Math. Proc. Camb. Phil. Soc. (2022), **173**, 525–537
doi:10.1017/S0305004121000682
First published online 15 December 2021

Non-classical polynomials and the inverse theorem

BY AARON BERGER, ASHWIN SAH, MEHTAAB SAWHNEY, AND JONATHAN TIDOR[†]
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, U.S.A
e-mails: bergera@mit.edu, asah@mit.edu, msawhney@mit.edu, jtidor@mit.edu

(*Received* 25 *July* 2021*; revised* 01 *November* 2021*; accepted* 27 *October* 2021)

Abstract

In this paper we *characterize* when non-classical polynomials are necessary in the inverse theorem for the Gowers U^k-norm. We give a brief deduction of the fact that a bounded function on $\mathbb{F}_p^n$ with large U^k-norm must correlate with a classical polynomial when $k \leq p+1$. To the best of our knowledge, this result is new for $k = p+1$ (when $p > 2$). We then prove that non-classical polynomials are necessary in the inverse theorem for the Gowers U^k-norm over $\mathbb{F}_p^n$ for all $k \geq p+2$, completely characterising when classical polynomials suffice.

1. *Introduction*

The inverse theorem for the Gowers U^k-norm states that a bounded function $f\colon G \to \mathbb{C}$ has large U^k-norm if and only if f correlates with a certain structured object. When $G = \mathbb{Z}/N\mathbb{Z}$, these structured objects are quite complicated and need the theory of nilsequences to describe. When $G = \mathbb{F}_p^n$, the situation is somewhat simpler. When $p \geq k$, a bounded function $f\colon \mathbb{F}_p^n \to \mathbb{C}$ has large U^k-norm if and only if f has non-negligible correlation with a polynomial phase function, i.e., $e^{2\pi i P(x)/p}$ where $P\colon \mathbb{F}_p^n \to \mathbb{F}_p$ is a polynomial of degree at most $k-1$.

The situation when p is small compared to k is more delicate. Green and Tao [3] and independently Lovett, Meshulam and Samorodnitsky [4] showed that the corresponding conjecture is false for $k = 4$ and $p = 2$. In other words, there exist bounded functions $f\colon \mathbb{F}_2^n \to \mathbb{C}$ with large U^4-norm but with correlation $o_{n\to\infty}(1)$ with every cubic phase function. Tao and Ziegler [7] clarified this situation by proving that for all k and p, a bounded function $f\colon \mathbb{F}_p^n \to \mathbb{C}$ has large U^k-norm if and only if f has non-negligible correlation with a non-classical polynomial phase function, i.e., $e^{2\pi i P(x)}$ where $P\colon \mathbb{F}_p^n \to \mathbb{R}/\mathbb{Z}$ is a non-classical polynomial of degree at most $k-1$. (See Section 2 for the relevant definitions.)

A natural question which remains from the above discussion is to determine for which pairs p, k does the U^k-inverse theorem over $\mathbb{F}_p^n$ hold with classical polynomials. In the positive direction, it is known due to Samorodnitsky [5] that the U^3-inverse theorem over $\mathbb{F}_2^n$ holds with classical polynomials. In the negative direction, Lovett, Meshulam and

[†] Berger, Sah, Sawhney, and Tidor were supported by NSF Graduate Research Fellowship Program DGE-1745302.

Samorodnitsky [4] proved that the U^{p^ℓ}-inverse theorem over $\mathbb{F}_p^n$ requires non-classical polynomials for all p and $\ell \geq 2$. (A curious feature of this problem is that it is not monotone in k, e.g., the Lovett–Meshulam–Samorodnitsky result does not imply that non-classical polynomials are necessary in the U^k-inverse theorem for all $k \geq p^2$.)

In this paper we completely *characterize* when classical polynomials suffice in the statement of the inverse theorem. We first prove the inverse theorem for the Gowers U^{p+1}-norm with classical polynomials. This result is proved via a short deduction from the usual inverse theorem for the U^{p+1}-norm that involves non-classical polynomials.[1]

THEOREM 1·1 *Fix a prime p and $\delta > 0$. There exists $\epsilon > 0$ such that the following holds. Let V be a finite-dimensional $\mathbb{F}_p$-vector space. Given a function $f : V \to \mathbb{C}$ satisfying $\|f\|_\infty \leq 1$ and $\|f\|_{U^{p+1}} > \delta$, there exists a classical polynomial $P \in \mathrm{Poly}_{\leqslant p}(V \to \mathbb{F}_p)$ such that*

$$|\mathbb{E}_{x \in V} f(x) e_p(-P(x))| \geq \epsilon.$$

Second, we give an example showing that non-classical polynomials are necessary in the U^k-inverse theorem for all $k \geq p + 2$.

THEOREM 1·2 *Fix a prime p and an integer $k \geq p + 2$. For all n, there exists a function $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfying $\|f\|_\infty \leq 1$ and $\|f\|_{U^k} = 1$ such that for all (classical) polynomials $P \in \mathrm{Poly}_{\leqslant k-1}(\mathbb{F}_p^n \to \mathbb{F}_p)$,*

$$|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x) e_p(-P(x))| = o_{p,k;n\to\infty}(1).$$

Our example is fairly simple to write down. For $k \geq p + 2$, we write $k - 1 = r + (p-1)\ell$ where $\ell \geq 1$ and $0 < r < p$. Then our function is

$$f(x) = e^{2\pi i \frac{\sum_{i=1}^n |x_i|^r}{p^{\ell+1}}}$$

(where $|\cdot| : \mathbb{F}_p \to \{0, \ldots, p-1\}$ is the standard map). Note that this function f is a non-classical polynomial phase function of degree $k - 1$, so the content of this result is that it does not correlate with any classical polynomial phase functions of the same degree.

The $o(1)$ correlation in Theorem 1·2 is fairly bad – the inverse of many iterated logarithms. This is due to our use of a Ramsey-theoretic argument inspired by an argument of Alon and Beigel. (A similar argument appeared in the previous works [3,4].) We conjecture that this bound on the correlation can be improved.

CONJECTURE 1·3 *Fix a prime p and an integer $k \geq p + 2$. For all n there exist $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfying $\|f\|_\infty \leq 1$ and $\|f\|_{U^k} \geq c_{p,k} > 0$ such that for all (classical) polynomials $P \in \mathrm{Poly}_{\leqslant k-1}(\mathbb{F}_p^n \to \mathbb{F}_p)$,*

$$|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x) e_p(-P(x))| \leq \exp(-\Omega_{p,k}(n)).$$

In fact, we believe that this conjecture is true with the same functions that we use to prove Theorem 1·2.

