The function $d^5\psi$ applied to this cube is the sum of

$$\sum_{\omega\in\{0,1\}^5} (-1)^{5-|\omega|} \frac{[X^{(1)}(\omega)]^2[H^{(2)}(\omega)]^2}{4} \mod 1 \tag{22}$$

and

$$\sum_{\omega\in\{0,1\}^5} (-1)^{5-|\omega|} \frac{X^{(1)}(\omega)H^{(1)}(\omega)X^{(2)}(\omega)}{2} \mod 1 \tag{23}$$

where

$$X^{(a)}(\omega) := x^{(a)} + \sum_{i=1}^5 h_i^{(a)}\omega_i + \sum_{1\leq i<j\leq 5} h_{ij}^{(a)}\omega_i\omega_j$$

and

$$H^{(a)}(\omega) := h_0^{(a)} + \sum_{i=1}^5 h_{0i}^{(a)}\omega_i$$

for $a = 1, 2$. We first consider (23). The numerator $X^{(1)}(\omega)H^{(1)}(\omega)X^{(2)}(\omega)$ is quintic in the ω_i, so the alternating sum $\sum_{\omega\in\{0,1\}^5}(-1)^{5-|\omega|}$ is extracting the $\omega_1 \dots \omega_5$ coefficient of this numerator, which after expanding out all the definitions can be expressed as

$$\frac{\sum^* h_{ab}^{(1)}h_{cd}^{(1)}h_{ef}^{(2)}}{2} \mod 1 \tag{24}$$

where the sum $\sum^*$ ranges over the 30 pairs of sets $\{\{a, b\}, \{c, d\}\}, \{e, f\}$ with $\{0, 1, 2, 3, 4, 5\} = \{a, b\} \cup \{c, d\} \cup \{e, f\}$ such that 0 lies in one of $\{a, b\}$ or $\{c, d\}$.

Now consider (22). Using the easily verified identities $[a + b]^2 = [a]^2 + [b]^2 + 2[ab]$ and $[a\omega]^2 = [a]^2\omega$ for $a, b \in \mathbb{F}_2$ and $\omega \in \{0, 1\}$ (and noting that the map $a \mapsto 2[a]$ is an additive homomorphism), we can expand out

$$[H^{(2)}(\omega)]^2 = \left[h_0^{(2)} + \sum_{i=1}^5 h_{0i}^{(2)}\omega_i\right]^2 = [h_0^{(2)}]^2 + \sum_{i=1}^5 [h_{0i}^{(2)}]^2\omega_i + 2[Q(\omega)]$$

where $Q\colon \{0,1\}^5 \to \mathbb{F}_2$ is the quadratic

$$Q(\omega) := \sum_{i=1}^5 h_0^{(2)} h_{0,1}^{(2)}\omega_i + \sum_{1\le i<j\le 5} h_{0i}^{(2)} h_{0j}^{(2)}\omega_i\omega_j,$$

and similarly

$$[X^{(1)}(\omega)]^2 = [x^{(1)}]^2 + \sum_{i=1}^5 [h_i^{(1)}]^2\omega_i + \sum_{1\le i<j\le 5} [h_{ij}^{(1)}]^2\omega_i\omega_j + 2[R(\omega)]$$

where $R\colon \{0,1\}^5 \to \mathbb{F}_2$ is the quartic

$$\begin{aligned} R(\omega) := &\sum_{i=1}^5 x^{(1)} h_i^{(1)}\omega_i + \sum_{1\le i<j\le 5} (h_i^{(1)}h_j^{(1)} + x^{(1)}h_{ij}^{(1)})\omega_i\omega_j \\ &+ \sum_{1\le i<j<k\le 5} (h_i^{(1)}h_{jk}^{(1)} + h_j^{(1)}h_{ik}^{(1)} + h_k^{(1)}h_{ij}^{(1)})\omega_i\omega_j\omega_k \\ &+ \sum_{1\le i<j<k<l\le 5} (h_{ij}^{(1)}h_{kl}^{(1)} + h_{ik}^{(1)}h_{jl}^{(1)} + h_{il}^{(1)}h_{jk}^{(1)})\omega_i\omega_j\omega_k\omega_l. \end{aligned}$$

The product $[X^{(1)}(\omega)]^2[H^{(2)}(\omega)]^2$ is then quintic (the product of $2Q$ and $2R$ would be sextic, but vanishes modulo 4), and the alternating sum $\sum_{\omega\in\{0,1\}^5}(-1)^{5-|\omega|}$ is then extracting the $\omega_1\dots\omega_5$ coefficient, which can only arise from the terms

$$2[R(\omega)]\cdot\sum_{i=1}^5 [h_{0i}^{(2)}]^2\omega_i$$

in the numerator. Inspecting the cubic terms of $R(\omega)$, we conclude that (23) is of the form

$$\frac{\sum^{**} h_{ab}^{(1)}h_{cd}^{(1)}h_{ef}^{(2)}}{2} \mod 1 \tag{25}$$

where the sum $\sum^{**}$ ranges over the 15 pairs of sets $\{\{a,b\},\{c,d\}\},\{e,f\}$ with $\{0,1,2,3,4,5\} = \{a,b\}\cup\{c,d\}\cup\{e,f\}$ such that 0 does not lie in either $\{a,b\}$ or $\{c,d\}$. Summing (24), (25), we obtain the claim. This concludes the proof of Theorem 3.1.

4. Two key nilspaces

We now use the non-trivial cocycle ρ introduced in the previous section to construct family of finite 5-step nilspaces $X_{5,r}$ for $1 \leq r \leq 5$ that will play a key role in our counterexamples. To prove our main result in Theorem 1.6 we will use the larger and more complicated nilspace $X_{5,5}$, however in Proposition 4.5 below we obtain a weaker counterexample with significantly less effort using the smaller and simpler nilspace $X_{5,1}$.

Fix $1 \leq r \leq 5$. We define X_2 by (16), and let ρ be the non-trivial cocycle from Theorem 3.1. We define the nilspace $X_{5,r}$ to be the Cartesian product

$$X_{5,r} := X_2 \times \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$$

with the n-cubes $C^n(X_{5,r})$ defined to be the space of all tuples $((Q, S)(\omega))_{\omega\in\{0,1\}^n}$, where $Q\colon \mathbb{F}_2^n \to X_2$ and $S : \mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ are functions (identifying $\{0, 1\}^n$ with $\mathbb{F}_2^n$) that obey the following axioms:

(i) Q is a nilspace morphism from $\mathbb{F}_2^n$ to X_2 (or equivalently by (62), that $Q \in C^n(X_2)$). In other words, $Q = (Q_1, Q_2) \in \mathrm{Poly}^2(\mathbb{F}_2^n \to \mathbb{F}_2^2)$ is a pair of classical quadratic polynomials $Q_1, Q_2\colon \mathbb{F}_2^n \to \mathbb{F}_2$. In particular, one has $d^3Q = 0$.

(ii) S obeys the equation (1) for all $x, h_1, \dots, h_6 \in \mathbb{F}_2^n$. Equivalently, one has $d^6S = Q^*\rho$, where $Q^*\rho\colon C^6(\mathbb{F}_2^n) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is the pullback of ρ, defined by

$$Q^*\rho((x_\omega)_{\omega\in\{0,1\}^6}) := \rho((Q(x_\omega))_{\omega\in\{0,1\}^6}).$$

More succinctly, one has

$$C^n(X_{5,r}) = \{(Q, S)\colon \mathbb{F}_2^n \to X_{5,r} : d^3Q = 0; d^6S = Q^*\rho\}.$$

We will shortly verify that $X_{5,r}$ is indeed a nilspace, but first we establish an important lemma that exploits the strong 2-homogeneity of ρ to allow one to lift n-cubes in X_2 to n-cubes in $X_{5,r}$.

Lemma 4.1 (Lifting lemma)**.** *Let $r \geq 1$ and $n \geq 0$, and let $Q \in C^n(X_2)$. Then there exists a map $S : \mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ such that $(Q, S) \in C^n(X_{5,r})$. Furthermore, the set of such S forms a coset of* $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z})$.

Proof. We first show existence. Since ρ is a strongly 2-homogeneous degree 6 cocycle, it is not difficult to see that the pullback $Q^*\rho$ is also. Hence by Theorem 2.6, $Q^*\rho$ is a degree 6 coboundary in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, thus there exists $S : \mathbb{F}_2^n \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ such that $Q^*\rho = d^6 S$, which is precisely the condition (1). Since $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is contained in $\frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$, we have obtained an n-cube (Q, S) in $X_{5,r}$ as required.

Now suppose that $(Q, S), (Q, S')$ are both n-cubes in $X_{5,r}$. Then $d^6 S = d^6 S' = Q^*\rho$ and hence $d^6(S - S') = 0$, thus S and S' differ by an element of $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z})$. Reversing these implications, we see that the set of S for which $(Q, S) \in C^n(X_{5,r})$ is a coset of $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z})$ as claimed. □

In fact, with the specific choice of cocycle we have constructed, we can describe the coset in Lemma 4.1 explicitly.

Lemma 4.2 (Explicit description of lift)**.** *Let the notation and hypotheses be as in Lemma 4.1. Write $Q = (Q_1, Q_2)$, thus $Q_1, Q_2 : \mathbb{F}_2^2 \to \mathbb{F}_2$ are classical quadratic polynomials. Let $R \in \mathrm{Poly}^3(\mathbb{F}_2^2 \to \mathbb{Z}/4\mathbb{Z})$ be a cubic polynomial such that $2\frac{R}{4} = \frac{Q_1}{2} \mod 1$ (or equivalently that $R = Q_1 \mod 2$); the existence of such a polynomial follows from* (61)*. Then the coset of S in Lemma 4.1 is equal to*

$$\frac{\binom{R}{2}Q_2}{2} + \mathrm{Poly}^5\left(\mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}\right)$$

where (as in Section 1.3) $\binom{a}{2} \in \mathbb{F}_2$ is equal to 1 when $a = 2, 3 \mod 4$ and 0 for $a = 0, 1 \mod 4$.

Proof. By Lemma 4.1, it suffices to show that

$$\partial_{h_1} \dots \partial_{h_6} \frac{\binom{R}{2}Q_2}{2}(x) = \rho((Q(x + \omega \cdot \vec{h}))_{\omega \in \{0,1\}^6}) \mod 1$$

for $x \in \mathbb{F}_2^n$ and $\vec{h} = (h_1, \dots, h_6) \in (\mathbb{F}_2^n)^6$. By construction of ρ, it suffices to show that

$$\partial_{h_1} \dots \partial_{h_6} \left(\binom{R}{2}Q_2\right) = \sum_{\{\{a,b\},\{c,d\}\},\{e,f\}:\{1,\dots,6\}=\{a,b\}\cup\{c,d\}\cup\{e,f\}} (\partial_{h_a}\partial_{h_b}Q_1)(\partial_{h_c}\partial_{h_d}Q_1)(\partial_{h_e}\partial_{h_f}Q_2)$$

for all $h_1, \dots, h_6 \in \mathbb{F}_2^n$. The expressions in parentheses on the right-hand side are all constants since Q is quadratic. By the Leibniz rule (60), it suffices to show that

$$\partial_{h_1} \dots \partial_{h_4} \binom{R}{2} = \sum_{\{\{a,b\},\{c,d\}\}:\{1,\dots,4\}=\{a,b\}\cup\{c,d\}} (\partial_{h_a}\partial_{h_b}Q_1)(\partial_{h_c}\partial_{h_d}Q_1)$$

or equivalently that $d^4\binom{R}{2} = \mathrm{Sym}^2(d^2Q_1)$. But this follows from [23, Lemma 6.4, Example 6.5] (or from several direct applications of the Leibniz rule (60) using the identity

$$\partial_h\binom{F}{2} = \binom{\partial_h F}{2} + F\partial_h F \mod 2 \tag{26}$$

for any $F\colon \mathbb{F}_2^n \to \mathbb{Z}/4\mathbb{Z}$ and $h \in \mathbb{F}_2^n$, as well as the identities $R = Q_1 \mod 2$, $d^3Q_1 = 0$, and $d^4R = 0$). □

Proposition 4.3. *Let $1 \leq r \leq 5$. Then $X_{5,r}$ is an ergodic 2-homogeneous 5-step nilspace, and the projection map $\pi\colon X_{5,r} \to X_2$ given by $\pi(q,s) := q$ for $q \in X_2$ and $s \in \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ is a nilspace morphism.*

Proof. We begin by verifying the nilspace axioms from Definition A.1. The composition axiom is easy: if $(Q,S)\colon \mathbb{F}_2^n \to X_{5,r}$ is an n-cube in $X_{5,r}$ and $\phi\colon \{0,1\}^m \to \{0,1\}^n$ is a cube morphism, then one can view ϕ as an affine map from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$, in which case it is clear that $(Q,S)\circ\phi\colon \mathbb{F}_2^m \to X_{5,r}$ is an m-cube in $X_{5,r}$.

Now we verify ergodicity. Let $(Q,S)\colon \mathbb{F}_2 \to X_{5,r}$ be an arbitrary map. Then Q is linear, so certainly $d^3Q = 0$. Since $r \leq 5$, every map $S : \mathbb{F}_2 \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ lies in $\mathrm{Poly}^6(\mathbb{F}_2 \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z})$ by Lemma A.23, and hence by Lemma 4.1 all pairs (Q,S) lie in $C^1(X_{5,r})$, giving the claim.

Now we verify the corner completion axiom. Let $(Q,S)\colon \mathbb{F}_2^n\backslash\{1\}^n \to X_{5,r}$ be a map such that the restriction of (Q,S) to any $(n-1)$-face of $\{0,1\}^n \equiv \mathbb{F}_2^n$ containing 0^n is in $C^{n-1}(X_{5,r})$. From the corner completion property of X_2, we may extend Q to an n-cube $Q\colon \mathbb{F}_2^n \to X_2$, and then by Lemma 4.1 we can find a lift $(Q,S')\colon \mathbb{F}_2^n \to X_{5,r}$ which is an n-cube. By (1), we conclude that the difference $S - S'\colon \mathbb{F}_2^n\backslash\{1\}^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ is a degree 5 polynomial on each $(n-1)$-face of $\{0,1\}^n \equiv \mathbb{F}_2^n$ containing 0^n. By the corner completion property of $\mathcal{D}^5(\frac{1}{2^r}\mathbb{Z}/\mathbb{Z})$, we may extend $S - S'$ to a degree 5 polynomial from $\mathbb{F}_2^n$ to $\frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$; the resulting extension $S : \mathbb{F}_2^n \to \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ then obeys (1), so that (Q,S) is now extended to an n-cube on $X_{5,r}$ as required. When $n = 6$, the extension of Q is unique, and equation (1) (with $x = 0$ and $h_1,\dots,h_6$ the standard basis) also shows that the extension of S is unique, so that $X_{5,r}$ is 5-step as claimed.

The nilspace morphism property of π is clear from chasing definitions, so it remains to verify 2-homogeneity. Let $(Q, S)\colon \mathbb{F}_2^n \to X_{5,r}$ be an n-cube in $X_{5,r}$; we need to show that (Q, S) is also a nilspace morphism from $\mathcal{D}^1(\mathbb{F}_2^n)$ to $X_{5,r}$. But an m-cube in $\mathcal{D}^1(\mathbb{F}_2^n)$ can be viewed as an affine map $\phi\colon \mathbb{F}_2^m \to \mathbb{F}_2^n$, and then $(Q, S) \circ \phi\colon \mathbb{F}_2^m \to X_{5,r}$ can then be easily verified to obey the axioms (i), (ii) for an m-cube in $X_{5,r}$, and so (Q, S) is a nilspace morphism as claimed. □

Remark 4.4. When $r = 1$, one can think of $X_{5,1}$ as the skew product $X_2 \rtimes_{\rho}^{(5)} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, in the sense of Proposition A.9, and the fact that $X_{5,1}$ is a 2-homogeneous nilspace can also be established from Lemma A.27 and Lemma 4.1 in this case. For larger values of r, however, the situation is more complicated; the nilspace $X_{5,r}$ appears at first glance to be a degree 5 extension of X_2 by $\frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$, but the cube structure is slightly smaller than what would arise from such an extension (the equation (1) provides more constraints on S than the constraint (53) used to define a skew product, because the shifts $h_1, \dots, h_6$ are not required to be distinct basis vectors). Instead, by making the (slightly artificial) identification

$$(q, s) \equiv ((q, 2s), s - \{2s\}/2)$$

between $X_2 \times \frac{1}{2^r}\mathbb{Z}/\mathbb{Z}$ and $(X_2 \times \frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}) \times (\frac{1}{2}\mathbb{Z}/\mathbb{Z})$, where $\{\}\colon \mathbb{R}/\mathbb{Z} \to [0, 1)$ denotes the fractional part map, we can identify $X_{5,r}$ with the skew product

$$(X_2 \times \frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}) \rtimes_{\tilde{\rho}}^{(5)} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

where we give $\frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}$ the 2-adic filtration $(\frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z})_i = \frac{1}{2^{\min(r-i,0)}}\mathbb{Z}/\mathbb{Z}$ for $i \geq 1$ (so that $X_2 \times \frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}$ is a $\max(2, r-1)$-step filtered abelian group), and $\tilde{\rho}\colon C^6(X_2 \times \frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is the modified cocycle

$$\tilde{\rho}((q_\omega, t_\omega)_{\omega \in \{0,1\}^6}) := \rho((q_\omega)_{\omega \in \{0,1\}^6}) - \sum_{\omega \in \{0,1\}^6} (-1)^{|\omega|}\{t_\omega\}/2$$

for all 6-cubes $(q_\omega, t_\omega)_{\omega \in \{0,1\}^6}$ in $X_2 \times \frac{1}{2^{r-1}}\mathbb{Z}/\mathbb{Z}$ (one can check that $2\tilde{\rho} = 0$, so that this cocycle does indeed take values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$). As we will not need this description of $X_{5,r}$ here, we leave the justification of this claim to the interested reader.

