THE GREEN-TAO THEOREM

Abstract. Version 0.01b. June 27, 2004

1. Introduction

Recently Green and Tao proved that there are arbitrarily long arithmetic progressions of primes. In this note we rewrite the "ergodic theory" part of their argument in the language of analytic number theory. Much of this is simply a difference in terminology or just notation, but we do remove the need of phrasing their "generalised Koopman theorem" in terms of an algorithm. In our various propositions we indicate the place in Green-Tao that a similar result appears via, e.g., "[GT:3.1]" for Lemma 3.1 of Green-Tao.

We shall assume the "linear forms" and "correlation" conditions which Green and Tao prove via analytic number theory techniques of Goldston and Yildirim. However, we attempt to keep the error terms in these explicit, rather than using a "o(1)" notation as Green and Tao do. The integer $k \geq 3$ will be the length of the arithmetic progression we are trying to find, while N will be a large prime parameter whose size depends only on k. It is unfortunate that our inputs of the Goldston and Yildirim results (and also the theorem of Szemerédi) are not sufficiently explicit to indicate how large N should be in terms of k, though this is possible in principle and perhaps not all that difficult.

We define an **averaged sum** of a function $f : A \to \mathbf{R}$, denoted by a bullet on the sum, for a nonempty finite set A to be

$$\sum_{x\in A}^{\bullet} f(x) = \frac{1}{\#A}\sum_{x\in A} f(x).$$

An **equifibred map** from finite nonempty sets A to B is a function such that the cardinality of the inverse image of any member of B is equal to $\#A/\#B$. Note that for such a map Φ we have

$$(1) \qquad \sum_{x\in A}^{\bullet} f(\Phi(x)) = \frac{1}{\#A}\sum_{y\in B} f(y) \sum_{\substack{x\in A\\ \Phi(x)=y}} 1 = \frac{1}{\#B}\sum_{y\in B} f(y) = \sum_{x\in B}^{\bullet} f(x)$$

for any function $f : B \to \mathbf{R}$.

Our first considerations are with the linear forms condition (LFC). Let $v : \mathbf{Z}_N \to \mathbf{R}$ and $m \leq k \cdot 2^{k-1}$ and $t \leq 3k-4$. Here m is the number of linear forms and t is the number of variables. For $1 \leq i \leq m$ and $1 \leq j \leq t$ we let L_{ij} be rational numbers with numerator and denominator bounded in absolute value by k. For $1 \leq i \leq m$ we define linear forms $\psi_i(\vec{x}) = b_i + \sum_j L_{ij}x_j$ where $\vec{x} \in \mathbf{Z}_N^t$ and for each i we have $b_i \in \mathbf{Z}_N$. The rational numbers L_{ij} are interpreted as elements of $\mathbf{Z}_N$, which is feasible since N is prime and larger than k.

Condition 1.1. Suppose that for each i that the t-tuple $(L_{ij})_{j=1}^t$ is nonzero, and none of these t-tuples are multiples of one another. Then we have

$$\sum_{\vec{x}\in\mathbf{Z}_N^t}^{\bullet}\prod_{i=1}^{m} v(\psi_i(\vec{x})) = 1 + O(\mathbf{Y}_L), \tag{2}$$

where $\mathbf{Y}_L$ is a function that goes to zero as $N \to \infty$ (when k is fixed). This should be uniform in the choice of the inhomogeneous part $\vec{b}$. Throughout the paper we shall use the big-Oh notation to mean an error term with a constant of 1. Note that the $m = 1$ case with $\psi_1(x) = x$ implies that

$$\sum_{x\in\mathbf{Z}_N}^{\bullet} v(x) = 1 + O(\mathbf{Y}_L). \tag{3}$$

For the Correlation Condition we consider $m \leq 2^{k-1}$.

Condition 1.2. For each m with $1 \leq m \leq 2^{k-1}$ there is a weight function $\tau_m : \mathbf{Z}_N \to \mathbf{R}_{\geq 0}$ with

$$\sum_{x\in\mathbf{Z}_N}^{\bullet} \tau_m(x)^q \leq \mathbf{Y}_C(m, q)$$

for all $q \geq 1$ that satisfies

$$\sum_{x\in\mathbf{Z}_N}^{\bullet}\prod_{i=1}^{m} v(x + h_i) \leq \sum_{1\leq i<j\leq m}\sum \tau_m(h_i - h_j)$$

for all $\vec{h} \in \mathbf{Z}_N^m$. The only requirement on $\mathbf{Y}_C(m, q)$ is that the bound is uniform in $\vec{h}$; also, we can take $\tau_m = \tau_{2^{k-1}}$ for all m.

The choice of τ_m given by Green-Tao is essentially $\tau_m(n) = c_1(m)\prod_{p|n}\big(1 + 1/\sqrt{p}\big)^{c_2(m)}$ for some functions c_1 and c_2, with $\tau_m(0) = \exp\big(Cm\frac{\log N}{\log\log N}\big)$. Note that this is a definition of τ_m as a function from $\mathbf{Z}$, and we wish to define τ_m on $\mathbf{Z}_N$, while retaining symmetry upon negation. One way to do this appears to be to extend the product in the definition of τ_m to $p|n(N - n)$; Green and Tao do not discuss this detail in their Proposition 8.10.

Both of the above conditions can be proved for our choice of v using the work of Goldston and Yildirim, though the second should probably be provable using only the Selberg sieve. If a function satisfies both conditions, it will be called **pseudo-random**. We note the following lemma.

Lemma 1.3. *Suppose that v satisfies the LFC and the Correlation Condition. Then so does $v_2 = (1 + v)/2$, with the same error terms.*

Proof. This follows from considering (2) for v_2 and expanding out the product of $(1 + v)$ terms, and then repeatedly using the LFC for v on the resulting terms. A similar argument shows that the Correlation Condition also holds. □

We next indicate the choice of function v that will be used in the proof. We shall not, however, prove that this choice of v satisfies the LFC or the Correlation Condition (this is done in sections 8–10 of Green-Tao), and so our naming of v is largely for expository reasons.

We let W be the product of the primes up to $4(k+1)!^2$ and let $R = N^{1/k2^{k+4}}$. We define the truncated von Mangoldt function to be

$$\Lambda_R(n) = \sum_{\substack{d|n \\ d\le R}} \mu(d)\log(R/d)$$

where μ is the Möbius function. We define $v : \mathbf{Z}_N \to \mathbf{R}$ to be

$$v(n) = \begin{cases} \frac{\phi(W)}{W}\frac{\Lambda_R(Wn+1)^2}{\log R} & \text{when } N/2^k(k+4)! \le n \le 2N/2^k(k+4)!, \\ 1 & \text{otherwise.} \end{cases}$$

The work of Goldston and Yildirim as modified and extended by Green and Tao then shows that v satisfies the LFC and the Correlation Condition.

2. Setup

We shall assume Szemerédi's Theorem in the following form.

Condition 2.1. Let $\delta > 0$ and k be fixed. Suppose that $f : \mathbf{Z}_N \to [0,1]$ and that $\sum^{\bullet}_{x\in\mathbf{Z}_N} f(x) \ge \delta$. Then there is some constant $\mathbf{S}(k,\delta)$ such that for sufficiently large N (which can be made explicit in terms of k) we have

$$\sum^{\bullet}_{X\in\mathbf{Z}_N}\sum^{\bullet}_{R\in\mathbf{Z}_N}\prod_{j=1}^{k} f(X+jR) \ge \mathbf{S}(k,\delta).$$

The main idea shall be to replace the upper bound of 1 for f by the function v. We should stress that the passing from Szemerédi's Theorem to the theorem below, called a transference principle by Green and Tao, does not rely on number theoretical considerations. The following theorem is one of the main results of Green-Tao.

Theorem 2.2. *[GT:3.5] Let $\delta > 0$ and k be fixed. Let $v : \mathbf{Z}_N \to \mathbf{R}_{\ge 0}$ be k-pseudorandom Suppose that $f : \mathbf{Z}_N \to \mathbf{R}_{\ge 0}$ satisfies $0 \le f(x) \le v(x)$ for all $x \in \mathbf{Z}_N$ and that $\sum^{\bullet}_{x\in\mathbf{Z}_N} f(x) \ge \delta$. Then (for sufficiently large N) we have*

$$\sum^{\bullet}_{X\in\mathbf{Z}_N}\sum^{\bullet}_{R\in\mathbf{Z}_N}\prod_{j=1}^{k} f(X+jR) \ge 0.99\mathbf{S}(k,\delta/2).$$

The significance of the 0.99 and 1/2 is negligible; both can be made arbitrarily close to 1. We finish the introduction by indicating how this theorem allows one to prove that there are arbitrarily long arithmetic progressions of primes. We choose

$$f(x) = \begin{cases} \tilde\Lambda(x)/k2^{k+5} & \text{when } N/2^k(k+4)! \le x \le 2N/2^k(k+4)!, \\ 0 & \text{otherwise.} \end{cases}$$

Here $\tilde\Lambda(x)$ is equal to $\frac{\phi(W)}{W}\log(Wn+1)$ when $(Wn+1)$ is prime and 0 otherwise. From Dirichlet's Theorem for primes in arithmetic progressions it follows that for large N the average of f is more than half of $1/k2^{2k+9}(k+4)!$, and thus the above theorem implies that for sufficiently large N we have that

$$\sum^{\bullet}_{X\in\mathbf{Z}_N}\sum^{\bullet}_{R\in\mathbf{Z}_N}\prod_{j=1}^{k} f(X+jR) \ge 0.99\mathbf{S}\big(k, 1/k2^{2k+10}(k+4)!\big).$$

The contribution from the degenerate $R = 0$ case can be seen to be negligible for large N, as it contributes only on the order of $(\log N)^k/N$. Due to the fact that $1/2^k(k+4)! < 1/k$, the support of f implies that each of these $\mathbf{Z}_N$-progressions is an actual progression. The effect of W is to make everything in the progression congruent to 1 modulo W, but this does not matter as we still obtain progressions. This so-called "W-trick" allows us to eliminate the non-uniformity of primes in congruence classes to small moduli. We conclude that for every k there are arithmetic progressions of primes of length k; in the above notation they are given by $W(X + jR) + 1$ for $1 \le j \le k$ for various X and R.