Structure of the paper: in Section 2 we give the definition of the Gowers U^k-norm and of non-classical polynomials. In Section 3 we prove Theorem 1·1. We prove Theorem 1·2 in the remainder of the paper. Section 4 develops the *symmetrization* tool that we use and Section 5 gives the full proof.

[1] See Section 2 for the definitions and notation used in the statement of these results.

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Notation: we use $|\cdot|$ for the standard map $\mathbb{F}_p \to \{0, \dots, p-1\}$. We often treat $\mathbb{F}_p$ as an additive subgroup of $\mathbb{R}/\mathbb{Z}$ via the map $x \mapsto |x|/p$ and, by some abuse of notation, freely switch between these two viewpoints. We use $e\colon \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ for the function $e(x) = e^{2\pi i x}$ and $e_p\colon \mathbb{F}_p \to \mathbb{C}$ for the function $e_p(x) = e^{2\pi i|x|/p}$.

2. *Background on non-classical polynomials*

Definition 2·1 Fix a prime p, a finite-dimensional $\mathbb{F}_p$-vector space V, and an abelian group G. Given a function $f\colon V \to G$ and a shift $h \in V$, define the *additive derivative* $\Delta_h f\colon V \to G$ by

$$(\Delta_h f)(x) = f(x+h) - f(x).$$

Given a function $f\colon V \to \mathbb{C}$ and a shift $h \in V$, define the *multiplicative derivative* $\partial_h f\colon V \to \mathbb{C}$ by

$$(\partial_h f)(x) = f(x+h)\overline{f(x)}.$$

Definition 2·2 Fix a prime p and a finite-dimensional $\mathbb{F}_p$-vector space V. Given a function $f\colon V \to \mathbb{C}$ and $d \geq 1$, the *Gowers uniformity norm* $\|f\|_{U^d}$ is defined by

$$\|f\|_{U^d} = |\mathbb{E}_{x,h_1,\dots,h_d \in V}(\partial_{h_1} \cdots \partial_{h_d} f)(x)|^{1/2^d}.$$

See [7, lemma B.1] for some basic facts about the Gowers uniformity norms.

Definition 2·3 Fix a prime p and a non-negative integer $d \geq 0$. Let V be a finite-dimensional $\mathbb{F}_p$-vector space. A *non-classical polynomial* of degree at most d is a map $P\colon V \to \mathbb{R}/\mathbb{Z}$ that satisfies

$$(\Delta_{h_1} \cdots \Delta_{h_{d+1}} P)(x) = 0$$

for all $h_1, \dots, h_{d+1}, x \in V$. We write $\mathrm{Poly}_{\leqslant d}(V \to \mathbb{R}/\mathbb{Z})$ for the set of non-classical polynomials of degree at most d.

A classical polynomial is a map $V \to \mathbb{F}_p$ satisfying the same property. By composing with the standard map $x \mapsto |x|/p$ we can view $\mathrm{Poly}_{\leqslant d}(V \to \mathbb{F}_p)$ as a subset of $\mathrm{Poly}_{\leqslant d}(V \to \mathbb{R}/\mathbb{Z})$.

See [7, lemma 1·7] for some properties of non-classical polynomials. We give one property below which will be used several times in this paper.

LEMMA 2·4 ([7, lemma 1·7(iii)]) *Fix a prime p and a finite-dimensional $\mathbb{F}_p$-vector space $V = \mathbb{F}_p^n$. Then $P\colon V \to \mathbb{R}/\mathbb{Z}$ is a non-classical polynomial of degree at most d if and only if it can be expressed in the form*

$$P(x_1, \dots, x_n) = \alpha + \sum_{\substack{0 \leq i_1, \dots, i_n < p,\, j \geq 0: \\ 0 < i_1 + \cdots + i_n \leq d - j(p-1)}} \frac{c_{i_1,\dots,i_n,j}|x_1|^{i_1} \cdots |x_n|^{i_n}}{p^{j+1}} \pmod 1,$$

for some $\alpha \in \mathbb{R}/\mathbb{Z}$ and coefficients $c_{i_1,\dots,i_n,j} \in \{0, \dots, p-1\}$. Furthermore, this representation is unique.

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Define $\mathbb{U}_k \subset \mathbb{R}/\mathbb{Z}$ to be $\{0, 1/p^k, \ldots, (p^k-1)/p^k\}$. As a corollary we see that in characteristic p, every non-classical polynomial of degree at most d takes values in a coset of $\mathbb{U}_{\lfloor (d-1)/(p-1) \rfloor + 1}$.

Finally we state the inverse theorem of Tao and Ziegler.

THEOREM 2·5 ([7, theorem 1·10]) *Fix a prime p, a positive integer k, and a parameter $\delta > 0$. There exists $\epsilon > 0$ such that the following holds. Let V be a finite-dimensional $\mathbb{F}_p$-vector space. Given a function $f : V \to \mathbb{C}$ satisfying $\|f\|_\infty \leq 1$ and $\|f\|_{U^k} > \delta$, there exists a non-classical polynomial $P \in \mathrm{Poly}_{\leqslant k-1}(V \to \mathbb{R}/\mathbb{Z})$ such that*

$$|\mathbb{E}_{x \in V} f(x) e^{-2\pi i P(x)}| \geq \epsilon.$$

Earlier works of Bergelson, Tao and Ziegler [2] and Tao and Ziegler [6] show this result in the high-characteristic regime $p \geq k$, with the additional guarantee that P is a classical polynomial of degree at most $k-1$.

3. *Classical polynomials for the U^{p+1}-inverse theorem*

The inverse theorem for the U^k-norm does not require non-classical polynomials when $p \geq k$ for the simple reason that every non-classical polynomial of degree at most $p-1$ is a classical polynomial of the same degree (up to a constant shift). To prove Theorem 1·1, about the U^{p+1}-inverse theorem, we use the following fact. Every non-classical polynomial of degree p agrees with a classical polynomial on a codimension 1 hyperplane (up to a constant shift).