As an application of the smaller $X_{5,1}$ of the two nilspaces $X_{5,r}$, we have

Proposition 4.5. *There is no injective nilspace morphism from $X_{5,1}$ to a 5-step compact filtered abelian group.*

This gives a negative answer (in the case $p = 2, k = 5$) to [4, Question 5.18], which asked the more general question of whether every k-step compact p-homogeneous nilspace has an injective nilspace morphism into a k-step compact filtered abelian group. As noted in that paper, an affirmative answer to this question for a given value of p and k would imply an affirmative answer to Conjecture 1.2 (and hence Conjecture 1.3 and Conjecture 1.1) for those values of p, k. Indeed, [4, Question 5.18] was answered affirmatively for $k \leq p + 1$, leading to the corresponding results on Conjectures 1.2, 1.3, 1.1 mentioned in the introduction. Thus, Proposition 4.5 can be viewed as a weaker version of Theorem 1.6.

Proof. Suppose for contradiction that there was an injective nilspace morphism $\iota \colon X_{5,1} \to G$ from $X_{5,1}$ to some 5-step compact filtered abelian group G. Let μ be the finite measure on G defined via Riesz representation as

$$\int_G f \, d\mu := \sum_{(q,s) \in X_{5,1}} f(\iota(q, s)) e(s).$$

This is a non-trivial measure, hence must have a non-zero Fourier coefficient. In other words, there exists a continuous homomorphism $\xi \colon G \to \mathbb{T}$ such that

$$\sum_{(q,s) \in X_{5,1}} e(s - P(q, s)) \neq 0$$

where $P \colon X_{5,1} \to \mathbb{T}$ is the map $P := \xi \circ \iota$. By Lemma A.5, ξ is a quintic polynomial on the 5-step filtered abelian group G, hence P is a quintic polynomial on $X_{5,1}$.

Now we consider the "vertical derivative"

$$\partial_u P(q, s) := P(q, s + \frac{1}{2}) - P(q, s)$$

of the polynomial P. We claim that this derivative is constant, by the following standard argument. If $(q_0, s_0), (q_1, s_1) \in X_{5,1}$, then the tuple $(Q, S) \colon \mathbb{F}_2^6 \to X_{5,1}$ defined by

$$(Q, S)(\omega) := \left(q_{\omega_1}, s_{\omega_1} + 1_{\omega_2 = \cdots = \omega_{k+1} = 0} \frac{1}{2} \right)$$

can easily be verified to obey the axioms (i), (ii) required to be a 6-cube in $X_{5,1}$. From the quintic nature of P we conclude that

$$\sum_{\omega\in\{0,1\}^6} (-1)^{|\omega|} P((Q,S)(\omega)) = 0$$

which simplifies to

$$\partial_u P(q_0, s_0) = \partial_u P(q_1, s_1), \tag{27}$$

giving the claim.

Another way of phrasing this is that the function $e(P)$ is an eigenfunction of the vertical Koopman operator V^u defined by

$$V^u F(q,s) := F\left(q, s+\frac{1}{2}\right).$$

On the other hand, the function $(q,s) \mapsto e(s)$ is also an eigenfunction of this operator with eigenvalue $e(\frac{1}{2})$. Since the Koopman operator V^u is unitary, and $e(P)$ has a non-zero inner product with $e(s)$, the eigenvalue of $e(P)$ must also be $e(\frac{1}{2})$, thus

$$\partial_u P = \frac{1}{2}.$$

Equivalently, we may write

$$P(q,s) = s - F(q)$$

for some function $F\colon X_2 \to \mathbb{T}$. Applying d^6 to eliminate the quintic polynomial P, we conclude that

$$0 = \rho - d^6 F$$

and hence ρ is a degree 5 coboundary (in $\mathbb{T}$), contradicting Theorem 3.1. □

Remark 4.6. While the above proposition shows that $X_{5,1}$ cannot be embedded into a finite filtered abelian group, [4, Theorem 1.7] does show that there is an *fibration* $\pi\colon Y \to X_{5,1}$ (as defined in [14, Definition 7.1], [3, Definition 3.3.7]) that has the structure of a finite filtered abelian group and has good lifting properties; this result was in particular used in [4] to give an alternate proof of Conjecture 1.1 in both high and low characteristic. In fact, we can explicitly give such an extension. Let G denote the abelian group $\mathbb{Z}/4\mathbb{Z}$ with the degree 3 filtration

$$G_0 = G_1 = G_2 = G; \quad G_3 = 2\mathbb{Z}/4\mathbb{Z}; \quad G_i = \{0\} \forall i > 3,$$

and consider the filtered abelian group

$$Y := G \times \mathcal{D}^2(\mathbb{F}_2) \times \mathcal{D}^5(\mathbb{F}_2).$$

One can show using Lemma 4.2 that the map $\pi\colon Y \to X_{5,1}$ defined by

$$\phi(a,b,c) = \left(a \mod 2, b, \frac{\binom{a}{2}b + c}{2}\right),$$

is a fibration; we leave the details to the interested reader.

5. Counterexample to the strong inverse conjecture

We now use the larger nilspace $X_{5,5}$ introduced in the previous section to establish Theorem 1.6. (The reason for using $X_{5,5}$ instead of $X_{5,1}$ will only be apparent near the end of the argument.)

5.1. **Constructing the counterexample.**

To locate the counterexample to Conjecture 1.3 (for a suitable choice of parameters), we use a probabilistic construction. Let n be a large parameter (which will eventually be sent to infinity). We let $(Q, S)\colon \mathbb{F}_2^n \to X_{5,5}$ be an n-cube in $X_{5,5}$, chosen uniformly at random from $C^n(X_{5,5})$. In view of Lemma 4.1, one way to generate such an element is as follows. First, one generates an n-cube $Q\colon \mathbb{F}_2^n \to X_2$ of X_2, uniformly at random; in other words, Q is a pair (Q_1, Q_2) of independent classical quadratic polynomials $Q_1, Q_2\colon \mathbb{F}_2^n \to \mathbb{F}_2$. By Lemma 4.1, the set of all $S : \mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ for which (Q, S) is an n-cube in $X_{5,5}$ is a coset (depending on Q) of the finite group $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$, and so once Q is chosen, one simply selects an element of this coset uniformly at random, or equivalently one chooses uniformly at random a solution $S : \mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ to the equation (1). This gives a uniformly distributed element on the entirety of $C^n(X_{5,5})$, a product of two uniform distributions, because all cosets of $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ have the same cardinality.

Remark 5.1. Thanks to Lemma 4.2, we can also generate (Q, S) as

$$(Q, S) = \left((2R, Q^{(2)}), \frac{\binom{R}{2}Q^{(2)}}{2} + P\right),$$

where $R, Q^{(2)}, P$ are elements of $\mathrm{Poly}^3(\mathbb{F}_2^n \to \mathbb{Z}/4\mathbb{Z})$, $\mathrm{Poly}^2(\mathbb{F}_2^n \to \mathbb{F}_2)$, and $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ respectively, chosen uniformly and independently at random; compare with Remark 4.6. However, we will not make significant use of this representation here.

The random function $f = e(S)$ will be used as our counterexample (or more precisely, as a sequence of counterexamples as $n \to \infty$) to Conjecture 1.3. We first record a deterministic lower bound on the U^6 norm of $e(S)$:

Lemma 5.2 (Deterministic lack of Gowers uniformity)**.** *Whenever $(Q, S)\colon \mathbb{F}_2^n \to X_{5,5}$ is an n-cube in $X_{5,5}$, we have*

$$\|e(S)\|_{U^6(\mathbb{F}_2^n)} \geq \eta$$

for some absolute constant $\eta > 0$ (independent of n).

Informally, this lemma asserts that S behaves (in some weak statistical sense) like a "pseudo-quintic", and indeed Conjecture 1.1 could now be invoked to conclude that $e(S)$ correlated with an actual (non-classical) quintic polynomial. For instance, from Remark 5.1 we see that with high probability $e(S)$ would correlate with the function $e(P)$, where P is as in that remark, as the phase $\frac{\binom{R}{2}Q^{(2)}}{2}$ will vanish approximately three quarters of the time. However, we will show that (with high probability) such quintic polynomials cannot be (approximately) constructed out of a bounded number of translates of S, leading to the proof of Theorem 1.6.

Proof. From (1) we have

$$\mathbb{E}_{x,h_1,\dots,h_6\in\mathbb{F}_2^n} e((d^6 S)_{h_1,\dots,h_6}(x)) e(-\rho((Q(x+\omega\cdot\vec{h}))_{\omega\in\{0,1\}^6})) = 1$$

where $\vec{h} := (h_1, \dots, h_6)$. Performing a Fourier expansion of $e(-\rho)$ (which one extends arbitrarily to a function on the finite abelian group $X_2^{\{0,1\}^6}$) and using the pigeonhole principle, we conclude that

$$\mathbb{E}_{x,h_1,\dots,h_6\in\mathbb{F}_2^n} e((d^6 S)_{h_1,\dots,h_6}(x))(-1)^{\sum_{\omega\in\{0,1\}^6} c_\omega\cdot Q(x+\omega\cdot\vec{h})} \geq \eta$$

for some absolute constant $\eta > 0$ and some Fourier coefficients $c_\omega \in X_2$ (which may depend on n and S), using the usual $\mathbb{F}_2$-valued inner product

$$(c_1, c_2)\cdot(q_1, q_2) := c_1 q_1 + c_2 q_2$$

on the vector space X_2. Applying the Cauchy–Schwarz–Gowers inequality (see e.g., [10, (5.5)]) we conclude that

$$\|e(S)(-1)^{c_{0^6}\cdot Q}\|_{U^6(\mathbb{F}_2^n)} \geq \eta.$$

As Q is of degree $2 < 5$, multiplication by the quadratic phase $(-1)^{c_{0^6}\cdot Q}$ does not affect the $U^6(\mathbb{F}_2^n)$ norm, and the claim follows. □

Now let $\varepsilon\colon \mathbb{R}^+ \to \mathbb{R}^+$ be an increasing function to be chosen later with $\varepsilon(1/m) \to 0$ sufficiently quickly as $m \to \infty$. Suppose for contradiction that Conjecture 1.3 held for $p = 2$ and $k = 5$. Then by the above lemma, applying that conjecture to each of the random functions $e(S)$ and then using the law of total probability, there exists M (depending on $\varepsilon()$, but deterministic and independent of n) such that, for any n, and with the random n-cube $(Q, S) \in C^n(X_{5,5})$ chosen as above, and $\vec{h} = (h_1, \dots, h_M) \in (\mathbb{F}_2^n)^M$ chosen uniformly at random, with probability at least $1/2$, there exist $1 \leq m \leq M$, $P \in \mathrm{Poly}^5(\mathbb{F}_2^n)$ and a function $F\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{C}$ (which may depend on $Q, S, h_1, \dots, h_M$), such that

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(S(x) - P(x))| \geq \frac{1}{m} \tag{28}$$

and

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(P(x)) - F((S(x + a\cdot\vec{h}))_{a\in\mathbb{F}_2^M})| \leq \varepsilon(m).$$

(We drop the Lipschitz condition on F as being of little use due to the finite nature of the domain.) By projecting F to the unit circle we may assume that $F = e(\Phi)$ for some $\Phi\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{T}$, thus

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(P(x)) - e(\Phi((S(x + a\cdot\vec{h}))_{a\in\mathbb{F}_2^M}))| \leq \varepsilon(m). \tag{29}$$

We have two independent sources of randomness present in the above assertions: one coming from the uniformly chosen n-cube (Q, S), and one coming from the uniformly chosen sampling vectors $h_1, \dots, h_M$. It will be convenient to normalize the $h_1, \dots, h_M$ by the following argument. By Fubini's theorem, we can choose the sampling vectors $h_1, \dots, h_M \in \mathbb{F}_2^n$ *first*, and then choose the n-cube $(Q, S) \in C^n(X_{5,5})$ *second*, and it will still be the case with probability at least $1/2$ that we can find m, P, Φ obeying (28), (29). For n sufficiently large (depending on M), the probability that the $h_1, \dots, h_M$ are linearly dependent is less than $1/4$ (say). Deleting this event and applying the pigeonhole principle for the $h_1, \dots, h_M$, we conclude that for all sufficiently large n, we may find linearly independent (and now deterministic) $h_1, \dots, h_M \in \mathbb{F}_2^n$ such that, for a uniformly chosen n-cube (Q, S) in $X_{5,5}$, with probability at least $1/4$, there exists a quintic polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^n)$, a natural number $1 \leq m \leq M$, and a function $\Phi\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{T}$, obeying the properties (28), (29).

The above claim is invariant with respect to general linear transformations on $\mathbb{F}_2^n$ (i.e., changes of coordinate basis), so without loss of generality we may take $h_i = e_i$ for $1 \leq i \leq M$, where $e_1, \dots, e_n$ is the standard basis for $\mathbb{F}_2^n$. Then we can simplify the tuple $(S(x+a\cdot\vec{h}))_{a\in\mathbb{F}_2^M}$ as $(S(x+(a,0^{n-M})))_{a\in\mathbb{F}_2^M}$. We summarize the situation so far as follows.

Proposition 5.3 ($e(S)$ can be approximated by a measurable quintic)**.** *Suppose that Conjecture 1.3 holds for $p = 2$ and $k = 5$, and let $\varepsilon\colon \mathbb{N} \to \mathbb{R}^+$ be a function decreasing to zero. Then there exists $M \geq 1$ such that for all sufficiently large n, and (Q, S) a uniformly chosen n-cube in $X_{5,5}$, one has with probability at least $1/4$ that there exist a quintic polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^n)$, $1 \leq m \leq M$ and a function $\Phi\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{T}$ (which are all permitted to depend on (Q, S)) such that*

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(P(x)) - e(\Phi((S(x + (a, 0^{n-M})))_{a\in\mathbb{F}_2^M}))| \leq \varepsilon(m) \tag{30}$$

and

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(S(x) - P(x))| \geq \frac{1}{m} \tag{31}$$

where we split $\mathbb{F}_2^n$ as $\mathbb{F}_2^M \times \mathbb{F}_2^{n-M}$ (so that an element a of $\mathbb{F}_2^M$ induces a corresponding element $(a, 0^{n-M})$ of $\mathbb{F}_2^n$).

5.2. **Equidistribution theory for Q, S.** In order to extract a contradiction from the estimates (30), (31) and the polynomial nature of P, we will need to understand the asymptotic equidistribution properties of the n-cube (Q, S) in the following randomly sampled sense. Given a choice of n-cube (Q, S), and a natural number d, let $v_1, \dots, v_d \in \mathbb{F}_2^n$ be vectors drawn uniformly and independently from $\mathbb{F}_2^n$ (and also independently of (Q, S)), and consider the random functions $(\tilde{Q}, \tilde{S}) = (\tilde{Q}, \tilde{S})_{(Q,S),v_1,\dots,v_d}\colon \mathbb{F}_2^{M+d} \to X_{5,5}$ defined by sampling (Q, S) in the directions $e_1, \dots, e_M, v_1, \dots, v_d$, or more precisely by the formula

$$(\tilde{Q}, \tilde{S})(a_1, \dots, a_M, b_1, \dots, b_d) := (Q, S)(a_1e_1 + \dots + a_Me_M + b_1v_1 + \dots + b_dv_d)$$

for all $a_1, \dots, a_M, b_1, \dots, b_d \in \mathbb{F}_2$. This is the composition of the nilspace morphism $(Q, S)\colon \mathcal{D}^1(\mathbb{F}_2^n) \to X_{5,5}$ with a (random) linear transformation from $\mathbb{F}_2^{M+d}$ to $\mathbb{F}_2^n$, and so $(\tilde{Q}, \tilde{S})$ is a (random) nilspace morphism from $\mathcal{D}^1(\mathbb{F}_2^{M+d})$ to $X_{5,5}$, or equivalently a (random) $M + d$-cube in $X_{5,5}$. Also, regardless of the choice of sampling vectors $v_1, \dots, v_d$, $(\tilde{Q}, \tilde{S})$ must agree with (Q, S) on $\mathbb{F}_2^M$ in the sense that

$$(\tilde{Q}, \tilde{S})(a, 0^d) = (Q_0, S_0)(a) \tag{32}$$

for all $a \in \mathbb{F}_2^M$, where $(Q_0, S_0) \colon \mathbb{F}_2^M \to X_{5,5}$ is the restriction of (Q, S) to $\mathbb{F}_2^M$, defined by the formula

$$(Q_0, S_0)(a) \coloneqq (Q, S)(a, 0^{n-M}). \tag{33}$$

Note that (Q_0, S_0) is an M-cube in $X_{5,5}$, since (Q, S) is an n-cube in $X_{5,5}$.

Let

$$\Sigma^{(d)}_{Q_0,S_0} \subset C^{M+d}(X_{5,5})$$

denote the space of all $M + d$-cubes $(\tilde{Q}, \tilde{S})$ that agree with the M-cube (Q_0, S_0) on the face $\mathbb{F}_2^M \times \{0^d\}$ in the sense of (32); this is a non-empty finite set whose cardinality is bounded uniformly in n. For each choice of $(Q, S), d$, let $\mu^{(d)}_{Q,S}$ denote the distribution of the random variable $(\tilde{Q}, \tilde{S})$ generated by the random variables $v_1, \dots, v_d$, thus $\mu^{(d)}_{Q,S}$ is the probability measure on $\Sigma^{(d)}_{Q_0,S_0}$ defined by the formula

$$\int_{\Sigma^{(d)}_{Q_0,S_0}} G(\tilde{Q}, \tilde{S})\, d\mu^{(d)}_{Q,S}(\tilde{Q}, \tilde{S}) = \mathbb{E}_{v_1,\dots,v_d \in \mathbb{F}_2^n} G(\tilde{Q}_{Q,v_1,\dots,v_d}, \tilde{S}_{S,v_1,\dots,v_d})$$

for any observable $G \colon \Sigma^{(d)}_{Q_0,S_0} \to \mathbb{C}$. Meanwhile, let $\overline{\mu}^{(d)}_{Q_0,S_0}$ denote the uniform probability measure on $\Sigma^{(d)}_{Q_0,S_0}$.

The following key equidistribution theorem asserts that, for (Q, S) a uniformly chosen n-cube, $\mu^{(d)}_{Q,S}$ converges to $\overline{\mu}^{(d)}_{Q_0,S_0}$ "in probability". More precisely:

Theorem 5.4 (Equidistribution theorem). *Let d be fixed. Then, we have*

$$d_{\mathrm{TV}}(\mu^{(d)}_{Q,S}, \overline{\mu}^{(d)}_{Q_0,S_0}) = o(1) \tag{34}$$

with probability $1 - o(1)$*, where* $o(1)$ *denotes any quantity that goes to zero as $n \to \infty$ holding all other parameters not depending on n (such as d) fixed. Here d_{TV} denotes the total variation distance between probability measures.*

Informally, this theorem asserts that the condition (32) on the $M+d$-cube $(\tilde{Q}, \tilde{S})$ is asymptotically the *only* constraint that could control (or even bias) the distribution of this $M+d$-cube. One could replace the total variation distance here by any other reasonable metric, since $\mu^{(d)}_{Q,S}, \overline{\mu}^{(d)}_{Q_0,S_0}$ are supported on finite sets of cardinality bounded uniformly on n.

