A short proof of an inverse theorem in bounded torsion groups *

Pablo Candela†1, Diego González-Sánchez‡2, and Balázs Szegedy§2

1UAM and ICMAT, Ciudad Universitaria de Cantoblanco Madrid 28049 Spain
2HUN-REN Alfréd Rényi Institute of Mathematics, Reáltanoda u. 13-15. Budapest, Hungary, H-1053

Abstract

Let Z be a finite abelian group of bounded torsion m and $f : \mathrm{Z} \to \mathbb{C}$ a 1-bounded function. Jamneshan, Shalom, and Tao proved the following inverse theorem: If $\|f\|_{U^{k+1}} \geq \delta > 0$, then f correlates non-trivially with a polynomial phase function of degree bounded in terms of m and k. They also ask whether the same holds with polynomials of degree at most k. In this paper we use the nilspace approach to investigate this problem proving: *a)* an inverse theorem for bounded torsion abelian groups where we replace the polynomial phase functions of degree k by *projected* polynomial phase functions of degree k, a notion introduced by the third-named author. *b)* Relying on *a)* we give a short proof of the result of Jamneshan, Shalom, and Tao.

1 Introduction

This work is a shortened version of [6] and some parts have been taken from the latter directly.

Since their introduction in the seminal work of Gowers [9], the study of Gowers norms (denoted by $\|\cdot\|_{U^{k+1}}$) have been central in the area of higher-order Fourier analysis. An important question related to these norms is inverse theorems. Such results were initially proved for finite cyclic groups (or intervals of $\mathbb{Z}$) in [12] and state, loosely speaking, that if a function has a large U^{k+1}-norm then it must correlate with a *nil-function*. The precise notion of what a *nil-function* is depends on the type of abelian groups we are considering (e.g., cyclic groups, finite torsion vector spaces $\mathbb{F}_p^n$, etc.) We refer to [7, 10, 14, 16] for more background on these results. In this paper, we will focus on finite abelian groups with fixed finite torsion $m \geq 1$ (or m-torsion abelian groups). That is, abelian groups Z such that $mx = 0$ for all $x \in \mathrm{Z}$.

Our work is motivated by a recent paper of Jamneshan, Shalom, and Tao [15] where they prove an inverse theorem for m-torsion abelian groups where the *nil-function* mentioned above is a *polynomial phase function* of degree bounded in terms of m and k. Recall that given abelian groups Z, Z', a map $P : \mathrm{Z} \to \mathrm{Z}'$ and any $h \in \mathrm{Z}$, we may take the discrete derivative $\partial_h P : \mathrm{Z} \to \mathrm{Z}'$ defined by $\partial_h P(x) = P(x+h) - P(x)$. Then we say that P is *polynomial of degree at most* k if $\partial_{h_1} \cdots \partial_{h_{k+1}}(P)(x) = 0$ for all $x, h_1, \ldots, h_{k+1} \in \mathrm{Z}$. A *polynomial phase function* of degree at most k is then a *polynomial of degree* at most k where $\mathrm{Z}' = \mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$.

*The full version of this work can be found in [6] and will be published elsewhere. All authors used funding from project PID2020-113350GB-I00 of Spain's MICINN. The second-named author received funding from projects KPP 133921 and Momentum (Lendület) 30003 of the Hungarian Government. The research was also supported partially by the NKFIH "Élvonal" KKP 133921 grant and by the Hungarian Ministry of Innovation and Technology NRDI Office in the framework of the Artificial Intelligence National Laboratory Program.

†Email: pablo.candela@uam.es.
‡Email: diegogs@renyi.hu.
§Email: szegedyb@gmail.com.