PROPOSITION 3·1 *Let $P \in \mathrm{Poly}_{\leqslant p}(V \to \mathbb{R}/\mathbb{Z})$ be a non-classical polynomial of degree at most p. Then there exists a codimension 1 hyperplane $U \leq V$, a classical polynomial $Q \in \mathrm{Poly}_{\leqslant p}(V \to \mathbb{F}_p)$, and $\alpha \in \mathbb{R}/\mathbb{Z}$ such that $P(x) = \alpha + |Q(x)|/p$ for all $x \in U$.*

Proof. Pick an isomorphism $V \simeq \mathbb{F}_p^n$. By Lemma 2·4, we have

$$P(x_1, \ldots, x_n) = \alpha + P'(x_1, \ldots, x_n) + \frac{c_1|x_1| + \cdots + c_n|x_n|}{p^2} \pmod 1$$

for $\alpha \in \mathbb{R}/\mathbb{Z}$, a polynomial P' taking values in $\mathbb{U}_1 = \{0, 1/p, \ldots, (p-1)/p\}$, and $c_1, \ldots, c_n \in \{0, \ldots, p-1\}$. Define the codimension 1 hyperplane $U \leq V$ by $c_1 x_1 + \cdots + c_n x_n = 0$. Note that for $(x_1, \ldots, x_n) \in U$, we have $c_1|x_1| + \cdots + c_n|x_n| \equiv 0 \pmod p$. Thus $P|_U$ takes values in $\alpha + \mathbb{U}_1$. Thus by our identification of $\mathbb{U}_1$ with $\mathbb{F}_p$, $P|_U - \alpha$ is a classical polynomial of degree at most p.

Proof of Theorem 1·1. By the usual inverse theorem, Theorem 2·5, there exists $P \in \mathrm{Poly}_{\leqslant p}(V \to \mathbb{R}/\mathbb{Z})$ such that $|\mathbb{E}_{x \in V} f(x) e(-P(x))| \geq \epsilon$. By Proposition 3·1, there exists a codimension 1 hyperplane U and $\alpha \in \mathbb{R}/\mathbb{Z}$ such that $P|_U$ takes values in $\alpha + \mathbb{U}_1$, i.e., $P|_U - \alpha$ is classical. Pick an isomorphism $V \simeq \mathbb{F}_p^n$ such that U is the hyperplane defined by $x_1 = 0$. In this basis, there exists a classical polynomial $Q \in \mathrm{Poly}_{\leqslant p}(\mathbb{F}_p^n \to \mathbb{F}_p)$ and $c \in \{0, \ldots, p-1\}$ so that

$$P(x_1, \ldots, x_n) = \alpha + \frac{|Q(x_1, \ldots, x_n)|}{p} + \frac{c|x_1|}{p^2} \pmod 1.$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Thus we have

$$\begin{aligned}\epsilon &\leq |\mathbb{E}_{x\in\mathbb{F}_p^n} f(x)e(-P(x))| \\ &\leq \mathbb{E}_{x_1\in\mathbb{F}_p}\left|\mathbb{E}_{y\in\mathbb{F}_p^{n-1}} f(x_1,y)e(-P(x_1,y))\right| \\ &= \mathbb{E}_{x_1\in\mathbb{F}_p}\left|\mathbb{E}_{y\in\mathbb{F}_p^{n-1}} f(x_1,y)e_p(-Q(x_1,y))\right| \\ &\leq \left(\mathbb{E}_{x_1\in\mathbb{F}_p}\left|\mathbb{E}_{y\in\mathbb{F}_p^{n-1}} f(x_1,y)e_p(-Q(x_1,y))\right|^2\right)^{1/2}.\end{aligned}$$

By Parseval and the pigeonhole principle, there exists $a\in\mathbb{F}_p$ such that

$$\left|\mathbb{E}_{x_1\in\mathbb{F}_p} e(-ax_1)\mathbb{E}_{y\in\mathbb{F}_p^{n-1}} f(x_1,y)e_p(-Q(x_1,y))\right| \geq \epsilon/\sqrt{p}.$$

Therefore f has correlation at least $\epsilon/\sqrt{p}$ with the classical polynomial $Q(x_1,\ldots,x_n)+ax_1$.

4. *Symmetrisation techniques*

We now extend a symmetrisation technique of Alon and Beigel [1] which will be needed to prove the non-correlation property of our example. The original version of this technique uses Ramsey theory to show that if a function correlates with a bounded degree multilinear polynomial, then some restriction of coordinates correlates with a symmetric polynomial. This result was used in the previous works [3,4] on this problem.

For our application we need a result which applies to arbitrary polynomials. We show that if a function correlates with a bounded degree polynomial, then some restriction of coordinates correlates with a so-called quasisymmetric polynomial. These are a generalisation of the notion of symmetric polynomials which have found extensive use in enumerative and algebraic combinatorics.

Definition 4·1 For a prime p and a tuple $(\alpha_1,\ldots,\alpha_s)$ of positive integers satisfying $\alpha_i<p$ for all i, the *elementary quasisymmetric polynomial associated to* $(\alpha_1,\ldots,\alpha_s)$ in n variables is the polynomial $Q_\alpha:\mathbb{F}_p^n\to\mathbb{F}_p$ defined by

$$Q_\alpha(x_1,\ldots,x_n)=\sum_{1\leq i_1<\cdots<i_s\leq n}\prod_{j=1}^{s}x_{i_j}^{\alpha_j}.$$

We additionally note the total degree is $|\alpha|:=\alpha_1+\cdots+\alpha_s$.

THEOREM 4·2 *Fix a prime p and an integer $d\geq 1$. For any n, there exists $m=\omega_{p,d;n\to\infty}(1)$ such that the following holds. Let $P(x_1,\ldots,x_n)$ be a polynomial of degree at most d with coefficients in $\mathbb{F}_p$. There exists $I\subseteq[n]$ of size $|I|=m$ such that for any $y_{[n]\setminus I}\in\mathbb{F}_p^{[n]\setminus I}$, the function $P(x_I,y_{[n]\setminus I})$ (viewed as a polynomial in the x_I) can be written as a quasisymmetric polynomial of degree d plus an arbitrary polynomial of degree at most $d-1$.*

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Proof. We can uniquely express P in the form

$$P(x_1,\dots,x_n)=\sum_{s=0}^{d}\sum_{1\le i_1<\cdots<i_s\le n}\sum_{\substack{\alpha\in\{1,\dots,p-1\}^s\\ |\alpha|\le d}} c_{i_1,\dots,i_s,\alpha}\prod_{j=1}^{s}x_{i_j}^{\alpha_j},$$

where the $c_{i_1,\dots,i_s,\alpha}\in\mathbb{F}_p$ are arbitrary.

