Next, define the iterated convolutions $f^{(n)}$ for $n = 1, 2, \ldots$ inductively by $f^{(1)} := f$ and $f^{(n+1)} := f * f^{(n)}$, and show that $\lim_{n\to\infty} f^{(n)} = \frac{1}{\mathbf{P}_Z(H)} 1_H$. What can happen when the hypothesis $f(0) \neq 0$ is dropped?

4.2.7 Use Fourier-analytic methods to give another proof of Corollary 2.10.

4.2.8 Use Fourier-analytic methods to give another proof of Proposition 2.7.

4.2.9 Let f be a random variable which is not identically zero. By using (4.2) and (4.20), establish the *uncertainty principle*

$$|\mathrm{supp}(f)||\mathrm{supp}(\hat{f})| \geq |Z|. \tag{4.21}$$

Prove that equality occurs if and only if $f(x) = ce(\xi \cdot x)1_{H+x_0}(x)$ for some complex number $c \in \mathbf{C}$, some subgroup H of Z, and some $\xi, x_0 \in Z$. This inequality can be improved for certain groups Z: see Theorem 9.52.

4.2.10 Let $f \in \mathbf{C}^Z$ be normalized so that $\|f\|^2_{L^2(Z)} = \sum_{\xi\in Z} |\hat{f}(\xi)|^2 = 1$. By differentiating the Hausdorff–Young inequality in p, establish the *entropy uncertainty principle*

$$\mathbf{E}_{x\in Z} |f(x)|^2 \log \frac{1}{|f(x)|^2} + \sum_{\xi\in Z} |\hat{f}(\xi)|^2 \log \frac{1}{|\hat{f}(\xi)|^2} \geq 0,$$

where we adopt the convention that $0 \log \frac{1}{0} = 0$. (Hint: differentiate the Hausdorff–Young inequality in p at $p = 2$, using the fact that equality holds at that endpoint.) Using Jensen's inequality, show that this inequality implies (4.21).

4.3 Linear bias

One common way to apply the Fourier transform to the theory of sum sets or to arithmetic progressions is to introduce the notion of *Fourier bias* of that set (also known as *linear bias* or *pseudo-randomness*). Roughly speaking, this notion separates sets into two extremes, ones which are highly uniform (and behave like random sets, especially with regard to iterated sum sets), and ones which are highly non-uniform (and behave like arithmetic progressions).

Definition 4.12 (Fourier bias) Let Z be a finite additive group. If A is a subset of Z, we define the *Fourier bias* $\|A\|_u$ of the set A to be the quantity

$$\|A\|_u := \sup_{\xi\in Z\backslash\{0\}} |\hat{1}_A(\xi)|.$$

This quantity is always non-negative, with $\|A\|_u = 0$ if and only if A is equal to Z or the empty set (Exercise 4.3.1). It obeys the symmetries $\|A\|_u = \|-A\|_u = \|A + h\|_u = \|Z\backslash A\|_u$ for any $h \in Z$ (Exercise 4.3.2). We warn that this quantity

is not monotone: $A \subseteq B$ does not imply $\|A\|_u \leq \|B\|_u$. However, the Fourier bias does obey a triangle inequality (Exercise 4.3.3). The Fourier bias $\|A\|_u$ can be as large as the density $\mathbf{P}_Z(A)$, but is usually smaller (Exercise 4.3.4). Sets A with Fourier bias less than α are sometimes called *α-uniform* or *α-pseudo-random*; sets with small Fourier bias are called *linearly uniform*, *Gowers uniform of order 1*, or *pseudo-random*.

The connection between Fourier bias and sum sets can be described by the following lemma.