Theorem 1. ([15, Theorem 1.12]) *Let k, m be positive integers and let $\delta > 0$. Then there exist constants $\varepsilon = \varepsilon(\delta, k, m) > 0$ and $C = C(k, m) > 0$ such that for every finite m-torsion abelian group Z and every 1-bounded function $f : \mathrm{Z} \to \mathbb{C}$ with $\|f\|_{U^{k+1}} > \delta$, there exists a polynomial phase $Q : \mathrm{Z} \to \mathbb{S}^1$ of degree at most C such that $|\mathbb{E}_{x\in \mathrm{Z}} f(x)\overline{Q(x)}| > \varepsilon$.*

This result is inspired by the special case $m = p$ a prime number, where much more is known. In fact in this case Z is just $\mathbb{F}_p^n$ for some integer n, and it is known (see [18, Theorems 1.9 and 1.10] and [19, Theorem 1.10]) that we can take $C(k, p) = k$.[1] Jamneshan, Shalom, and Tao ask whether this holds also in the case of m not being a prime [15, Question 1.9]. An important aspect related to the constant $C(k, m)$ is that if it equals k for any $m \in \mathbb{N}$, then this would be the optimal value. The proof of this fact follows from the following result (valid for any finite abelian group Z, see Proposition 9):

Lemma 2. *Let $\delta > 0$. For any 1-bounded function $f : \mathrm{Z} \to \mathbb{C}$ if[2] $|\langle f, Q\rangle| \geq \delta$ for Q a polynomial phase function of degree k then $\|f\|_{U^{k+1}} \geq \delta$.*

Any function Q (not necessarily a polynomial phase) satisfying the conclusion of Lemma 2 is called an *obstruction* to the U^{k+1} norm.[3] For $k' > k$ in general (and in particular, in the case of m-torsion groups), polynomial phases of degree at most k' are not *necessarily* obstructions to the U^{k+1} norm.

In this paper, we prove an inverse theorem for m-torsion abelian groups where the *nil-functions* appearing are a generalization of polynomial phase functions of degree k but nevertheless, they are obstructions to the U^{k+1} Gowers norm for m-torsion groups. This notion was introduced originally by the third-named author in the unpublished work [17]. We recall its definition (see [17, Definition 1.2]).

Definition 3. *Let Z be a finite abelian group and let $k \in \mathbb{N}$. A* projected phase polynomial of degree *k on Z is a 1-bounded function $\phi_{*\tau} : \mathrm{Z} \to \mathbb{C}$ of the following form. There is a finite abelian group Z', a surjective homomorphism $\tau : \mathrm{Z}' \to \mathrm{Z}$, and a polynomial phase function $\phi : \mathrm{Z}' \to \mathbb{C}$ of degree at most k, such that $\phi_{*\tau}(x) = \mathbb{E}_{y\in\tau^{-1}(x)}\phi(y)$ for every $x \in \mathrm{Z}$. If the torsions of Z and Z' are respectively m and m' we say that $\phi_{*\tau}$ has torsion (m, m'). We say it is rank-preserving if the rank of Z is equal to the rank of Z' (where the rank is the minimal number of generators).*

We can now state our first main result (see [6, Theorem 1.12] and the discussion below).

Theorem 4. *Let k, m be positive integers and let $\delta > 0$. Then there exists $\gamma = \gamma(k) \in \mathbb{N}$ and $\varepsilon = \varepsilon(\delta, k, m) > 0$ such that the following holds. For any m-torsion abelian group Z and any 1-bounded function $f : \mathrm{Z} \to \mathbb{C}$ with $\|f\|_{U^{k+1}} \geq \delta$, there exists a rank-preserving projected phase polynomial $\phi_{*\tau}$ of degree k and torsion (m, m^γ) on Z such that $|\langle f, \phi_{*\tau}\rangle| \geq \varepsilon$. Conversely, if for any $\delta' > 0$ we have $|\langle f, \phi_{*\tau}\rangle| \geq \delta'$ for some projected phase polynomial $\phi_{*\tau}$ of degree k then $\|f\|_{U^{k+1}} \geq \delta'$.*

As we can see, the first part of Theorem 4 is very similar to Theorem 1, but it replaces the polynomial phase functions of degree $C(k, m)$ by projected phase polynomials of degree k. The second main result of this paper shows that the former result is strictly stronger.

Theorem 5. *Theorem 1 can be deduced from Theorem 4.*

2 An inverse theorem with bounded-torsion nilspaces

In this paper, we rely on the theory of nilspaces (see e.g., [1, 2, 13] and references therein). In a few words, a nilspace is an algebraic object (you can also endow it with a natural topology) that generalizes abelian groups. An important feature of nilspaces is the concept of step: the class of 1-step nilspaces

[1] These results are qualitative. We refer to [10, 11] and references therein for quantitative results.