Define $\Lambda=\{\lambda\in\{0,\dots,p-1\}^d:|\lambda|=d\}$. We define a colouring of the complete d-uniform hypergraph on n vertices where the set of colours is $\mathbb{F}_p^{\Lambda}$. For an edge $\{i_1,\dots,i_d\}$ with $1\le i_1<\cdots<i_d\le n$, let the colour of this edge be given by $c_{i_1,\dots,i_d}\colon\Lambda\to\mathbb{F}_p$. We define $c_{i_1,\dots,i_d}(\lambda)=c_{j_1,\dots,j_s,\alpha}$ where α is formed by removing the 0's from the tuple λ and $(j_1,\dots,j_s)$ is formed from $(i_1,\dots,i_d)$ by removing the coordinate i_k if $\lambda_k=0$.

Applying the hypergraph Ramsey theorem, there exists a subset $I\subseteq[n]$ such that the induced subhypergraph on vertex set I is coloured monochromatically with colour $c\colon\Lambda\to\mathbb{F}_p$ and $|I|=\omega_{p,d;n\to\infty}(1)$. Unwinding the definitions, we see that

$$P(x_I,y_{[n]\setminus I})=\sum_{s=0}^{d}\sum_{\substack{\alpha\in\{1,\dots,p-1\}^s\\ |\alpha|=d}} c(\alpha,\underbrace{0,\dots,0}_{d-s\ 0\text{'s}})Q_\alpha(x_I)+\text{mixed terms}.$$

Now the mixed terms involve at least one factor of $y_{[n]\setminus I}$, so their total x_I-degree is strictly smaller than d.

5. *Non-classical polynomials are necessary*

In this section we prove Theorem 1·2, namely that non-classical polynomials are necessary in the U^{k+1}-inverse theorem when $k>p$. To do this, we use the function $f_n^{(k)}\colon\mathbb{F}_p^n\to\mathbb{R}/\mathbb{Z}$ defined by

$$f_n^{(k)}(x)=\frac{1}{p^{\ell+1}}\sum_{i=1}^{n}|x_i|^r, \tag{5·1}$$

where $k=r+(p-1)\ell$ with $\ell\ge1$ and $0<r<p$. Note that $f_n^{(k)}$ is a non-classical polynomial of degree k, so $\|e(f_n^{(k)})\|_{U^{k+1}}=1$.

In order to motivate our proof, suppose for the sake of contradiction that $f_n^{(k)}$ has correlation at least ϵ with some classical polynomial of degree at most k. By Theorem 4·2, we will be able to reduce to the situation

$$\epsilon\le\left|\mathbb{E}_{x\sim\mathbb{F}_p^n}e(f_n^{(k)}(x)+g(x)+h(x))\right|$$

where g is a homogeneous quasisymmetric polynomial of degree k and h is a classical polynomial of degree at most $k-1$. By the monotonicity of the Gowers norms (alternatively by the Gowers–Cauchy–Schwarz inequality), we deduce

$$\begin{aligned}\epsilon^{2^k}&\le\left|\mathbb{E}_x e(f_n^{(k)}(x)+g(x)+h(x))\right|^{2^k}\\&=\mathbb{E}_{x,h_1,\dots,h_k}(\partial_{h_1}\cdots\partial_{h_k}e(f_n^{(k)}+g+h))(x)\\&=\mathbb{E}_{h_1,\dots,h_k}e(\Delta_{h_1}\cdots\Delta_{h_k}(f_n^{(k)}+g)).\end{aligned}$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Since $f_n^{(k)}$ and g are polynomials of degree k, the iterated derivatives $(\Delta_{h_1}\cdots\Delta_{h_k}f_n^{(k)})(x)$ and $(\Delta_{h_1}\cdots\Delta_{h_k}g)(x)$ are constants independent of x. Furthermore, they take values in $\mathbb{U}_1$ which (with some abuse of notation) we identify with $\mathbb{F}_p$. Many results on these objects are known, including the fact that in general they are multilinear functions of $h_1,\dots,h_k$ (see [7, section 4]). For the purposes of this paper, it is sufficient to do the following explicit computation.

LEMMA 5·1 *For $k=r+(p-1)\ell$ with $\ell\geq 0$ and $0<r<p$,*

$$\iota_k(h_1,\dots,h_k):=\Delta_{h_1}\cdots\Delta_{h_k}f_n^{(k)}=(-1)^\ell r!\sum_{i=1}^{n}(h_1)_i\cdots(h_k)_i,$$

and for $\alpha=(\alpha_1,\dots,\alpha_s)$ with $\alpha_1+\cdots+\alpha_s=k$ and $0\leq\alpha_i<p$,

$$\tau_\alpha(h_1,\dots,h_k):=\Delta_{h_1}\cdots\Delta_{h_k}Q_\alpha=\sum_{\pi\in\mathfrak{S}_k}\sum_{\vec{i}}(h_1)_{i_{\pi(1)}}\cdots(h_k)_{i_{\pi(k)}},$$

where the sum is over sequences $1\leq i_1\leq\cdots\leq i_k\leq n$ that satisfy $i_{\alpha_1+\cdots+\alpha_j+1}=\cdots=i_{\alpha_1+\cdots+\alpha_j+\alpha_{j+1}}$ and $i_{\alpha_1+\cdots+\alpha_j}<i_{\alpha_1+\cdots+\alpha_j+1}$ for all j.

Proof. For classical polynomials $P,Q\colon\mathbb{F}_p^n\to\mathbb{F}_p$, of degrees d_1,d_2, the discrete Leibniz rule, $\Delta_h(PQ)=(\Delta_hP)Q+P(\Delta_hQ)+(\Delta_hP)(\Delta_hQ)$, can be easily verified. This implies the more convenient

$$\Delta_h(PQ)\equiv(\Delta_hP)Q+P(\Delta_hQ)\pmod{\mathrm{Poly}_{\leqslant d_1+d_2-2}(\mathbb{F}_p^n\to\mathbb{F}_p)}.$$

Note that taking d discrete derivatives kills $\mathrm{Poly}_{\leqslant d}(\mathbb{F}_p^n\to\mathbb{F}_p)$, so if $P\equiv Q\pmod{\mathrm{Poly}_{\leqslant d}(\mathbb{F}_p^n\to\mathbb{F}_p)}$, then $\Delta_{h_1}\cdots\Delta_{h_d}P(x)=\Delta_{h_1}\cdots\Delta_{h_d}Q(x)$.

We compute τ_α first. Define $f\in\mathrm{Poly}_{\leqslant k}(V\to\mathbb{F}_p)$ by $f(x)=x_{i_1}\cdots x_{i_k}$. By many applications of the discrete Leibniz rule, we see that

$$\Delta_{h_1}\cdots\Delta_{h_k}f(x)=\sum_{\pi\in\mathfrak{S}_k}\Delta_{h_1}(x_{i_{\pi(1)}})\cdots\Delta_{h_k}(x_{i_{\pi(k)}})=\sum_{\pi\in\mathfrak{S}_k}(h_1)_{i_{\pi(1)}}\cdots(h_k)_{i_{\pi(k)}}.$$

Extending this result by linearity gives the formula for τ_α.