3. Gowers uniformity norms and a von Neumann theorem

In this section we rework some results essentially due to Gowers. They involve averages of functions over multi-dimensional cubes. Let C_d be the discrete unit cube, that is, the 2^d vectors in $\mathbf{Z}^d$ whose entries are all 0 or 1. For vectors $\vec{\omega}$ and $\vec{h}$ we, as usual, denote their dot product as $\vec{\omega} \cdot \vec{h} = \sum_j \omega_j h_j$. Our first lemma tells us that that a pseudorandom function is rather close to 1 in this norm of Gowers that comes from the multi-dimensional cubes.

Lemma 3.1. *[GT:5.2] Suppose that v is k-pseudorandom. Then for $1 \le d \le k-1$ we have*

$$\left| \sum_{x \in \mathbf{Z}_N}^{\bullet} \sum_{\vec{h} \in \mathbf{Z}_N^d}^{\bullet} \prod_{\vec{\omega} \in C_d} \left[v(x + \vec{\omega} \cdot \vec{h}) - 1 \right] \right| \le 2^d \mathbf{Y}_L.$$

Proof. We expand the left side as

$$\sum_{x \in \mathbf{Z}_N}^{\bullet} \sum_{\vec{h} \in \mathbf{Z}_N^d}^{\bullet} \prod_{\vec{\omega} \in C_d} \left[v(x + \vec{\omega} \cdot \vec{h}) - 1 \right] = \sum_{A \subseteq \mathbf{2}^d} (-1)^{\#A} \sum_{x \in \mathbf{Z}_N}^{\bullet} \sum_{\vec{h} \in \mathbf{Z}_N^d}^{\bullet} \prod_{\vec{\omega} \in A} v(x + \vec{\omega} \cdot \vec{h}).$$

The inner sum can be estimated as $1 + O(\mathbf{Y}_L)$ by the LFC with the $(d+1)$ variables x and $\vec{h}$ and the $\#A$ forms given by $\left(x + \vec{\omega} \cdot \vec{h}\right)$ for $\vec{\omega} \in A$ with coefficients whose numerators and denominators are bounded by 1. Summing over $A \subseteq \mathbf{2}^d$, via the binomial theorem we get $O(2^d \mathbf{Y}_L)$. □

We are about to examine a k-dimensional average which will turn out to be equal to a 2-dimensional average over arithmetic progressions. In order to bound the k-dimensional average, we wish to apply Cauchy's inequality one variable at a time, and so we set up notation to allow us to do this in a reasonable way.

Let $\mathbf{k}$ be the set of integers from 1 to k. For a set $S \subseteq \mathbf{k}$ define the complement $\bar{S} = \mathbf{k} \backslash S$. Further define C_S to be the subset of C_k for which the jth component is always zero unless $j \in S$. Similarly define $(\mathbf{Z}_N)_S^k$ to be the subset of $\mathbf{Z}_N^k$ where the jth component is always zero unless $j \in S$, and finally define $\hat{\jmath}$ to be the complement of $\{j\}$ in $\mathbf{k}$.

For $\vec{\alpha} \in C_k$ define $T_{\vec{\alpha}} : \mathbf{Z}_N^k \times \mathbf{Z}_N^k \to \mathbf{Z}_N^k$ to map $(\vec{y}, \vec{z})$ to the vector whose jth component is y_j when $\alpha_j = 0$, and is z_j when $\alpha_j = 1$. Select a special $s \in \mathbf{k}$, and for each $j \in \mathbf{k}$ define a function $\phi_j : \mathbf{Z}_N^k \to \mathbf{Z}_N$ by

$$\phi_s(\vec{y}) = \sum_{l \ne s} y_l \quad \text{and} \quad \phi_j(\vec{y}) = \phi_s(\vec{y}) + (j - s) \sum_{l \ne s} \frac{y_l}{s - l} \text{ for } j \ne s.$$

For a fixed $\vec{y}$ the $\phi_j(\vec{y})$ form an arithmetic progression with common difference given by $\sum_{l \ne s} \frac{y_l}{s-l}$. Also, the numerators and denominators of the coefficients of $\phi_j(\vec{y})$ are all bounded by k in absolute value. Note that none of the ϕ's depends on y_s and that ϕ_j does not depend on y_j; this is the main fact our next Cauchy-Schwarz lemma will use.

For $1 \le j \le k$ let $f_j : \mathbf{Z}_N \to \mathbf{R}$ be functions. For $S \subseteq \mathbf{k}$ define

$$J_S = \sum^{\bullet}_{\vec{y}\in\mathbf{Z}_N^k} \sum^{\bullet}_{\vec{z}\in(\mathbf{Z}_N)^k_{\bar{S}}} \prod_{\vec{\omega}\in C_{\bar{S}}} \prod_{i\in S} f_i[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))] \prod_{i\in\bar{S}} \sqrt{2}v_2[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))]^{1/2},$$

and define $S_\beta = S\backslash\{\beta\}$.

Lemma 3.2. *[GT:5.4] For $1 \le j \le k$ let $f_j : \mathbf{Z}_N \to \mathbf{R}$ be functions that satisfy $|f_j(x)| \le 1 + v(x) = 2v_2(x)$ for all $x \in \mathbf{Z}_N$. Let $S \subseteq \mathbf{k}$ with $s \in S$. With the above definitions we have that*

$$|J_S|^2 \le 2^{2^{k-1}}(1+\mathbf{Y}_L)\cdot J_{S_\beta} \qquad \text{for every } \beta \in S_s.$$

Proof. Let $\beta \in S_s$. Due to the fact that ϕ_β does not depend on y_β we can factor out the terms involving it from the definition of J_S; this gives that

$$J_S = \sum^{\bullet}_{\vec{y}\in(\mathbf{Z}_N)^k_{\hat{\beta}}} \sum^{\bullet}_{\vec{z}\in(\mathbf{Z}_N)^k_{\bar{S}}} \Bigg[\prod_{\vec{\omega}\in C_{\bar{S}}} f_\beta[\phi_\beta(T_{\vec{\omega}}(\vec{y},\vec{z}))]v_2[\phi_\beta(T_{\vec{\omega}}(\vec{y},\vec{z}))]^{-1/2}/\sqrt{2}$$
$$\cdot \sum^{\bullet}_{y_\beta\in\mathbf{Z}_N} \prod_{\vec{\omega}\in C_{\bar{S}}} \prod_{i\in S_\beta} f_i[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))] \prod_{i\in\bar{S_\beta}} v_2[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))]^{1/2}\Bigg].$$

We now use the Cauchy-Schwarz inequality. We get

$$J_S^2 \le \sum^{\bullet}_{\vec{y}\in(\mathbf{Z}_N)^k_{\hat{\beta}}} \sum^{\bullet}_{\vec{z}\in(\mathbf{Z}_N)^k_{\bar{S}}} \prod_{\vec{\omega}\in C_{\bar{S}}} f_\beta[\phi_\beta(T_{\vec{\omega}}(\vec{y},\vec{z}))]^2 v_2[\phi_\beta(T_{\vec{\omega}}(\vec{y},\vec{z}))]^{-1}/2$$
$$\cdot \sum^{\bullet}_{\vec{y}\in(\mathbf{Z}_N)^k_{\hat{\beta}}} \sum^{\bullet}_{\vec{z}\in(\mathbf{Z}_N)^k_{\bar{S}}} \sum^{\bullet}_{y_\beta\in\mathbf{Z}_N} \sum^{\bullet}_{z_\beta\in\mathbf{Z}_N}$$
$$\prod_{\vec{\omega}\in C_{\bar{S}}} \prod_{i\in S_\beta} f_i[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))] f_i\big[\phi_i(T_{\vec{\omega}}(\vec{y}+\vec{\mathbf{e}}_\beta(z_\beta-y_\beta),\vec{z}))\big]\times$$
$$\times \prod_{i\in\bar{S_\beta}} v_2[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{z}))]^{1/2} v_2\big[\phi_i(T_{\vec{\omega}}(\vec{y}+\vec{\mathbf{e}}_\beta(z_\beta-y_\beta),\vec{z}))\big]^{1/2}$$

The first term can be estimated using the bound $|f_\beta(x)| \le 2v_2(x)$ for all $x \in \mathbf{Z}_N$. This gives a bound of

$$\sum^{\bullet}_{\vec{y}\in(\mathbf{Z}_N)^k_{\hat{\beta}}} \sum^{\bullet}_{\vec{z}\in(\mathbf{Z}_N)^k_{\bar{S}}} \prod_{\vec{\omega}\in C_{\bar{S}}} 2v_2[\phi_\beta(T_{\vec{\omega}}(\vec{y},\vec{z}))],$$

which can be bounded as $2^{2^{\#\bar{S}}}(1+\mathbf{Y}_L)$ using the LFC with at most $2k$ variables from $\vec{y}$ and $\vec{z}$ and at most 2^{k-1} forms from choices of $\vec{\omega}$, with coefficients whose numerator and denominator are bounded in absolute value by k. The second term, in which $\vec{\mathbf{e}}_\beta$ indicates the vector which is 1 in the βth component and 0 elsewhere, is simply equal to J_{S_β}. Indeed, we combine the sums over y_β and z_β into the sums of $\vec{y} \in \mathbf{Z}_N^k$ and $\vec{z} \in (\mathbf{Z}_N)^k_{\bar{S_\beta}}$ and note that $T_{\vec{\omega}}(\vec{y}+\vec{\mathbf{e}}_\beta(z_\beta-y_\beta),\vec{z}) = T_{\vec{\omega}+\vec{\mathbf{e}}_\beta}(\vec{y},\vec{z})$ when $\omega_\beta = 0$, so that by extending the $\vec{\omega}$ product to $C_{\bar{S_\beta}}$ we get exactly the definition of J_{S_β}. □

Our next lemma will first rewrite $J_{\mathbf{k}}$ in terms of arithmetic progressions and then use the above lemma to bound products of the f_j over arithmetic progressions by the size of f_s averaged over cubes (this is the so-called Gowers norm). Since we can do this for every s, unless each f_j is non-uniform over cubes we will obtain a good bound.