[2] For any finite abelian group Z and any pair of functions $f, g : \mathrm{Z} \to \mathbb{C}$ we denote $\langle f, g\rangle := \mathbb{E}_{x\in\mathrm{Z}} f(x)\overline{g(x)}$.

[3] To be fully precise, we need to fix a family of finite abelian groups $\mathcal{F}$ and $\delta > 0$. Then, given a family of functions $\mathcal{T} = \{Q : \mathrm{Z} \to \mathbb{C} : \mathrm{Z} \in \mathcal{F}\}$ we say that the functions of that family are obstructions to the U^{k+1} norm for $\mathcal{F}$ if there exists $\epsilon = \epsilon(\delta, \mathcal{F}) > 0$ such that for any $\mathrm{Z} \in \mathcal{F}$, any 1-bounded $f : \mathrm{Z} \to \mathbb{C}$, and any $Q \in \mathcal{T}$ if $|\langle f, Q\rangle| > \delta$ then $\|f\|_{U^{k+1}} > \epsilon$.

equals the class of (affine[4]) abelian groups. For higher step $k \geq 2$, nilspaces can be seen as a tower of k extensions (or bundles) by abelian groups, called structure groups (see [2, §1.2 and §3.2] for details). In this paper, we will be interested in the class of nilspaces such that all the abelian groups in these extensions are m-torsion abelian groups. We denote such nilspaces by *m-torsion* nilspaces (see [6]).

Similarly to abelian groups, where we have the concept of homomorphism $\varphi : \mathrm{Z} \to \mathrm{Z}'$ between abelian groups, for nilspaces, this generalizes to the concept of nilspace morphism $\varphi : \mathrm{X} \to \mathrm{Y}$. The importance of nilspaces and nilspace morphisms is that we can formulate the most general inverse theorem known at the time of writing this paper (valid for any compact abelian group or even any nilmanifold) as shown in [7, Theorem 1.6]. This result can be specialized in the case that we want to find inverse theorems among various classes of groups (see [7, Theorem 1.7] and [5, §6]). In this paper, we are interested in the class of finite abelian m-torsion groups. The following result is a version of [6, Theorem 2.3]:

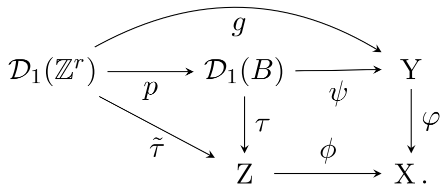
Theorem 6. *For any $k, m \in \mathbb{N}$ and $\delta > 0$ there exists $C > 0$ such that the following holds. Let Z be a finite abelian m-torsion group, and let $f : \mathrm{Z} \to \mathbb{C}$ be a 1-bounded function with $\|f\|_{U^{k+1}} \geq \delta$. Then there is a finite m-torsion k-step nilspace X of cardinality $|\mathrm{X}| \leq C$, a morphism $\phi : \mathcal{D}_1(\mathrm{Z}) \to \mathrm{X}$, and a 1-bounded function $F : \mathrm{X} \to \mathbb{C}$, such that $\langle f, F \circ \phi \rangle \geq \frac{1}{2}\delta^{2^{k+1}}$.*

Hence, we can reduce the question of studying the inverse theorem for m-torsion groups to studying morphisms $\phi : \mathcal{D}_1(\mathrm{Z}) \to \mathrm{X}$. The nilspace $\mathcal{D}_1(\mathrm{Z})$ or more generally $\mathcal{D}_k(\mathrm{Z})$ for any $k \geq 1$ is a special type of nilspace constructed from any abelian group Z, see [2, §2.2.4] for the precise definition of $\mathcal{D}_k(\mathrm{Z})$. What matters for us is that these nilspaces are the *simplest* types of nilspaces. For example, by [4, Lemma A.2] we have that the morphisms $\varphi : \mathcal{D}_\ell(\mathrm{Z}) \to \mathcal{D}_k(\mathrm{Z}')$ are exactly the polynomials $\mathrm{Z} \to \mathrm{Z}'$ of degree at most $\lfloor k/\ell \rfloor$.