Now for ι_k. For any $k\geq 1$, write $k=r+(p-1)\ell$ with $0<r<p$ and $\ell\geq 0$. Define $Q_k\in\mathrm{Poly}_{\leqslant k}(\mathbb{F}_p\to\mathbb{R}/\mathbb{Z})$ by $Q_k(x)=|x|^r/p^{\ell+1}$. By linearity, it suffices to prove that $\Delta_{h_1}\cdots\Delta_{h_k}Q_k(x)=r!(-1)^\ell h_1\cdots h_k$. We prove that $\Delta_hQ_k(x)\equiv r|h|Q_{k-1}(x)\pmod{\mathrm{Poly}_{\leqslant k-2}(\mathbb{F}_p\to\mathbb{R}/\mathbb{Z})}$ for $k\geq 2$, while obviously $\Delta_hQ_1(x)=|h|/p$. Iterating (and applying the fact that $(p-1)!\equiv -1\pmod p$) gives the desired result.

We break into two cases. First, if $r=1$ (and $\ell\geq 1$) then

$$\begin{aligned}\Delta_hQ_k(x)&=\frac{|x+h|-|x|}{p^{\ell+1}}\\&=\frac{|h|}{p^{\ell+1}}-\frac{\mathbb{1}(|x|+|h|\geq p)}{p^\ell}\\&=\frac{|h|}{p^{\ell+1}}-\sum_{c=p-|h|}^{p-1}\frac{\mathbb{1}(|x|=c)}{p^\ell}\\&=\frac{|h|}{p^{\ell+1}}+|h|\frac{|x|^{p-1}}{p^\ell}-\sum_{c=p-|h|}^{p-1}\frac{\mathbb{1}(|x|=c)+|x|^{p-1}}{p^\ell}.\end{aligned}$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Now $\mathbb{1}(|x|=c) \equiv 1-(|x|-c)^{p-1} \pmod p$, say $\mathbb{1}(|x|=c) = 1-(|x|-c)^{p-1} + pE_{c,p}(x)$ for some function $E_{c,p}$. Then we see

$$\Delta_h Q_k(x) - |h|\frac{|x|^{p-1}}{p^\ell} = \frac{|h|}{p^{\ell+1}} - \sum_{c=p-|h|}^{p-1} \frac{1-(|x|-c)^{p-1}+|x|^{p-1}}{p^\ell} - \sum_{c=p-|h|}^{p-1} \frac{E_{c,p}(x)}{p^{\ell-1}}.$$

We know that every term in this equation is a non-classical polynomial of degree at most $k-1$ except for the last term. Thus we conclude that the last term is also a non-classical polynomial of degree $k-1$. Furthermore, of the three terms on the right-hand side, the first is a constant, the second is a non-classical polynomial of degree at most $(p-1)(\ell-1)+(p-2) = k-2$ (since the $|x|^{p-1}/p^\ell$ terms cancel), and the third has degree at most $(p-1)(\ell-1) = k-p$ (since it takes values in $\mathbb{U}_{\ell-1}$). Thus the right-hand side lies in $\mathrm{Poly}_{\leqslant k-2}(\mathbb{F}_p \to \mathbb{R}/\mathbb{Z})$, proving the desired result in the $r=1$ case.

Now assume that $k = r+(p-1)\ell$ where $r \geq 2$. We compute

$$\begin{aligned}\Delta_h Q_k(x) &= \frac{|x+h|^r - |x|^r}{p^{\ell+1}} \\ &= \frac{(|x|+|h|)^r - |x|^r}{p^{\ell+1}} - \mathbb{1}(|x|+|h| \geq p)\frac{(|x|+|h|)^r - (|x|+|h|-p)^r}{p^{\ell+1}} \\ &= \frac{\sum_{i=1}^r \binom{r}{i}|h|^i|x|^{r-i}}{p^{\ell+1}} - \mathbb{1}(|x|+|h|\geq p)\left(\sum_{i=1}^r \frac{(-1)^{i-1}\binom{r}{i}(|x|+|h|)^{r-i}}{p^{\ell+1-i}}\right).\end{aligned}$$

We rewrite this as

$$\begin{aligned}\Delta_h Q_k(x) - r|h|\frac{|x|^{r-1}}{p^{\ell+1}} =& \frac{\sum_{i=2}^r \binom{r}{i}|h|^i|x|^{r-i}}{p^{\ell+1}} \\ &- \mathbb{1}(|x|+|h|\geq p)\left(\sum_{i=1}^r \frac{(-1)^{i-1}\binom{r}{i}(|x|+|h|)^{r-i}}{p^{\ell+1-i}}\right).\end{aligned}$$

We know that every term in this equation is a non-classical polynomial of degree at most $k-1$ except for the last term, implying that the last term is also a non-classical polynomial of degree $k-1$. Furthermore, of the two terms on the right-hand side, the first is a non-classical polynomial of degree at most $(p-1)\ell + r - 2 = k-2$ and the second has degree at most $(p-1)\ell = k-r$ (since it takes values in $\mathbb{U}_{\ell-1}$). Thus the right-hand side lies in $\mathrm{Poly}_{\leqslant k-2}(\mathbb{F}_p \to \mathbb{R}/\mathbb{Z})$, proving the desired result in the $r \geq 2$ case. This completes the proof.

Define the maps $I_k, T_\alpha : \left(\mathbb{F}_p^n\right)^{k-1} \to \mathbb{F}_p^n$ by the equations $\iota_k(h_1,\dots,h_k) = I_k(h_1,\dots,h_{k-1})\cdot h_k$ and $\tau_\alpha(h_1,\dots,h_k) = T_\alpha(h_1,\dots,h_{k-1})\cdot h_k$. From Lemma 5·1, clearly $I_k(h_1,\dots,h_{k-1})_i = (-1)^\ell r!(h_1)_i\cdots(h_{k-1})_i$. To continue the argument we will need to show that T_α can be expressed in a particularly convenient form.