Lemma 4.13 (Uniformity implies large sum sets) *Let $n \geq 3$, and let $A_1, \ldots, A_n$ be additive sets in a finite additive group Z. Then for any $x \in Z$ we have*

$$\left| \frac{1}{|Z|^{n-1}} |\{(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n : x = a_1 + \cdots + a_n\}| - \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) \right|$$
$$\leq \|A_1\|_u \cdots \|A_{n-2}\|_u \mathbf{P}_Z(A_{n-1})^{1/2} \mathbf{P}_Z(A_n)^{1/2}.$$

In particular, if we have

$$\|A_1\|_u \cdots \|A_{n-2}\|_u < \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_{n-2}) \mathbf{P}_Z(A_{n-1})^{1/2} \mathbf{P}_Z(A_n)^{1/2}$$

then $A_1 + \cdots + A_n = Z$.

Of course, a similar result is true if we permute the $A_1, \ldots, A_n$. Note that the quantity $\mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n)$ is the quantity one would expect for $\frac{1}{|Z|^{n-1}} |\{(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n : x = a_1 + \cdots + a_n\}|$ if the events $a_1 \in A_1, \ldots, a_n \in A_n$ were jointly independent conditioning on $x = a_1 + \cdots + a_n$. This may help explain why uniformity is sometimes referred to as pseudo-randomness.

Proof By (4.9), the function $1_{A_1} * \cdots * 1_{A_n}$ has Fourier transform $\widehat{1_{A_1}} \cdots \widehat{1_{A_n}}$. Applying the Fourier inversion formula (4.4), (4.15), the Cauchy–Schwarz inequality and (4.16) we thus see that

$$\begin{aligned}
1_{A_1} * \cdots * 1_{A_n}(x) &= \mathrm{Re} 1_{A_1} * \cdots * 1_{A_n}(x) \\
&= \mathrm{Re} \sum_{\xi \in Z} \widehat{1_{A_1}}(\xi) \cdots \widehat{1_{A_n}}(\xi) e(x \cdot \xi) \\
&\geq \widehat{1_{A_1}}(0) \cdots \widehat{1_{A_n}}(0) - \sum_{\xi \in Z \backslash \{0\}} |\widehat{1_{A_1}}(\xi)| \cdots |\widehat{1_{A_n}}(\xi)| \\
&\geq \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \sum_{\xi \in Z} |\widehat{1_{A_{n-1}}}(\xi)| |\widehat{1_{A_n}}(\xi)| \\
&\geq \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \|\widehat{1_{A_{n-1}}}\|_{l^2(Z)} \|\widehat{1_{A_n}}(\xi)\|_{l^2(Z)} \\
&= \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) - \|A_1\|_u \cdots \|A_{n-2}\|_u \mathbf{P}_Z(A_{n-1})^{1/2} \mathbf{P}_Z(A_n)^{1/2}.
\end{aligned}$$

A similar argument gives

$$1_{A_1} * \cdots * 1_{A_n}(x) \leq \mathbf{P}_Z(A_1) \cdots \mathbf{P}_Z(A_n) + \|A_1\|_u \cdots \|A_{n-2}\|_u \mathbf{P}_Z(A_{n-1})^{1/2} \mathbf{P}_Z(A_n)^{1/2}.$$

Since by definition of convolution

$$1_{A_1} * \cdots * 1_{A_n}(x) = |Z|^{1-n} |\{(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n : x = a_1 + \cdots + a_n\}|,$$

and the lemma follows. □

We now give an application of the above machinery to the finite field Waring problem. We first need a standard lemma.

Lemma 4.14 (Gauss sum estimate) *Let F be a finite field of odd order, and let $A := F\hat{}2 = \{a^2 : a \in F\}$ be the set of squares in F. Then $\|A\|_u \leq \frac{1}{2|F|} + \frac{1}{2|F|^{1/2}}$.*

Proof Let $\xi \in F \backslash 0$. Since every non-zero element in A has exactly two representations of the form a^2, we have

$$\hat{1}_A(\xi) = \frac{1}{|F|} \sum_{x \in A} e(-\xi \cdot x) = \frac{1}{2|F|} + \frac{1}{2|F|} \sum_{a \in F} e(-\xi \cdot a^2).$$