Lemma 3.3. *[GT:5.4,5.5] For $1 \le j \le k$ let $f_j : \mathbf{Z}_N \to \mathbf{R}$ be functions that satisfy $|f_j(x)| \le v(x) + 1 = 2v_2(x)$ for all $x \in \mathbf{Z}_N$. Then for every $s \in \mathbf{k}$ we have that*

$$\Big| \sum_{X \in \mathbf{Z}_N}^{\bullet} \sum_{R \in \mathbf{Z}_N}^{\bullet} \prod_{j=1}^{k} f_j(X + jR) \Big|^{2^{k-1}} \le (2^{(k-1)/2} \cdot 2^{2^{k-1}})^{2^{k-1}} \Big[\sum_{x \in \mathbf{Z}_N}^{\bullet} \sum_{\vec{h} \in \mathbf{Z}_N^d}^{\bullet} \prod_{\vec{\omega} \in C_{\hat{s}}} f_s(x + \vec{\omega} \cdot \vec{h}) + 3 \cdot 2^{2^{k-1}} \sqrt{\mathbf{Y}_L} \Big].$$

Proof. First we apply the previous lemma $(k-1)$ times. This gives us that $|J_{\mathbf{k}}|^{2^{k-1}} \le \big[2^{2^{k-1}}(1 + \mathbf{Y}_L)\big]^{2^{k-1}-1} J_{\{s\}}$. From the definition of J_S we note that

$$J_{\mathbf{k}} = \sum_{\vec{y} \in \mathbf{Z}_N^k}^{\bullet} \prod_{j=1}^{k} f_j(\phi_j(\vec{y})) = \sum_{\vec{y} \in \mathbf{Z}_N^k}^{\bullet} \prod_{j=1}^{k} f_j \Big(\sum_{l \ne s} y_l + (j - s) \sum_{l \ne s} \frac{y_l}{s - l} \Big),$$

and that the map $\Phi : \mathbf{Z}_N^k \to \mathbf{Z}_N^2$ given by

$$\Phi(\vec{y}) = \Big(\sum_{l \ne s} y_l - s \sum_{l \ne s} \frac{y_l}{s - l}, \sum_{l \ne s} \frac{y_l}{s - l} \Big) = (X, R)$$

is equifibred, and so from (1) we have

$$J_{\mathbf{k}} = \sum_{X \in \mathbf{Z}_N}^{\bullet} \sum_{R \in \mathbf{Z}_N}^{\bullet} \prod_{j=1}^{k} f_j(X + jR).$$

We still need to bound $J_{\{s\}}$. We have

$$J_{\{s\}} = \sum_{\vec{y} \in \mathbf{Z}_N^k}^{\bullet} \sum_{\vec{z} \in (\mathbf{Z}_N)_{\hat{s}}^k}^{\bullet} \prod_{\vec{\omega} \in C_{\hat{s}}} f_s\big[\phi_s(T_{\vec{\omega}}(\vec{y}, \vec{z}))\big] \prod_{i \in \mathbf{k}_s} \sqrt{2} v_2 \big[\phi_i(T_{\vec{\omega}}(\vec{y}, \vec{z}))\big]^{1/2}.$$

We can eliminate the sum over y_s, since nothing depends on it. For a fixed $\vec{y} \in \mathbf{Z}_N^k$ we expand ϕ_s and define $x = \sum_{l \ne s} y_l$ and $\vec{h} = \vec{z} - \vec{y}$ so that

$$\phi_s(T_{\vec{\omega}}(\vec{y}, \vec{z})) = \sum_{l \ne s} y_l + \vec{\omega} \cdot (\vec{z} - \vec{y}) = x + \vec{\omega} \cdot \vec{h}.$$

We have

$$J_{\{s\}} = \sum_{x \in \mathbf{Z}_N}^{\bullet} \sum_{\vec{h} \in (\mathbf{Z}_N)_{\hat{s}}^k}^{\bullet} \prod_{\vec{\omega} \in C_{\hat{s}}} f_s(x + \vec{\omega} \cdot \vec{h}) \cdot \sum_{\substack{\vec{y} \in (\mathbf{Z}_N)_{\hat{s}}^k \\ x = \sum_{l \ne s} y_l}}^{\bullet} \prod_{i \in \mathbf{k}_s} \prod_{\vec{\omega} \in C_{\hat{s}}} \sqrt{2} v_2 \big[\phi_i(T_{\vec{\omega}}(\vec{y}, \vec{y} + \vec{h})\big]^{1/2}.$$

Since ϕ_i does not depend on the ith component, we can restrict the $\vec{\omega}$-product to $C_{\hat{s},\hat{i}}$ and then remove the square root by noting that each occurrence of v appears twice, getting

$$J_{\{s\}} = \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \Big[\prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) \cdot \sum_{\substack{\vec{y}\in(\mathbf{Z}_N)^k_{\hat{s}} \\ x=\sum_{l\neq s} y_l}}^{\bullet} \prod_{i\in\mathbf{k}_s} \prod_{\vec{\omega}\in C_{\hat{s},\hat{i}}} 2v_2\big[\phi_i(T_{\vec{\omega}}(\vec{y},\vec{y}+\vec{h})\big] \Big]$$

$$= (2^{2^{k-2}})^{k-1} \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \Big[\prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) \cdot W(x,\vec{h}) \Big],$$

where we have called the innermost sum $W(x,\vec{h})$. We shall denote the variable in the above restricted sum over $\vec{y}$ by $\vec{y}_\star$. Noting that our object of interest is the above with $W(x,\vec{h})$ replaced by 1, we look to estimate

$$D = \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) \cdot \big[W(x,\vec{h})-1\big].$$

Using Cauchy-Schwarz and the fact that $|f_s| \leq 2v_2$ we get that

$$D^2 \leq \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \prod_{\vec{\omega}\in C_{\hat{s}}} 2v_2(x+\vec{\omega}\cdot\vec{h}) \cdot \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \prod_{\vec{\omega}\in C_{\hat{s}}} 2v_2(x+\vec{\omega}\cdot\vec{h}) \cdot \big[W(x,\vec{h})-1\big]^2,$$

and the first sum over x and $\vec{h}$ is bounded in the same manner as in the proof of Lemma 3.1 as $2^{2^{k-1}}(1+\mathbf{Y}_L)$. We thus wish to estimate

$$\sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} W(x,\vec{h})^q \prod_{\vec{\omega}\in C_{\hat{s}}} 2v_2(x+\vec{\omega}\cdot\vec{h})$$

for $q = 0,1,2$, showing in each case that it is equal to $2^{2^{k-1}}\big(1+O(\mathbf{Y}_L)\big)$. The $q=0$ case has already been noted in the proof of Lemma 3.1 while the $q=1,2$ cases will also follow from the LFC condition. When $q=1$, our variables are $x,\vec{h},\vec{y}_\star$ which gives $(2k-2)$ variables in $\mathbf{Z}_N$, and our forms are $(x+\vec{\omega}\cdot\vec{h})$ ranging over $\vec{\omega}\in C_{\hat{s}}$ and $\phi_i(T_{\vec{\omega}}(\vec{y},\vec{y}+\vec{h}))$, ranging over $\vec{\omega}\in C_{\hat{s},\hat{i}}$ and $i\in\mathbf{k}_s$ for a total of $2^{k-1}+(k-1)2^{k-2}$ forms, with coefficients whose numerators and denominators are bounded in absolute value by k. Similarly, when $q=2$ our variables are $x,\vec{h},\vec{y}_\star,\vec{z}_\star$ which gives $(3k-4)$ variables; our forms are $(x+\vec{\omega}\cdot\vec{h})$ ranging over $\vec{\omega}\in C_{\hat{s}}$, and $\phi_i(T_{\vec{\omega}}(\vec{y},\vec{y}+\vec{h}))$ and $\phi_i(T_{\vec{\omega}}(\vec{z},\vec{z}+\vec{h}))$ ranging over $\vec{\omega}\in C_{\hat{s},\hat{i}}$ and $i\in\mathbf{k}_s$, for a total of $2^{k-1}+2(k-1)2^{k-2}$ forms with coefficients whose numerators and denominators are bounded in absolute value by k.

So from the LFC we get that $D^2 \leq 2^{2^{k-1}}(1+\mathbf{Y}_L)\cdot 2^{2^{k-1}}(4\mathbf{Y}_L) \leq 5\cdot 2^{2^k}\mathbf{Y}_L$, and thus we have

$$J_{\{s\}} = (2^{2^{k-2}})^{k-1} \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) \Big(1+\big[W(x,\vec{h})-1\big]\Big)$$

$$\leq (2^{k-1})^{2^{k-2}} \Big[\sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in(\mathbf{Z}_N)^k_{\hat{s}}}^{\bullet} \prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) + O\big(3\cdot 2^{2^{k-1}}\sqrt{\mathbf{Y}_L}\big) \Big]$$

From this we get the desired bound

$$\Big|\sum_{X\in\mathbf{Z}_N}^{\bullet}\sum_{R\in\mathbf{Z}_N}^{\bullet}\prod_{j=1}^{k} f_j(X+jR)\Big|^{2^{k-1}} = |J_{\mathbf{k}}|^{2^{k-1}} \le \big[2^{2^{k-1}}(1+\mathbf{Y}_L)\big]^{2^{k-1}-1}|J_{\{s\}}|$$
$$\le (2^{(k-1)/2}\cdot 2^{2^{k-1}})^{2^{k-1}}\Big[\sum_{x\in\mathbf{Z}_N}^{\bullet}\sum_{\vec{h}\in\mathbf{Z}_N^d}^{\bullet}\prod_{\vec{\omega}\in C_{\hat{s}}} f_s(x+\vec{\omega}\cdot\vec{h}) + 3\cdot 2^{2^{k-1}}\sqrt{\mathbf{Y}_L}\Big].$$

□

4. Basic anti-uniform functions

Let $\{f_{\vec{\omega}}\}$ be a set indexed by $\vec{\omega}\in C_d$ of 2^d functions that map $\mathbf{Z}_N$ to $\mathbf{R}$. The **Gowers inner product** of them is defined to be

$$\langle f_{\vec{\omega}}\rangle = \sum_{x\in\mathbf{Z}_N}^{\bullet}\sum_{\vec{h}\in\mathbf{Z}_N^d}^{\bullet}\prod_{\vec{\omega}\in C_d} f_{\vec{\omega}}(x+\vec{\omega}\cdot\vec{h}).$$

The main fact about this is the Gowers-Cauchy-Schwarz inequality which states

$$|\langle f_{\vec{\omega}}\rangle|^{2^d} \le \prod_{\vec{\omega}\in C_d}\sum_{x\in\mathbf{Z}_N}^{\bullet}\sum_{\vec{h}\in\mathbf{Z}_N^d}^{\bullet}\prod_{\vec{\varpi}\in C_d} f_{\vec{\omega}}(x+\vec{\varpi}\cdot\vec{h}). \tag{4}$$

This is easily proven by working with one variable of the hypercube at a time.