Proof. We first establish the equidistribution claim for Q only. Let $\Sigma^{(d)}_{Q_0} \subset C^{M+d}(X_2)$ be the collection of all $M+d$-cubes $\tilde{Q}$ in X_2 which agree with Q_0 on the face $\mathbb{F}_2^M \times \{0^d\}$ in the sense of (32). We then define $\mu^{(d)}_Q$ as before, and set $\overline{\mu}^{(d)}_{Q_0}$ to be uniform measure on $\Sigma^{(d)}_{Q_0}$. Observe that the projection map $(\tilde{Q}, \tilde{S}) \mapsto \tilde{Q}$ maps $\Sigma^{(d)}_{Q_0,S_0}$ to $\Sigma^{(d)}_{Q_0}$; by Lemma 4.1, the map is surjective, and the fibers of this map are essentially cosets of the finite group

$$K := \left\{ P \in \mathrm{Poly}^5\left(\mathbb{F}_2^{M+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}\right) : P(x, 0^d) = 0 \forall x \in \mathbb{F}_2^M \right\}. \tag{35}$$

In particular, all fibers have the same cardinality, and hence the uniform measure $\overline{\mu}^{(d)}_{Q_0,S_0}$ pushes forward to the uniform measure $\overline{\mu}^{(d)}_{Q_0}$. Also, by definition the sampling measure $\mu^{(d)}_{Q,S}$ pushes forward to the sampling measure $\mu^{(d)}_Q$. Hence, in order to establish (34) with probability $1 - o(1)$, a natural first step would be to first show the weaker claim that

$$d_{\mathrm{TV}}(\mu^{(d)}_Q, \overline{\mu}^{(d)}_{Q_0}) = o(1) \tag{36}$$

with probability $1 - o(1)$.

We use the second moment method. The set $\Sigma^{(d)}_{Q_0}$ is a (random) coset of the (deterministic) finite group

$$H := \{P \in \mathrm{Poly}^2(\mathbb{F}_2^{M+d} \to X_2) : P(x, 0^d) = 0 \forall x \in \mathbb{F}_2^M\}.$$

By the finite Fourier transform, it thus suffices to establish the claim

$$\int_{\Sigma^{(d)}_{Q_0}} e(\xi \cdot (\tilde{Q} - \tilde{Q}_*))\, d\mu^{(d)}_Q = o(1)$$

with probability $1-o(1)$ for any fixed non-trivial character $\xi \colon H \to \mathbb{T}$, where $\tilde{Q}_* = \tilde{Q}_*(Q)$ is an arbitrary element of $\Sigma^{(d)}_Q$ (the exact choice is unimportant as it does not affect the magnitude of the left-hand side). By Chebyshev's inequality, it suffices to show that

$$\mathbb{E}_{Q,S} \left| \int_{\Sigma^{(d)}_{Q_0}} e(\xi \cdot (\tilde{Q} - \tilde{Q}_*))\, d\mu^{(d)}_Q \right|^2 = o(1).$$

The left-hand side can be rewritten as

$$\mathbb{E}_{v_1,\dots,v_d,v'_1,\dots,v'_d\in\mathbb{F}_2^n}\mathbb{E}_Q e(\xi\cdot(\tilde{Q}_{Q,v_1,\dots,v_d}-\tilde{Q}_{Q,v'_1,\dots,v'_d})).$$

Since d is fixed and n is going to infinity, we see that the vectors $v_1,\dots,v_d$, $v'_1,\dots,v'_d$, $e_1,\dots,e_M$ will be linearly independent with probability $1-o(1)$. Hence we may restrict to this portion of the average with acceptable error. Applying a linear change of variables (which does not affect the distribution of the random variable Q), we may then normalize $v_i=e_{M+i}$ and $v'_i=e_{M+d+i}$ for $i=1,\dots,d$. It will thus suffice to show that

$$\mathbb{E}_Q e(\xi\cdot(\tilde{Q}_{Q,e_{M+1},\dots,e_{M+d}}-\tilde{Q}_{Q,e_{M+d+1},\dots,e_{M+2d}}))=o(1).$$

The random variable Q is uniformly distributed over a finite abelian group $\mathrm{Poly}^2(\mathbb{F}_2^n\to X_2)$, and the expression inside the $e()$ is a homomorphism in Q. Hence by Fourier analysis, the claim follows unless we have the vanishing

$$\xi\cdot(\tilde{Q}_{Q,e_{M+1},\dots,e_{M+d}}-\tilde{Q}_{Q,e_{M+d+1},\dots,e_{M+2d}})=0 \tag{37}$$

for all quadratic polynomials $Q\colon\mathbb{F}_2^n\to X_2$. But if we let $P\colon\mathbb{F}_2^{M+d}\to X_2$ be an element of the group H that is not annihilated by ξ, one easily checks that the function $Q\colon\mathbb{F}_2^n\to X_2$ defined by

$$Q(x_1,\dots,x_n):=P(x_1,\dots,x_{M+d})$$

is a quadratic polynomial for which the left-hand side of (37) is non-zero. Thus we have the desired equidistribution (36).

To show full equidistribution, it suffices by the triangle inequality to show, for each element $\tilde{Q}_*$ of $\Sigma^{(d)}_Q$, that

$$d_{\mathrm{TV}}(\mu^{(d)}_{Q,S}1_{\tilde{Q}=\tilde{Q}_*},\overline{\mu}^{(d)}_{Q_0,S_0}1_{\tilde{Q}=\tilde{Q}_*})=o(1),$$

with probability $1-o(1)$, where $1_{\tilde{Q}=\tilde{Q}_*}$ denotes the indicator function to the set $\{(\tilde{Q},\tilde{S})\in\Sigma^{(d)}_{Q_0,S_0}:\tilde{Q}=\tilde{Q}_*\}$. Note from (36) that with probability $1-o(1)$, both of these measures differ in mass by $o(1)$. Once one fixes $\tilde{Q}=\tilde{Q}_*$, the variable $\tilde{S}$ ranges in a coset $\tilde{S}_{(S_0,\tilde{Q}_*)}+K$ of the finite abelian group K defined in (35), where we arbitrarily choose one representative $\tilde{S}_{(S_0,\tilde{Q}_*)}$ of this coset for each choice of $S_0,\tilde{Q}_*$. By Fourier analysis, it thus suffices to show that

$$\int_{\Sigma^{(d)}_{Q_0,S_0}} e(\xi\cdot(\tilde{S}-\tilde{S}_{(S_0,\tilde{Q}_*)}))1_{\tilde{Q}=\tilde{Q}_*}\,d\mu^{(d)}_{Q,S}(\tilde{Q},\tilde{S})=o(1)$$

with probability $1 - o(1)$ for each non-trivial character $\xi \colon K \to \mathbb{T}$ of K. As before, it suffices by the Chebyshev inequality to show that

$$\mathbb{E}_{Q,S} \left| \int_{\Sigma^{(d)}_{Q,S}} e(\xi \cdot (\tilde{S} - \tilde{S}_{S_{0,\tilde{Q}_*}})) 1_{\tilde{Q}=\tilde{Q}_*} \, d\mu^{(d)}_{Q,S}(\tilde{Q}, \tilde{S}) \right|^2 = o(1).$$

The left-hand side can be rewritten as

$$\mathbb{E}_{v_1,\dots,v_d,v'_1,\dots,v'_d \in \mathbb{F}_2^n} \mathbb{E}_{Q,S}\, e(\xi \cdot (\tilde{S}_{S,v_1,\dots,v_d} - \tilde{S}_{S,v'_1,\dots,v'_d})) 1_{\tilde{Q}_{Q,v_1,\dots,v_d} = \tilde{Q}_{Q,v'_1,\dots,v'_d} = \tilde{Q}_0}.$$

As before we can restrict to the case where $v_1, \dots, v_d, v'_1, \dots, v'_d, e_1, \dots, e_M$ are linearly independent, and then after a change of basis it suffices to show that

$$\mathbb{E}_{Q,S}\, e(\xi \cdot (\tilde{S}_{S,e_{M+1},\dots,e_{M+d}} - \tilde{S}_{S,e_{M+d+1},\dots,e_{M+2d}})) 1_{\tilde{Q}_{Q,e_{M+1},\dots,M+d} = \tilde{Q}_{Q,e_{M+d+1},\dots,e_{M+2d}} = \tilde{Q}_0} = o(1).$$

Clearly it would suffice to show that

$$\mathbb{E}_S\, e(\xi \cdot (\tilde{S}_{S,e_{M+1},\dots,e_{M+d}} - \tilde{S}_{S,e_{M+d+1},\dots,e_{M+2d}})) = o(1)$$

uniformly over all Q with

$$\tilde{Q}_{Q,e_{M+1},\dots,M+d} = \tilde{Q}_{Q,e_{M+d+1},\dots,e_{M+2d}} = \tilde{Q}_0.$$

For fixed Q, S ranges over a coset of $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ by Lemma 4.1, and the expression inside $e()$ is an (affine) homomorphism of S on this coset. Thus by Fourier analysis we are done unless the expression

$$\xi \cdot (\tilde{S}_{S,e_{M+1},\dots,e_{M+d}} - \tilde{S}_{S,e_{M+d+1},\dots,e_{M+2d}})$$

is constant on this coset, or equivalently that

$$\xi \cdot (\tilde{S}_{P,e_{M+1},\dots,e_{M+d}} - \tilde{S}_{P,e_{M+d+1},\dots,e_{M+2d}}) = 0 \tag{38}$$

for all P in the group $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$. But if we let $P' \in K$ be an element of K not annihilated by ξ, and set

$$P(x_1, \dots, x_n) := P'(x_1, \dots, x_{M+d})$$

then we see that P lies in $\mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ and does not obey (38). This completes the proof of the theorem. □

We conclude

Corollary 5.5 (Equidistributed sequence)**.** *Suppose that Conjecture 1.3 holds for $p = 2$ and $k = 5$, and let $\varepsilon \colon \mathbb{N} \to \mathbb{R}^+$ be a function decreasing to zero. Let M be as in Proposition 5.3. Then there exists a sequence of n going* *to infinity, an integer* $1 \leq m \leq M$ *and a function* $\Phi\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{T}$ *such that, for n along some sequence going to infinity, and for each n in this sequence we may find a* deterministic *n-cube* (Q, S) *in* $X_{5,5}$*, with the resulting* M*-cube* (Q_0, S_0) *(and hence* $\Sigma^{(d)}_{Q_0,S_0}$ *and* $\overline{\mu}^{(d)}_{Q_0,S_0}$*) independent of n, obeying the estimates*

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(P(x)) - e(\Phi((S(x + (a, 0^{n-M})))_{a\in\mathbb{F}_2^M}))| \leq 2\varepsilon(m) \tag{39}$$

and

$$|\mathbb{E}_{x\in\mathbb{F}_2^n} e(S(x) - P(x))| \geq \frac{1}{m}, \tag{40}$$

such that $\mu^{(d)}_{Q,S}$ *converges in total variation norm to* $\overline{\mu}^{(d)}_{Q_0,S_0}$ *for each* $d \geq 0$.

Proof. Applying Theorem 5.4 and a standard diagonal argument, we obtain along a sequence n going to infinity, an n-cube (Q, S) in $X_{5,5}$, an integer $1 \leq m \leq M$, a polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^n)$, and a function $\Phi\colon (\frac{1}{2^5}\mathbb{Z}/\mathbb{Z})^{\mathbb{F}_2^M} \to \mathbb{T}$ obeying (30), (31) such that

$$d_{\mathrm{TV}}(\mu^{(d)}_{Q,S}, \overline{\mu}^{(d)}_{Q_0,S_0}) \to 0$$

as n goes to infinity along this sequence, for each $d \geq 0$. The quantity m currently depends on n, but it takes only finitely many values, so by the pigeonhole principle we may pass to a subsequence and assume that m is independent of n. Similarly, the number of possible restrictions (Q_0, S_0) of (Q, S) to $\mathbb{F}_2^M$ is bounded independently of n, because (Q_0, S_0) is an M-cube in the finite nilspace $X_{5,5}$. Hence by the pigeonhole principle, we may pass to a further subsequence of n and assume that this restriction (Q_0, S_0) is independent of n. Finally, with Φ, we may round Φ to the nearest multiple of $\varepsilon(m)/100$ in $[0, 1]$, at the cost of worsening (30) to (39). Now the number of possible Φ is bounded independently of n, so by another application of the pigeonhole principle we can make Φ independent of n, giving the claim. □

The next step is to construct a certain finite nilspace $X_{(Q_0,S_0)}$ associated to the M-cube (Q_0, S_0), that can be viewed as an abstraction of the random samples $((Q, S)(x + (a, 0^{n-M})))_{a\in\mathbb{F}_2^M}$ of (Q, S) in the limit $n \to \infty$ (somewhat in the spirit of the Furstenberg correspondence principle). The construction is as follows. As $X_{5,5}$ is 2-homogeneous, we see from (62) that we have the equivalence

$$C^M(X_{5,5}) \equiv \mathrm{Hom}_\square(\mathbb{F}_2^M, X_{5,5}).$$

By either Remark A.3 or A.4, this space has the structure of a finite 5-step 2-homogeneous nilspace (it is easy to see that the two nilspace structures given by these remarks agree). This space will not be ergodic in general, so the equivalence relation $\sim_0$ on this space introduced in Remark A.2 can be non-trivial. The morphism (Q_0, S_0) is a point in $\mathrm{Hom}_\square(\mathbb{F}_2^M, X_{5,5})$, and we define $X_{(Q_0,S_0)}$ to be the equivalence class of this point:

$$X_{(Q_0,S_0)} := \{(Q', S') \in C^M(X_{5,5}) : (Q', S') \sim_0 (Q_0, S_0)\}.$$

This is then an ergodic finite 5-step 2-homogeneous nilspace.

For every $s \geq 0$, we define a map $\pi_s \colon \Sigma^{(1+s)}_{Q_0,S_0} \to C^s(X_{(Q_0,S_0)})$ by the formula

$$\pi_s(\tilde{Q}, \tilde{S}) := ((\tilde{Q}, \tilde{S})(\cdot, 1, \omega))_{\omega\in\{0,1\}^s}$$

for all $(\tilde{Q}, \tilde{S}) \in \Sigma^{(1+s)}_{Q_0,S_0}$; thus $\pi_s(\tilde{Q}, \tilde{S})$ is the tuple formed by restricting $(\tilde{Q}, \tilde{S})$ to the affine subspaces $\mathbb{F}_2^M \times (1, \omega)$ of $\mathbb{F}_2^{M+1+s}$ for $\omega \in \{0, 1\}^s$. Let us first check that $\pi_s(\tilde{Q}, \tilde{S})$ lies in $C^s(X_{(Q_0,S_0)})$ as claimed. Since $(\tilde{Q}, \tilde{S})$ is a $M + 1 + s$-cube in $X_{5,5}$, the map

$$(a, \omega) \mapsto (\tilde{Q}, \tilde{S})(a, 1, \omega)$$

is a $M + s$-cube in $X_{5,5}$, and hence the map

$$\omega \mapsto (a \mapsto (\tilde{Q}, \tilde{S})(a, 1, \omega))$$

is an s-cube in $C^M(X_{5,5})$. Applying (62), the tuple $\pi_s(\tilde{Q}, \tilde{S})$ is thus a s-cube in $C^M(X_{5,5})$, and thus lies in a single equivalence class of $\sim_0$. A similar argument shows that the pair

$$((a \mapsto (\tilde{Q}, \tilde{S})(a, 0, 0^s)), (a \mapsto (\tilde{Q}, \tilde{S})(a, 1, 0^s)))$$

is a 1-cube in $C^M(X_{5,5})$, and so the two elements of this pair are also equivalent by $\sim_0$. By (32), the first map is (Q_0, S_0), and hence $\psi_s(\tilde{Q}, \tilde{S})$ is an s-cube in $X_{(Q_0,S_0)}$ as claimed.

Next, we claim that the map π_s is surjective. Let $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^s}$ be an s-cube in $X_{(Q_0,S_0)}$. Our goal is to locate an $M + 1 + s$-cube $(\tilde{Q}, \tilde{S})$ in $X_{5,5}$ such that

$$(\tilde{Q}, \tilde{S})(a, 0, 0^s) = (Q_0, S_0)(a)$$

and

$$(\tilde{Q}, \tilde{S})(a, 1, \omega) = (Q'_\omega, S'_\omega)(a)$$

for all $a \in \mathbb{F}_2^M$ and $\omega \in \{0,1\}^s$. So $(\tilde{Q}, \tilde{S})$ is already partially specified on the set

$$\mathbb{F}_2^M \times (\{(0, 0^s)\} \cup (\{1\} \times \mathbb{F}_2^s)). \tag{41}$$

By the construction of $X_{(Q_0,S_0)}$, this partially specified function is known to be an $M+s$-cube on

$$\mathbb{F}_2^M \times \{1\} \times \mathbb{F}_2^s \tag{42}$$

and an $M+1$-cube on

$$\mathbb{F}_2^M \times \{0,1\} \times \{0^s\}. \tag{43}$$

The claim then follows from a large number of applications of the completion axiom for nilspaces (or by [3, Lemma 3.1.5], after performing a reflection to move $(0^M, 1, 0^s)$ to the origin).