Let us now outline the rest of the proof idea:

(i) Given any m-torsion nilspace X there exists numbers $a_1, \ldots, a_k$ and γ such that the following holds. There is a totally surjective bundle morphism[5] $\tilde{\varphi} : \prod_{i=1}^k \mathcal{D}_i(\mathbb{Z}^{a_i}) \to \mathrm{X}$ which is m^γ periodic. We let $\mathrm{Y} := \prod_{i=1}^k \mathcal{D}_i(\mathbb{Z}_{m^\gamma}^{a_i})$. This notion is analogous to the known fact for finite abelian groups that if A is abelian and m-torsion, then there exists a surjective m-periodic homomorphism $\mathbb{Z}^a \to A$ for some $a \in \mathbb{N}$.

(ii) Letting $\tilde{\tau} : \mathbb{Z}^r \to \mathrm{Z}$ be a surjective homomorphism there exists a morphism $g : \mathcal{D}_1(\mathbb{Z}^r) \to \mathrm{Y}$ such that $\varphi \circ g = \phi \circ \tilde{\tau}$. Moreover, the map g is $m^{\gamma'}$-periodic for some $\gamma' = \gamma'(k)$. Letting $B := \mathbb{Z}_{m^{\gamma'}}^r$ the situation can be better seen in the following commutative diagram:



(1)

Coming back to the case of m-torsion abelian groups, note that if we have $\mathrm{X} = A$ and $\mathrm{Y} = \mathbb{Z}_m^a$ then the map $\varphi \circ g$ is m-periodic (no need for a γ' power).

(iii) Recall that we wanted to study the map $F \circ \phi : \mathrm{Z} \to \mathbb{C}$. By (1) note that $F \circ \phi \circ \tau = F \circ \varphi \circ \psi$. But now the map ψ is relatively easy to understand as it consists of polynomials of degree at most k. Hence, by using regular Fourier analysis on the abelian group Y (yes, it is a nilspace, but you can see it also as an abelian group and do Fourier analysis on it) we can write $F \circ \varphi$ as a sum of a bounded number of harmonics which yields the result.

[4]There is no fixed 0 element, but after choosing any arbitrary element to be 0 these classes can be proved to be equal.
[5]See [2, Definition 3.3.1].

3 Proof idea of Theorem 4

The point (i) from the previous section relies on generalizations of two well-known results for finite abelian groups. The first is that letting A be a finite abelian group there exists $a \in \mathbb{N}$ and a surjective homomorphism $\mathbb{Z}^a \to A$. The second is that if we further assume that A is m-torsion, then the former surjective homomorphism can be proved to be m-periodic. We need generalizations of these results for m-torsion nilspaces. Generalizing the first result, namely, that for a finite k-step nilspace X there exists a fibration $\prod_{i=1}^k \mathcal{D}_i(\mathbb{Z}^{a_i}) \to \mathrm{X}$ is a non-trivial result shown by the authors, [4, Theorem 4.4] (see also [6, Corollary 5.4]).

For the second result, the periodicity of morphisms of the form $\prod_{i=1}^k \mathcal{D}_i(\mathbb{Z}^{a_i}) \to \mathrm{X}$ when X is m-torsion, let us prove here the core lemma (a version of [6, Lemma 5.1]) that leads to the full result (see [6, Corollary 5.4] for details).

Lemma 7. *For any positive integer k there exists $\alpha > 0$ such that the following holds. Let A be any m-torsion abelian group and let $\phi : \mathbb{Z} \to A$ be a polynomial of degree at most k. Then ϕ is m^α-periodic.*

