Exercises

9.6.1 [176] Prove (9.13). (Hints: for the upper bound, use the pigeonhole principle. For the lower bound, take $n-1$ copies of $\{0,1\}^d$.)

9.6.2 [176] Prove (9.14). (Hint: modify the inductive argument in the proof of Theorem 9.28.)

9.6.3 Using Theorem 9.36 and (9.14) to deduce that $s(n,2) \leq \frac{41}{11}n$. (Hint: first verify the claim when all the prime divisors of n are less than 11, and then induce on n.)

9.6.4 [6] Modify the proof of Lemma 9.31 to prove that $s(n,d) = O_d(n)$.

9.7 Stepanov's method

In this section we fix a finite field F, and fix a multiplicative subgroup G of $F^\times$. The multiplicative structure of G can be determined explicitly:

Lemma 9.39 *Let G be a subgroup of $F^\times$. Then $|G|$ divides $|F^\times|$; thus we have $|F^\times| = |F| - 1 = |G|h$ for some $h \geq 1$. Furthermore we have the explicit formulas*

$$G = \left\{x \in F^\times : x^{|G|} = 1\right\} = \{y^h : y \in F^\times\}, \tag{9.15}$$

and if $G^\perp \subseteq F^\times$ denotes the orthogonal complement group $G^\perp := \{\xi \in F^\times : \xi^h = 1\}$, then $G^\perp$ indexes the multiplicative cosets $x \cdot G$ of G. Indeed if we define $G_\xi := \{x \in F^\times : x^{|G|} = \xi\}$ for all $\xi \in G^\perp$, then the sets $\{G_\xi : \xi \in G^\perp\}$ partition $F^\times$, and one has $x \cdot G = G_{x^{|G|}}$ for all $x \in F^\times$.

We leave the easy verification of this lemma to Exercise 9.7.1. In this section however we shall be more concerned with understanding the *additive* structure of G. A convenient way of quantifying this structure is via the sets $\Lambda(\xi) \subset F$ defined for all $\xi \in G^\perp$ by

$$\Lambda(\xi) := \left\{x \in F : x^{|G|} = (x-1)^{|G|} = \xi\right\} = G_\xi \cap (G_\xi + 1).$$

It is clear that these sets are disjoint as ξ ranges over $G^\perp$. The relevance of these sets to the additive structure of G lies in the easily verified identity

$$|G \cap (G+x)| = |(G-g) \cap \pm G_\xi| = |\Lambda(\xi^{-1})| \text{ whenever } \xi \in G^\perp, x \in G_\xi, g \in G; \tag{9.16}$$

see Exercise 9.7.2. As a consequence of (9.16) we have the following identities, whose verification we leave to Exercise 9.7.3.

Lemma 9.40 *We have* $\sum_{\xi\in G^\perp}|\Lambda(\xi)| = |\bigcup_{\xi\in G^\perp}\Lambda(\xi)| = |G| - 1$ *and* $E(G,G) = |G|^2 + |G|\sum_{\xi\in G^\perp}|\Lambda(\xi)|^2$, *where* $E(G,G)$ *is the additive energy of* G. *If* $-1 \in G^\perp$, *then we have* $|\Lambda(-\xi)| = |\Lambda(\xi)|$ *for all* $\xi \in G^\perp$.

In [337] Stepanov introduced a method for controlling various additive expressions involving G and related objects such as $|\Lambda(\xi)|$. For simplicity we shall restrict our attention just to the task of obtaining upper bounds on $|\Lambda(\xi)|$, following [180]. The idea is to use elementary linear algebra to construct a sparse polynomial P which vanishes to high order on several of the sets $\Lambda(\xi)$. One then applies tools such as Lemma 9.26 to obtain a non-trivial bound. We illustrate this method with the following result of Heath-Brown and Konyagin, which gives distributional information on the sizes of the $|\Lambda(\xi)|$.

Theorem 9.41 *[180] Let* $F = F_p$ *be a finite field of prime order, and let* G *be a multiplicative subgroup of* $F^\times$. *Let* $G^\perp$ *and* Λ *be defined as above. Then for any set* $\Gamma \subseteq G^\perp$ *with* $|\Gamma| = O(|F|^3/|G|^4)$, *we have*

$$\sum_{\xi\in\Gamma}|\Lambda(\xi)| = O\big(\min\big(|G|, |G|^{2/3}|\Gamma|^{2/3}\big)\big).$$

Proof Let $0 < c \ll 1$ be a small absolute constant to be chosen later. We may assume that G is large, $|G| > c^{-100}$, since the claim is trivial otherwise. Similarly we may assume that Γ is non-empty and that $|\Gamma| \leq c^{100}|F|^3/|G|^4$, since the claim for $|\Gamma| = \Theta(|F|^3/|G|^4)$ then follows by partitioning Γ into $O(1)$ sets of size at most $c^{100}|F|^3/|G|^4$.