Now we claim that all the fibers of π_s have the same cardinality. Observe that if $(\tilde{Q}, \tilde{S}), (\tilde{Q}', \tilde{S}') \in \Sigma^{(1+s)}_{Q_0,S_0}$ have the same image under π_s, then $\tilde{Q} - \tilde{Q}'$ is an element of $\mathrm{Poly}^2(\mathbb{F}_2^{M+1+s} \to X_2)$ that vanishes on the set (41); and if $\tilde{Q} = \tilde{Q}'$, then $\tilde{S} - \tilde{S}'$ is an element of $\mathrm{Poly}^5(\mathbb{F}_2^{M+1+s} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ that vanishes on (41). Conversely, if $(\tilde{Q}, \tilde{S}) \in \Sigma^{(1+s)}_{Q_0,S_0}$ and $\tilde{S} - \tilde{S}'$ is an element of $\mathrm{Poly}^5(\mathbb{F}_2^{M+1+s} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ that vanishes on (41), then $(\tilde{Q}, \tilde{S}')$ is an element of $\Sigma^{(1+s)}_{Q_0,S_0}$ with the same image as $(\tilde{Q}, \tilde{S})$ under π_s. To conclude the claim, it suffices to show that whenever $(\tilde{Q}, \tilde{S}) \in \Sigma^{(1+s)}_{Q_0,S_0}$ and $\tilde{Q} - \tilde{Q}'$ is an element of $\mathrm{Poly}^2(\mathbb{F}_2^{M+1+s} \to X_2)$ that vanishes on (41), then there exists $(\tilde{Q}', \tilde{S}') \in \Sigma^{(1+s)}_{Q_0,S_0}$ with the same image as $(\tilde{Q}, \tilde{S})$ under π_s. By Lemma 4.1, we can at least find a function $\tilde{S}'' \colon \mathbb{F}_2^n \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ with $(\tilde{Q}', \tilde{S}'')$ an n-cube in $X_{5,5}$. If the $\tilde{S}'' - \tilde{S}$ vanished on (41), we would be done; but the best that can be said at present is that this function is a polynomial of degree k on (42) and on (43), again thanks to Lemma 4.1. Applying the completion axiom (or [3, Lemma 3.1.5]) many times, we can then find $P \in \mathrm{Poly}^5(\mathbb{F}_2^n \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ which agrees with $\tilde{S}'' - \tilde{S}$ on (41); setting $\tilde{S}' := \tilde{S}'' - P$ gives the claim.

From the above properties of π_s we see that π_s pushes forward the uniform probability measure $\overline{\mu}^{(1+s)}_{Q_0,S_0}$ on $\Sigma^{(1+s)}_{Q_0,S_0}$ to the uniform probability measure on $C^s(X_{(Q_0,S_0)})$. Combining this with Corollary 5.5, we conclude

Corollary 5.6 (Equidistributed sequence, again)**.** *Suppose that Conjecture 1.3 holds for $p = 2$ and $k = 5$, and let $\varepsilon \colon \mathbb{N} \to \mathbb{R}^+$ be a function decreasing* *to zero. Let M be as in Proposition 5.3, and let $n, (Q, S), (Q_0, S_0), m, \Phi$ be as in Corollary 5.5. If for any $s \geq 0$ we select $x, h_1, \ldots, h_s \in \mathbb{F}_2^n$ uniformly and independently at random, then the random tuple*

$$((a \mapsto (Q, S)((a, 0^{n-M}) + x + \sum_{i=1}^{s} \omega_i h_i)))_{\omega \in \{0,1\}^s}$$

converges in distribution to the uniform distribution on $C^s(X_{(Q_0,S_0)})$.

Proof. Observe that this random tuple is nothing more than the image under π_s of the randomly sampled tuple $(\tilde{Q}, \tilde{S})_{(Q,S),x,h_1,\ldots,h_s}$. The claim follows. □

In the language of [5], this corollary asserts that the sampling map

$$x \mapsto (a \mapsto (Q, S)((a, 0^{n-M}) + x))$$

becomes an asymptotically balanced map from $\mathcal{D}^1(\mathbb{F}_2^n)$ to $X_{(Q_0,S_0)}$ as n goes to infinity along the sequence.

5.3. **Concluding the argument.** With the equidistribution theory for the n-cube (Q, S) in hand, we can now return to the task of deriving a contradiction. Let the notation be as in Proposition 5.3 and Corollary 5.6.

The first step is to use Corollary 5.6 to transfer the various structural conclusions of Proposition 5.3 to the nilspace $X_{(Q_0,S_0)}$, in order to obtain a situation somewhat resembling that in the proof of Proposition 4.5. Let n be in the indicated sequence going to infinity, and let $x, h_1, \ldots, h_6$ be drawn uniformly and independently at random from $\mathbb{F}_2^n$. By Corollary 5.6, the random tuple

$$((a \mapsto (Q, S)((a, 0^{n-M}) + x + \sum_{i=1}^{6} \omega_i h_i)))_{\omega \in \{0,1\}^6} \tag{44}$$

(which is a 6-cube in $X_{(Q_0,S_0)}$) converges in distribution to the uniform distribution on $C^6(X_{(Q_0,S_0)})$, while the random function

$$a \mapsto (Q, S)((a, 0^{n-M}) + x) \tag{45}$$

on $\mathbb{F}_2^M$ (which is an element of $X_{(Q_0,S_0)}$) converges in distribution to the uniform distribution on $X_{(Q_0,S_0)}$.

From (39), (31) we have (for $\varepsilon(m)$ small enough) that

$$\mathbb{E}_{x \in \mathbb{F}_2^n} |e(S(x)) - e(\Phi((S(x + a))_{a \in \mathbb{F}_2^M}))| \geq \frac{1}{2m}.$$

Since the random variable (45) converges to the uniform distribution on $X_{(Q_0,S_0)}$, we conclude that

$$|\mathbb{E}_{(Q',S')\in X_{(Q_0,S_0)}} e(S'(0) - \Phi(S'))| \geq \frac{1}{2m}. \tag{46}$$

Similarly, as P is a quintic polynomial, we have

$$\mathbb{E}_{x\in\mathbb{F}_2^n;\vec{h}\in(\mathbb{F}_2^n)^6}\left| e\left(\sum_{\omega\in\{0,1\}^6}(-1)^{|\omega|}P(x+\omega\cdot\vec{h})\right) - 1\right| = 0.$$

Hence by (30) and many applications of the triangle inequality

$$\mathbb{E}_{x\in\mathbb{F}_2^n;\vec{h}\in(\mathbb{F}_2^n)^6}\left| e\left(\sum_{\omega\in\{0,1\}^6}(-1)^{|\omega|}\Phi((S(x+a+\omega\cdot\vec{h}))_{a\in\mathbb{F}_2^M}\right) - 1\right| = O(\varepsilon(m))$$

where the implied constant in the $O()$ notation is absolute. Since the random variable (44) converges to the uniform distribution on $C^6(X_{(Q_0,S_0)})$, we conclude that

$$\mathbb{E}_{(Q',S')\in C^6(X_{(Q_0,S_0)})}\left| e\left(\sum_{\omega\in\{0,1\}^6}(-1)^{|\omega|}\Phi((S'(a,\omega)))_{a\in\mathbb{F}_2^M}\right) - 1\right| = O(\varepsilon(m)).$$

Applying Theorem A.25 (and Markov's inequality), we conclude (for ε sufficiently rapidly decreasing) that there exists a quintic polynomial $\Phi' \in \mathrm{Poly}^5(X_{(Q_0,S_0)})$ such that

$$\mathbb{E}_{(Q',S')\in X_{(Q_0,S_0)}}|e(\Phi(S')) - e(\Phi'(Q',S'))| \leq \frac{1}{4m}$$

and hence by (46) and the triangle inequality

$$|\mathbb{E}_{(Q',S')\in X_{(Q_0,S_0)}} e(S'(0) - \Phi'(Q',S')))| \geq \frac{1}{4m}. \tag{47}$$

To take advantage of this correlation, we perform vertical differentiation in the S' direction. Arguing exactly as in the proof of (27), we see that the vertical derivative $\Phi'(Q',S'+\frac{1}{2}) - \Phi'(Q',S')$ is constant, and thus $e(\Phi')$ is an eigenfunction of the vertical Koopman operator V^u defined by

$$V^u F(Q',S') := F(Q',S'+\frac{1}{2}).$$

As before, $(Q',S') \mapsto e(S'(0))$ is also an eigenfunction of this operator, with eigenvalue $e(\frac{1}{2})$. From (47), these two eigenfunctions of this unitary operator are not orthogonal, and hence the eigenvalue of $e(\Phi')$ must also be $e(\frac{1}{2})$. Thus, if we place an equivalence relation $\sim$ on $X_{(Q_0,S_0)}$ by declaring

$(Q', S') \sim (Q'', S'')$ if $Q' = Q''$ and S'' is equal to either S' or $S' + \frac{1}{2}$, then the function

$$(Q', S') \mapsto S'(0) - \Phi'(Q', S')$$

is invariant with respect to this equivalence and thus can be viewed as a function on the quotient space $X_{(Q_0,S_0)}/\sim$. In order to exploit this invariance to contradict Theorem 3.1, we will need to build a "lifting map" from X_2 to $X_{(Q_0,S_0)}/\sim$ that assigns to each $q \in X_2$ a certain element (Q^*_q, S^*_q) of $X_{(Q_0,S_0)}$ (defined up to the equivalence $\sim$) that has good properties. More precisely, we will show:

Lemma 5.7 (Existence of lift)**.** *One can assign an element (Q^*_q, S^*_q) of $X_{(Q_0,S_0)}$ to each $q \in X_2$ with the following properties:*

- *(Lift) For each $q \in X_2$, one has $Q^*_q(0) = q$.*
- *(Morphism up to equivalence) For any 6-cube $(q_\omega)_{\omega\in\{0,1\}^6} \in C^6(X_2)$ in X_2, there exists a 6-cube $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^6} \in C^6(X_{(Q_0,S_0)})$ in $X_{(Q_0,S_0)}$ such that $(Q'_\omega, S'_\omega) \sim (Q^*_{q_\omega}, S^*_{q_\omega})$ for all $\omega \in \{0,1\}^6$.*

Remark 5.8. Although we will not prove it here, one can show that the quotient space $X_{(Q_0,S_0)}/\sim$ is itself a nilspace which is an extension of the nilspace X_2. The map that sends q to (the equivalence class of) (Q^*_q, S^*_q) can then be viewed as a "splitting" of that extension by a section that is itself a nilspace morphism. It is in order to obtain this lifting that we were forced to use the larger nilspace $X_{5,5}$ instead of the smaller nilspace $X_{5,1}$, as we will need to take advantage of the freedom to modify S by non-classical polynomials, and not merely by classical ones.

Let us assume this lemma for the moment and obtain the desired contradiction. Let $(q_\omega)_{\omega\in\{0,1\}^6} \in C^6(X_2)$ be a 6-cube in X_2, and let $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^6} \in C^6(X_{(Q_0,S_0)})$ be as in the above lemma. Since Φ' is quintic on $X_{(Q_0,S_0)}$, we have

$$\sum_{\omega\in\{0,1\}^6} (-1)^{|\omega|}\Phi'(Q'_\omega, S'_\omega) = 0.$$

Also, from the nilspace structure of $X_{(Q_0,S_0)}$ we have

$$\sum_{\omega\in\{0,1\}^6} (-1)^{|\omega|} S'_\omega(0) = \rho((Q'_\omega(0))_{\omega\in\{0,1\}^6}).$$

Subtracting, we conclude that

$$\sum_{\omega\in\{0,1\}^6} (-1)^{|\omega|}(S'_\omega(0) - \Phi'(Q'_\omega, S'_\omega) = \rho((Q'_\omega(0))_{\omega\in\{0,1\}^6}).$$

Both sides are invariant with respect to $\sim$, so we may replace (Q'_ω, S'_ω) with $(Q^*_{q_\omega}, S^*_{q_\omega})$ in this identity, thus

$$\sum_{\omega\in\{0,1\}^6} (-1)^{|\omega|}(S^*_{q_\omega}(0) - \Phi'(Q^*_{q_\omega}, S^*_{q_\omega}) = \rho((Q^*_{q_\omega}(0))_{\omega\in\{0,1\}^6}).$$

By the lifting property we have $Q^*_{q_\omega}(0) = q_\omega$. We conclude that

$$\rho = dF$$

where $F\colon \mathbb{F}_2^2 \to \mathbb{T}$ is the function

$$F(q) := S^*_q(0) - \Phi'(Q^*_q, S^*_q).$$

But this contradicts Theorem 3.1.

It remains to construct the lift (Q^*_q, S^*_q) in Lemma 5.7. This will be accomplished by solving a certain system of constraints. More precisely:

Proposition 5.9 (Solving a system of constraints)**.** *Let $d \geq 0$, and let $(q_\omega)_{\omega\in\{0,1\}^d}$ be a d-cube in X_2. Then there exists a d-cube $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^d}$ in $X_{(Q_0,S_0)}$ obeying the following constraints:*

1. *For every $\omega \in \{0,1\}^d$, one has $Q'_\omega(a) = q_\omega + Q_0(a) - Q_0(0)$ for all $a \in \mathbb{F}_2^M$. In particular, $Q'_\omega(0) = q_\omega$.*
2. *For every $1 \leq l \leq k-1$ and $1 \leq i_1 < \cdots < i_l \leq M$, one has*

$$\partial_{e_{i_1}} \dots \partial_{e_{i_l}} S'_\omega(0) = \partial_{e_{i_2}} \dots \partial_{e_{i_l}} \psi_{\omega,i_l}(0) - \partial_{e_{i_2}} \dots \partial_{e_{i_l}} \psi_{*,i_l}(0) + \partial_{e_{i_1}} \dots \partial_{e_{i_l}} S_0(0)$$

where

$$\psi_{\omega,i_l}(a) := \psi(Q'_\omega(a), Q'_\omega(a+e_{i_l}))$$

and

$$\psi_{*,i_l}(a) := \psi(Q_0(a), Q_0(a+e_{i_l}))$$

for all $a \in \mathbb{F}_2^M$.

3. *One has $2S'_\omega(0) = 2S_0(0)$ for all $\omega \in \{0,1\}^d$.*

Furthermore, this cube is unique up to equivalence in the following sense: if $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^d}, ((Q''_\omega, S''_\omega))_{\omega\in\{0,1\}^d} \in C^d(X)$ both obey the properties (1)-(3), then we have $(Q'_\omega, S'_\omega) \sim (Q''_\omega, S''_\omega)$ for all $\omega \in \{0,1\}^d$.

Let us assume this proposition for the moment and see how it implies Lemma 5.7. Applying this proposition with $d = 0$, we see that for each $q \in X_2$, we can find $(Q^*_q, S^*_q) \in X_{(Q_0,S_0)}$ obeying the $d = 0$ conclusions (1)-(3) of the proposition; in particular, $Q^*_q(0) = q$. Now let $(q_\omega)_{\omega\in\{0,1\}^6} \in C^6(X_2)$ be a 6-cube in X_2, and let $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^6} \in C^6(X_{(Q_0,S_0)})$ be as in the proposition. For each $\omega \in \{0,1\}^6$, the point (Q'_ω, S'_ω) in $X_{(Q_0,S_0)}$ obeys the $d = 0$ axioms of (1)-(3) with respect to the 0-cube q_ω. Since $(Q^*_{q_\omega}, S^*_{q_\omega})$ does also, we conclude from the uniqueness component of this proposition that $(Q'_\omega, S'_\omega) \sim (Q^*_{q_\omega}, S^*_{q_\omega})$ for all $\omega \in \{0,1\}^d$. Lemma 5.7 follows.

It remains to establish Proposition 5.9. We first verify the uniqueness aspect. Suppose we have two cubes $((Q'_\omega, S'_\omega))_{\omega\in\{0,1\}^d}, ((Q''_\omega, S''_\omega))_{\omega\in\{0,1\}^d} \in C^d(X_{(Q_0,S_0)})$ both obeying axioms (1)-(3). From axiom (1) we see that $Q'_\omega = Q''_\omega$ for all $\omega \in \{0,1\}^d$. From axiom (2), we see that

$$\partial_{e_{i_1}} \dots \partial_{e_{i_l}} S'_\omega(0) = \partial_{e_{i_1}} \dots \partial_{e_{i_l}} S''_\omega(0) \tag{48}$$

whenever $1 \leq l \leq k-1$ and $1 \leq i_1 < \cdots \leq i_l \leq M$. We claim that the same statement also holds for $l = k$. Indeed, by construction of $X_{(Q_0,S_0)}$, we can find $(\tilde{Q}, \tilde{S}) \in \Sigma^{(1+d)}_{(Q,S)}$ such that

$$(Q'_\omega, S'_\omega)(a) = (\tilde{Q}, \tilde{S})(a, 1, \omega)$$

for all $\omega \in \{0,1\}^d$ and $a \in \mathbb{F}_2^M$. Since $\tilde{S}$ agrees with S on $\mathbb{F}_2^M$, we conclude that

$$\partial_{e_{i_1}} \dots \partial_{e_{i_k}} S'_\omega(0) = \partial_{e_{i_1}} \dots \partial_{e_{i_k}} S_0(0) + \partial_{(0,1,\omega)} \partial_{e_{i_1}} \dots \partial_{e_{i_k}} \tilde{S}(0).$$

As $(\tilde{Q}, \tilde{S})$ is an $M + 1 + d$-cube in $X_{5,5}$, the right-hand side is equal to

$$\partial_{e_{i_1}} \dots \partial_{e_{i_k}} S_0(0) + \rho((\tilde{Q}(\sum_{j=1}^{k+1} \alpha_j w_j))_{\alpha\in\{0,1\}^{k+1}})$$

where $w_j := e_{i_j}$ for $j = 1, \dots, k$ and $w_{k+1} := (0, 1, \omega)$. This expression depends only on Q'_ω, Q_0, and S_0. We have a similar formula for S''_ω. Since $Q'_\omega = Q''_\omega$, we conclude that (48) holds for $l = k$.

Now we claim that (48) also holds for $l > k$. It suffices to show that

$$\partial_{e_{i_1}} \dots \partial_{e_{i_{k+1}}} S'_\omega(a) = \partial_{e_{i_1}} \dots \partial_{e_{i_{k+1}}} S''_\omega(a)$$

whenever $a \in \mathbb{F}_2^M$ and $1 \le i_1 < \cdots < i_{k+1} \le M$. As (Q'_ω, S'_ω) is an M-cube in $X_{5,5}$, one has

$$\partial_{e_{i_1}} \ldots \partial_{e_{i_{k+1}}} S'_\omega(a) = \Psi((Q'_\omega((a + \sum_{j=1}^{k+1} \alpha_j e_{i_j}))_{\alpha \in \{0,1\}^{k+1}})).$$

Similarly for S''_ω and Q''_ω. Since $Q'_\omega = Q''_\omega$, we obtain (48) for all $l > k$.