Proof. By [4, Theorem A.6], any polynomial ϕ of the latter type has an expression of the form $\phi(x) = \sum_{i=1}^k a_i \binom{x}{i}$ for some $a_i \in A$. Let us prove now that $\binom{x+m^{k+1}}{i} - \binom{x}{i}$ is a multiple of m for any $x \in \mathbb{Z}$ and $i \in [k]$. For any prime $p|m$ suppose that $m = p^c m'$ where p and m' are coprime. If we prove that $\binom{x+m^{k+1}}{i} - \binom{x}{i}$ is a multiple of p^c then we are done (as we can then argue similarly for every prime dividing m). Using the identity $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i}$ we have $\binom{x+m^{k+1}}{i} - \binom{x}{i} = \frac{m^{k+1}}{i!} Q(x,m,i)$ for some integer-valued polynomial Q. If we prove that $\frac{m^{k+1}}{i!}$ is always a multiple of p^c then we will be done. Note that the largest power of p dividing m^{k+1} is precisely $c(k+1)$. On the other hand, in $i!$ we have at most $\sum_{j=1}^\infty \lfloor i/p^j \rfloor \le \sum_{j=1}^\infty i/p^j = \frac{i}{p-1} \le \frac{k}{p-1}$ factors of p. But as for any $c \in \mathbb{N}$ and p prime we have that $\frac{k}{p-1} + c \le c(k+1)$ the result follows. □

To prove (ii), we again rely on generalizing a known result for abelian groups. Namely, let A, C be abelian groups, $\varphi : C \to A$ be a surjective homomorphism, and $q : \mathbb{Z}^n \to A$ be any homomorphism. Then there exists $\tilde{q} : \mathbb{Z}^n \to C$ such that $\varphi \circ \tilde{q} = q$. This result generalizes to nilspaces as shown in [5, Corollary A.6]. Thus, the diagram (1) follows.

Proof sketch of first part of Theorem 4. We apply Theorem 6 and let X be the resulting nilspace of torsion m, ϕ the resulting morphism $\mathcal{D}_1(\mathrm{Z}) \to \mathrm{X}$, and $F : \mathrm{X} \to \mathbb{C}$ the resulting 1-bounded function such that $\mathbb{E}_{x\in Z} f(x) F(\phi(x)) \ge \delta^{2^{k+1}}/2$. We construct now Diagram (1) as explained before. Let $h := F \circ \varphi : \mathrm{Y} \to \mathbb{C}$. Then $\mathbb{E}_{x\in Z} f(x) F(\phi(x)) = \mathbb{E}_{y \in B} f \circ \tau(y) h \circ \psi(y)$. By the Fourier decomposition of h on the finite abelian group Y, and the pigeonhole principle, there is a character $\chi \in \widehat{B}$ such that $\varepsilon \le \mathbb{E}_{y\in B} f(\tau(y)) \chi(\psi(y)) = \mathbb{E}_{x \in Z} f(x) \mathbb{E}_{y \in \tau^{-1}(x)} \chi(\psi(y))$, which proves the result with $\phi := \chi \circ \psi$. □

The second part of Theorem 4 follows from the next results.

Lemma 8. *Let $\phi_{*\tau}$ be a projected phase polynomial of degree k on a finite abelian group. Then $\|\phi_{*\tau}\|^*_{U^{k+1}} \le 1$ where $\|\cdot\|^*_{U^{k+1}}$ is the U^{k+1}-dual-norm.*

Proof. Recall the definition $\|\phi_{*\tau}\|^*_{U^{k+1}} = \sup_{g:\mathrm{Z}\to\mathbb{C}:\|g\|_{U^{k+1}}\le 1} |\langle \phi_{*\tau}, g\rangle|$. Denoting by Z' the (abelian group) domain of τ, the map $\tau^{[\![k+1]\!]} : \mathrm{C}^{k+1}(\mathrm{Z}') \to \mathrm{C}^{k+1}(\mathrm{Z})$ defined by $\tau^{[\![k+1]\!]}(\mathrm{c}) : v \mapsto \tau(\mathrm{c}(v))$ is a surjective homomorphism. It follows that for every map $g : \mathrm{Z} \to \mathbb{C}$ we have $\|g \circ \tau\|_{U^{k+1}(\mathrm{Z}')} = \|g\|_{U^{k+1}(\mathrm{Z})}$. Then we have $|\langle \phi_{*\tau}, g\rangle_{\mathrm{Z}}| = |\mathbb{E}_{x\in\mathrm{Z}} \mathbb{E}_{y\in\tau^{-1}(x)} g\circ\tau(y)\phi(y)| = |\langle g\circ\tau, \phi\rangle_{\mathrm{Z}'}| \le \|g\circ\tau\|_{U^{k+1}(\mathrm{Z}')} \|\phi\|^*_{U^{k+1}(\mathrm{Z}')} = \|g\|_{U^{k+1}(\mathrm{Z})} \|\phi\|^*_{U^{k+1}(\mathrm{Z}')}$. Therefore $\|\phi_{*\tau}\|^*_{U^{k+1}(\mathrm{Z})} \le \|\phi\|^*_{U^{k+1}(\mathrm{Z})}$. Since ϕ is a phase polynomial of degree k, we have that $|\langle \phi, g\rangle| = \|\phi\overline{g}\|_{U^1} \le \|\phi\overline{g}\|_{U^{k+1}} = \|g\|_{U^{k+1}}$, see [11, (2.1)]. Thus $\|\phi\|^*_{U^{k+1}(\mathrm{Z}')} \le 1$. □

