whenever n is large and $1 \le \alpha_1 + \cdots + \alpha_n \le k-1$. From the definition of $\mathcal{A}'_n$ we see that we may take $\alpha_j = 0$ for all $j \le n^{0.1}$, and all the other α_j equal to 0 or 1, since the above partial derivative vanishes otherwise. One can then compute the partial derivative and reduce our problem to showing that

$$\mathbf{E}\left(\sum_{A \in \mathcal{A}'_n : A \supset A_0} \prod_{j \in A \setminus A_0} t_j\right) \le n^{-\gamma}$$

whenever A_0 is any subset of $[n^{0.1}, n]$ of cardinality $1 \le |A_0| \le k-1$ (this is the set of indices where $\alpha_j = 1$). Applying linearity of expectation and independence, and noting that $j \in [n^{0.1}, n]$ for all $j \in A \setminus A_0$, we conclude that

$$\begin{aligned}\mathbf{E}\left(\sum_{A \in \mathcal{A}'_n : A \supset A_0} \prod_{j \in A \setminus A_0} t_j\right) &\le \sum_{A \in A'_n : A \supset A_0} O_{C,k}\big(n^{1/k-1} \log^{1/k} n\big)^{k-|A_0|} \\ &\le O_k\big(n^{k-|A_0|-1}\big) O_{C,k}\big(n^{1/k-1} \log^{1/k} n\big)^{k-|A_0|} \\ &\le O_{C,k}\big(n^{-1/k} \log n\big)\end{aligned}$$

and the claim follows for large n. □

Remark 1.45 The proof above is from [378] and is based on the proof of Theorem 1.48 in [379]. The original proof in [98] was different and did not use Theorem 1.37.

Exercises

1.8.1 Let $A \in \mathbf{Z}^+$ be a set of n different integers. Prove that A contains a subset B of cardinality $\Omega(\log n)$ with the following property. No two elements of B add up to an element of A (thus $r_{2,B}(m)$ vanishes for all $m \in A$, or equivalently $A \cap 2B = \emptyset$).

1.8.2 Prove Lemma 1.41. (Hint: first use the pigeonhole principle to show that if $|\mathcal{A}| > (l-1)k$, then either $\mathcal{A}$ contains l disjoint sets, or that there exist at least $|\mathcal{A}|/(l-1)k$ sets in $\mathcal{A}$ which all have a common element x_0. Then use induction on k.)

1.9 Thin Waring bases

Recall that a thin basis of order k is a set $B \subset \mathbf{N}$ such that $r_{k,B}(n) = O(\log n)$ for all large n. Theorem 1.15, proved above, asserts that $\mathbf{N}$ contains a thin basis of any order. Given the abundance of classical bases such as the squares and primes, it is then natural to pose the following question:

Question 1.46 *Let A be any fixed basis of order k. Does A contain a thin subbasis B?*

Note that Sidon's original question can be viewed as the $k = 2$, $A = \mathbf{N}$ case of this question. From (1.21) we know that a thin basis B enjoys the bounds

$$|B \cap [0, N]| = \Omega_k\big(N^{1/k}\big); \qquad |B \cap [0, N]| = O_k\big(N^{1/k} \log^{1/k} N\big)$$

for all large N. Thus we can consider the following weaker version of Question 1.46:

Question 1.47 *Let A be any fixed basis of order k. Does A contain a subbasis B with $|B \cap [0, N]| = O_k(N^{1/k} \log^{1/k} N)$ for all large N?*

Question 1.47 has been investigated intensively for the Waring bases $\mathbf{N}\hat{}r = \{0^r, 1^r, 2^r, \ldots\}$, especially when $r = 2$ [90, 56, 387, 388, 384, 331]. For these bases it is known that if k is sufficiently large depending on r, then $\mathbf{N}\hat{}r$ is a basis of order k, and furthermore that

$$r_{k,\mathbf{N}\hat{}r}(n) = \Theta_{k,r}\big(n^{\frac{k}{r}-1}\big); \tag{1.42}$$

note that this is consistent with (1.21).