We define $C_d^\star$ to be the nonzero elements of C_d. Given a function $F:\mathbf{Z}_N\to\mathbf{R}$, we define the d-dual function $F^\star:\mathbf{Z}_N\to\mathbf{R}$ as

$$F^\star(x) = \sum_{\vec{h}\in\mathbf{Z}_N^d}^{\bullet}\prod_{\vec{\omega}\in C_d^\star} F(x+\vec{\omega}\cdot\vec{h}). \tag{5}$$

We shall be exclusively interested in the $(k-1)$-dual function, and shall not incorporate this into the notation.

Lemma 4.1. *[GT:6.1] Suppose that v is k-pseudorandom and $f:\mathbf{Z}_N\to\mathbf{R}$ satisfies $|f(x)|\le v(x)+1 = 2v_2(x)$ for all $x\in\mathbf{Z}_N$. Then $|f^\star(x)|\le 2^{2^{k-1}-1}(1+\mathbf{Y}_L)\le 2^{2^{k-1}}$ for all $x\in\mathbf{Z}_N$.*

Proof. We have that

$$|f^\star(x)| = \Big|\sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet}\prod_{\vec{\omega}\in C_{k-1}^\star} f(x+\vec{\omega}\cdot\vec{h})\Big|$$
$$\le \sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet}\prod_{\vec{\omega}\in C_{k-1}^\star} 2v_2(x+\vec{\omega}\cdot\vec{h}) \le 2^{2^{k-1}-1}(1+\mathbf{Y}_L)$$

using the inhomogeneous LFC in the $(k-1)$ variables from $\vec{h}$ and the $(2^{k-1}-1)$ forms from $C_{k-1}^\star$ with coefficients bounded by 1 and all the inhomogeneous parts equal to x. □

Given a pseudorandom function v we wish to show that $v-1$ is essentially orthogonal to any continuous function of the image of any function that is bounded by $v+1$. We shall first show this for the image itself, then for polynomial functions of the image, and then pass to continuous functions in the standard manner. We also do this in a multi-variable format.

Lemma 4.2. *[GT:6.3] For $1 \le j \le J$ let $E_j : \mathbf{Z}_N \to \mathbf{R}$ be functions that satisfy the bound $|E_j(x)| \le v(x) + 1 = 2v_2(x)$ for all $x \in \mathbf{Z}_N$. Then we have that*

$$\left| \sum_{x\in\mathbf{Z}_N}^{\bullet} [v(x) - 1] \prod_{j=1}^{J} E_j^{\star}(x) \right| \le \mathbf{Y}_L^{1/2^k} (2^{2^k})^J 4^{kJ} \cdot \mathbf{Y}_C(2^{k-1}, J).$$

Note here that only Y_L depends on N, and thus for fixed k the right side can be made as small as desired by letting $N \to \infty$.

Proof. Denote by D the expression in the left-hand absolute value. By the definition of $E_j^{\star}$ this leads us to consider

$$D = \sum_{x\in\mathbf{Z}_N}^{\bullet} [v(x) - 1] \prod_{j=1}^{J} \sum_{\vec{h}^j \in Z_N^{k-1}}^{\bullet} \prod_{\vec{\omega}\in C_{k-1}^{\star}} E_j(x + \vec{\omega} \cdot \vec{h}^j).$$

We now use the standard trick of "shifted intervals" in which we make multiple changes of variables and average over them. We make the change of variables $\vec{h}^j = \vec{h} + \vec{H}^j$ for every $\vec{h} \in Z_N^{k-1}$ and then average over the $\vec{h}$ to get

$$D = \sum_{\vec{h}\in Z_N^{k-1}}^{\bullet} \sum_{x\in\mathbf{Z}_N}^{\bullet} [v(x) - 1] \prod_{j=1}^{J} \sum_{\vec{H}^j \in Z_N^{k-1}}^{\bullet} \prod_{\vec{\omega}\in C_{k-1}^{\star}} E_j(x + \vec{\omega} \cdot \vec{H}^j + \vec{\omega} \cdot \vec{h}).$$

We next expand the j-product and move the $\vec{H}^j$-sums to the outside, getting

$$D = \sum_{\overleftrightarrow{H} \in (\mathbf{Z}_N^{k-1})^J}^{\bullet} \sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet} \sum_{x\in\mathbf{Z}_N}^{\bullet} [v(x) - 1] \prod_{\vec{\omega}\in C_{k-1}^{\star}} \prod_{j=1}^{J} E_j(x + \vec{\omega} \cdot \vec{H}^j + \vec{\omega} \cdot \vec{h}),$$

where here $\overleftrightarrow{H}$ indicates the vector of length J whose components are the vectors $\vec{H}^j$. For each $\overleftrightarrow{H}$ the above sum over x and $\vec{h}$ is a Gowers inner product; for each $\vec{\omega} \in C_{k-1}^{\star}$ our function is the product over $1 \le j \le J$ of the $E_j(x + \vec{\omega} \cdot \vec{H}^j)$ and for $\vec{\omega} = \vec{0}$ the function is just $[v(x) - 1]$.

Thus by the Gowers-Cauchy-Schwarz inequality (4) we get

$$|D| \le \sum_{\overleftrightarrow{H} \in (\mathbf{Z}_N^{k-1})^J}^{\bullet} \Bigg(\sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet} \left| \prod_{\vec{\varpi}\in C_{k-1}} v(x + \vec{\varpi} \cdot \vec{h}) - 1 \right| \cdot$$
$$\cdot \prod_{\vec{\omega}\in C_{k-1}^{\star}} \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet} \prod_{\vec{\varpi}\in C_{k-1}} \prod_{j=1}^{J} \left| E_j\big((x + \vec{\omega} \cdot \vec{H}^j) + \vec{\varpi} \cdot \vec{h}\big) \right| \Bigg)^{1/2^{k-1}}$$

Lemma 3.1 bounds the first double sum in the parentheses as $2^{k-1}\mathbf{Y}_L$ through the use of the LFC. We shall now show that for every $\vec{\omega} \in C_{k-1}^{\star}$ we have

(6)
$$\sum_{\overleftrightarrow{H} \in (\mathbf{Z}_N^{k-1})^J}^{\bullet} \sum_{x\in\mathbf{Z}_N}^{\bullet} \sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}^{\bullet} \prod_{\vec{\varpi}\in C_{k-1}} \prod_{j=1}^{J} \left| E_j\big((x + \vec{\omega} \cdot \vec{H}^j) + \vec{\varpi} \cdot \vec{h}\big) \right| \le (2^{2^k})^J 4^{kJ} \mathbf{Y}_C(2^{k-1}, J),$$

and then apply Hölder's inequality. We first use the fact that $\overleftrightarrow{H} \to \vec{\omega} \cdot \overleftrightarrow{H}$ is an equifibred map from $(\mathbf{Z}_N^{k-1})^J$ to $(\mathbf{Z}_N)^J$. So by (1) the left side of (6) is

$$\sum^{\bullet}_{\overleftarrow{u} \in (\mathbf{Z}_N)^J} \sum^{\bullet}_{x \in \mathbf{Z}_N} \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \prod_{\vec{\varpi} \in C_{k-1}} \prod_{j=1}^{J} |E_j(x + u^j + \vec{\varpi} \cdot \vec{h})|$$

which factorises as

$$\sum^{\bullet}_{x \in \mathbf{Z}_N} \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \prod_{j=1}^{J} \sum^{\bullet}_{\overleftarrow{u} \in (\mathbf{Z}_N)^J} \prod_{\vec{\varpi} \in C_{k-1}} |E_j(x + u^j + \vec{h} \cdot \vec{\varpi})|.$$

We now use the fact that $|E_j(x)| \leq 2v_2(x)$ to get that this is bounded by

$$\sum^{\bullet}_{x \in \mathbf{Z}_N} \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \left(\sum^{\bullet}_{u \in \mathbf{Z}_N} \prod_{\vec{\varpi} \in C_{k-1}} 2v_2(x + u + \vec{h} \cdot \vec{\varpi}) \right)^J.$$

Next we change variables with $y = x + u$ to eliminate u, and then ignore the averaged sum over x to get the bound

$$(2^{2^{k-1}})^J \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \left(\sum^{\bullet}_{y \in \mathbf{Z}_N} \prod_{\varpi \in C_{k-1}} v_2(y + \vec{h} \cdot \vec{\varpi}) \right)^J.$$

For each $\vec{h}$ we apply the Correlation Condition to the inside average, getting that

$$\sum^{\bullet}_{y \in \mathbf{Z}_N} \prod_{\vec{\varpi} \in C_{k-1}} v_2(y + \vec{h} \cdot \vec{\varpi}) \leq \sum_{\vec{\varpi}_1, \vec{\varpi}_2 \in C_{k-1}} \sum^{\star} \tau_m(h \cdot (\vec{\varpi}_1 - \vec{\varpi}_2)),$$

where $m = 2^{k-1}$ and the star indicates that $\vec{\varpi}_1 \neq \vec{\varpi}_2$ in the double sum. So we are left to bound

$$\sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \left(\sum_{\vec{\varpi}_1, \vec{\varpi}_2 \in C_{k-1}} \sum^{\star} \tau_m(h \cdot (\vec{\varpi}_1 - \vec{\varpi}_2)) \right)^J$$
$$\leq \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} (4^{k-1})^{J-1} \sum_{\vec{\varpi}_1, \vec{\varpi}_2 \in C_{k-1}} \sum^{\star} \tau_m(h \cdot (\vec{\varpi}_1 - \vec{\varpi}_2))^J,$$

where we have used Hölder's inequality. For every distinct $\vec{\varpi}_1$ and $\vec{\varpi}_2$ the map $\vec{h} \to \vec{h} \cdot (\vec{\varpi}_1 - \vec{\varpi}_2)$ is an equifibred map from $\mathbf{Z}_N^{k-1}$ to $\mathbf{Z}_N$, so again by (1) the right side of the above is