When $|\Gamma| = \Omega(|G|^{1/2})$ then the claim already follows from Lemma 9.40, so we may assume that $|\Gamma| < c^{100}|G|^{1/2}$. Let us define the normalized quantities

$$A := \lfloor c^{10}|G|^{2/3}|\Gamma|^{-1/3}\rfloor; \quad B := \lfloor c|G|^{1/3}|\Gamma|^{1/3}\rfloor;$$

observe from our hypotheses on $|\Gamma|$ that we have the bounds

$$1 \leq B \leq A; \quad AB < |G|; \quad A^2|\Gamma| \leq cAB^2; \quad A + 2|G|B < |F| \tag{9.17}$$

if c is chosen suitably small. By the disjointness of the $\Lambda(\xi)$, it then suffices to show that

$$\Big|\bigcup_{\xi\in\Gamma}\Lambda(\xi)\Big| = O\left(1 + \frac{|G|B}{A}\right). \tag{9.18}$$

We now let $V \subseteq F[t]$ be the linear subspace (over F) of $F[t]$ generated by the AB^2 polynomials $t^a t^{b|G|}(t-1)^{b'|G|}$ where $0 \leq a < A$ and $0 \leq b, b' < B$. We first observe that V has large dimension:

Lemma 9.42 V *has linear dimension exactly* AB^2 *over* F.

Proof Suppose for contradiction that V had dimension less than AB^2. Then we could find coefficients $c_{a,b,b'} \in F$, not all zero, such that

$$\sum_{0\leq a<A} \sum_{0\leq b<B} \sum_{0\leq b'<B} c_{a,b,b'} t^a t^{b|G|} (t-1)^{b'|G|} = 0.$$

We may assume that there is at least one non-zero coefficient $c_{a,b,0}$, otherwise we could divide out by $(t-1)^{|G|}$. But then the polynomial $\sum_{0\leq a<A} \sum_{0\leq b<B} c_{a,b,0} t^a t^{b|G|}$ would have a zero of order $|G|$ at $t=1$. On the other hand, this polynomial is non-zero and its Newton diagram contains at most AB points, which contradicts Lemma 9.26 and (9.17). □

We then exploit this large dimension to locate a polynomial which vanishes to high order on $\bigcup_{\xi\in\Gamma} \Lambda(\xi)$.

Lemma 9.43 *V contains a non-zero polynomial P which vanishes to order A at all elements of $\bigcup_{\xi\in\Gamma} \Lambda(\xi)$.*

Proof It is convenient to use an algebraic geometry perspective and work via commutative rings. Let R be the commutative ring over F generated by indeterminates $t, t^{-1}, s, s^{-1}, r, \varepsilon$ subject to the constraints

$$tt^{-1} = ss^{-1} = 1; \quad s = t-1; \quad t^{|G|} = s^{|G|} = r; \prod_{\xi\in\Gamma} (r-\xi) = 0; \quad \varepsilon^A = 0; \tag{9.19}$$

in other words, R is the polynomial ring $F[t, t^{-1}, s, s^{-1}, r, \varepsilon]$ quotiented out by the ideal generated by the polynomials $tt^{-1}-1$, $ss^{-1}-1$, $s-t+1$, $t^{|G|}-r$, $s^{|G|}-r$, $\prod_{\xi\in\Gamma}(r-\xi)$, and ε^A. Let $\iota : F[t] \mapsto R$ be the ring homomorphism that maps t to $t+\varepsilon$. We shall show that the image $\iota(V)$ of V has linear dimension strictly less than AB^2. By Lemma 9.42, this will force the existence of a non-zero polynomial $P \in V$ such that $\iota(P) = 0$; in other words we can find $Q_1, \ldots, Q_7 \in F[t, t^{-1}, s, s^{-1}, r, \varepsilon]$ such that

$$\begin{aligned} P(t+\varepsilon) = {} & Q_1(tt^{-1}-1) + Q_2(ss^{-1}-1) + Q_3(s-t+1) \\ & + Q_4\big(t^{|G|}-r\big) + Q_5\big(s^{|G|}-4\big) + Q_6 \prod_{\xi\in\Gamma} (r-\xi) + Q_7 \varepsilon^A \end{aligned}$$

for any indeterminates $t, t^{-1}, s, s^{-1}, r, \varepsilon$. Restricting this to $r := \xi \in \Gamma$, $t := x \in \Lambda(\xi) \subset F^\times$, $s := x-1 \in F^\times$, $t^{-1} := x^{-1} \in F^\times$, $s^{-1} := (x-1)^{-1} \in F^\times$, $\varepsilon \in F$, we obtain

$$P(x+\varepsilon) = Q_7(x, x^{-1}, x-1, (x-1)^{-1}, \xi, \varepsilon)\varepsilon^A$$

which shows that P vanishes to order A at x, which is an arbitrary element of $\bigcup_{\xi\in\Gamma} \Lambda(\xi)$.