LEMMA 5·2 *For $\alpha = (\alpha_1,\dots,\alpha_s)$ with $\alpha_1+\cdots+\alpha_s = k$ and $0<\alpha_i<p$ for all i,*

$$T_\alpha(h_1,\dots,h_{k-1})_i = \sum_{J\subseteq[k-1]} C_{i,\alpha,J}(h_{[k-1],<i}, (\tau_\beta(h_I))_{\beta,I}) \prod_{j\in J}(h_j)_i$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

for some functions $C_{i,\alpha,J}(\cdot,\cdot)$, evaluated at the tuple of $(h_j)_{i'}$ for all $j \in [k-1]$ and $i' < i$ and the tuple of $\tau_\beta(h_I)$ for all $I \subseteq [k-1]$ and $\beta = (\beta_1, \dots, \beta_t)$ with $\beta_1 + \cdots + \beta_t = |I|$ and $0 < \beta_i < p$ for all i. Furthermore,

$$C_{i,\alpha,[k-1]} = (-1)^{s-1}\alpha_1(k-1)!.$$

Proof. Fix $i \in [n]$ for the rest of the proof. We introduce some notation. We have $h_1, \dots, h_{k-1} \in \mathbb{F}_p^n$. For $I \subseteq [k-1]$, we write $h_I = (h_j)_{j\in I}$. We use

$$h_{I,<} = ((h_j)_1, \dots, (h_j)_{i-1})_{j\in I} \in (\mathbb{F}_p^{i-1})^I \quad \text{and} \quad h_{I,>} = ((h_j)_{i+1}, \dots, (h_j)_n)_{j\in I} \in (\mathbb{F}_p^{n-i})^I.$$

For $\alpha = (\alpha_1, \dots, \alpha_s)$ we write $\alpha_{<\ell} = (\alpha_1, \dots, \alpha_{\ell-1})$ and $\alpha_{>\ell} = (\alpha_{\ell+1}, \dots, \alpha_s)$. We define $\alpha_{\leqslant \ell}$ analogously. Recall that we use $|\alpha| = \alpha_1 + \cdots + \alpha_s$.

By inspection, we can write

$$T_\alpha(h_{[k-1]})_i = \sum_{\ell=1}^{s} \alpha_\ell! \sum_{\substack{I\sqcup J\sqcup K=[k-1]:\\ |I|=|\alpha_{<\ell}|,\\ |J|=\alpha_\ell-1,\\ |K|=|\alpha_{>\ell}|}} \left(\prod_{j\in J}(h_j)_i\right) \tau_{\alpha_{<\ell}}(h_{I,<})\tau_{\alpha_{>\ell}}(h_{K,>}). \tag{5·2}$$

We now remove the terms depending on $h_{[k-1],>}$. Take $\beta = (\beta_1, \dots, \beta_t)$ with $0 < \beta_i < p$ for all i and $L \subseteq [k-1]$ with $|L| = |\beta|$. We have the identity

$$\begin{aligned}\tau_\beta(h_{L,>}) = \tau_\beta(h_L) &- \sum_{\ell=1}^{t} \sum_{\substack{I\sqcup K=L:\\ |I|=|\beta_{\leqslant\ell}|,\\ |K|=|\beta_{>\ell}|}} \tau_{\beta_{\leqslant\ell}}(h_{I,<})\tau_{\beta_{>\ell}}(h_{K,>}) \\ &- \sum_{\ell=1}^{t} \beta_\ell! \sum_{\substack{I\sqcup J\sqcup K=L:\\ |I|=|\beta_{<\ell}|,\\ |J|=\beta_\ell,\\ |K|=|\beta_{>\ell}|}} \left(\prod_{j\in J}(h_j)_i\right) \tau_{\beta_{<\ell}}(h_{I,<})\tau_{\beta_{>\ell}}(h_{K,>}).\end{aligned} \tag{5·3}$$

Repeatedly applying this identity eventually puts $T_\alpha(h_{[k-1]})_i$ into the desired form. To see this, note that applying this identity to $\tau_\beta(h_{L,>})$ produces many terms of the form $\tau_{\beta_{>\ell}}(h_{K,>})$ but all of these satisfy $|\beta_{>\ell}| = |K| < |\beta| = |L|$, so we always make progress.

Finally we need to compute $C_{i,\alpha,[k-1]}$. Obviously this coefficient is a constant since the final decomposition that we produce is multilinear in the $h_1, \dots, h_{k-1}$. Furthermore, the only way to produce a term that is a multiple of $(h_1)_i \cdots (h_{k-1})_i$ is to have no factors of $\tau_{\beta_{<\ell}}(h_{I,<})$ in that term. (However, we have a choice of I, J, K in (5·2).) This means that in the initial decomposition we need to be in the $\ell = 1$ case of the sum and every time we use the identity (5·3) we need to be in the $\ell = 1$ case of the second sum. Again, in every subsequent choice although $\ell = 1$ is fixed, we have a choice of I, J, K. Tracing through all of these reductions, we see that we produce the coefficient

$$\alpha_1!\binom{k-1}{\alpha_1-1}\prod_{j=2}^{s}\left(-(\alpha_j!)\binom{k-\alpha_1-\cdots-\alpha_{j-1}}{\alpha_j}\right) = (-1)^{s-1}\alpha_1(k-1)!.$$

This proves the desired result.

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

So far we have developed the tools to, starting with the assumption of correlation with a classical polynomial, reduce to a situation in which

$$\epsilon^{2^k} \leq \mathbb{E}\left[e_p\left(\iota_k - \sum_\alpha c_\alpha \tau_\alpha\right)\right] = \mathbb{P}\left(I_k + \sum_\alpha c_\alpha T_\alpha = 0\right)$$
$$= \mathbb{P}_{h_1,\ldots,h_{k-1}\sim\mathbb{F}_p^n}\left(\forall i \in [n],\ I_k(h_1,\ldots,h_{k-1})_i + \sum_\alpha c_\alpha T_\alpha(h_1,\ldots,h_{k-1})_i = 0\right).$$

Therefore, we need a bound on the probability that a multiaffine function equals zero.

LEMMA 5·3 *Let $L\colon \mathbb{F}_p^r \to \mathbb{F}_p$ be a multiaffine function whose leading coefficient (i.e., coefficient of $x_1 \cdots x_r$) is non-zero. Then*

$$\mathbb{P}_{x_1,\ldots,x_r\sim\mathbb{F}_p}(L(x_1,\ldots,x_r)=0) \leq 1 - \left(1-\frac{1}{p}\right)^r =: 1 - c_{p,r}.$$

Proof. We prove this result by induction on r. The bound is trivially true for $r = 0$.