$$(4^{k-1})^{J-1} \sum_{\vec{\varpi}_1, \vec{\varpi}_2 \in C_{k-1}} \sum^{\star} \sum^{\bullet}_{\vec{h} \in \mathbf{Z}_N^{k-1}} \tau_m(h \cdot (\vec{\varpi}_1 - \vec{\varpi}_2))^J$$
$$= (4^{k-1})^{J-1} \sum_{\vec{\varpi}_1, \vec{\varpi}_2 \in C_{k-1}} \sum^{\star} \sum^{\bullet}_{x \in \mathbf{Z}_N} \tau_m(x)^J \leq 4^{kJ} \mathbf{Y}_C(2^{k-1}, J),$$

where we used the Correlation Condition in the last step. Now we have shown (6), and thus apply Hölder's inequality to get that

$$|D|^{2^{k-1}} \leq (2^{k-1}\mathbf{Y}_L) \cdot \left((2^{2^{k-1}})^J 4^{kJ} \mathbf{Y}_C(2^{k-1}, J) \right)^{2^{k-1}-1}$$

so that

$$|D| \leq \mathbf{Y}_L^{1/2^k} (2^{2^k})^J 4^{kJ} \mathbf{Y}_C(2^{k-1}, J).$$

□

Lemma 4.3. *[GT:6.3] Let $d, K \geq 1$ be integers, and let P be a polynomial in K variables of degree no more than d in each variable. Let B be the sum of the absolute values of the coefficients of P. For $1 \leq j \leq K$ let $F_j : \mathbf{Z}_N \to \mathbf{R}$ be functions with $|F_j(x)| \leq v(x) + 1 = 2v_2(x)$ for all $x \in \mathbf{Z}_N$. Then*

$$\left| \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) - 1\big] P(\vec{F}^{\star}(x)) \right| \leq B \mathbf{Y}_L^{1/2^k} (2^{2^k})^{dK} 4^{dkK} \cdot \mathbf{Y}_C(2^{k-1}, dK).$$

Proof. By linearity we can reduce to the case where P is a monic monomial. For each of the variables z_j of P we define d functions for $1 \leq l \leq d$ by $E_{d(j-1)+l} = F_j$ if the degree of z_j in P is at least l and $E_{d(j-1)+l} = 1$ if not. Then we use previous lemma on the dK functions $\vec{E}$, getting the result. □

5. Average bounds outside exceptional sets

In this section we wish to show that if we partition $\mathbf{Z}_N$ based upon the values taken by a function bounded by $v + 1$, then the average value of v on each part of the partition is essentially bounded by 1. To achieve this result, we will have to throw out a possible small exceptional set on which the value of v might be large.

Let $f : \mathbf{Z}_N \to \mathbf{R}$ and let $\mathbf{P}$ be a partition of $\mathbf{Z}_N$. We define $f^{\bullet}_{\mathbf{P}}(x)$ to be the average value of f over the elements of $\mathbf{Z}_N$ that are in the same part $P \in \mathbf{P}$ as x; that is, we have

$$f^{\bullet}_{\mathbf{P}}(x) = \sum_{\substack{P \in \mathbf{P} \\ P \ni x}} \sum_{y \in P}^{\bullet} f(y),$$

where the first sum is just a device to obtain the part P of $\mathbf{P}$ to which x belongs. Note

$$\sum_{x \in P} f^{\bullet}_{\mathbf{P}}(x) = \sum_{x \in P} f(x) \quad \text{for } P \in \mathbf{P}. \tag{7}$$

Let $I = [0, 1)$. For every $\epsilon > 0$ and $\alpha \in I$ let $I^{\alpha}_{\epsilon}(n) = \big[\epsilon(n + \alpha), \epsilon(n + 1 + \alpha)\big)$, and note that $\bigcup_{n \in \mathbf{Z}} I^{\alpha}_{\epsilon}(n)$ always gives a partition of the real line. Given a function $f : \mathbf{Z}_N \to \mathbf{R}$, we define $\mathbf{P}^{\alpha,\epsilon}(f)$ to be the partition of $\mathbf{Z}_N$ given by the function images, that is

$$\mathbf{P}^{\alpha,\epsilon}(f) = \Big\{ f^{-1}\big(I^{\alpha}_{\epsilon}(n)\big) : n \in \mathbf{Z} \Big\}$$

as a set of sets. We note an easy lemma.

Lemma 5.1. *[GT:6.6] Let $f : \mathbf{Z}_N \to \mathbf{R}$ and $\epsilon > 0$ and $\alpha \in I$. Then*

$$\big| f(x) - f^{\bullet}_{\mathbf{P}^{\alpha,\epsilon}(f)}(x) \big| \leq \epsilon \qquad \text{for all } x \in \mathbf{Z}_N.$$

Proof. Let $P \in \mathbf{P}^{\alpha,\epsilon}(f)$ and note that for $x, y \in P$ we have that $|f(x) - f(y)| \leq \epsilon$. By averaging this over all $y \in P$ we get the result. □

We can extend this to a setting where we have K such functions $f_j : \mathbf{Z}_N \to \mathbf{R}$ for $1 \leq j \leq K$. For $\epsilon > 0$ and $\vec{\alpha} \in I^K$ we define

$$\mathbf{P}^{\vec{\alpha},\epsilon}(\vec{f}) = \Bigg\{ \bigcap_{j=1}^{K} \Big\{ f_j^{-1}\big(I^{\alpha_j}_{\epsilon}(n_j)\big) \Big\} : \vec{n} \in Z^K \Bigg\}.$$

We see that $x, y \in \mathbf{Z}_N$ are in the same partition if their images under each component function are in the same interval of length ϵ. We will eventually take

$$K = 9\lceil 2^{2^k}/\epsilon\rceil \qquad \text{and} \quad \epsilon = \frac{1}{17}\left(\frac{\mathbf{S}(k,\delta/2)}{100\cdot 2^{2^k}}\right)^{2^k}. \tag{8}$$

In our application, we shall apply the above with $\vec{f} = \vec{F}^\star$ for a function $\vec{F}$ as in the lemma of the previous section; recalling that by Lemma 4.1 the components of the image are all bounded by $2^{2^{k-1}}$ in absolute value, the fact that $N \to \infty$ while k is fixed implies that the resulting partition will not have that many parts compared to N.

Again by Lemma 4.1 we see that the image of each component function of $\vec{F}$ can be covered by $1 + 2\cdot 2^{2^{k-1}}/\epsilon$ intervals of length ϵ. This implies that the partition $\mathbf{P}^{\vec{\alpha}} = \mathbf{P}^{\vec{\alpha},\epsilon}(\vec{F}^\star)$ has at most $\left(1 + 2\cdot 2^{2^{k-1}}/\epsilon\right)^K \le (2^{2^k}/\epsilon)^K$ parts. We next define a parameter σ. We need that

$$K\sigma^{1/2} \le \epsilon, \quad \sigma \le 10^{-16}, \quad \text{and} \quad 6(2^{2^k}/\epsilon)^K\sigma^{1/8} \le \epsilon/2^{2^k}, \tag{9}$$

and simply take equality in the third of these to define σ.

We write $\mathcal{X}_S$ for the characteristic function of a set S and define $\Omega^{\vec{\alpha}} = \Omega^{\vec{\alpha},\epsilon}(\vec{F}^\star)$ to be the union of the parts P for which

$$\sum_{x\in\mathbf{Z}_N}^{\bullet}\big[v(x)+1\big]\mathcal{X}_P(x) \le \sigma^{1/8}, \tag{10}$$

so that

$$\sum_{x\in\mathbf{Z}_N}^{\bullet}\big[v(x)+1\big]\mathcal{X}_{\Omega^{\vec{\alpha}}}(x) \le (1+2\cdot 2^{2^{k-1}}/\epsilon)^K\sigma^{1/8} \le \left(\frac{2^{2^k}}{\epsilon}\right)^K\sigma^{1/8} \le \epsilon/2^{2^k}. \tag{11}$$

For $1 \le j \le K$ define

$$\Gamma_j^{\vec{\alpha}} = \Gamma_j^{\vec{\alpha},\epsilon} = \bigcup_{n\in\mathbf{Z}}\big[\epsilon(-\sigma+n+\alpha_j), \epsilon(\sigma+n+\alpha_j)\big].$$

This can be interpreted as surrounding each integer point on the real line by an interval of length 2σ, shifting by α_j, and then dilating by ϵ. Observe that for every $y \in \mathbf{Z}_N$ and $1 \le j \le K$ we have

$$\int_I \mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(y)\,d\alpha_j = 2\sigma.$$

Combined with the fact (3) that v is bounded by $1 + \mathbf{Y}_L$ on average, this implies that

$$\sum_{x\in\mathbf{Z}_N}^{\bullet}\big[v(x)+1\big]\cdot\int_{I^K}\sum_{j=1}^{K}\mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(F_j^\star(x))d\vec{\alpha} \le [2+\mathbf{Y}_L]\cdot 2K\sigma \le 6K\sigma.$$

Let $\mathbf{A} = \mathbf{A}^\epsilon(\vec{F}^\star)$ be the set of $\vec{\alpha} \in I^K$ such that

$$\sum_{x\in\mathbf{Z}_N}^{\bullet}\big[v(x)+1\big]\cdot\sum_{j=1}^{K}\mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(F_j^\star(x)) \ge K\sigma^{1/2} \tag{12}$$

Positivity implies that this set has measure not more than $6\sigma^{1/2}$.

Lemma 5.2. *[GT:6.5] Let v be k-pseudorandom. Let $K \geq 1$ be a fixed integer and $F_j : \mathbf{Z}_N \to \mathbf{R}$ be such that $|F_j(x)| \leq v(x) + 1$ for all $x \in \mathbf{Z}_N$ and $1 \leq j \leq K$. Let $\epsilon > 0$ be fixed. Then for all $\vec{\alpha} \notin \mathbf{A}$ we have*

$$v^{\bullet}_{\mathbf{P}^{\vec{\alpha},\epsilon}(\vec{F}^{\star})}(x) = v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}}(x) = 1 + O(\epsilon) \qquad \textit{for all } x \in \mathbf{Z}_N \backslash \Omega^{\vec{\alpha}}.$$

Proof. Let $P \in \mathbf{P}^{\vec{\alpha}}$ with $P \not\subseteq \Omega^{\vec{\alpha}}$. Our plan shall be to bound

$$\sum_{x \in \mathbf{Z}_N}^{\bullet} [v(x) - 1]\mathcal{X}_P(x)$$

by approximating $\mathcal{X}_P$ first by a continuous function and then by polynomials. This bound will then be used in conjunction with the defining property (10) of a set $P \not\subseteq \Omega^{\vec{\alpha}}$ to get a bound on

$$\sum_{x \in \mathbf{Z}_N}^{\bullet} v(x)\mathcal{X}_P(x) = v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}}(y) \cdot \sum_{x \in \mathbf{Z}_N}^{\bullet} \mathcal{X}_P(x) \qquad \text{for } y \in P,$$

which then will be used to bound $v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}}(y)$.