It remains to bound the linear dimension of $\iota(V)$. Observe that this space is generated by the polynomials $\iota(t^a t^{b|G|}(t-1)^{b'|G|}) = (t+\varepsilon)^a (t+\varepsilon)^{b|G|}(s+\varepsilon)^{b'|G|}$. But by the Taylor expansion of $(t+\varepsilon)^{b|G|}$ and using the constraints (9.19), we have

$$\begin{aligned}(t+\varepsilon)^{b|G|} &= t^{b|G|}\left(1 + \binom{b|G|}{1} t^{-1}\varepsilon + \binom{b|G|}{2} t^{-2}\varepsilon^2 + \cdots\right) \\ &= r^b \left(1 + \binom{b|G|}{1} t^{-1}\varepsilon + \cdots + \binom{b|G|}{A-1} t^{-A+1}\varepsilon^{A-1}\right).\end{aligned}$$

In particular we see that $(t+\varepsilon)^{b|G|}$ is equal in R to a polynomial expression in $t, t^{-1}, s, s^{-1}, r, \varepsilon$ of degree $O(A)$. Similarly for $(t+\varepsilon)^a$ and $(s+\varepsilon)^{b'|G|}$. Thus $\iota(V)$ lies in the space of polynomials in $t, t^{-1}, s, s^{-1}, r, \varepsilon$ of degree at most $O(A)$. Taking out a common denominator of $(ts)^{-O(A)}$, we obtain a space of polynomials in t, s, r, ε of degree at most $O(A)$. The variable s can be eliminated since $s = t-1$ from (9.19). The variable r is limited to have degree at most $|\Lambda|$, again by (9.19). This shows that the dimension of $\iota(V)$ is at most $O(|\Lambda|A^2)$, which (9.17) is indeed less than the dimension AB^2 of V, as desired. □

Let P be as in Lemma 9.43. Since $P \in V$, we have $\deg(P) \leq A + 2|G|B < |F|$ thanks to (9.17). Since P can have at most $\deg(P)$ zeroes (counting multiplicity) in F, we obtain

$$A\left|\bigcup_{\xi\in\Gamma} \Lambda(\xi)\right| \leq A + 2|G|B,$$

which gives (9.18) as desired. □

Theorem 9.41 can already be used to give non-trivial sum set bounds on G, for instance via controlling the additive energy $E(G,G)$. In fact we can also control the additive energy $E(A,A)$ of subsets of G:

Lemma 9.44 *[44] Let $F = F_p$ be a finite field of prime order, and let G be a multiplicative subgroup of $F^\times$ of order $|G| = O(|F|^{3/4})$. Let A be an additive set in G. Then we have*

$$E(A,A) = O\big(|G||A|^{3/2}\big). \tag{9.20}$$

Comparing this with (2.7) we see that this bound is non-trivial when $|A| \geq |G|^{2/3}$. See also Corollary 2.62.

Proof For every $\xi \in G^\perp$, we define the counting function $\alpha(\xi)$ by

$$\alpha(\xi) := |\{(a_1, a_2) \in A \times A : a_1 - a_2 \in G_\xi\}|.$$

We observe that

$$\begin{aligned} E(A,A) &= |\{(a_1,a_2,a_3,a_4) \in A\times A\times A\times A : a_1-a_2=a_3-a_4\}| \\ &= |A|^2 + \sum_{\xi\in G^\perp} |\{(a_1,a_2,a_3,a_4) \in A\times A\times A\times A : a_1-a_2=a_3-a_4 \in G_\xi\}| \\ &\leq |A|^2 + \sum_{\xi\in G^\perp} \alpha(\xi) \sup_{d\in G_\xi} |\{(g_1,g_2)\in G\times G : g_1-g_2=d\}| \\ &= |A|^2 + \sum_{\xi\in G^\perp} \alpha(\xi)|\Lambda(\xi^{-1})| \end{aligned}$$

thanks to (9.16). Since $|A|^2 = |A|^{1/2}|A|^{3/2} = O(|G||A|^{3/2})$, it thus suffices to show that

$$\sum_{\xi\in G^\perp} \alpha(\xi)|\Lambda(\xi^{-1})| = O\big(|G||A|^{3/2}\big).$$

From the identity

$$\sum_{\xi\in G^\perp} \alpha(\xi) = |A|^2$$

we see that it suffices to show that

$$\sum_{\xi\in G^\perp:\Lambda(\xi^{-1})\geq |G||A|^{-1/2}} \alpha(\xi)|\Lambda(\xi^{-1})| = O\big(|G||A|^{3/2}\big).$$