Proposition 9. *Let $\phi_{*\tau}$ be a projected phase polynomial of degree k on a finite abelian group Z, and suppose that $f : \mathrm{Z} \to \mathbb{C}$ satisfies $|\langle f, \phi_{*\tau}\rangle| \ge \delta$. Then $\|f\|_{U^{k+1}} \ge \delta$.*

Proof. By Lemma 8, $\delta \le |\langle f, \phi_{*\tau}\rangle| \le \|f\|_{U^{k+1}} \|\phi_{*\tau}\|^*_{U^{k+1}} \le \|f\|_{U^{k+1}}$. □

4 Proof of Theorem 5

The idea is to prove that the projected phase polynomials appearing in Theorem 4 can be written as averages of polynomials of possibly larger degree. We shall prove this below and then apply it to give an alternative proof of [15, Theorem 1.12]. Given a surjective homomorphism $\tau : B \to \mathrm{Z}$, by a *polynomial cross-section* for τ we mean a map $\iota : \mathrm{Z} \to B$ which is polynomial and such that $\tau \circ \iota$ is the identity map on Z. The main result that we will use is the following.

Theorem 10. *Let $m, m' \in \mathbb{N}$. Then there exists a constant $C(m, m') \in \mathbb{N}$ such that the following holds. Let Z, B be finite abelian groups of torsion m and m' respectively and let $\tau : B \to \mathrm{Z}$ be a surjective homomorphism. Then there exists a polynomial cross-section $\iota : \mathrm{Z} \to B$ of degree at most $C(m, m')$.*

The full proof of Theorem 10 can split into several lemmas, see [6, §5.1] for details. Here we are only going to show the first one. See also [15, Lemma 8.2] for an alternative approach.

Lemma 11. *Let $d \geq s$ be positive integers and let p be a prime. Let $\varphi : \mathbb{Z}_{p^d} \to \mathbb{Z}_{p^s}$ be the map $x \mod p^d \mapsto x \mod p^s$. Let $\iota : \mathbb{Z}_{p^s} \to \mathbb{Z}_{p^d}$ be defined by $n \mod p^s \mapsto n \mod p^d$ for each $n \in [0, p^s - 1]$. Then ι is a polynomial cross-section for φ of degree at most $(d - s)p^s + 1$.*

The argument has similarities with the proof of [5, Proposition B.2]. We want to prove that if we take sufficiently many derivatives of ι then we obtain the 0 map. Without loss of generality, it suffices to take derivatives $\partial_a \iota(x) := \iota(x + a) - \iota(x)$ with respect to the generator $a = 1 \in \mathbb{Z}_{p^s}$. Note that $\partial_1 \iota(x) = 1$ if $x \neq p^s - 1$ and $\partial_1 \iota(p^s - 1) = 1 - p^s$. Taking one more derivative, $\partial_1^2 \iota(x) = 0$ if $x \neq p^s - 1$, $\partial_1^2 \iota(p^s - 2) = -p^s$ and $\partial_1^2 \iota(p^s - 1) = p^s$. To take derivatives of higher degree, as is standard, we can view the map $\partial_1^2 \iota$ as a vector in $\mathbb{Z}_{p^d}^{p^s}$ and take the derivatives by left-multiplying this vector by the forward difference matrix, i.e. the circulant matrix $C_{p^s} := \begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \\ 1 & 0 & \cdots & 0 & -1 \end{pmatrix} \in M_{p^s \times p^s}(\mathbb{Z})$. Known results on circulant matrices imply the following fact.