Write out

$$P = \bigcap_{j=1}^{K} (F_j^{\star})^{-1}\big(I_{\epsilon}^{\alpha_j}(n_j)\big)$$

for some $\vec{n} \in \mathbf{Z}^K$. Let $Q = Q^{\epsilon}$ be the cube given by

$$Q = \prod_{j=1}^{K} I_{\epsilon}^{\alpha_j}(n_j),$$

where we note that for $x \in P$ we have $\vec{F}^{\star}(x) \in Q$. The boundary of Q lies in the set $\Sigma^{\vec{\alpha}} = \Sigma^{\vec{\alpha},\epsilon}$ defined by

$$\Sigma^{\vec{\alpha}} = \{\vec{z} \in \mathbf{R}^K : z_j \in \Gamma_j^{\vec{\alpha}} \text{ for some } 1 \leq j \leq K.\}$$

We can thus construct a continuous function $\Phi : \mathbf{R}^K \to [0,1]$ which is equal to $\mathcal{X}_Q$ outside of $\Sigma^{\vec{\alpha}}$. We take Φ to be the product of the coordinate functions $\Phi_j(y)$ that are equal to

$$\begin{cases} 1 & \text{for } y \in [\epsilon(\sigma + n_j + \alpha_j), \epsilon(-\sigma + n_j + 1 + \alpha_j)], \\ \frac{1}{2\sigma\epsilon}\big(x - \epsilon(-\sigma + n_j + \alpha_j)\big) & \text{for } y \in [\epsilon(-\sigma + n_j + \alpha_j), \epsilon(\sigma + n_j + \alpha_j)], \\ \frac{-1}{2\sigma\epsilon}\big(x - \epsilon(\sigma + n_j + 1 + \alpha_j)\big) & \text{for } y \in [\epsilon(-\sigma + n_j + 1 + \alpha_j), \epsilon(\sigma + n_j + 1 + \alpha_j)], \\ 0 & \text{otherwise.} \end{cases}$$

So we essentially have that each coordinate function Φ_j is 1 on $I_{\epsilon}^{\alpha_j}(n_j)$ and 0 elsewhere, but of course we need to take a continuous approximation to this, whose steepness is controlled via the parameter σ.

The Weierstrass Approximation Theorem tells us that we can uniformly approximate by polynomials each Φ_j within ϵ on the compact interval $|y| \leq 2^{2^{k-1}}$, and in fact we can do this explicitly using the Bernstein polynomials. We recall how to do this. Let Ψ be a (uniformly) continuous function on the closed unit interval, and define the dth Bernstein polynomial as

$$B_d(y) = \sum_{m=0}^{d} \Psi(m/d)\binom{d}{m} y^m (1-y)^{d-m}.$$

By uniform continuity we know there is $\delta > 0$ for which $|\Psi(y) - \Psi(z)| \le \epsilon$ whenever $|y - z| \le \delta$, and Bernstein's Theorem says that the uniform bound $\big|B_d(y) - \Psi(y)\big| \le \epsilon$ holds for all $y \in I$ when $d \ge \log(2/\epsilon)/\delta^2$. Translating this back to our situation, we have $\delta = \epsilon\sigma/2^{2^k}$ and get a polynomial of degree $d = \log(2/\epsilon)(2^{2^k})^2/\epsilon^2\sigma^2$ given by

$$\tilde{\Phi}_j(y) = \sum_{m=0}^{d} \Phi_j(m/d) \binom{d}{m} \left(\frac{y}{2 \cdot 2^{2^{k-1}}} + \frac{1}{2} \right)^m \left(1 - \frac{y}{2 \cdot 2^{2^{k-1}}} - \frac{1}{2} \right)^{d-m}$$

for which $\big|\Phi_j(y) - \tilde{\Phi}_j(y)\big| \le \epsilon$ for $|y| \le 2^{2^{k-1}}$. The lth coefficient of $\tilde{\Phi}_j(y)$ is bounded by

$$\frac{1}{2^d} \sum_{m=0}^{d} \binom{d}{m} \binom{m}{l} \frac{1}{(2^{2^{k-1}})^l} \le \binom{d}{l} \frac{1}{(2^{2^{k-1}})^l} \frac{1}{2^d} \sum_{m=0}^{d} \binom{d}{m} = \binom{d}{l} \frac{1}{(2^{2^{k-1}})^l}.$$

Write $\tilde{\Phi}(\vec{z}) = \prod_j \tilde{\Phi}_j(z_j)$. We have that $\big|\Phi(\vec{z}) - \tilde{\Phi}(\vec{z})\big| \le \epsilon(1+\epsilon)^{2^{2^{k-1}}} \le 2\epsilon$ when $|z_j| \le 2^{2^{k-1}}$ for all j, where we have used the smallness of ϵ given by (8). We get that

$$\begin{aligned} \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) - 1\big] \cdot \Phi(\vec{F}^\star(x)) &= \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) - 1\big] \cdot \tilde{\Phi}(\vec{F}^\star(x)) + O(2\epsilon \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) + 1\big]) \\ &= \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) - 1\big] \cdot \tilde{\Phi}(\vec{F}^\star(x)) + O(5\epsilon), \end{aligned}$$

where the last step again follows from (3).

From our above construction the fact that $x \in P$ implies that $\vec{F}^\star(x) \in Q$ gives us the pointwise estimate

$$\mathcal{X}_P(x) = \Phi(\vec{F}^\star(x)) + O\bigg(\sum_{j=1}^{K} \mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(F_j^\star(x)) \bigg).$$

From the above definition (12) of $\mathbf{A}$, for $\vec{\alpha} \notin \mathbf{A}$ we have the estimate

$$\sum_{x \in \mathbf{Z}_N}^{\bullet} \big|v(x) - 1\big| \cdot \sum_{j=1}^{K} \mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(F_j^\star(x)) \le \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) + 1\big] \cdot \sum_{j=1}^{K} \mathcal{X}_{\Gamma_j^{\vec{\alpha}}}(F_j^\star(x)) \le K\sigma^{1/2} \le \epsilon,$$

where we used the first inequality in (9) in the last step. We have that the sum of the absolute value of the coefficients of $\tilde{\Phi}$ is bounded by

$$\prod_{j=1}^{K} \sum_{l=0}^{d} \frac{\binom{d}{m}}{(2^{2^{k-1}})^l} = (1 + 1/2^{2^{k-1}})^{dK} \le 2^{dK},$$

and so from Lemma 4.3 we have that

$$\bigg| \sum_{x \in \mathbf{Z}_N}^{\bullet} \big[v(x) - 1\big] \cdot \tilde{\Phi}(\vec{F}^\star(x)) \bigg| \le 2^{dK} \mathbf{Y}_L^{1/2^k} (2^{2^k})^{dK} 4^{dK} \mathbf{Y}_C(2^{k-1}, dK) \le \epsilon,$$

where the last inequality can be obtained by making N large, as here only $\mathbf{Y}_L$ depends on N.

So by combining the previous three estimates we get

$$\bigg| \sum_{x \in \mathbf{Z}_N}^{\bullet} [v(x) - 1] \mathcal{X}_P(x) \bigg| \le 7\epsilon.$$

Since $P \not\subseteq \Omega^{\vec{\alpha}}$ by (12) we have

$$\sum_{x \in Z_N}^{\bullet} [v(x)+1]\mathcal{X}_P(x) \geq \sigma^{1/8} \geq 1/100,$$

where in the last step we have used the second inequality in (9). This implies that

$$\left|\sum_{x \in \mathbf{Z}_N}^{\bullet} [v(x)-1]\mathcal{X}_P(x)\right| \leq 7\epsilon \leq \frac{\epsilon}{10} \sum_{x \in Z_N}^{\bullet} [v(x)+1]\mathcal{X}_P(x).$$

We now group the $v(x)$-terms to get that

$$\frac{1-\epsilon/10}{1+\epsilon/10} \sum_{x \in \mathbf{Z}_N}^{\bullet} \mathcal{X}_P(x) \leq \sum_{x \in \mathbf{Z}_N}^{\bullet} v(x)\mathcal{X}_P(x) \leq \frac{1+\epsilon/10}{1-\epsilon/10} \sum_{x \in \mathbf{Z}_N}^{\bullet} \mathcal{X}_P(x).$$

The quotient of the middle sum over the other sum is the definition of $v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}}(y)$ for $y \in P$; since this is true for all $P \in \mathbf{P}^{\vec{\alpha}}$ with $P \not\subseteq \Omega^{\vec{\alpha}}$, we get the lemma. □

6. Construction of Partitions and Exceptional Sets

Let $f : \mathbf{Z}_N \to \mathbf{R}$ satisfy $0 \leq f(x) \leq v(x)$ for all $x \in \mathbf{Z}_N$. Let K be $9\lceil 2^{2^k}/\epsilon \rceil$. For $0 \leq j \leq K$ we now inductively define partitions $\mathbf{P}_j$, sets Ω_j, and functions G_j that make up vectors of functions $\vec{F}^j$. Let $\vec{F}^j$ be the vector of functions for which $F^j_n = G_n$ for $1 \leq n \leq j$ and $F^j_n \equiv 0$ for $j < n \leq K$, so that the first j components of $\vec{F}^j$ are equal to G_1-G_j, while the other components are zero. Let $\Omega^{\vec{\alpha}}_j = \Omega^{\vec{\alpha},\epsilon}\big((\vec{F}^j)^\star\big)$ and $\mathbf{P}^{\vec{\alpha}}_j = \mathbf{P}^{\vec{\alpha},\epsilon}\big((\vec{F}^j)^\star\big)$. Since $\vec{F}^0$ is a vector of zero functions, we get that $\mathbf{P}_0 = \{\mathbf{Z}_N\}$ and Ω_0 is empty. For $1 \leq j \leq K$ let

$$G_j = \frac{1}{1+\epsilon}\big(1 - \mathcal{X}_{\Omega^{\vec{\alpha}}_{j-1}}\big)\big(f - f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}\big), \tag{13}$$

which completes our inductive definition. Note that $G_j(x)$ is bounded (in absolute value) by $\frac{v(x)+1+\epsilon}{1+\epsilon} \leq v(x)+1 = 2v_2(x)$; here we bounded $f(x) \leq v(x)$ and $f^{\bullet}_{\mathbf{P}}(x) \leq v^{\bullet}_{\mathbf{P}}(x)$ and then applied Lemma 5.2. We can note that $\Omega^{\vec{\alpha}}_{j-1} \subseteq \Omega^{\vec{\alpha}}_j$ for all j, due to the "building-up" nature of the $\vec{F}^j$. Similarly, the partition $\mathbf{P}^{\vec{\alpha}}_j$ is finer than the partition $\mathbf{P}^{\vec{\alpha}}_{j-1}$, in the sense that if $P \in \mathbf{P}^{\vec{\alpha}}_{j-1}$ then P is the union of elements of $\mathbf{P}^{\vec{\alpha}}_j$.