On the other hand, we may square

$$\begin{aligned} \left| \sum_{a \in F} e(-\xi \cdot a^2) \right|^2 = \left| \sum_{a \in F} e(\xi \cdot a^2) \right|^2 &= \sum_{a,b \in F} e(\xi \cdot (a^2 - b^2)) \\ &= \sum_{a,h \in F} e(\xi \cdot (a^2 - (a+h)^2)) \\ &= \sum_{h \in F} e(-\xi \cdot h^2) \sum_{a \in F} e(\xi \cdot 2ah). \end{aligned}$$

If $h \neq 0$, then $2h \neq 0$, and $\sum_{a \in F} e(\xi \cdot 2ah) = \sum_{c \in F} e(\xi \cdot c) = 0$ thanks to Lemma 4.5. On the other hand, if $h = 0$, then $\sum_{a \in F} e(\xi \cdot 2ah) = |F|$. We conclude that $|\sum_{a \in F} e(\xi \cdot a^2)|^2 = |F|$, and the claim follows. □

By combining this lemma with Lemma 4.13, one immediately obtains

Corollary 4.15 *Let F be a finite field of odd order, and let $A = F\hat{}2$ be the set of squares in F. Then $kA = F$ for all $k \geq 3$. Indeed, for any $x \in F$, the number of representations of x as a sum $x = a_1 + \cdots + a_k$ with $a_1, \ldots, a_k \in F$ is $(2^{1-k} + O_k(|F|^{-(k-2)/2}))|F|^{k-1}$.*

We leave the verification of this corollary as an exercise. It shows that the sum sets kA are more or less uniformly distributed for $k \geq 3$. Note that when $k = 2$, one can still prove that $2A = F$, but the sum sets can be quite irregular; for instance, if -1 is not a square in F, then 0 only has one representation as the sum of two elements in F.

We now present a lemma which asserts, roughly speaking, that if B is a randomly-chosen subset of A, then $\|B\|_u$ is approximately equal to $\frac{|B|}{|A|}\|A\|_u$; thus the Fourier bias decreases proportionally when passing to random subsets.

Lemma 4.16 *[149] Let A be an additive set in a finite additive group Z, and let $0 < \tau \leq 1$. Let B be a random subset of A defined by letting the events $a \in B$ be independent with probability τ. Then for any $\lambda > 0$ we have*

$$\mathbf{P}(|\|B\|_u - \tau\|A\|_u| \geq \lambda\sigma) \leq 4|Z| \max\left(e^{-\lambda^2/8}, e^{-\lambda\sigma/2\sqrt{2}}\right),$$

where $\sigma^2 := |A|\tau(1-\tau)/|Z|^2$.

The lemma is an easy consequence of Chernoff's inequality and is left as an exercise. Applying it with $\lambda = C\log^{1/2}|Z|$ for some large C, and assuming $|A|\tau(1-\tau) \gg \log|Z|$, we see in particular that

$$\mathbf{P}\big(\|B\|_u = \tau\|A\|_u + O\big(\sigma\log^{1/2}|Z|\big)\big) = 1 - O(|Z|^{-100})$$

(for instance). In particular if we set $A = Z$ then we have $\|B\|_u = \tau Z + O(\tau(1-\tau)\frac{\log^{1/2}|Z|}{|Z|})$ with high probability; thus random subsets of Z tend to be extremely uniform. Note that $\mathbf{P}_Z(B) \approx \tau$ with high probability, thanks to Corollary 1.10.

A major application of Fourier bias is in the study of arithmetic progressions of length 3. We will study this application in detail in Chapter 10.

Exercises

4.3.1 Let A be a subset of a finite additive group Z. Show that $\|A\|_u = 0$ if and only if $A = Z$ or $A = \emptyset$.

4.3.2 Let A be a subset of a finite additive group Z. Show that $\|A\|_u = \|-A\|_u = \|T^h A\|_u = \|Z\backslash A\|_u$ for any $h \in Z$. More generally, if $\phi : Z \to Z'$ is any isomorphism from one additive group to another, show that $\|\phi(A)\|_u = \|A\|_u$. In a similar spirit, show that the Fourier bias of a set A does not depend on the choice of symmetric non-degenerate bilinear form.