For $r \geq 1$, we can write

$$L(x_1,\ldots,x_r) = x_r M(x_1,\ldots,x_{r-1}) + N(x_1,\ldots,x_{r-1}),$$

where M and N are multiaffine and the leading coefficient of M is non-zero. Then for each fixed $x_1,\ldots,x_{r-1}$, there is at most 1 choice of x_r that makes L vanish unless $M(x_1,\ldots,x_r) = 0$. Then

$$\mathbb{P}_{x_1,\ldots,x_r\sim\mathbb{F}_p}(L(x_1,\ldots,x_r)\neq 0) \geq \left(1-\frac{1}{p}\right)\mathbb{P}_{x_1,\ldots,x_{r-1}\sim\mathbb{F}_p}(M(x_1,\ldots,x_{r-1})\neq 0).$$

The second term can be handled by the inductive hypothesis, completing the desired induction.

We now have the tools to prove the main theorem. The probability we are considering is the probability that n multiaffine functions vanish simultaneously. If these were independent, by the above lemma, we could bound the probability by $(1-c_{p,k})^n = o_{p,k;n\to\infty}(1)$.

In order to introduce such independence, we can take a union bound over all possible $\tau_\beta(h_I)$. Then Lemma 5·2 shows that our multiaffine forms have the following property: if we plug in values for $((h_1)_{i'},\ldots,(h_{k-1})_{i'})_{i'<i}$ and $\tau_\beta(h_I)$ for all β, I, then $T_\alpha(h_1,\ldots,h_{k-1})_i$ is multiaffine in $(h_1)_i,\ldots,(h_{k-1})_i$ with non-zero leading coefficient. Then we may reveal $((h_1)_i,\ldots,(h_{k-1})_i)$ one-by-one for $i \in [n]$, and find that the total probability is bounded by $(1-c_{p,k})^n$. As the number of possible choices in the union bound is $O_{p,k}(1)$ we will be able to prove the desired bound.

Proof of Theorem 1·2. Take $k \geq p+1$. Consider $f_n^{(k)}\colon \mathbb{F}_p^n \to \mathbb{R}/\mathbb{Z}$ defined in (5·1). Since $f_n^{(k)}$ is a non-classical polynomial of degree k, we know that $\|e(f_n^{(k)})\|_{U^{k+1}} = 1$. For a classical polynomial $P \in \mathrm{Poly}_{\leqslant k}(\mathbb{F}_p^n \to \mathbb{F}_p)$, set $\epsilon = |\mathbb{E}_x e(f_n^{(k)}(x) + |P(x)|/p)|$. We will prove that $\epsilon = o_{p,k;n\to\infty}(1)$.

By Theorem 4·2, there exists $m = \omega_{p,k;n\to\infty}(1)$ and a subset $I \subseteq [n]$ such that for all $y_{[n]\setminus I} \in \mathbb{F}_p^{[n]\setminus I}$,

$$P(x_I, y_{[n]\setminus I}) = Q(x_I) + P_{y_{[n]\setminus I}}(x_I),$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

where Q is a homogeneous quasisymmetric polynomial of degree k and $P_{y_{[n]\setminus I}}$ is a polynomial of degree at most $k-1$.

Without loss of generality, assume that $I=[m]$. Then

$$\epsilon = |\mathbb{E}_{x\sim\mathbb{F}_p^n} e(f_n^{(k)}(x)+|P(x)|/p)| \le \mathbb{E}_{y\sim\mathbb{F}_p^{n-m}}|\mathbb{E}_{x\sim\mathbb{F}_p^m} e(f_n^{(k)}(x,y)+|P(x,y)|/p)|.$$

Then by the pigeonhole principle, there exists $y\in\mathbb{F}_p^{n-m}$ such that the inner expectation is at least ϵ. Fix this choice of y for the rest of the proof. Note that $f_n^{(k)}(x,y)=f_m^{(k)}(x)+c_y$ where $c_y=f_{n-m}^{(k)}(y)\in\mathbb{R}/\mathbb{Z}$ is a constant. Thus we have

$$\epsilon \le |\mathbb{E}_{x\sim\mathbb{F}_p^m} e(f_m^{(k)}(x)+|Q(x)|/p+|P_y(x)|/p+c_y)|.$$

Note that the right-hand side is a U^1-norm. Using the monotonicity of the Gowers norms (see, e.g., [7, lemma B.1.(ii)]) we deduce

$$\begin{aligned}
\epsilon^{2^k} &\le \|e(f_m^{(k)}+|Q|/p+|P_y|/p+c_y)\|_{U^1}^{2^k}\\
&\le \|e(f_m^{(k)}+|Q|/p+|P_y|/p+c_y)\|_{U^k}^{2^k}\\
&= \mathbb{E}_{x,h_1,\dots,h_k}\partial_{h_1}\cdots\partial_{h_k} e(f_m^{(k)}+|Q|/p+|P_y|/p+c_y)(x)\\
&= \mathbb{E}_{x,h_1,\dots,h_k} e(\Delta_{h_1}\cdots\Delta_{h_k}(f_m^{(k)}+|Q|/p+|P_y|/p+c_y)(x)).
\end{aligned}$$

Taking k discrete derivatives kills (non-classical) polynomials of degree at most $k-1$ and turns those of degree k into constants. Thus the final expression is equal to

$$\mathbb{E}_{h_1,\dots,h_k} e(\Delta_{h_1}\cdots\Delta_{h_k}(f_m^{(k)}+|Q|/p)).$$

Since Q is a homogeneous quasisymmetric polynomial of degree k, it can be written as $\sum_\alpha c_\alpha Q_\alpha$ where α ranges over all tuples $(\alpha_1,\dots,\alpha_s)$ with $|\alpha|=k$ and $0<\alpha_i<p$ for all i and the $c_\alpha\in\mathbb{F}_p$ are arbitrary coefficients.

We computed $\Delta_{h_1}\cdots\Delta_{h_k}f_m^{(k)}$ and $\Delta_{h_1}\cdots\Delta_{h_k}Q_\alpha$ in Lemma 5·1. These are the k-linear forms denoted ι_k, $\tau_\alpha\colon(\mathbb{F}_p^m)^k\to\mathbb{F}_p$ respectively. Thus so far we have shown that

$$\epsilon^{2^k} \le \mathbb{E}_{h_1,\dots,h_k} e_p\left(\iota_k(h_1,\dots,h_k)+\sum_\alpha c_\alpha\tau_\alpha(h_1,\dots,h_k)\right).$$