Lemma 6.1. *[GT:7.1] Suppose that*

$$\sum_{x \in \mathbf{Z}_N}^{\bullet} G_j(x) G^\star_j(x) \geq 7\epsilon.$$

Then for every $\vec{\alpha} \in I^K \backslash \mathbf{A}^\epsilon(\vec{F}^j)$ we have

$$\frac{1}{N} \sum_{x \in \mathbf{Z}_N \backslash \Omega^{\vec{\alpha}}_j} f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)^2 \geq \frac{1}{N} \sum_{x \in \mathbf{Z}_N \backslash \Omega^{\vec{\alpha}}_{j-1}} f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)^2 + \epsilon/2^{2^k}.$$

Proof. By the definition of G_j, we have

$$\frac{1}{N} \sum_{x \in \mathbf{Z}_N \backslash \Omega^{\vec{\alpha}}_{j-1}} \big[f(x) - f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\big] \cdot G^\star_j(x) = (1+\epsilon) \sum_{x \in \mathbf{Z}_N}^{\bullet} G_j(x) G^\star_j(x) \geq 4\sqrt{\epsilon}.$$

First we switch from $\Omega^{\vec{\alpha}}_{j-1}$ to $\Omega^{\vec{\alpha}}_{j}$ using the fact (11) that the Ω-sets are small. We can note the bound

$$\begin{aligned}
&\frac{1}{N}\Bigg|\sum_{x\in\Omega^{\vec{\alpha}}_{j}\setminus\Omega^{\vec{\alpha}}_{j-1}}\big[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\big]\cdot G^{\star}_{j}(x)\Bigg| \\
&\qquad\le 2^{2^k}\sum_{x\in\mathbf{Z}_N}{}^{\bullet}\,\mathcal{X}_{\Omega^{\vec{\alpha}}_{j}\setminus\Omega^{\vec{\alpha}}_{j-1}}(x)[v(x)+v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)] \\
&\qquad\le 2^{2^k}\sum_{x\in\mathbf{Z}_N}{}^{\bullet}\,\mathcal{X}_{\Omega^{\vec{\alpha}}_{j}}(x)[v(x)+1+\epsilon]\le(1+2\epsilon)\cdot 2^{2^k}\left(\frac{2^{2^k}}{\epsilon}\right)^{K}\sigma^{1/8}\le\epsilon\le\sqrt{\epsilon},
\end{aligned}$$

where we used the fact that $|G_j|\le 2v_2$ and so by Lemma 4.1 we can bound the dual function as $|G^{\star}_{j}(x)|\le 2^{2^{k-1}}$; the bound on the sum of v on $\Omega^{\vec{\alpha}}_{j}$ given by (11). Thus by the triangle inequality we have

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_{j}}\big[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\big]\cdot G^{\star}_{j}(x)\ge 3\sqrt{\epsilon}. \tag{14}$$

We wish to replace $f(x)$ in the left side of this by $f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)$. This is not directly possible, but we can ameliorate the problem by simultaneously considering what happens when we replace $G^{\star}_{j}$ by its average over parts of $\mathbf{P}^{\vec{\alpha}}_{j}$. Since we know from Lemma 5.1 that $G^{\star}_{j}$ and $(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}$ differ by at most ϵ, this will give us a good bound. We first show that $(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}$ is orthogonal to $(f-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}})$ in an appropriate normed space, where we need to remove the set $\Omega^{\vec{\alpha}}_{j}$ from $\mathbf{Z}_N$. To re-interpret this in our notation, we expand the natural sum that comes from the inner product over $\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_{j}$ over parts of $\mathbf{P}^{\vec{\alpha}}_{j}$ and get that

$$\begin{aligned}
&\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_{j}}\big[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)\big]\cdot(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)= \\
&\qquad=\frac{1}{N}\sum_{\substack{P\in\mathbf{P}^{\vec{\alpha}}_{j}\\ P\not\subseteq\Omega^{\vec{\alpha}}_{j}}}\sum_{x\in P}(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)\big[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)\big] \\
&\qquad=\frac{1}{N}\sum_{\substack{P\in\mathbf{P}^{\vec{\alpha}}_{j}\\ P\not\subseteq\Omega^{\vec{\alpha}}_{j}}}(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(P)\sum_{x\in P}\big[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)\big]=0,
\end{aligned}$$

where in the last steps we have used the notation $(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(P)$ for the common value of $(G^{\star}_{j})^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)$ on the set P, and then noted that the innermost sum over $x\in P$ is always zero by the fact (7) regarding $f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j}}(x)$.

We now split $\left(f - f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}\right)$ in the left side of (14) by $f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}$ and use the result of the previous paragraph to get

$$\begin{aligned}
&\frac{1}{N}\sum^{\bullet}_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]\cdot G^{\star}_j(x)\\
&\quad=\frac{1}{N}\sum^{\bullet}_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]\cdot G^{\star}_j(x)+\frac{1}{N}\sum^{\bullet}_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]\cdot G^{\star}_j(x)\\
&\quad=\frac{1}{N}\sum^{\bullet}_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]\cdot\left[G^{\star}_j(x)-(G^{\star}_j)^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]+\\
&\qquad\qquad+\frac{1}{N}\sum^{\bullet}_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]\cdot G^{\star}_j(x)
\end{aligned}$$

From Lemma 5.1 we have $\left|G^{\star}_j(x)-(G^{\star}_j)^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right|\le\epsilon$ for all $x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j$ and by using the fact that $|f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)|\le v(x)+v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)$ for all $x\in\mathbf{Z}_N$ in conjunction with (3) and Lemma 5.2 we see that the first term is bounded by

$$\begin{aligned}
&\frac{1}{N}\left|\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]\cdot\left[G^{\star}_j(x)-(G^{\star}_j)^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]\right|\\
&\qquad\le\frac{\epsilon}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[v(x)+v^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)\right]\le 3\epsilon\le\sqrt{epsilon}.
\end{aligned}$$

So again by the triangle inequality from this and (14) we obtain

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]\cdot G^{\star}_j(x)\ge 2\sqrt{\epsilon}.$$

By using the Cauchy-Schwarz inequality and our bound from Lemma 4.1 that $|G^{\star}_j(x)|\le 2^{2^{k-1}}$ for all $x\in\mathbf{Z}_N$ we get that

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]^2\ge 4\epsilon/2^{2^k}. \tag{15}$$

By expanding the square of the left side we note that

$$\begin{aligned}
&\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right]^2\\
&\qquad=\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)^2-\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)^2-\\
&\qquad\qquad-2\sum_{x\in\mathbf{Z}_N\setminus\Omega^{\vec{\alpha}}_j}f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\left[f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_j}(x)-f^{\bullet}_{\mathbf{P}^{\vec{\alpha}}_{j-1}}(x)\right].
\end{aligned}\tag{16}$$

We proceed to estimate the third term on the right. We split the sum over $\mathbf{Z}_N\backslash\Omega_j^{\vec{\alpha}}$ into the difference of sums over $\mathbf{Z}_N\backslash\Omega_{j-1}^{\vec{\alpha}}$ and $\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}$, and expand these respectively in terms of the parts of the partitions $\mathbf{P}_{j-1}^{\vec{\alpha}}$ and $\mathbf{P}_j^{\vec{\alpha}}$. This gives us that

$$\begin{aligned}
\sum_{x\in\mathbf{Z}_N\backslash\Omega_j^{\vec{\alpha}}} & f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big] \\
&= \sum_{\substack{P\in\mathbf{P}_{j-1}^{\vec{\alpha}}\\ P\not\subseteq\Omega_{j-1}^{\vec{\alpha}}}} \sum_{x\in P} f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]- \\
&\qquad - \sum_{\substack{P\in\mathbf{P}_j^{\vec{\alpha}}\\ P\subseteq\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}}} \sum_{x\in P} f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big] \\
&= \sum_{\substack{P\in\mathbf{P}_{j-1}^{\vec{\alpha}}\\ P\not\subseteq\Omega_{j-1}^{\vec{\alpha}}}} f_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(P) \sum_{x\in P} \big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]- \\
&\qquad - \sum_{\substack{P\in\mathbf{P}_j^{\vec{\alpha}}\\ P\subseteq\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}}} f_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(P) \sum_{x\in P} \big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big],
\end{aligned}$$

where in the last step we have, as before, written $f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(P)$ for the common value of $f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}$ on the set P.