Lemma 12. *For any prime p and any integer $s \geq 1$ all the entries of $C_{p^s}^{p^s}$ are multiples of p.*

Proof. By equation (8) in [8], for every $q \in \mathbb{N}$ we have $C_{p^s}^q = \sum_{j=0}^q \binom{q}{j}(-1)^j A_{p^s}^{q-j}$, where A_{p^s} is the cyclic permutation matrix (see [8]). Taking $q = p^s$, we claim that it suffices to prove that $\binom{p^s}{j} = \frac{p^s!}{j!(p^s-j)!}$ is a multiple of p if $0 < j < p^s$. In fact, the contributions for $j = 0$ and $j = p^s$ cancel each other if p is odd as $A_{p^s}^0 = A_{p^s}^{p^s} = \mathrm{id}_{p^s \times p^s}$ and thus $\binom{p^s}{0}(-1)^0 \mathrm{id}_{p^s \times p^s} + \binom{p^s}{p^s}(-1)^{p^s} \mathrm{id}_{p^s \times p^s} = 0$. If $p = 2$ we have $\binom{2^s}{0}(-1)^0 \mathrm{id}_{2^s \times 2^s} + \binom{2^s}{2^s}(-1)^{2^s} \mathrm{id}_{2^s \times 2^s} = 2\mathrm{id}_{2^s \times 2^s}$ which is a multiple of $p = 2$ as claimed. To see the general case $0 < j < p^s$, note first that the number of p factors in $j!$ is precisely $\sum_{i=1}^{s-1} \lfloor j/p^i \rfloor$. Thus, it suffices to prove that $\sum_{i=1}^{s-1} \lfloor j/p^i \rfloor + \sum_{i=1}^{s-1} \lfloor (p^s - j)/p^i \rfloor < 1 + p + \cdots + p^{s-1} = \frac{p^s - 1}{p - 1}$, where the right hand side is the number of p factors of $p^s!$. The left hand side can be estimated using the bound $\sum_{i=1}^{s-1} \lfloor j/p^i \rfloor \leq \sum_{i=1}^{s-1} j/p^i = j \frac{p^{s-1} - 1}{(p-1)p^{s-1}}$. Hence, the left side is bounded above by $j \frac{p^{s-1} - 1}{(p-1)p^{s-1}} + (p^s - j) \frac{p^{s-1} - 1}{(p-1)p^{s-1}} = \frac{p^s - p}{p - 1}$, which is smaller than the number of p factors in $p^s!$. □

Proof of Lemma 11. Note that after two derivatives, the map $\partial_1^2 \iota$ has already a factor p^s. Each time that we differentiate p^s additional times we add (at least) a factor p by Lemma 12. It follows that $\partial_1^{kp^s + 2} \iota(x)$ is a multiple of p^{k+s} for any $x \in \mathbb{Z}_{p^s}$. Thus, if $k + s = d$ then we have $\partial_1^{kp^s + 2} \iota = 0 \mod p^d$. Hence ι is a polynomial of degree at most $(d - s)p^s + 1$. □

The rest of the proof of Theorem 10 follows by first taking the Sylow decomposition on Z and B, thus reducing the problem to the case of p-groups. And then, by proving that any surjective homomorphism between p-groups can be reduced (via isomorphisms and projections) to the case of Lemma 11.