Choi, Erdős and Nathanson proved in [56] that $\mathbf{N}\hat{}2$, the set of squares, contains a subbasis B of order 4, with $|B \cap [0, N]| = O_\varepsilon(N^{1/3} + \varepsilon)$ for all $N > 1$ and all $\varepsilon > 0$. This was generalized by Zöllner [387, 388], who showed that for any $k \geq 4$ there was a subbasis $B \subset \mathbf{N}\hat{}2$ of order k with $|B \cap [0, N]| = O_{k,\varepsilon}(N^{1/k+\varepsilon})$ for any $\varepsilon > 0$ and $N > 1$. This bound was then sharpened further to $|B \cap [0, N]| = O_k(N^{1/k} \log^{1/k} N)$; from (1.21) we know that this is sharp except for the logarithmic factor. A short proof of Wirsing's result for the case $k = 4$ was given by Spencer in [331]. For $r \geq 3$, much less was known. In 1980, Nathanson [259] proved that $\mathbf{N}\hat{}r$ contains a subbasis of some order with density $o(N^{1/r})$. In the same paper, he posed a special case of Question 1.47, when $A = \mathbf{N}\hat{}r$.

In [379], Vu positively answered Question 1.46 (and hence Question 1.47) for the case $A = \mathbf{N}\hat{}r$ for any $r \geq 1$:

Theorem 1.48 *For any fixed r there is an integer k_0 such that the following holds. For any $k \geq k_0$, the set $\mathbf{N}\hat{}r$ of all rth powers contains a thin basis B of order k. In particular, from (1.21) we have $|B \cap [0, n)| = O_k(N^{1/k} \log^{1/k} N)$ for all large N.*

Remark 1.49 The sharp concentration result in Theorem 1.37 was first developed in order to prove Theorem 1.48.

Just as Theorem 1.15 followed from Proposition 1.44, Theorem 1.48 is an immediate consequence of

Proposition 1.50 *Let $k, r \geq 2$, and let B be a random subset of $(\mathbf{Z}^+)^\wedge r$, defined by letting $x^r \in B$ be independent with probability*

$$\mathbf{P}(x^r \in B) = \min\left(Cx^{\frac{r}{k}-1}\log^{1/k} x, 1\right)$$

for some positive constant $C > 1$. If k is sufficiently large depending on r, and C is sufficiently large depending on k, r, then with probability 1 *we have $r_{k,B}(n) = \Theta_{C,k,r,B}(\log n)$ for all but finitely many n. In particular, B is a thin basis of order k with probability* 1.

Proof (Sketch) As in the proof of Proposition 1.44, it suffices to show that with probability 1 we have

$$E(n) = O_{C,k,r,B}(1); \qquad R(n) = \Theta_{C,k,r,B}(\log n)$$

for all but finitely many n, where $R(n)$ and $E(n)$ were defined in (1.40), (1.41). The contribution of $E(n)$ can be dealt with by similar arguments to the previous section and is left as an exercise, so we focus on $R(n)$. As before we can write $R(n)$ as a boolean polynomial $Y_n = Y_n(t_1, \ldots, t_m)$, where $m = \lfloor n^{1/k} \rfloor$, $t_x = \mathbf{I}(x^r \in B)$, and

$$Y_n = \sum_{A \in \mathcal{A}_n} \prod_{x \in A} t_x$$

where $\mathcal{A}_n$ is the collection of sets $\{x_1, \ldots, x_k\}$ of positive integers with $x_1^r + \cdots + x_k^r = n$ and $n^{0.1} < x_1^r < \cdots < x_k^r$. Given the framework presented in the last section, the substantial difficulty remaining is to estimate the expectations of Y_n and its partial derivatives. In the following, we shall focus on the expectation of Y_n, establishing in particular that

$$\mathbf{E}(Y_n) = \Theta_{k,r}(C^k \log n).$$

This is the main estimate, and the remainder of the argument proceeds as in Proposition 1.44. Notice that

$$\mathbf{E}(Y_n) = C^k \sum_{x_1 < \cdots < x_k : \{x_1, \ldots, x_k\} \in \mathcal{A}_n} \prod_{j=1}^{k} x_j^{\frac{r}{k}-1} \log^{1/k} x_j;$$

since all the x_j range between $n^{1/10r}$ and $n^{1/r}$, it thus suffices to show that

$$\sum_{x_1 < \cdots < x_k : \{x_1, \ldots, x_k\} \in \mathcal{A}_n} x_1^{\frac{r}{k}-1} \ldots x_k^{\frac{r}{k}-1} = \Theta_{r,k}(1). \tag{1.43}$$

This bound implies, but is a little bit stronger than, the standard bound (1.42), as the estimate also asserts some improved bound on the counting function $r_{k,\mathbf{N}^\wedge r}(n)$ when