4.3.3 Let A, B be disjoint subsets of a finite additive group Z. Show that $|\|A\|_u - \|B\|_u| \leq \|A \cup B\|_u \leq \|A\|_u + \|B\|_u$.

4.3.4 Let A be an additive set in a finite additive group Z. Show that $\|A\|_u \leq \mathbf{P}_Z(A)$, with equality if and only if A is contained in a coset of a proper subgroup of Z.

4.3.5 Let A and A' be subsets of finite additive groups Z and Z' respectively. Show that $\|A \times A'\|_u = \|A\|_u\|A'\|_u$.

4.3.6 Let A be a subset of a finite additive group Z. Show that $\|A\|_u = \sup_\phi |\langle 1_A, e(\phi)\rangle_{\mathbf{C}^Z}|$, where $\phi : Z \to \mathbf{R}/\mathbf{Z}$ ranges over all non-constant linear phase functions (as defined in Exercise 4.1.4).

4.3.7 Let A, B be additive sets in a finite additive group Z. Show that

$$E(A, B) \leq \frac{|A|^2|B|^2}{|Z|} + |Z|^2\|A\|_u^2|B|.$$

Using (2.8), conclude that if $\|A\|_u \leq \alpha \mathbf{P}_Z(A)$, then

$$|A + B| \geq \frac{1}{2}\min\left(|Z|, \frac{1}{\alpha^2}|B|\right). \tag{4.22}$$

Thus α-uniform sets tend to expand sum sets by a factor of roughly α^{-2} (unless this is impossible due to the trivial bound $|A + B| \leq |Z|$).

4.3.8 Let A be an additive set in a finite additive group Z. Show that

$$\|A\|_u^4 \leq \frac{1}{|Z|^3}E(A, A) - \mathbf{P}_Z(A)^4 \leq \|A\|_u^2\mathbf{P}_Z(A). \tag{4.23}$$

Thus uniform sets have additive energy $E(A, A)$ close to the minimal value of $\mathbf{P}_Z(A)^4|Z|^3$, and vice versa.

4.3.9 Let A be an additive set in a finite additive group Z, and let $n \geq 3$ be an integer. Using Lemma 4.13, show that if $nA \neq Z$, then $\mathbf{P}_Z(A)^{1+\frac{1}{n-2}} \leq \|A\|_u \leq \mathbf{P}_Z(A)$. This estimate is especially useful when n is very large, as it shows that 1_A has a very large non-trivial Fourier coefficient.

4.3.10 Prove Corollary 4.15. Also show the identity $A \cdot 2A = A$ and conclude that $2A = F$ (using the fact that $3A = F$ to show that $2A \neq A$).

4.3.11 Use Chernoff's inequality (in the form of Exercise 1.3.4) to prove Lemma 4.16.

4.3.12 [149] Let A, B be additive sets in a finite additive group Z. Use Lemma 4.13 to establish the inequality

$$\|S\|_u \geq \mathbf{P}_Z(A)^{1/2}\mathbf{P}_Z(B)^{1/2}\mathbf{P}_Z(S)$$

whenever S is disjoint from $A + B$. In particular, this inequality holds when $S = Z\backslash(A + B)$. This shows that complements of sum sets are "hereditarily non-uniform".

4.3.13 Let A be a subset of a cyclic group $\mathbf{Z}_p$ of prime order. Show that for any arithmetic progression P in $\mathbf{Z}_p$, we have the uniform distribution estimate

$$\mathbf{P}_{\mathbf{Z}_p}(A \cap P) = \mathbf{P}_{\mathbf{Z}_p}(A)\mathbf{P}_{\mathbf{Z}_p}(P) + O(\varepsilon) + O\left(\log\frac{1}{\varepsilon}\|A\|_u\right)$$

for any $0 < \varepsilon \leq 1$. (Hint: apply a change of variables to make $P = [-N, N]$ for some N. Approximate the indicator 1_P by something a bit