Now that (48) has been established for all $l > 0$, we see from Taylor expansion that

$$S''_\omega = S'_\omega - S'_\omega(0) + S''_\omega(0).$$

From axiom (3), $2(-S'_\omega(0) + S''_\omega(0)) = -2S(0) + 2S(0) = 0$, hence for each $\omega \in \{0,1\}^d$, S''_ω is either equal to S'_ω or $S'_\omega + \frac{1}{2}$. Since also $Q'_\omega = Q''_\omega$, we conclude that $(Q'_\omega, S'_\omega) \sim (Q''_\omega, S''_\omega)$. This completes the proof of uniqueness.

Now we establish existence. Let $d \ge 0$, and let $(q_\omega)_{\omega \in \{0,1\}^d}$ be a d-cube in X_2. By the construction of $X_{(Q_0, S_0)}$, our task is to find a $M + 1 + d$-cube $(\tilde{Q}, \tilde{S})$ in $X_{5,5}$ obeying the following properties:

(0) For $a \in \mathbb{F}_2^M$, we have $(\tilde{Q}, \tilde{S})(a, 0^{n-M}) = (Q_0, S_0)(a)$.

(1) For every $\omega \in \{0,1\}^d$ and $a \in \mathbb{F}_2^M$, one has $\tilde{Q}(a, 1, \omega) = q_\omega + Q_0(a) - Q_0(0)$.

(2) For every $1 \le l \le k - 1$ and $1 \le i_1 < \cdots < i_l \le M$, one has

(49)
$$\partial_{e_{i_1}} \ldots \partial_{e_{i_l}} \tilde{S}(0,1,\omega) = \partial_{e_{i_2}} \ldots \partial_{e_{i_l}} \psi_{i_l}(0,1,\omega) - \partial_{e_{i_2}} \ldots \partial_{e_{i_l}} \psi_{i_l}(0,0,0) + \partial_{e_{i_1}} \ldots \partial_{e_{i_l}} \tilde{S}(0,0,0)$$

where

$$\psi_{i_l}(x) := \psi(\tilde{Q}(x), \tilde{Q}(x + e_{i_l}))$$

for all $x \in \mathbb{F}_2^{M+1+d}$.

(3) We have $2\tilde{S}(0^M, 1, \omega) = 2S_0(0)$ for all $\omega \in \{0,1\}^d$.

To obey (1) (and the $\tilde{Q}$ component of (0)), we define $\tilde{Q} \colon \mathbb{F}_2^{M+1+d} \to Y$ by the formula

$$\tilde{Q}(a, t, \omega) := q_\omega + tq_0 - q_0 + Q(a) - tQ(0)$$

for $a \in \mathbb{F}_2^M$, $t \in \mathbb{F}_2$, $\omega \in \mathbb{F}_2^d$. One easily verifies that $\tilde{Q}$ is a polynomial of degree 2 that obeys (2) and the $\tilde{Q}$ component of (1). By Lemma 4.1, we can then find a map $\tilde{S}_0 \colon \mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ such that $(\tilde{Q}, \tilde{S}_0)$ is a $M + 1 + d$-cube in $X_{5,5}$ (and in fact in $X_{5,1}$). We need to then find an element $\tilde{S}$ of the coset $\tilde{S}_0 + \mathrm{Poly}(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ which obeys the following properties:

(0) For $a \in \mathbb{F}_2^M$, we have $\tilde{S}(a, 0^{n-M}) = S_0(a)$. It is not necessarily the case that $\tilde{S}$ agrees with S on $\mathbb{F}_2^M$ (so that $(\tilde{Q}, \tilde{S})$ lies in $\Sigma^{(1+d)}_{(Q,S)}$).

(2) For every $1 \leq l \leq k-1$ and $1 \leq i_1 < \cdots < i_l \leq M$, (49) holds.

(3) We have $2\tilde{S}(0^M, 1, \omega) = 2S_0(0)$ for all $\omega \in \{0,1\}^d$.

We will enforce each of these properties (0), (2), (3) in turn (making sure that each modification of $\tilde{S}$ that we make does not destroy any properties that we have already established).

We first locate a function $\tilde{S} \in \tilde{S}_0 + \mathrm{Poly}(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ obeying (0). Observe that $(Q_0, \tilde{S}(\cdot, 0^{1+d}))$ and (Q_0, S_0) are both M-cubes in $X_{5,5}$, and hence the restriction of $\tilde{S}_0 - S$ to $\mathbb{F}_2^M$ lies in $\mathrm{Poly}^5(\mathbb{F}_2^M \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$. By composing this polynomial with the obvious projection from $\mathbb{F}_2^{M+1+d}$ to $\mathbb{F}_2^M$, we conclude that $\tilde{S}_0 - S$ agrees on $\mathbb{F}_2^M \times \{0\} \times \{0^d\}$ with some polynomial in $\mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$. Subtracting this polynomial from $\tilde{S}_0$, we obtain an element $\tilde{S}$ of $\tilde{S}_0 + \mathrm{Poly}(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ oyeing property (0).

We now enforce the property (2) by induction on i_1. More precisely, we assume inductively that we have found $\tilde{S} \in \tilde{S}_0 + \mathrm{Poly}(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ obeying (0) for which (1) has already been established in the case $i_1 < i_*$ for some $1 \leq i_* \leq M$, and wish to modify $\tilde{S}$ so that it still obeys (0) but now also obeys (1) in the case $i_1 \leq i_*$.

Observe that if we add or subtract to $\tilde{S}$ a polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ which vanishes on $\mathbb{F}_2^M \times \{0\} \times \{0^d\}$, and which also does not depend on the first $i_* - 1$ coordinates in the sense that $\partial_{e_i} P = 0$ for $1 \leq i < i_*$, then $\tilde{S}$ continues to obey (0) and (1) for $i_1 < i_*$ (though again this may destroy property (d)). We exploit this freedom to modify $\tilde{S}$ as follows.

First, we use the fact that $\rho = d^5\psi$ to write the condition (1) on the $M+1+d$-cube $(\tilde{Q}, \tilde{S})$ as

$$\partial_{h_1} \dots \partial_{h_5} (\partial_h \tilde{S} - \psi(\tilde{Q}(\cdot), \tilde{Q}(\cdot + h))) = 0$$

for all $h, h_1, \dots, h_5 \in \mathbb{F}_2^{M+1+d}$. Equivalently, one has

$$\partial_h \tilde{S} - \psi(\tilde{Q}(\cdot), \tilde{Q}(\cdot + h)) \in \mathrm{Poly}^4(\mathbb{F}_2^{M+1+d}) \tag{50}$$

for each $h \in \mathbb{F}_2^{M+1+d}$. Applying this with $h = e_{i_*}$, we conclude that the function

$$P := \partial_{e_{i_*}} \tilde{S} - \psi_{i_*}$$

lies in $\mathrm{Poly}^4(\mathbb{F}_2^{M+1+d})$. Now we look at the expression

$$P(a,1,\omega)-P(a,0,0^d) = \partial_{e_{i_*}}\tilde{S}(a,1,\omega)-\psi_{i_*}(a,1,\omega)-\partial_{e_{i_*}}\tilde{S}(a,0,0^d)+\psi_{i_*}(a,0,0^d)$$

for $a \in 0^{i_*} \times \mathbb{F}_2^{M-i_*}$ and $\omega \in \mathbb{F}_2^d$. Expanding P out into monomials using Lemma A.23, we can write

$$P(a,1,\omega) - P(a,0,0^d) = \sum_{l=1}^{4} \sum_{i_*<i_1<\dots<i_l\leq M+1+d; i_l>M} \frac{c_{i_1,\dots,i_l}|x_{i_1}|\dots|x_{i_l}|}{2^{5-l}} \mod 1$$

for some coefficients $c_{i_1,\dots,i_l} \in \mathbb{Z}$, where $(x_1,\dots,x_{M+1+d}) := (a,1,\omega)$. If we then introduce the function $R\colon \mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ by the formula

$$R(x_1,\dots,x_{M+1+d}) := \sum_{l=1}^{4} \sum_{i_*<i_1<\dots<i_l\leq M+1+d; i_l>M} \frac{c_{i_1,\dots,i_l}|x_{i_*}||x_{i_1}|\dots|x_{i_l}|}{2^{k-l}} \mod 1$$

for $(x_1,\dots,x_{M+1+d}) \in \mathbb{F}_2^M$, then from Lemma A.23 we see that[3] $R \in \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ and that

$$P(a,1,\omega) - P(a,0,0^d) = \partial_{e_{i_*}}R(a,1,\omega)$$

for $a \in 0^{i_*} \times \mathbb{F}_2^{M-i_*}$ and $\omega \in \mathbb{F}_2^d$. Also R vanishes on $\mathbb{F}_2^M$ and is invariant with respect to the first i_* coordinates, so as discussed above we may freely subtract R from $\tilde{S}$. If we do so, then we now have

$$P(a,1,\omega) - P(a,0,0^d) = 0$$

for all $a \in \mathbb{F}_2^M$ and $\omega \in \mathbb{F}_2^d$, which on further differentiation gives (49) for $i_1 = i_*$ as required.

Finally, we enforce the property (3). As already observed, if we add or subtract to $\tilde{S}$ a polynomial $P \in \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$ which vanishes on $\mathbb{F}_2^M$, and which also does not depend on the first M coordinates, then the properties (0), (2) remain unaffected. To exploit this, recall that $\tilde{S}$ lies in the coset $\tilde{S}_0 + \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$; since $\tilde{S}_0$ takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, we conclude from (61) that

$$2\tilde{S} \in \mathrm{Poly}^4(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^4}\mathbb{Z}/\mathbb{Z})$$

and hence from (61) again we may write

$$2\tilde{S} = 2P \tag{51}$$

[3] It is here that we need to have worked with $X_{5,5}$ instead of $X_{5,1}$, as we cannot guarantee that the quintic polynomial R will be classical.

for some $P \in \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$. The function

$$(a, t, \omega) \mapsto P(0^M, t, \omega) - P(0^M, 0, 0^d)$$

is then a quintic polynomial on $\mathbb{F}_2^{M+1+d}$ that vanishes on $\mathbb{F}_2^M$ and does not depend on the first M coordinates; if we then define

$$\tilde{S}'(a, t, \omega) := S(a, t, \omega) - P(0^M, t, \omega) + P(0^M, 0, 0^d)$$

then $\tilde{S}'$ lies in $\tilde{S}_0 + \mathrm{Poly}^5(\mathbb{F}_2^{M+1+d} \to \frac{1}{2^5}\mathbb{Z}/\mathbb{Z})$, obeys (0) and (2), and for each $\omega \in \{0, 1\}^d$ we have

$$2\tilde{S}'(0^M, 1, \omega) = 2P(0^M, 0, 0^d) = 2\tilde{S}(0^M, 0, 0^d) = 2S_0(0)$$

giving (3). This completes the proof of Proposition 5.9, and thus Theorem 1.6.

Remark 5.10. If one replaces $X_{5,5}$ by $X_{5,1}$ in the above construction then one no longer obtains a counterexample to Conjecture 1.3. We sketch the proof of this as follows. By Remark 5.1, the pseudo-quintic function S takes the form

$$S = \frac{\binom{R}{2}Q^{(2)} + P}{2} \mod 1$$

for some randomly chosen polynomials $R \in \mathrm{Poly}^3(\mathbb{F}_2^n \to \mathbb{Z}/4\mathbb{Z})$, $Q^{(1)}, Q^{(2)} \in \mathrm{Poly}^2(\mathbb{F}_2^n \to \mathbb{F}_2)$, $P \in \mathrm{Poly}^5(\mathbb{F}_2^n \to \mathbb{F}_2)$ with $Q^{(1)} = R \mod 2$; note crucially that P now takes values in tje classical range $\mathbb{F}_2$ as opposed to the non-classical range $\frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$. After many applications of the Leibniz rule (60) (and (26)) we see that for any shifts $a, b, c, d, e \in \mathbb{F}_2^n$ we have the fifth derivative computation

$$\partial_a\partial_b\partial_c\partial_d\partial_e S = \frac{\partial_a\partial_b Q^{(1)}\partial_c\partial_d Q^{(1)}\partial_e Q^{(2)} + \dots}{2}$$

where the $\dots$ are a sum of terms that are either constants in $\mathbb{F}_2$ (depending on a, b, c, d, e), or linear functions that resemble permutations of $\partial_a\partial_b Q^{(1)}\partial_c\partial_d Q^{(1)}\partial_e Q^{(2)}$ (in fact there are 44 terms of this latter type). For a, b, c, d, e chosen at random, it is true with positive probability that $\partial_a\partial_b Q^{(1)} = \partial_c\partial_d Q^{(1)} = 1$, so that the displayed term $\partial_a\partial_b Q^{(1)}\partial_c\partial_d Q^{(1)}\partial_e Q^{(2)}$ simplifies to $\partial_e Q^{(2)}$, while the other permutations of this term vanish. From this one can conclude that with high probability, and for a given random shift e the linear functions $\partial_e Q^{(2)}$ are measurable in the sense that they are a function of boundedly many shifts of S by e and other random shifts. Similarly for $\partial_e Q^{(1)}$. In a similar spirit, we have the fourth derivative computation

$$\partial_a\partial_b\partial_c\partial_d S = \frac{\partial_a\partial_b Q^{(1)}\partial_c\partial_d Q^{(1)} Q^{(2)} + \dots}{2}$$

where the terms in $\dots$ take values in $\mathbb{F}_2$ and are either permutations of the displayed term, are combinations of functions already known to be measurable, or are linear. By the preceding argument one can show that with high probability $Q^{(2)}$ is measurable up to a classical linear polynomial; and similarly for $Q^{(1)}$. Finally, we have the second derivative computation

$$\partial_a\partial_b S = \frac{\binom{R}{2}\partial_a\partial_b Q^{(2)} + \dots}{2}$$

where the terms in $\dots$ take values in $\mathbb{F}_2$ and are either combinations of functions already known to be measurable, or are cubic. Repeating the previous argument, we conclude with high probability that $\binom{R}{2}$ (which one can check to be a classical quartic polynomial) is measurable up to a classical cubic polynomial. Taking advantage of the ability to pointwise multiply in the classical range $\mathbb{F}_2$ using Lemma A.21, we conclude with high probability that $\binom{R}{2}Q^{(2)}$ is measurable up to a classical quintic polynomial. Hence S is measurable up to a quintic polynomial, which must then also be measurable since S is measurable. By a Fourier expansion, one can then show that S correlates with a measurable quintic polynomial, giving Conjecture 1.3 in this case. Thus one can explain the need to work with the more complicated space $X_{5,5}$ instead of $X_{5,1}$ in order to destroy the ability to multiply polynomials together by working in non-classical ranges such as $\frac{1}{2^5}\mathbb{Z}/\mathbb{Z}$ instead of $\mathbb{F}_2$.

Remark 5.11. By combining these constructions with the arguments in Appendix B, we obtain a counterexample to Conjecture 1.2. It is natural to ask whether there is a shortcut approach that could construct the counterexample to Conjecture 1.2 more directly, without first building a counterexample to Conjecture 1.3. Morally speaking, this should proceed by starting with the space $\mathrm{Hom}_{\square}(\mathcal{D}^1(\mathbb{F}_2^{\omega}) \to X_{5,5})$, which is a compact $\mathbb{F}_2^{\omega}$-system that can be naturally equipped with a Haar measure. This system is not ergodic, but a generic component of the ergodic decomposition should be a 5-step ergodic $\mathbb{F}_2^{\omega}$-system that fails to be Abramov of order 5 (cf., the role of the pair

(Q_0, S_0) in the above analysis); however, in the spirit of Remark 4.6, one would expect that this system would admit an extension that is Abramov of order 5 (and it should even be a Weyl system of order 5, in the sense of e.g., [16]). The rigorous verification of these claims seems to be of comparable complexity to the arguments just presented, and so we do not detail this more direct approach here.

Appendix A. Nilspaces, filtered abelian groups, and non-classical polynomials

In this section we gather some standard (and mostly algebraic) facts about nilspaces, filtered abelian groups, and polynomial maps.

A.1. **Nilspaces.**

Nilspaces were introduced by Host–Kra [15] (under the equivalent formulation of *parallelepiped structures*) and Camarena–Szegedy [2] as an abstraction of the concept of a parallelepiped in a group or dynamical system. They can be defined in the set-theoretic, topological, and measurable categories, but we will only need to consider finite nilspaces, which allows us to work in the technically simpler set-theoretic category. We recall the definition of a nilspace, following [3, Definition 1.2.1]:

Definition A.1 (Nilspaces)**.** A nilspace is a set X together with a collection of sets $C^n(X) \subset X^{\{0,1\}^n}$ for each non-negative integer n, satisfying the following axioms:

(i) (Composition) For every $m, n \geq 0$ and every cube morphism $\phi \colon \{0,1\}^m \to \{0,1\}^n$ (by which we mean a function that extends to an affine map from $\mathbb{R}^m$ to $\mathbb{R}^n$) and every $c \in C^n(X)$, we have $c \circ \phi \in C^m(X)$.

(ii) (0-ergodicity) $C^0(X) = X$. If we have the stronger property $C^1(X) = X^{\{0,1\}}$, we say that the nilspace is *ergodic* (or 1*-ergodic*).

(iii) (Corner completion) Let $n \geq 1$, and let $c' \colon \{0,1\}^n \backslash \{1\}^n \to X$ be a function such that every restriction of c' to an $(n-1)$-face containing 0^n is in $C^{n-1}(X)$. Then there exists $c \in C^n(X)$ such that $c(v) = c'(v)$ for all $v \neq 1^n$. If this c is unique, we say that X is an $(n-1)$*-step nilspace*.

Elements of $C^n(X)$ will be referred to as *n-cubes* in X.

A *nilspace morphism* $\phi\colon X \to Y$ between two nilspaces is a function that preserves n-cubes for every $n \geq 0$, in the sense that $(\phi(x_\omega))_{\omega\in\{0,1\}^n}) \in C^n(Y)$ whenever $(x_\omega)_{\omega\in\{0,1\}^n} \in C^n(X)$. The space of such morphisms will be denoted $\mathrm{Hom}_\square(X \to Y)$.

Clearly the collection of nilspaces and their morphisms form a category. It is also easy to see that if a nilspace X is k-step, then it is also k'-step for any $k' \geq k$.