For an arbitrary k-linear form $\sigma\colon\left(\mathbb{F}_p^m\right)^k\to\mathbb{F}_p$, there is a unique $(k-1)$-linear function $S\colon\left(\mathbb{F}_p^m\right)^{k-1}\to\mathbb{F}_p^m$ that satisfies $\sigma(h_1,\dots,h_k)=S(h_1,\dots,h_{k-1})\cdot h_k$. Furthermore, we have

$$\begin{aligned}
\mathbb{E}_{h_1,\dots,h_k} e_p(\sigma(h_1,\dots,h_k)) &= \mathbb{E}_{h_1,\dots,h_k} e_p(S(h_1,\dots,h_{k-1})\cdot h_k)\\
&= \mathbb{P}_{h_1,\dots,h_{k-1}}(S(h_1,\dots,h_{k-1})=0).
\end{aligned}$$

From this we conclude

$$\epsilon^{2^k} \le \mathbb{P}_{h_1,\dots,h_{k-1}}\left(\forall i\in[m],\ I_k(h_1,\dots,h_{k-1})_i+\sum_\alpha c_\alpha T_\alpha(h_1,\dots,h_{k-1})_i=0\right).$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

Recall that $I_k(h_1,\dots,h_{k-1})_i = (-1)^\ell r!(h_1)_i\cdots(h_{k-1})_i$ where $k = r+(p-1)\ell$ with $\ell \geq 1$ and $0 < r < p$. Note that $(-1)^\ell r! \neq 0$ in $\mathbb{F}_p$. Furthermore, Lemma 5·2 states that

$$T_\alpha(h_1,\dots,h_{k-1})_i = \sum_{J\subseteq[k-1]} C_{i,\alpha,J}(h_{[k-1],<i},(\tau_\beta(h_I))_{\beta,I})\prod_{j\in J}(h_j)_i.$$

In other words $T_\alpha(h_1,\dots,h_{k-1})_i$, viewed just as a function of $(h_1)_i,\dots,(h_{k-1})_i$ is multiaffine with coefficients given by $C_{i,\alpha,J}$. Additionally, Lemma 5·2 also gives the critical fact that the leading coefficient, $C_{i,\alpha,[k-1]}$, is equal to $(-1)^{s-1}\alpha_1(k-1)!$ for all i. Since $k \geq p+1$, we have that $C_{i,\alpha,[k-1]} = 0$ (recall that the coefficients live in $\mathbb{F}_p$).

This implies that $I_k(h_1,\dots,h_{k-1})_i + \sum_\alpha c_\alpha T_\alpha(h_1,\dots,h_{k-1})_i$, viewed just as a function of $(h_1)_i,\dots,(h_{k-1})_i$ is multiaffine with non-zero leading coefficient, say

$$I_k(h_1,\dots,h_{k-1})_i + \sum_\alpha c_\alpha T_\alpha(h_1,\dots,h_{k-1})_i = \sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(\tau_\beta(h_I))_{\beta,I})\prod_{j\in J}(h_j)_i,$$

where $C_{i,[k-1]} = (-1)^\ell r! \neq 0$ for all i.

By Lemma 5·3, if the coefficients are fixed then this function vanishes with probability at most $1-c_{p,k} < 1$. To complete the proof, we need to show that we can approximately decouple these events. Formally,

$$\begin{aligned}
\epsilon^{2^k} &\leq \mathbb{P}_{h_1,\dots,h_{k-1}}\left(\forall i\in[m],\ \sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(\tau_\beta(h_I))_{\beta,I})\prod_{j\in J}(h_j)_i = 0\right)\\
&= \sum_{(A_{\beta,I})_{\beta,I}} \mathbb{P}_{h_1,\dots,h_{k-1}}\left(\forall\beta,I,\ \tau_\beta(h_I) = A_{\beta,I}\right.\\
&\qquad\qquad \left.\cap \sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(\tau_\beta(h_I))_{\beta,I})\prod_{j\in J}(h_j)_i = 0\right)\\
&\leq \sum_{(A_{\beta,I})_{\beta,I}} \mathbb{P}_{h_1,\dots,h_{k-1}}\left(\sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(A_{\beta,I})_{\beta,I})\prod_{j\in J}(h_j)_i = 0\right).
\end{aligned}$$

The final replacement simply comes by substituting in the values $A_{\beta,I}$.

Now for each $i\in[m]$, let E_i be the event that

$$\sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(A_{\beta,I})_{\beta,I})\prod_{j\in J}(h_j)_i = 0.$$

We wish to bound

$$\mathbb{P}_{h_1,\dots,h_{k-1}}\left(E_i\ \middle|\forall i'<i,\ E_{i'}\right).$$

Since the event we are conditioning on only depends on $h_{[k-1],<i}$, the conditional distribution of $(h_1)_i,\dots,(h_{k-1})_i$ is still uniform. Thus we can upper bound the above probability by

$$\sup_{h_{[k-1],<i}} \mathbb{P}_{(h_1)_i,\dots,(h_{k-1})_i\sim\mathbb{F}_p}\left(\sum_{J\subseteq[k-1]} C_{i,J}(h_{[k-1],<i},(A_{\beta,I})_{\beta,I})\prod_{j\in J}(h_j)_i = 0\right).$$

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press

By Lemma 5·3, and the fact that $C_{i,[k-1]} = (-1)^{\ell} r! \neq 0$ always, this probability is upper-bounded by $1 - c_{p,k} < 1$. Putting everything together, we have shown that $\epsilon^{2^k} \leq O_{p,k}((1 - c_{p,k})^m)$. (The hidden constant is the number of terms in the sum over $(A_{\beta,I})_{\beta,I}$, which depends on p, k but not on m, n. It can be bounded by p^{4^k}.) We showed that $m = \omega_{p,k;n\to\infty}(1)$, implying that $\epsilon = o_{p,k;n\to\infty}(1)$.

REFERENCES

[1] N. ALON and R. BEIGEL. Lower bounds for approximations by low degree polynomials over $\mathbb{Z}/m\mathbb{Z}$. *Proceedings 16th Annual IEEE Conference on Computational Complexity* pp. 184–187.

[2] 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** (2010), 1539–1596.

[3] B. GREEN and T. TAO. The distribution of polynomials over finite fields, with applications to the Gowers norms.. *Contrib Discrete Math.* **4** (2009), 1–36.

[4] S. LOVETT, R. MESHULAM and A. SAMORODNITSKY. Inverse conjecture for the Gowers norm is false. *Theory Comput.* **7** (2011), 131–145.

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

[6] T. TAO and T. ZIEGLER. The inverse conjecture for the Gowers norm over finite fields via the correspondence principle. *Analysis & PDE* **3** (2010), 1–20.

[7] T. TAO and T. ZIEGLER. The inverse conjecture for the Gowers norm over finite fields in low characteristic. *Ann. Comb.* **16** (2012), 121–188.

https://doi.org/10.1017/S0305004121000682 Published online by Cambridge University Press