But from (9.16) we also have the trivial bound

$$\alpha(\xi) \leq |A| \sup_{g_1\in G} |\{g_2\in G : g_1-g_2\in G_\xi\}| = |A||\Lambda(\xi^{-1})|$$

and so it suffices to show that

$$\sum_{\xi\in G^\perp:\Lambda(\xi^{-1})\geq |G||A|^{-1/2}} |\Lambda(\xi^{-1})|^2 = O\big(|G||A|^{1/2}\big).$$

But if we order $G^\perp = \{\xi_1,\dots,\xi_M\}$ in decreasing order of $\Lambda(\xi_j^{-1})$, then by Theorem 9.41 we then have

$$j\big|\Lambda\big(\xi_j^{-1}\big)\big| = O\big(\min\big(|G|,|G|^{2/3}j^{2/3}\big)\big) \text{ for all } 1\leq j\leq M,$$

which implies that

$$\sum_{\xi\in G^\perp:\Lambda(\xi)\geq |G||A|^{-1/2}} |\Lambda(\xi^{-1})|^2 = \sum_{j=O(|A|^{3/2}/|G|)} O\big(|G|^{2/3}j^{2/3}/j\big)^2 = O\big(|G||A|^{1/2}\big)$$

as desired. □

As a consequence we can now give a sum-product estimate which improves somewhat on the results in Section 2.8.

Theorem 9.45 *[44] Let $F = F_p$ be a finite field of prime order, and let A be an additive set in $F^\times$. Let $Q[A] = \frac{A-A}{(A-A)\backslash 0}$ be the quotient set of A, as defined in Definition 2.49. Then there exists $\xi \in Q[A]$ such that*

$$|A + \xi \cdot A| \geq c \min\left(|F|, \frac{|A|^{5/2}}{|A \pm A|}, \frac{|A|^3}{|A \cdot A|}\right)$$

for either choice of sign $\pm$.

Proof If $|A| \geq |F|^{1/2}$ then the claim follows from Corollary 2.51, so suppose $|A| < |F|^{1/2}$. Let D be the set of popular quotients,

$$D := \left\{d \in F^* : |\{(a', a'') \in A \times A : a'/a'' = d\}| \geq \frac{2|A|^2}{9|A \cdot A|}\right\},$$

and let G be the multiplicative group generated by D. Then by the multiplicative version of Exercise 2.6.10, there exists a coset $\xi_0 \cdot G$ of G for some $\xi_0 \in F^*$ such that $|A \cap (\xi_0 \cdot G)| \geq |A|/3$. By dividing A by ξ_0 we may assume that $\xi_0 = 1$.

Lemma 9.46 *Let $H \subseteq G$ be the set of those $\xi \in G$ such that*

$$|A + \xi \cdot A| \geq \min\left(\frac{|A|^2|G|}{|A|^2 + |G|}, \frac{2|A|^3}{9|A \cdot A|}\right).$$

Then $H \cap Q[A]$ is non-empty.

Proof Suppose for contradiction that H and $Q[A]$ are disjoint. From Exercise 2.8.4 there exists a $\xi \in G$ such that $|A + \xi \cdot A| \geq \frac{|A|^2|G|}{|A|^2+|G|}$, and hence H is non-empty. Thus, $G\backslash Q[A]$ is non-empty, and is also a proper subset of G (since $1 \in Q[A] \cap G$). Next, observe that if $\xi \in G\backslash Q[A]$ and $d \in D$, then by Lemma 2.50, all the sums in $A + \xi \cdot A$ are distinct, and hence

$$|A + (\xi d) \cdot A| \geq |A||A \cap (d \cdot A)| \geq \frac{2|A|^2}{9|A \cdot A|}.$$

This shows that $D \cdot (G\backslash Q[A]) \subseteq H$. Since $H \subseteq G$ and H and $Q[A]$ are disjoint, we conclude $D \cdot (G\backslash Q[A]) \subseteq G\backslash Q[A]$; since D generates G, this implies that $G \cdot (G\backslash Q[A]) \subseteq G\backslash Q[A]$. But this contradicts the previous observation that $G\backslash Q[A]$ was a proper non-empty subset of G. □

Let ξ be as in the above lemma; thus

$$|A + \xi \cdot A| \geq c \min\left(|G|, |A|^2, \frac{|A|^3}{|A \cdot A|}\right).$$

Note that since $|A \cdot A| \geq |A|$, we can drop the $|A|^2$ term from the right-hand side. We will now be done unless $|G| \leq c|A|^{5/2}/|A \pm A|$ for some small $c > 0$.