Remark A.2 (Ergodic decomposition)**.** In much of the literature (e.g., [3]) the term "nilspace" is used to denote what we call an "ergodic nilspace", but it will be convenient for us to only impose the weaker axiom of 0-ergodicity in our basic definitions. In any event, it is often not difficult to reduce to the ergodic case via the following *ergodic decomposition*. If X is a nilspace, we can define a relation[4] $\sim_0$ on X by declaring $x \sim_0 y$ if $(x, y) \in C^1(X)$. It is not difficult to verify that this is an equivalence relation, that each equivalence class has the structure of an ergodic nilspace, and the original nilspace X is the disjoint union of these ergodic nilspaces; see [3, Lemma 3.1.8]. Because of this, many of the foundational results on ergodic nilspaces (such as those set out in [3]) extend without difficulty to the more general nilspace setting.

Remark A.3 (Cube spaces as nilspaces)**.** If X is a nilspace and $d \geq 0$, then the collection $C^d(X)$ of d-cubes in X is itself a nilspace, with cube structure given by

$$C^n(C^d(X)) := C^{d+n}(X)$$

for all $n \geq 0$, after performing the identification

$$(x_\omega)_{\omega\in\{0,1\}^{d+n}} \equiv ((x_{\omega,\omega'})_{\omega\in\{0,1\}^d})_{\omega'\in\{0,1\}^n} \tag{52}$$

that interprets any $(d + n)$-cube $(x_\omega)_{\omega\in\{0,1\}^{d+n}} \in C^{d+n}(X)$ as an n-cube of d-cubes. One can easily check that $C^d(X)$ obeys the nilspace axioms, and is k-step if X is k-step, although we caution that $C^d(X)$ need not be ergodic even when X is ergodic (this is a primary reason why we do not impose ergodicity in our definition of a nilspace).

[4] This is a special case of a more general class of equivalence relations $\sim_k$ one can define on nilspaces; see [3, Definition 3.2.3].

Remark A.4 (Morphism spaces as nilspaces)**.** If X, Y are nilspaces, then the collection $\mathrm{Hom}_\Box(X \to Y)$ of nilspace morphisms from X to Y is itself a nilspace, with the cube structure given by

$$C^n(\mathrm{Hom}_\Box(X \to Y)) := \mathrm{Hom}_\Box(X \to C^n(Y))$$

for all $n \geq 0$, where we view a map from X to $C^n(Y) \subset Y^{\{0,1\}^n}$ as a $\{0,1\}^n$-tuple of maps from X to Y in the obvious fashion. One can easily check that $\mathrm{Hom}_\Box(X \to Y)$ obeys the nilspace axioms, and is k-step if Y is k-step. Again, we caution that $\mathrm{Hom}_\Box(X \to Y)$ need not be ergodic even when X, Y are both ergodic.

By definition, a nilspace morphism $\phi \colon X \to Y$ has to preserve n-cubes for every $n \geq 0$. But if Y is k-step, it turns out one only has to check preservation of $k+1$-cubes:

Lemma A.5 (Preserving $k+1$-cubes suffice)**.** *Let X be a nilspace, Y be a k-step nilspace for some $k \geq 0$, and let $\phi \colon X \to Y$ be a map that preserves $k+1$-cubes. Then ϕ is a a nilspace morphism.*

Proof. From the composition axiom (i) one easily verifies that if ϕ preserves $k+1$-cubes, then it also preserves n-cubes for any $n \leq k+1$. In the opposite direction, if ϕ preserves $k+1$-cubes and $n > k+1$, then ϕ maps an n-cube to a tuple $(y_\omega)_{\omega\in\{0,1\}^n}$ with the property that every $k+1$-dimensional face of this tuple is a $k+1$-cube. Using the completion axiom (and the fact that Y is k'-step for every $k' \geq k$) one easily then verifies by induction that every n'-dimensional face of this tuple is a n'-cube for $k+1 \leq n' \leq n$; setting $n' = n$ gives the claim. □

If $F \colon X \to Z$ is a map from a nilspace X to an abelian group $Z = (Z, +)$, we can define the *derivative* $dF \colon C^1(X) \to Z$ on the nilspace $C^1(X)$ by the formula

$$dF(a, b) := F(b) - F(a).$$

We can iterate this construction using Remark A.3 to define higher derivatives[5] $d^kF \colon C^k(X) \to Z$ for any $k \geq 0$, with the convention $d^0F = F$.

[5] In particular, we caution that d does *not* form a chain complex and should *not* be interpreted as an exterior derivative: $d^2 \neq 0$.

Explicitly, we have

$$d^k F((x_\omega)_{\omega\in\{0,1\}^k}) = \sum_{\omega\in\{0,1\}^k} (-1)^{k-|\omega|} F(x_\omega).$$

Now we give a construction for extending a nilspace by a cocycle.

Definition A.6 (Cocycles on nilspaces)**.** [3, Definitions 3.3.14, 3.3.18] Let X be a nilspace, Z be an abelian group, and $k \geq 0$. A *cocycle of degree k on X taking values in Z* is a function $\rho\colon C^{k+1}(X) \to Z$ obeying the following axioms:

(i) (Symmetry) If $(x_\omega)_{\omega\in\{0,1\}^{k+1}} \in C^{k+1}(X)$ is a $k+1$-cube in X, and $\sigma\colon \{0,1\}^{k+1} \to \{0,1\}^{k+1}$ is any map formed by permuting the $k+1$ coordinates, then

$$\rho((x_{\sigma(\omega)})_{\omega\in\{0,1\}^{k+1}}) = \rho((x_\omega)_{\omega\in\{0,1\}^{k+1}}).$$

(ii) (Cocycle) If $x, y, z \in C^k(X)$ are k-cubes with $(x, y), (y, z) \in C^1(C^k(X)) \equiv C^{k+1}(X)$ are $k+1$-cubes (which implies that (x, z) is also a $k+1$-cube, thanks to Remark A.3), then

$$\rho(x, z) = \rho(x, y) + \rho(y, z).$$

We say that $\rho\colon C^{k+1}(X) \to Z$ is a *coboundary of degree k on X taking values in Z* if we have $\rho = d^{k+1}F$ for some $F\colon X \to Z$.

Example A.7. A degree 1 cocycle is a map $\rho\colon C^2(X) \to Z$ obeying the symmetry axiom

$$\rho(x_{00}, x_{01}, x_{10}, x_{11}) = \rho(x_{00}, x_{10}, x_{01}, x_{11})$$

for all $(x_{00}, x_{01}, x_{10}, x_{11}) \in C^2(X)$, and the cocycle axiom

$$\rho(x_0, x_1, z_0, z_1) = \rho(x_0, x_1, y_0, y_1) + \rho(y_0, y_1, z_0, z_1)$$

whenever $(x_0, x_1, y_0, y_1), (y_0, y_1, z_0, z_1) \in C^2(X)$. A degree 1 coboundary is a map $\rho\colon C^2(X) \to Z$ of the form

$$\rho(x_{00}, x_{01}, x_{10}, x_{11}) = F(x_{00}) - F(x_{01}) - F(x_{10}) + F(x_{11})$$

for all $(x_{00}, x_{01}, x_{10}, x_{11}) \in C^2(X)$.

It is easy to see that every coboundary of degree k is a cocycle of degree k; indeed, the collection of coboundaries of degree k forms a subgroup of the abelian group of cocycles of degree k. However, it will be crucial for our main results that the converse is not always true, so that nilspaces can have non-trivial "degree k cohomology".

Remark A.8. Axiom (ii) and the nilspace axioms imply that $\rho(x, x) = 0$ for all $x \in C^k(X)$, and that $\rho(x, y) = -\rho(y, x)$ for all $(x, y) \in C^{k+1}(X)$. As a consequence, the symmetry axiom (i) is equivalent to the stronger axiom

$$\rho((x_{\theta(\omega)})_{\omega\in\{0,1\}^{k+1}}) = (-1)^{r(\theta)}\rho((x_\omega)_{\omega\in\{0,1\}^{k+1}})$$

whenever $\theta\colon \{0, 1\}^{k+1} \to \{0, 1\}^{k+1}$ is a cube morphism and $r(\theta)$ is the number of 1s in $\theta(0^{k+1})$ (informally, $r(\theta)$ is the number of face reflections needed to generate θ). This alternate formulation of axiom (i) is the one used in [3, Definition 3.3.14].

Now we introduce a key construction.

Proposition A.9 (Skew products)**.** *Let $k \geq 0$, let X be a k-step nilspace, and let $\rho\colon C^{k+1}(X) \to Z$ be a cocycle of degree k on X taking values in an abelian group Z. Then we can define a nilspace $X \rtimes^{(k)}_\rho Z$ to be the Cartesian product $X\times Z$ whose n-cubes for $n \geq 0$ consist of those tuples $((x_\omega, z_\omega))_{\omega\in\{0,1\}^n}$ for which $(x_\omega)_{\omega\in\{0,1\}^n}$ is an n-cube in X, and one has the equation*

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} z_{\phi(\omega)} = \rho((x_{\phi(\omega)})_{\omega\in\{0,1\}^{k+1}}) \tag{53}$$

whenever $\phi\colon \{0, 1\}^{k+1} \to \{0, 1\}^n$ is a $k + 1$-dimensional face of $\{0, 1\}^n$ (this condition is vacuous when $n < k + 1$). If X is k-step, then so is $X \rtimes^{(k)}_\rho Z$.

Finally, every n-cube $(x_\omega)_{\omega\in\{0,1\}^n}$ in X has at least one lift $((x_\omega, z_\omega))_{\omega\in\{0,1\}^n}$ to an n-cube in $X \rtimes^{(k)}_\rho Z$.

Proof. The claim that $X \rtimes^{(k)}_\rho Z$ is a nilspace is [3, Proposition 3.3.26] (with slightly different notation). The conclusion about the k-step nature of $X\rtimes^{(k)}_\rho Z$ follows from the k-step nature of X and the equation (53) applied to the identity face $\phi\colon \{0, 1\}^{k+1} \to \{0, 1\}^{k+1}$, which constrains the final component $z_{1^{k+1}}$ of the z_ω in terms of the other components z_ω and the base $k + 1$-cube $(x_\omega)_{\omega\in\{0,1\}^{k+1}}$.

To prove the final claim, we set $z_\omega := 0$ for $|\omega| < k + 1$, and whenever $|\omega| = k + 1$ we set

$$z_\omega := \rho((x_{\phi_\omega(\alpha)})_{\alpha\in\{0,1\}^{k+1}})$$

where $\phi_\omega \colon \{0,1\}^{k+1} \to \{0,1\}^n$ is the unique face map that sends 1^{k+1} to ω. The tuple $((x_\omega, z_\omega))_{|\omega| \leq k+1}$ then is an n'-cube on $X \rtimes_\rho^{(k)} Z$ when restricted to any n'-face in $\{\omega \in \{0,1\}^n : |\omega| \leq k+1\}$ with $n' \leq k+1$. By multiple applications of the completion axiom on the k-step nilspace $X \rtimes_\rho^{(k)} Z$ (or by [3, Lemma 3.1.5]), we may (uniquely) complete this tuple to an n-cube $((x_\omega, z_\omega))_{\omega \in \{0,1\}^n}$ on $X \rtimes_\rho^{(k)} Z$, whose first coordinates x_ω must agree with the original n-cube $(x_\omega)_{\omega \in \{0,1\}^n}$ on X since X is k-step. This gives the claim. □

We refer to $X \rtimes_\rho^{(k)} Z$ as the *degree k skew product* of the nilspace X and the abelian group Z by the cocycle ρ. The map $\pi \colon X \rtimes_\rho^{(k)} Z \to X$ defined by $\pi(x,z) := x$ will be called the *factor map*; it is immediate that this is a nilspace morphism.

Example A.10. If Z is an abelian group, then the k-step nilspace $\mathcal{D}^k(Z)$ (defined in the next section) can be thought of as the skew product $\mathrm{pt} \rtimes_0^{(k)} Z$ of a point pt and Z by the zero cocycle 0.

Example A.11. If $\rho = d^{k+1}F$ is a coboundary of degree k, then the skew product $X \rtimes_\rho^{(k)} Z$ is isomorphic as a nilspace to the product nilspace $X \times \mathcal{D}^k(Z) = X \rtimes_0 Z$, with the isomorphism defined by mapping (x,z) to $(x, z - F(x))$. More generally, adding or subtracting a degree k coboundary from a cocycle does not affect the skew product up to nilspace isomorphism.

Remark A.12. In [3, Definition 3.3.13], a more abstract notion of a degree k extension of a nilspace X is defined, and it is shown in [3, Lemma 3.3.21] that any such extension can be written as a degree k skew product $X \rtimes_\rho^{(k)} Z$ for some degree k cocycle after specifying a section of the extension; the degree k coboundaries correspond to those extensions which are *split*. It is also shown in [3, Theorem 3.2.19, Lemma 3.3.28] that an ergodic k-step nilspace can be expressed as a tower

$$\mathrm{pt} \rtimes_{\rho_1}^{(1)} Z_1 \rtimes_{\rho_2}^{(2)} Z_2 \cdots \rtimes_{\rho_k}^{(k)} Z_k$$

of k successive skew products with abelian groups $Z_1, \dots, Z_k$ (where we apply the skew product construction from left to right). However, we will not need these results here.

A.2. **Filtered abelian groups.** The nilspaces that we shall consider in this paper shall be constructed out of filtered abelian[6] groups, and their extension by cocycles. We first review the definition of a filtered abelian group.

Definition A.13 (Filtered abelian group)**.** (see e.g., [12, §6]) A *filtered abelian group* $G = (G, (G_i)_{i\geq 0})$ is an abelian group $G = (G, +)$ (which we will usually think of as being discrete), equipped with a filtration

$$G = G_0 \geq G_1 \geq G_2 \geq \dots$$

of subgroups G_i. If $G_1 = G_0 = G$, we say that the filtered abelian group is *ergodic*.

A *filtered homomorphism* from one filtered group $G = (G, (G_i)_{i\geq 0})$ to another $H = (H, (H_i)_{i\geq 0})$ is a group homomorphism $\phi \colon G \to H$ such that $\phi(G_i) \leq H_i$ for all $i \geq 0$.

If G is a filtered group and $k \geq 0$, we define the k^{th} *Host–Kra group* $G^{[k]} \leq G^{\{0,1\}^k}$ of G to be the filtered abelian group of tuples of the form

$$(\sum_{\alpha\in\{0,1\}^k} h_\alpha \prod_{i:\alpha_i=1} \omega_i)_{\omega\in\{0,1\}^k} \tag{54}$$

where $h_\alpha \in G_{|\alpha|}$ for all $\alpha \in \{0,1\}^k$, where $|\alpha| := \alpha_1 + \dots + \alpha_n$, and with the subgroup $(G^{[k]})_i$ of the filtered abelian group $G^{[k]}$ defined to be the group of tuples of the form (54) with $h_\alpha \in G_{|\alpha|+i}$ for all $A \in \{0,1\}^k$. One can easily verify that $G^{[k]}$ is also a filtered abelian group.

If $G_i = \{0\}$ for $i > d$, we say that the filtered group G is *of degree at most d*. An abelian group G is given the *degree d filtration* for some $d \geq 0$ if $G_i = G$ for $i \leq d$ and $G_i = \{0\}$ for $i > d$, in which case we denote the associated filtered abelian group as $\mathcal{D}^d(G)$ (cf. [3, Definition 2.2.30]).

Example A.14. After some routine relabeling, we have

$$G^{[0]} = G = \{x : x \in G\},$$

$$G^{[1]} = \{(x, x + h_1) : x \in G; h_1 \in G_1\} \tag{55}$$

and

$$G^{[2]} = \{(x, x+h_1, x+h_2, x+h_1+h_2+h_{12}) : x \in G; h_1, h_2 \in G_1; h_{12} \in G_2\} \tag{56}$$

[6] One can also build nilspace structures out of non-abelian filtered groups, and in particular out of nilpotent abelian groups; see for instance [3, §2.2]. However, we will not need these more general nilspaces.

and

$$\begin{aligned} G^{[3]} =&\{(x, x+h_1, x+h_2, x+h_3, x+h_1+h_2+h_{12}, x+h_1+h_3+h_{23}, \\ &x+h_2+h_3+h_{13}, x+h_1+h_2+h_3+h_{12}+h_{13}+h_{23}+h_{123}) : \\ &x \in G; h_1, h_2, h_3 \in G_1; h_{12}, h_{13}, h_{23} \in G_2; h_{123} \in G_3\}. \end{aligned} \tag{57}$$

In the case when G has the degree 1 filtration $\mathcal{D}^1(G)$, one can omit the $h_{12}, h_{13}, h_{23}, h_{123}$ terms in the above formulae.

From the construction one has a canonical identification

$$(G^{[d]})^{[n]} \equiv G^{[d+n]} \tag{58}$$

of filtered abelian groups for any $d, n \geq 0$ defined by

$$(g_\omega)_{\omega\in\{0,1\}^{d+n}} \equiv ((g_{(\omega,\omega')})_{\omega\in\{0,1\}^d})_{\omega'\in\{0,1\}^n}$$

for all $(g_\omega)_{\omega\in\{0,1\}^{d+n}} \in G^{[d+n]}$; compare with (52).

Every filtered abelian group can be viewed as a nilspace.

Lemma A.15 (Filtered groups are nilspaces)**.** *If $G = (G, (G_i)_{i\geq 0})$ is a filtered abelian group, then G can be given the structure of a nilspace by setting $C^n(G) := G^{[n]}$. This will be an ergodic nilspace if and only if G is ergodic. If $k \geq 0$, then G is of degree at most k as a filtered abelian group if and only if it is a k-step nilspace.*

Proof. See [3, Proposition 2.2.8] (which in fact proves this result even in the non-abelian case). The proof in [3] is written only in the ergodic case, but an inspection of the arguments reveals that it also holds in the non-ergodic setting. □

Remark A.16. If G is a filtered abelian group, then we may potentially have defined two nilspace structures on $G^{[k]}$; one arising from applying the above lemma to the filtered abelian group $G^{[k]}$, and the other by applying the above lemma to G and then using the nilspace structure on n-cubes $C^n(G)$ from Remark A.3. However, it is easy to see that these two nilspace structures coincide.