Proof of Theorem 5. By Theorem 4, the function f correlates with a projected phase polynomial $(\chi \circ \psi)_{*\tau}$ of degree k and torsion $(m, m^{O_k(1)})$, for some homomorphism $\tau : B \to \mathrm{Z}$. By Theorem 10 there exists a polynomial cross-section $\iota : \mathrm{Z} \to B$ of degree $O_{m,k}(1)$. Moreover, for any $u \in \ker(\tau)$ we have that $\iota_u(x) := \iota(x) + u$ is clearly also a polynomial cross-section. Recall that $(\chi \circ \psi)_{*\tau}$ is the map $\mathbb{E}_{y \in \tau^{-1}(x)} \chi(\psi(y))$ defined for $x \in \mathrm{Z}$. However, for any $x \in \mathrm{Z}$ we have $\mathbb{E}_{y \in \tau^{-1}(x)} \chi(\psi(y)) = \mathbb{E}_{u \in \ker(\tau)} \chi(\psi(\iota_u(x)))$. Thus $\varepsilon < |\mathbb{E}_{x \in \mathrm{Z}} f(x) \mathbb{E}_{u \in \ker(\tau)} \chi(\psi(\iota_u(x)))| = |\mathbb{E}_{u \in \ker(\tau)} \mathbb{E}_{x \in \mathrm{Z}} f(x) \chi(\psi(\iota_u(x)))|$. Hence, $\varepsilon < |\mathbb{E}_{x \in \mathrm{Z}} f(x) \chi(\psi(\iota_u(x)))|$ for some $u \in \ker(\tau)$. Finally note that by [4, Lemma A.2], $\psi \circ \iota_u$ is in fact a polynomial map with degree bounded by $\deg(\iota)k = O_{m,k}(1)$. The result follows. □

References

[1] O. A. Camarena and B. Szegedy, *Nilspaces, nilmanifolds and their morphisms*, preprint (2010), `arXiv:1009.3825`.

[2] P. Candela, *Notes on nilspaces: algebraic aspects*, Discrete Anal. (2017), Paper No. 15, 59 pp.

[3] P. Candela, D. González-Sánchez and B. Szegedy *On nilspace systems and their morphisms*, Ergodic Theory Dynam. Systems **40** (2020), no. 11, 3015–3029.

[4] P. Candela, D. González-Sánchez, B. Szegedy, *Free nilspaces, double-coset nilspaces, and Gowers norms*, preprint (2023), `arxiv:2305.11233`.

[5] P. Candela, D. González-Sánchez, B. Szegedy, *On higher-order Fourier analysis in characteristic p*, Ergodic Theory Dynam. Systems **43** (2023), no. 12, 3971–4040.

[6] P. Candela, D. González-Sánchez, B. Szegedy, *On the inverse theorem for Gowers norms in abelian groups of bounded torsion*, preprint, arXiv:2311.13899.

[7] P. Candela and B. Szegedy, *Regularity and inverse theorems for uniformity norms on compact abelian groups and nilmanifolds*, J. Reine Angew. Math. **789** (2022), 1–42.

[8] J. Feng, *A note on computing of positive integer powers for circulant matrices*, Appl. Math. Comput. Appl. Math. Comput. **223** (2013), 472–475.

[9] W. T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588.

[10] W. T. Gowers, L. Milićević, *An inverse theorem for Freiman multi-homomorphisms*, preprint (2020) `arXiv:2002.11667` .

[11] B. Green, T. Tao, *An inverse theorem for the Gowers $U^3(G)$-norm*, Proc. Edinb. Math. Soc. (2) **51** (2008), no. 1, 73–153.

[12] B. Green, T. Tao and T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Ann. of Math. (2) **176** (2012), no. 2, 1231–1372.

[13] Y. Gutman, F. Manners, P. P. Varjú, *The structure theory of nilspaces I*, J. Anal. Math. **140** (2020), no. 1, 299–369.

[14] A. Jamneshan, T. Tao, *The inverse theorem for the U^3 Gowers uniformity norm on arbitrary finite abelian groups: Fourier-analytic and ergodic approaches*, Discrete Anal., 2023:11, 48 pp.

[15] A. Jamneshan, O. Shalom, 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*, preprint (2023), `arXiv:2303.04860`.

[16] F. Manners, *Quantitative bounds in the inverse theorem for the Gowers U^{s+1}-norms over cyclic groups*, preprint (2018), `arXiv:1811.00718`.

[17] B. Szegedy, *Structure of finite nilspaces and inverse theorems for the Gowers norms in bounded torsion groups*, preprint (2010), `arXiv:1011.1057`.

[18] T. Tao and T. Ziegler, *The inverse conjecture for the Gowers norm over finite fields via the correspondence principle*, Anal. PDE **3** (2010), no. 1, 1–20.

[19] T. Tao and T. Ziegler, *The inverse conjecture for the Gowers norm over finite fields in low characteristic*, Ann. Comb. **16** (2012), no. 1, 121–188.