We can now use (7) replace $\sum_{x\in P} f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)$ by $\sum_{x\in P} f(x)$ in the both inner sums and similarly with $\sum_{x\in P} f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)$ in the first inner sum, and so get

$$\begin{aligned}
\Bigg| \sum_{x\in\mathbf{Z}_N\backslash\Omega_j^{\vec{\alpha}}} & f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]\Bigg| \\
&= \Bigg|0 - \sum_{\substack{P\in\mathbf{P}_j^{\vec{\alpha}}\\ P\subseteq\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}}} f_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(P)\sum_{x\in P}\big[f(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]\Bigg| \\
&= \Bigg| \sum_{x\in\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}} f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[f(x)-f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]\Bigg| \\
&\leq \Bigg(\sum_{x\in\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}} v^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big[v(x)+v^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)\big]\Bigg) \\
&\leq \sum_{x\in\Omega_j^{\vec{\alpha}}\backslash\Omega_{j-1}^{\vec{\alpha}}} [1+\epsilon]\big[v(x)+1+\epsilon\big] \leq 6\bigg(\frac{2^{2^k}}{\epsilon}\bigg)^K \sigma^{1/8} \leq \epsilon/2^{2^k}
\end{aligned}$$

again using Lemma 5.2 and (11) and also the third bound on σ given in (9). So by using (15) and (16) we get that

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\backslash\Omega_j^{\vec{\alpha}}} f^\bullet_{\mathbf{P}_j^{\vec{\alpha}}}(x)^2 - \frac{1}{N}\sum_{x\in\mathbf{Z}_N\backslash\Omega_j^{\vec{\alpha}}} f^\bullet_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)^2 \geq 2\epsilon/2^{2^k}.$$

Our last step is to replace $\Omega_j^{\vec{\alpha}}$ by $\Omega_{j-1}^{\vec{\alpha}}$ in the second sum, and so we estimate

$$\frac{1}{N}\sum_{x\in\Omega_j^{\vec{\alpha}}\setminus\Omega_{j-1}^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)^2$$

$$\leq \frac{1}{N}\sum_{x\in\Omega_j^{\vec{\alpha}}\setminus\Omega_{j-1}^{\vec{\alpha}}} v^{\bullet}_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)^2 \leq \frac{1}{N}\sum_{x\in\Omega_j^{\vec{\alpha}}}(1+\epsilon)^2 \leq 2\left(\frac{2^{2^k}}{\epsilon}\right)^K \sigma^{1/8} \leq \epsilon/2^{2^k}.$$

where in the last step we used (11). From the previous two displays we conclude that

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega_j^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_j^{\vec{\alpha}}}(x)^2 \geq \frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega_{j-1}^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)^2 + \epsilon/2^{2^k}.$$

□

Lemma 6.2. *[GT:7.1] Let $\vec{\alpha} \in I^K\setminus\mathbf{A}$ where $\mathbf{A} = \bigcup_{j=1}^K \mathbf{A}^{\epsilon}(\vec{F}^j)$. Then there is some j with $1 \leq j \leq K$ and*

$$\sum_{x\in\mathbf{Z}_N}^{\bullet} G_j(x)G_j^{\star}(x) \leq 4\sqrt{\epsilon}.$$

Proof. Suppose not. Then by the previous, for all $1 \leq j \leq K$ we have

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega_j^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_j^{\vec{\alpha}}}(x)^2 \geq \frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega_{j-1}^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_{j-1}^{\vec{\alpha}}}(x)^2 + \epsilon/2^{2^k}.$$

Adding these together for all j from 1 to K gives

$$\frac{1}{N}\sum_{x\in\mathbf{Z}_N\setminus\Omega_K^{\vec{\alpha}}} f^{\bullet}_{\mathbf{P}_K^{\vec{\alpha}}}(x)^2 \geq \frac{1}{N}\sum_{x\in\mathbf{Z}_N} f^{\bullet}_{\mathbf{P}_0^{\vec{\alpha}}}(x)^2 + K\epsilon/2^{2^k} \geq 2,$$

where we have used the definition of K given by (8). This contradicts the pointwise bound from Lemma 5.2 that

$$0 \leq f^{\bullet}_{\mathbf{P}_K^{\vec{\alpha}}}(x) \leq v^{\bullet}_{\mathbf{P}_K^{\vec{\alpha}}}(x) \leq 1+\epsilon \leq 1.1 \quad \text{for } x \in \mathbf{Z}_N\setminus\Omega_K^{\vec{\alpha}}.$$

□

Corollary 6.3. *Let v be k-pseudorandom and $f : \mathbf{Z}_N \to \mathbf{R}$ satisfy $0 \leq f(x) \leq v(x)$ for all $x \in \mathbf{Z}_N$. Then there exists a partition $\mathbf{P}$ of $\mathbf{Z}_N$ and an exceptional set Ω that is the union of various parts of $\mathbf{P}$ such that*

$$\sum_{x\in\mathbf{Z}_N}^{\bullet} v(x)\mathcal{X}_{\Omega}(x) \leq \epsilon, \quad \max_{x\in\mathbf{Z}_N\setminus\Omega} v^{\bullet}_{\mathbf{P}}(x) = 1 + O(\epsilon),$$

and

$$\left(\frac{1}{1+\epsilon}\right)^{2^{k-1}} \sum_{x\in\mathbf{Z}_N}\sum_{\vec{h}\in\mathbf{Z}_N^{k-1}}\prod_{\vec{\omega}\in C_{k-1}}(1-\mathcal{X}_{\Omega}(x+\vec{\omega}\cdot\vec{h}))\big(f(x+\vec{\omega}\cdot\vec{h})-f^{\bullet}_{\mathbf{P}}(x+\vec{\omega}\cdot\vec{h})\big) \leq 4\sqrt{\epsilon}.$$

Proof. From the above, it follows immediately that there is some j with $1 \leq j \leq K$ and some $\vec{\alpha} \in I^K$ such that $\mathbf{P}_j^{\vec{\alpha}}$ is the desired partition and $\Omega_j^{\vec{\alpha}}$ is the desired set. We have that the size of $\mathbf{A}$ in the previous lemma is at most $6K\sigma^{1/2}$, and so there is some choice of $\vec{\alpha} \in I^K$ and some j with $1 \leq j \leq K$ such that $\mathbf{P}_j^{\vec{\alpha}}$ is the desired partition and $\Omega_j^{\vec{\alpha}}$ is the desired set. Note that the first bound is simply a restating of (11), the second is Lemma 5.2, and the third is the result of the previous lemma with the definitions (13) of G_j and (5) of $G_j^\star$ expanded. $\square$

7. Proof of Theorem 2.2

We now prove [GT:3.5], which is Theorem 2.2 here. Let f satisfy $0 \le f(x) \le v(x)$ for all $x \in \mathbf{Z}_N$ with $\sum^\bullet_{x\in\mathbf{Z}_N} f(x) \ge \delta = 1/k2^{2k+9}(k+4)!.$ and $\mathbf{P}$ and Ω be as in the above lemma. Define

$$g_U = \frac{1}{1+\epsilon}(1-\mathcal{X}_\Omega)(f - f^\bullet_{\mathbf{P}}) \qquad \text{and} \quad g_V = \frac{1}{1+\epsilon}(1-\mathcal{X}_\Omega)(f^\bullet_{\mathbf{P}}).$$

We have

$$\begin{aligned}\sum^\bullet_{x\in\mathbf{Z}_N} g_V(x) &= \frac{1}{N}\frac{1}{1+\epsilon}\sum_{x\in\mathbf{Z}_N\setminus\Omega} f^\bullet_{\mathbf{P}}(x) = \frac{1}{N}\frac{1}{1+\epsilon}\sum_{x\in\mathbf{Z}_N\setminus\Omega} f(x)\\ &\ge \frac{1}{1+\epsilon}\sum^\bullet_{x\in\mathbf{Z}_N} f(x) - \frac{1}{N}\sum_{x\in\Omega} v(x) \ge \frac{\delta}{1+\epsilon} - \epsilon \ge \delta/2,\end{aligned}$$

where the second equality uses (7) and the last inequalities use (11) and then the simplistic bound $\delta \ge \frac{2\epsilon(1+\epsilon)}{1-2\epsilon}$, which readily follows from the above choice of δ and the choice of ϵ in (8). [This is specific to the choice of δ in the application, though in general ϵ can simply be taken sufficiently small so that this condition is met.]

We next note from Lemma 5.2 that $0 \le g_V(x) \le 1$ for all $x \in \mathbf{Z}_N$, and apply Szemerédi's Theorem (Condition 2.1) to get

$$\sum^\bullet_{X\in\mathbf{Z}_N}\sum^\bullet_{R\in\mathbf{Z}_N}\prod_{j=1}^k g_V(X+jR) \ge \mathbf{S}(k,\delta/2).$$

We are now going to apply Lemma 3.3 to the situation where all the f_j-functions are equal to g_U or g_V, with at least one equal to g_U; as before we have $|g_U(x)| \le v(x)+1$. Since we have that $\sum^\bullet_{x\in\mathbf{Z}_N} g_U(x)g_U^\star(x) \le 4\sqrt{\epsilon}$ from the above corollary, this gives us that

$$\begin{aligned}\sum^\bullet_{X\in\mathbf{Z}_N}\sum^\bullet_{R\in\mathbf{Z}_N}\prod_{j=1}^k f_j(X+jR) &\le 2^{(k-1)/2}\cdot 2^{2^{k-1}}\left[4\sqrt{\epsilon} + 3\cdot 2^{2^{k-1}}\sqrt{Y_L}\right]^{1/2^{k-1}}\\ &\le 2^{(k-1)/2}\cdot 2^{2^{k-1}}(17\epsilon)^{1/2^k}.\end{aligned}$$

Adding up all the 2^k ways of choosing the f_j as either g_U or g_V we get

$$\begin{aligned}\sum^\bullet_{X\in\mathbf{Z}_N}\sum^\bullet_{R\in\mathbf{Z}_N}\prod_{j=1}^k &[g_U(X+jR) + g_V(X+jR)]\\ &\ge \mathbf{S}(k,\delta/2) - 2^{(k-1)/2}\cdot 2^{2^{k-1}}\cdot(2^k-1)\cdot(17\epsilon)^{1/2^k}\\ &\ge \mathbf{S}(k,\delta/2) - 2^{2^k}\cdot(17\epsilon)^{1/2^k} \ge 0.99\mathbf{S}(k,\delta/2),\end{aligned}$$

with the last step following by the definition of ϵ in (8). Finally, by using the fact that $0 \le g_U + g_V = (1-\mathcal{X}_\Omega)f \le f$ we get the statement of Theorem 2.2, that

$$\sum^\bullet_{X\in\mathbf{Z}_N}\sum^\bullet_{R\in\mathbf{Z}_N}\prod_{j=1}^k f(X+jR) \ge 0.99\mathbf{S}(k,\delta/2).$$