In view of the above lemma, we can now define nilspace morphisms between filtered abelian groups. As it turns out, these nilspace morphisms have a nice characterisation in terms of difference operators. If G, H are (filtered) abelian groups and $h \in G$ is a shift, we define the shift operator T^h and the difference operator ∂_h on functions $f\colon G \to H$ by the formula

$$T^h f(x) := f(x+h)$$

and

$$\partial_h f(x) := f(x+h) - f(x),$$

thus $\partial_h = T^h - 1$. Clearly these operators commute with each other, with $h \mapsto T^h$ being an action of G; we also note the cocycle identity

$$\partial_{h+k} = \partial_h + T^h \partial_k \tag{59}$$

for any $h, k \in G$.

Lemma A.17 (Characterization of nilspace morphisms)**.** *Let $f\colon G \to H$ be a map from one filtered abelian group $G = (G, (G_i)_{i \geq 0})$ to another $H = (H, (H_i)_{i \geq 0})$. Then f is a nilspace morphism if and only if*

$$\partial_{h_1} \dots \partial_{h_l} f(x) \in H_{i_1 + \dots + i_l}$$

for all $l \geq 0$, $i_1, \dots, i_l \geq 0$, $x \in G$, and $h_j \in G_{i_j}$ for $j = 1, \dots, l$. In fact, it suffices to check this condition for $h_j \in E_{i_j}$, where for each i, E_i is a set of generators for G_i.

Proof. See [13, Theorem B.3, Proposition B.8] or [3, Theorem 2.2.14] (the latter statement is written in the ergodic case, but the proof extends without difficulty to the non-ergodic setting). □

As one corollary of this lemma, we see that the space $\mathrm{Hom}_\square(G \to H)$ of nilspace morphisms from one filtered abelian group G to another H is an abelian group, which contains the space of filtered homomorphisms from G to H as a subgroup. In fact $\mathrm{Hom}_\square(G \to H)$ naturally has the structure of a filtered abelian group, in a manner consistent with the nilspace structure on $\mathrm{Hom}_\square(G \to H)$ already constructed in Remark A.3: see [13, Proposition B.6]. The translation operators $x \mapsto x + h$ on G are also nilspace morphisms for any $h \in H$.

A.3. **Polynomials.** We now define the notion of a polynomial:

Definition A.18 (Polynomials)**.** If X is nilspace, H is an abelian group, and $d \geq 0$, a *polynomial of degree at most d* from X to H is a nilspace morphism from X to $\mathcal{D}^d(H)$. When X is a filtered abelian group G, we can equivalently define a polynomial by requiring that

$$\partial_{h_1} \dots \partial_{h_l} P = 0$$

whenever $i_1, \dots, i_l \geq 0$ are such that $i_1 + \dots + i_l > d$, and $h_j \in G_{i_j}$ for $j = 1, \dots, l$; see [3, Theorem 2.2.14] for a proof of this equivalence. The space of such polynomials will be denoted $\mathrm{Poly}^d(X \to H)$, thus

$$\mathrm{Poly}^d(X \to H) \equiv \mathrm{Hom}_\square(X \to \mathcal{D}^d(H)).$$

In particular, $\mathrm{Poly}^d(X \to H)$ is an abelian group, and when X is a filtered abelian group it acquires a translation action $h \mapsto T^h$ of G. If $H = \mathbb{T}$, we abbreviate $\mathrm{Poly}^d(X \to \mathbb{T})$ as $\mathrm{Poly}^d(X)$, and refer to elements of $\mathrm{Poly}^d(X)$ as *non-classical polynomials of degree at most d* on X. By convention, we set $\mathrm{Poly}^d(X \to H) = \{0\}$ for $d < 0$. For an abelian group G, we often abbreviate $\mathrm{Poly}^d(\mathcal{D}^1(G) \to H)$ as $\mathrm{Poly}^d(G \to H)$ (and $\mathrm{Poly}^d(\mathcal{D}^1(G))$ as $\mathrm{Poly}^d(G)$).

From the definitions we see that we can define polynomials recursively on filtered abelian groups G: a map $P\colon G \to H$ lies in $\mathrm{Poly}^d(G \to H)$ if and only if $\partial_h P \in \mathrm{Poly}^{d-i}(G \to H)$ for all $i \geq 1$ and $h \in G_i$. We remark that *classical polynomials* correspond to the case when H is a field $\mathbb{F}$, and G is a vector space over that field (equipped with the degree 1 filtration).

Remark A.19. The space of polynomials $\mathrm{Poly}^d(G)$ in a filtered abelian group G is sensitive to the filtration structure on G. For instance, the function $P\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{T}$ defined by $P(x) := x/2$ is a polynomial of degree 1 if $\mathbb{Z}/2\mathbb{Z}$ is given the degree 1 filtration $\mathcal{D}^1(\mathbb{Z}/2\mathbb{Z})$, but is a polynomial of degree 2 if $\mathbb{Z}/2\mathbb{Z}$ is instead given the degree 2 filtration $\mathcal{D}^2(\mathbb{Z}/2\mathbb{Z})$. Informally, the difference operator ∂_1 is a first-order operator in the former case, but a second-order operator in the latter case.

If $P\colon G \to H$ is a map from a filtered abelian group G to an abelian group H, recall from Section A.1 that we can define derivatives $d^k P\colon G^{[k]} \to H$ for any $k \geq 0$. By expanding all the definitions, we obtain a familiar-looking relationship between polynomials and derivatives:

Proposition A.20 (Polynomials and derivatives)**.** *Let $P\colon G \to H$ be a map from a filtered abelian group G to an abelian group H. If $k \geq -1$, then P is* *a polynomial of degree at most k if and only if $d^{k+1}P = 0$. In particular, for $k \geq 0$, we see that P is a polynomial of degree at most k if and only if dP is a polynomial of degree at most $k-1$.*

As one application of this proposition, we have the following familiar-looking result about multiplication of polynomials (cf. [21, Exercise 1.6.10]):

Lemma A.21 (Products of polynomials)**.** *Let G be a filtered abelian group, and let R be a ring. If $P_1 \colon G \to R$, $P_2 \colon G \to R$ are polynomials of degree at most d_1, d_2 respectively, then $P_1P_2 \colon G \to R$ is a polynomial of degree at most $d_1 + d_2$.*

Proof. Observe the Leibniz rule

$$\partial_h(P_1P_2) = (\partial_h P_1)P_2 + (T^h P_1)\partial_h P_2 = (\partial_h P_1)P_2 + P_1\partial_h P_2 + (\partial_h P_1)\partial_h P_2 \tag{60}$$

for any $h \in G$. The claim now follows by induction on the combined degree $d_1 + d_2$. □

If G is a filtered abelian group which is also an elementary abelian 2-group, then by (4) we have $2\partial_h = -\partial_h^2$ for any $h \in G$. When combined with Proposition A.20, this gives

Proposition A.22 (Doubling lowers degree in 2-groups)**.** *Let G be a filtered abelian group that is also an elementary abelian 2-group, and let H be an abelian group. If $P \in \mathrm{Poly}^k(G \to H)$ for some $k \geq 1$, then $2P \in \mathrm{Poly}^{k-1}(G \to H)$.*

In fact this property holds in the larger class of 2-homogeneous filtered abelian groups, but we will not need to establish this fact here.

In the case of non-classical polynomials on a finite-dimensional vector space $\mathbb{F}_2^n$ over the field of two elements, we have an explicit description of such polynomials:

Lemma A.23 (Explicit description of polynomials)**.** *Let $n \geq 0$ and $d \geq 0$. Then a function $P \colon \mathbb{F}_2^n \to \mathbb{T}$ is of degree at most d if and only if it takes the form*

$$P(x_1, \dots, x_n) = \alpha + \sum_{k=1}^{d} \sum_{1 \leq i_1 < \dots < i_k \leq n} \frac{c_{i_1,\dots,i_k}|x_{i_1}| \dots |x_{i_k}|}{2^{d+1-k}} \mod 1$$

for all $x_1, \dots, x_n \in \mathbb{F}_2$ *and some* $0 \leq \alpha < 1$ *and some integers* $0 \leq c_{i_1,\dots,i_k} < 2^{d+1-k}$*, where* $|x| := 1_{x=1}$*. The coefficients* α *and* $c_{i_1,\dots,i_k}$ *are uniquely determined. Indeed we have*

$$\alpha = P(0) \mod 1$$

and

$$\frac{c_{i_1,\dots,i_k}}{2^{d+1-k}} = \partial_{i_1} \dots \partial_{i_k} P(0) \mod 1.$$

Proof. This follows from [23, Lemma 1.7(iii)], with the latter identities following from a routine calculation. There is an analogous classification of polynomials in other characteristics than 2, but we will only need the characteristic two theory here. □

One quick corollary of this lemma is the *exact roots property*

$$\mathrm{Poly}^d(\mathbb{F}_2^n) = 2 \cdot \mathrm{Poly}^{d+1}(\mathbb{F}_2^n) \tag{61}$$

for all $d \geq 0$, refining Proposition A.22 in this case; thus, every polynomial P of degree d can be expressed in the form $P = 2Q$ for some polynomial Q of degree $d + 1$, and conversely if Q is of degree $d + 1$ then $2Q$ is of degree d; see [23, Lemma 1.7(v)]. In a similar spirit, we have

Lemma A.24 (Inverting $1 + T^e$)**.** *Let* $n \geq 1$*, let* e *be a non-zero vector in* $\mathbb{F}_2^n$*, let* $d \in \mathbb{Z}$*, and let* $P \colon \mathbb{F}_2^n \to \mathbb{T}$ *be a a polynomial of degree at most* d *with* $\partial_e P = 0$*. Then one can write* $P = (1 + T^e)Q$ *where* $Q \colon \mathbb{F}_2^n \to \mathbb{T}$ *is a polynomial of degree at most* $d + 1$*.*

Proof. If $d < 0$ then P vanishes and we can simply take $Q = 0$. Hence we may assume $d \geq 0$. Applying a change of variables we may assume $e = e_n$ is the final generator of $\mathbb{F}_2^n$. By [23, Lemma 1.7(iii)] we can write the e_n-invariant polynomial P explicitly as

$$P(x_1, \dots, x_n) = \alpha + \sum_{k=1}^{d} \sum_{1 \leq i_1 < \dots < i_k \leq n-1} \frac{c_{i_1,\dots,i_k} |x_{i_1}| \dots |x_{i_k}|}{2^{d+1-k}} \mod 1$$

for all $x_1, \dots, x_n \in \mathbb{F}_2$ and some $0 \leq \alpha < 1$ and some integers $0 \leq c_{i_1,\dots,i_k} < 2^{d+1-k}$, where $|x| = 1_{x=1}$. We then define $Q(x_1, \dots, x_n)$ explicitly by the formula

$$Q(x_1, \dots, x_n) = \frac{\alpha}{2} + \sum_{k=1}^{d} \sum_{1 \leq i_1 < \dots < i_k \leq n-1} \frac{c_{i_1,\dots,i_k} |x_{i_1}| \dots |x_{i_k}| |x_n|}{2^{d+1-k}} \mod 1.$$

From [23, Lemma 1.7(iii)] again, Q is a polynomial of degree at most $d+1$, and the identity $P = (1 + T^e)Q$ follows from direct calculation. □

We will use the following stability property for polynomials on nilspaces, which we phrase in the setting of finite nilspaces as this is all we will need here.

Theorem A.25 (Stability of polynomials)**.** *For every $k \geq 0$ and $\varepsilon > 0$ there exists $\delta > 0$ such that if X is a finite ergodic nilspace, and $\phi\colon X \to \mathbb{T}$ is a function such that*

$$\left| e\left(\sum_{\omega \in \{0,1\}^{k+1}} (-1)^{k+1-|\omega|} \phi(x_\omega) \right) - 1 \right| \leq \delta$$

for at least $1 - \delta$ of the $k+1$-cubes $(x_\omega)_{\omega \in \{0,1\}^{k+1}}$ in X, then there exists a polynomial $P \in \mathrm{Poly}^k(X)$ such that

$$\mathbb{E}_{x \in X} |e(\phi(x)) - e(P(x))| \leq \varepsilon.$$

Proof. This is a special case of [5, Theorem 4.2] (with Y the compact nilspace $\mathcal{D}^k(\mathbb{T})$ with metric $d(x, y) := |e(x) - e(y)|$), noting that for a finite ergodic nilspace we can use the uniform probability measure on $C^n(X)$ as a Haar measure on that space. □

A.4. ***p*-homogeneous nilspaces.** The following definition was introduced in [4]:

Definition A.26 (p-homogeneity)**.** [4, Definitions 1.2, 3.1] Let p be a prime. A nilspace X is said to be *p-homogeneous* if, whenever $n \geq 0$ and $f\colon \mathcal{D}^1(\mathbb{Z}^n) \to X$ is a nilspace morphism, then the periodization $\tilde{f}\colon \mathcal{D}^1(\mathbb{F}_p^n) \to X$, defined by restricting f to $\{0, \dots, p-1\}^n$ and then extending periodically, is also a nilspace morphism.

A nilspace X is said to be *weakly p-homogeneous* if, for every n-cube $(x_\omega)_{\omega \in \{0,1\}^n} \in C^n(X)$ for some $n \geq 0$, there exists a nilspace morphism $\tilde{f}\colon \mathcal{D}^1(\mathbb{F}_p^n) \to X$ such that $\tilde{f}(\omega) = x_\omega$ for all $\omega \in \{0,1\}^n$ (viewing $\{0,1\}^n$ as a subset of $\mathbb{F}_p^n$).

In [4, Remark 3.3] it is noted that p-homogeneity implies weak p-homogeneity, and that the two concepts are equivalent when $p = 2$. In [4, Question 3.4] it is posed as an open question whether these two concepts are equivalent for

$p > 2$; we do not address this question here. From this remark, we see that X is 2-homogeneous (or equivalently, weakly 2-homogeneous), if and only if we have a bijection

$$C^n(X) \equiv \mathrm{Hom}_{\square}(\mathcal{D}^1(\mathbb{F}_2^n) \to X) \tag{62}$$

for any $n \geq 0$, where we identify maps from $\mathbb{F}_2^n$ to X with tuples in $X^{\{0,1\}^n}$ by identifying $\{0,1\}^n$ with $\mathbb{F}_2^n$. From this identification we obtain the following consequence:

Lemma A.27 (Preserving 2-homogeneity)**.** *Let $k \geq 0$, let X be a 2-homogeneous k-step nilspace, and let $X \rtimes_\rho^{(k)} Z$ be a degree k skew product of that nilspace with an elementary abelian 2-group Z. Then $X \rtimes_\rho^{(k)} Z$ is 2-homogeneous if and only if, for any $n \geq 0$, every nilspace morphism $\phi\colon \mathcal{D}^1(\mathbb{F}_2^n) \to X$ has a lift $\tilde{\phi}\colon \mathcal{D}^1(\mathbb{F}_2^n) \to X \rtimes_\rho^{(k)} Z$, thus $\tilde{\phi}$ is a nilspace morphism with $\phi = \pi \circ \tilde{\phi}$, where $\pi\colon X \rtimes_\rho^{(k)} Z \to X$ is the factor map.*

Remark A.28. There is an analogue of this result for general p, but it is more difficult to prove; see [4, Proposition 3.12].

Proof. We first prove the "only if" direction. Suppose that $X \rtimes_\rho^{(k)} Z$ is 2-homogeneous, and $\phi\colon \mathcal{D}^1(\mathbb{F}_2^n) \to X$ is a nilspace morphism. By (62) for the 2-homogeneous nilspace X, we may view ϕ as an n-cube on X, which has a lift to an n-cube on $X \rtimes_\rho^{(k)} Z$ by Proposition A.9. Applying (62) again to the 2-homogeneous nilspace $X \rtimes_\rho^{(k)} Z$, we obtain the claim.

Now we prove the "if" direction. Let $n \geq 0$, and let $((x_\omega, z_\omega))_{\omega\in\{0,1\}^n} \in C^n(X \rtimes_\rho^{(k)} Z)$ be an n-cube in $X \rtimes_\rho^{(k)} Z$. We would like to interpret this n-cube as a nilspace morphism from $\mathbb{F}_2^n$ to $X \rtimes_\rho^{(k)} Z$. As X is already 2-homogeneous, we know that the n-cube $(x_\omega)_{\omega\in\{0,1\}^n}$ can already be identified with a nilspace morphism ϕ from $\mathbb{F}_2^n$ to X, which by hypothesis can be lifted to a nilspace morphism $\tilde{\phi}$ from $\mathbb{F}_2^n$ to $X \rtimes_\rho^{(k)} Z$. In particular, we can write

$$\tilde{\phi}(\omega) = (x_\omega, z_\omega + P(\omega)) \tag{63}$$

for all $\omega \in \{0,1\}^n$ and some map $P\colon \mathbb{F}_2^n \to Z$ (identifying $\{0,1\}^n$ with $\mathbb{F}_2^n$).

Since $((x_\omega, z_\omega))_{\omega\in\{0,1\}^n} \in C^n(X \rtimes_\rho^{(k)} Z)$ is an n-cube, we have from (53) that

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} z_{\iota(\omega)} = \rho((x_{\iota(\omega)})_{\omega\in\{0,1\}^{k+1}})$$

whenever $\iota\colon \{0,1\}^{k+1} \to \{0,1\}^n$ is a $k+1$-dimensional face of $\{0,1\}^n$. As $(\tilde{\phi}(\omega))_{\omega\in\{0,1\}^n}$ is also an n-cube, the same statement is true with z_ω replaced by $z_\omega + P(\omega)$. Subtracting, we conclude that

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} P(\iota(\omega)) = 0$$

for all $k+1$-dimensional faces. Equivalently, we have

$$\partial_{e_{i_1}} \dots \partial_{e_{i_{k+1}}} P = 0$$

whenever $1 \leq i_1 < \dots < i_{k+1} \leq n$, where $e_1, \dots, e_n$ is the standard basis of $\mathbb{F}_2^n$. For any $i = 1, \dots, n$, we have

$$\partial_{e_i}\partial_{e_i} = \partial_{2e_i} - 2\partial_{e_i} = -2\partial_{e_i}$$

since $2e_i = 0$ (cf. (4)); since Z is assumed to be an elementary abelian 2-group, we thus also have

$$\partial_{e_{i_1}} \dots \partial_{e_{i_{k+1}}} P = 0$$

whenever two of the $i_1, \dots, i_{k+1}$ are equal. We conclude that $P \in \mathrm{Poly}^k(\mathbb{F}_2^n \to Z)$.

Now let $(a_\omega)_{\omega\in\{0,1\}^{k+1}} \in C^{k+1}(\mathcal{D}^1(\mathbb{F}_2^n))$ be a $k+1$-cube in $\mathbb{F}_2^n$ (with the degree 1 filtration). As $\tilde{\phi}$ is a nilspace morphism, $(\tilde{\phi}(a_\omega))_{\omega\in\{0,1\}^{k+1}}$ is a $k+1$-cube in $X \rtimes_\rho^{(k)} Z$, which in particular implies from (63) that

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} (z_{a_\omega} + P(a_\omega)) = \rho((x_{a_\omega})_{\omega\in\{0,1\}^{k+1}}).$$

Since P is a polynomial, we also have

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} P(a_\omega) = 0;$$

subtracting, we conclude that

$$\sum_{\omega\in\{0,1\}^{k+1}} (-1)^{k+1-|\omega|} z_{a_\omega} = \rho((x_{a_\omega})_{\omega\in\{0,1\}^{k+1}}).$$

As a consequence, we see that $(x_{a_\omega}, z_{a_\omega})_{\omega\in\{0,1\}^{k+1}}$ is a $k+1$-cube in $X \rtimes_\rho^{(k)} Z$. Thus the map $a \mapsto (x_a, z_a)$ preserves $k+1$-cubes, and is thus a nilspace morphism from $\mathcal{D}^1(\mathbb{F}_2^n)$ to $X \rtimes_\rho^{(k)} Z$ thanks to Lemma A.5. This gives the claim. □

Finally, we remark that the notion of p-homogeneity greatly simplifies in the case of ergodic filtered abelian groups:

Proposition A.29 (p-homogeneous filtered abelian groups)**.** *Let G be a filtered ergodic abelian group, and p a prime. Then G is p-homogeneous if and only if $p \cdot G_i \leq G_{i+1}$ for all $i \geq 1$.*

Proof. See [4, Theorem 1.4]. In fact the ergodicity hypothesis can be dropped here, but we will not need to use this fact. □

Appendix B. Deducing the strong inverse conjecture from the BTZ conjecture

We now prove Theorem 1.5, by refining the correspondence principle argument used in [23]. Our arguments here follow [23] fairly closely, and familiarity with that argument will be assumed here.

Fix $p, k, \eta, \varepsilon()$; all quantities below are permitted to depend on these parameters. Suppose for contradiction that Conjecture 1.2 was true, but Conjecture 1.3 failed for the indicated choice of $\eta, \varepsilon()$. Without loss of generality we may assume $\varepsilon(m) \leq \frac{1}{m}$ (for instance). Then for every M, there exists $G = \mathbb{F}_p^n$ for some $n = n_M$ and a function $f = f_M \colon G \to \mathcal{D}$ with $\|f\|_{U^{k+1}(G)} \geq \eta$, such that if $h_1, \ldots, h_M \in G$ are chosen independently and uniformly at random, then with probability greater than $1/2$, there does *not* exist $1 \leq m \leq M$ and $P \in \mathrm{Poly}^k(G)$ and a function $F \colon \mathbb{C}^{\mathbb{F}_p^M} \to \mathbb{C}$ of Lipschitz constant at most M, such that

$$|\mathbb{E}_{x \in G} f(x) e(-P(x))| \geq \frac{1}{m}$$

and

$$|\mathbb{E}_{x \in G} e(P(x)) - F((f(x + \sum_{i=1}^{M} a_i h_i))_{(a_1, \ldots, a_M) \in \mathbb{F}_p^M})| \leq \varepsilon(m).$$

We use the following construction of a *sampling sequence* from [23]:

Proposition B.1 (Existence of accurate sampling sequence)**.** *Let $\varepsilon_0 > 0$. Then there exists a sequence of scales*

$$0 = H_0 < H_1 < \ldots$$

such that for any $G = \mathbb{F}_p^n$ and $f \colon G \to \mathcal{D}$, if $v_1, v_2, v_3, \cdots \in G$ are chosen uniformly and independently at random, then with probability at least $1 - \varepsilon_0$, the following "accurate sampling" statement holds: for every sequence

$$0 \leq r_0 < r_1 < r_2 < \cdots < r_{k+1}$$

and every Lipschitz $F\colon \mathcal{D}^{\{0,1\}^{k+1}\times\mathbb{F}_p^{r_0}} \to \mathbb{C}$*, we have*

$$\mathbb{E}_{x\in G}|F_{f,r_0,\dots,r_{k+1}}(x) - F_f(x)| \leq \frac{\|F\|_{\mathrm{Lip}}}{r_1}$$

where

$$F_{f,r_0,\dots,r_{k+1}}(x) := \mathbb{E}_{\vec{a}_1\in\mathbb{F}_p^{H_{r_1}},\dots,\vec{a}_{k+1}\in\mathbb{F}_p^{H_{r_{k+1}}}} F((f(x+\omega\cdot\mathbf{u}+\vec{b}\cdot\vec{v}_0))_{\omega\in\{0,1\}^{k+1},\vec{b}\in\mathbb{F}_p^{H_{r_0}}})$$

with

$$\mathbf{u} := (\vec{a}_1\cdot\vec{v}_1,\dots,\vec{a}_{k+1}\cdot\vec{v}_{k+1});\quad \vec{v}_j := (v_1,\dots,v_{H_{r_j}}),\ j=0,\dots,k+1$$

and

$$F_{f,r_0}(x) := \mathbb{E}_{h_1,\dots,h_{k+1}\in G}F((f(x+\omega\cdot\mathbf{h}+\vec{b}\cdot\vec{v}_0))_{\omega\in\{0,1\}^{k+1},\vec{b}\in\mathbb{F}_p^{H_{r_0}}})$$

where $\mathbf{h} := (h_1,\dots,h_{k+1})$*.*

Proof. See [1, Proposition 3.13] (with some mild relabeling, for instance replacing k by $k+1$). In that proposition the sampling property was only asserted to hold with positive probability, but an inspection of the proof shows that it can be established with probability at least $1-\varepsilon_0$ for any fixed $\varepsilon_0 > 0$. □

For each M, we apply the above proposition with $\varepsilon_0 = 1/2$, $n = n_M$, and $f = f_M$ to conclude that the claimed accurate sampling property holds for randomly chosen $v_1, v_2, \dots \in \mathbb{F}_p^n$ with probability at least $1/2$. By combining this with the construction of f_M, we conclude that there exists (deterministic) $v_i = v_{i,M} \in \mathbb{F}_p^n$ for all $i \geq 1$ with the accurate sampling property, and also the property that there does *not* exist $1 \leq m \leq M$, $P \in \mathrm{Poly}^k(G)$ and a function $F\colon \mathbb{C}^{\mathbb{F}_p^M} \to \mathbb{C}$ of Lipschitz constant at most M, such that

$$|\mathbb{E}_{x\in G}f(x)e(-P(x))| \geq \frac{1}{m}$$

and

$$|\mathbb{E}_{x\in G}e(P(x)) - F((f(x+\sum_{i=1}^M a_iv_i))_{(a_1,\dots,a_M)\in\mathbb{F}_p^M})| \leq \varepsilon(m).$$

We fix this data for each M. Following [23], we now introduce the universal Furstenberg space $X := \mathcal{D}^{\mathbb{F}_p^\omega}$ of functions $\zeta\colon \mathbb{F}_p^\omega \to \mathcal{D}$ with the product σ-algebra and shift action

$$T^h\zeta(x) := \zeta(x+h).$$

As in [23, §4], for each M, the above data generate an invariant probability measure μ_M on X by the formula

$$\mu_M := \mathbb{E}_{x\in\mathbb{F}_p^{n_M}} \delta_{\zeta_{M,x}}$$

where $\zeta_{M,x} \in X$ is given by the formula

$$\zeta_{M,x}((a_i)_{i=1}^\infty) := f_M(x + \sum_{i=1}^\infty a_i v_{i,M}).$$

By Prokhorov's theorem, we may restrict M to a subsequence and assume that μ_M converges weakly to an invariant probability measure μ. Henceforth X is understood to be endowed with μ.

Let $f_\infty \colon X \to \mathcal{D}$ be the coordinate function

$$f_\infty(\zeta) := \zeta(0).$$

As noted in [23, (4.3)], we have the identity

$$\begin{aligned}&\int_X F(T_{\vec{a}_1} f_\infty, \dots, T_{\vec{a}_l} f_\infty)\, d\mu_M \\ &\quad = \mathbb{E}_{x\in\mathbb{F}_p^{n_M}} F\left(f_M\left(x + \sum_{i=1}^\infty a_{1,i} v_{i,M}\right), \dots, f_M\left(x + \sum_{i=1}^\infty a_{l,i} v_{i,M}\right)\right)\end{aligned} \tag{64}$$

for any $l, m \geq 1$, any $\vec{a}_j = (a_{j,i})_{i=1}^\infty \in \mathbb{F}_p^\omega$ for $j = 1, \dots, l$, and any continuous function $F \colon \mathcal{D}^\ell \to \mathbb{C}$. This allows us to pass back and forth between integral expressions on X (using the measure μ_M) and combinatorial averages on $\mathbb{F}_p^{n_M}$.

In [23, Lemma 4.2], it is shown that the σ-algebra of X is generated by f_∞ and its shifts. By [23, Lemma 4.3] the identity (64) was used to show that X is an ergodic $\mathbb{F}_p^\omega$-system; from [23, Lemma 4.4] this identity was also used to show that

$$\|f_\infty\|_{U^{k+1}(X)} \geq \eta.$$

Applying the hypothesis that Conjecture 1.2 held, we can find $P \in \mathrm{Poly}^k(X)$ and some m such that

$$\left|\int_X f_\infty e(-P)\, d\mu\right| > \frac{3}{m}$$

(say). Let $c : \mathbb{R}^+ \to \mathbb{R}^+$ be a decreasing function to be chosen later (depending on k, p) such that $c(\varepsilon) \to 0$ decays to zero sufficiently rapidly as $\varepsilon \to 0$. Then, as X is generated by f_∞ and its shifts, we see that there exists a natural number M_0 and shifts $\vec{b}_1, \dots, \vec{b}_{M_0} in \mathbb{F}_p^{\omega}$, and a Lipschitz function $F\colon \mathcal{D}^{M_0} \to \mathcal{D}$ of Lipschitz constant at most M_0 such that

$$\int_X |e(P) - F(T_{\vec{b}_1} f_\infty, \dots, T_{\vec{b}_{M_0}} f_\infty)|\, d\mu < c(\varepsilon(m)) \tag{65}$$

so in particular by the triangle inequality (if c decays rapidly enough)

$$\left|\int_X f_\infty \overline{F}(T_{\vec{b}_1} f_\infty, \dots, T_{\vec{b}_{M_0}} f_\infty)\, d\mu\right| > \frac{2}{m}.$$

By vague convergence we thus have

$$\left|\int_X f_\infty \overline{F}(T_{\vec{b}_1} f_\infty, \dots, T_{\vec{b}_{M_0}} f_\infty)\, d\mu_M\right| \geq \frac{2}{m}.$$

for arbitrarily large M (in particular we can assume $M > M_0, m$). Applying (64), we conclude that

$$\left|\mathbb{E}_{x \in \mathbb{F}_p^{n_M}} f_\infty(x) \overline{F}(f_M(x + \sum_{i=1}^{\infty} b_{1,i} v_{i,M}), \dots, f_M(x + \sum_{i=1}^{\infty} b_{M_0,i} v_{i,M})\right| \geq \frac{2}{m}. \tag{66}$$

Now let r_1 be sufficiently large depending on $M_0, \vec{b}_1, \dots, \vec{b}_{M_0}$, and $c(\varepsilon(m))$, and set $r_j := r_1 + j - 1$ for $j = 2, \dots, k+1$. Using the triangle inequality as in the argument after [23, (4.5)], we conclude from (65) that

$$\mathbb{E}_{\vec{d}_1 \in \mathbb{F}_p^{Hr_1}, \dots, \vec{d}_{k+1} \in \mathbb{F}_p^{Hr_{k+1}}} \int_X |\Delta_{\vec{d}_1} \dots \Delta_{\vec{d}_{k+1}} F(T_{\vec{b}_1} f_\infty, \dots, T_{\vec{b}_{M_0}} f_\infty) - 1|\, d\mu_M \ll c(\varepsilon(m))$$

for all sufficiently large M along the indicated subsequence, where we use $X \ll Y$ to denote the estimate $X \leq CY$ for some C depending only on p, k, and we use the notation $\Delta_a f(x) := f(x+a)\overline{f(x)}$. Continuing the argument after [23, [(4.5)], we can use (64) and the accurate sampling sequence property to conclude (for r_1 large enough) that

$$\mathbb{E}_{x, h_1, \dots, h_{k+1} \in \mathbb{F}_p^{n_M}} \left|\Delta_{h_1} \dots \Delta_{h_{k+1}} F\left(f_M\left(x + \sum_{i=1}^{\infty} b_{1,i} v_{i,M}\right), \dots, f_M\left(x + \sum_{i=1}^{\infty} b_{M_0,i} v_{i,M}\right)\right) - 1\right|$$
$$\ll c(\varepsilon(m))$$

where the operators Δ_h are applied in the x variable. Applying [23, Lemma 4.5] (or [5, Theorem 4.2]), and assuming that the function c decays sufficiently rapidly, we may find a polynomial $P_M \in \mathrm{Poly}^k(\mathbb{F}_p^{n_M})$ such that

$$\mathbb{E}_{x \in \mathbb{F}_p^{n_M}} \left|F\left(f_M\left(x + \sum_{i=1}^{\infty} b_{1,i} v_{i,M}\right), \dots, f_M\left(x + \sum_{i=1}^{\infty} b_{M_0,i} v_{i,M}\right)\right) - e(P_M(x))\right| \leq \varepsilon(m)$$

From this, (66), and the triangle inequality (recalling that $\varepsilon(m) \leq 1/m$) we conclude that

$$|\mathbb{E}_{x\in\mathbb{F}_p^{n_M}} f_\infty(x)e(-P_M(x))| > \frac{1}{m}.$$

But this contradicts the construction of the sampling sequence $v_{i,M}$. This concludes the proof of Theorem 1.5.

References

[1] V. Bergelson, T. Tao, and T. Ziegler. An inverse theorem for the uniformity seminorms associated with the action of $\mathbb{F}_p^\infty$. *Geom. Funct. Anal.*, 19(6):1539–1596, 2010.

[2] O. A. Camarena and B. Szegedy. Nilspaces, nilmanifolds and their morphisms, 2010.

[3] P. Candela. Notes on nilspaces: algebraic aspects. *Discrete Anal.*, pages Paper No. 15, 59, 2017.

[4] P. Candela, D. González-Sánchez, and B. Szegedy. On higher-order fourier analysis in characteristic p, 2021.

[5] P. Candela and B. Szegedy. Regularity and inverse theorems for uniformity norms on compact abelian groups and nilmanifolds. *J. für die Reine und Angew. Math.*, 789:1–42, 2022.

[6] P. Gopalan, A. R. Klivans, and D. Zuckerman. List-decoding Reed-Muller codes over small fields. In *STOC'08*, pages 265–274. ACM, New York, 2008.

[7] W. T. Gowers and L. Milićević. A quantitative inverse theorem for the u^4 norm over finite fields, 2017.

[8] W. T. Gowers and L. Milićević. An inverse theorem for freiman multi-homomorphisms, 2020.

[9] B. Green and T. Tao. An inverse theorem for the Gowers $U^3(G)$ norm. *Proc. Edinb. Math. Soc. (2)*, 51(1):73–153, 2008.

[10] B. Green and T. Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math. (2)*, 167(2):481–547, 2008.

[11] B. Green and T. Tao. The distribution of polynomials over finite fields, with applications to the Gowers norms. *Contrib. Discrete Math.*, 4(2):1–36, 2009.

[12] B. Green and T. Tao. The quantitative behaviour of polynomial orbits on nilmanifolds. *Ann. of Math. (2)*, 175(2):465–540, 2012.

[13] B. Green, T. Tao, and T. Ziegler. An inverse theorem for the Gowers $U^{s+1}[N]$-norm. *Ann. of Math. (2)*, 176(2):1231–1372, 2012.

[14] Y. Gutman, F. Manners, and P. P. Varjú. The structure theory of nilspaces I. *J. Anal. Math.*, 140(1):299–369, 2020.

[15] B. Host and B. Kra. Parallelepipeds, nilpotent groups and Gowers norms. *Bull. Soc. Math. France*, 136(3):405–437, 2008.

[16] A. Jamneshan, O. Shalom, and T. Tao. The structure of totally disconnected host–kra–ziegler factors, and the inverse theorem for the u^k gowers uniformity norms on finite abelian groups of bounded torsion. *forthcoming*, 2022.

[17] D. Kim, A. Li, and J. Tidor. Cubic goldreich-levin, 2022.

[18] L. Milićević. Quantitative inverse theorem for gowers uniformity norms U^5 and U^6 in $\mathbb{F}_2^n$, 2022.

[19] A. Samorodnitsky. Low-degree tests at large distances. In *STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 506–515. ACM, New York, 2007.

[20] M. Sudan. List decoding. *ACM SIGACT News*, 31(1):16–27, Mar. 2000.

[21] T. Tao. *Higher Order Fourier Analysis*. Graduate studies in mathematics. American Mathematical Society, 2012.

[22] T. Tao and T. Ziegler. The inverse conjecture for the gowers norm over finite fields via the correspondence principle. *Anal. PDE*, 3(1):1–20, 2010.

[23] T. Tao and T. Ziegler. The inverse conjecture for the gowers norm over finite fields in low characteristic. *Ann. Comb.*, 16:121–188, 2012.

[24] J. Tidor. Quantitative bounds for the u^4-inverse theorem over low characteristic finite fields, 2021.

[25] M. Tulsiani and J. Wolf. Quadratic Goldreich-Levin theorems. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science—FOCS 2011*, pages 619–628. IEEE Computer Soc., Los Alamitos, CA, 2011.

Department of Mathematics, Koç University, Rumelifeneri Yolu, 34450, Sariyer, Istanbul, Turkey
Email address: `ajamneshan@ku.edu.tr`

Institute for Advanced Study, 1 Einstein Drive, Princeton, New Jersey, 08540, USA
Email address: `Or.Shalom@ias.edu`

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA
Email address: `tao@math.ucla.edu`