vector lie in a fairly small generalized progression). These exceptional hyperplanes however are rather rare and can be treated by a direct counting argument.

Let us conclude by a refinement of Theorem 7.29, which allows us to fix a few rows of M_n. Let Y be a set of l independent vectors $y_1, \ldots, y_l$ and denote by M_n^Y the random matrix with rows $X_1, \ldots, X_{n-l}, y_1, \ldots, y_l$, where X_i are i.i.d copies of the random Bernoulli vector X.

Theorem 7.32 *[366] For any non-negative integer l, there is a positive constant ε such that the probability that M_n^Y is singular is at most $(1-\varepsilon)^n$.*

Exercises

7.5.1 Prove (7.9) and (7.10).

7.5.2 Prove (7.12).

7.5.3 Show that $\det(M_n) \in 2^{n-1} \cdot \mathbf{Z}$ and $|\det(M_n)| \leq n^{n/2}$ for all Bernoulli matrices M_n.

7.5.4 Show that $\det(M_n)$ has expectation zero and variance $n!$, and $|\det(M_n)|^2$ has expectation $n!$ and variance $n(n!)^2$. Derive a upper bound for $|\delta(M_n)|$. (For a matching lower bound, see [364].)

7.5.5 [195] Show that $\sup_{x \in \mathbf{R}} \mathbf{P}(\det(M_n) = x) = (1 - \varepsilon + o(1))^n$ for some absolute $\varepsilon > 0$.

7.5.6 [195] Show that for any $\varepsilon > 0$ we have

$$\sum_{(1-\varepsilon)^n \leq \mathbf{P}(X \in V) \leq O(\frac{1}{\sqrt{n}})} \mathbf{P}(X_1, \ldots, X_n \text{ lie in } V) = (o_{\varepsilon \to 0}(1))^n.$$

7.5.7 [195] Show that there exists an absolute constant $C > 0$ such that $\mathbf{P}(X_1, \ldots, X_{n-C} \text{ dependent}) = (\frac{1}{2} + o(1))^n$ whenever n is sufficiently large depending on ε, C. Conclude in particular that the probability that M_n has rank $n - C$ or less is $(\frac{1}{2} + o(1))^n$.

7.6 The quadratic Littlewood–Offord problem

The preceding sections studied the concentration of linear combinations of random variables such as $\eta_1 v_1 + \cdots + \eta_n v_n$. It is also of interest to study more general polynomial combinations. For simplicity we shall restrict ourselves to the quadratic expression

$$Q(\eta_1, \ldots, \eta_n) = \sum_{1 \leq i < j \leq n} c_{i,j} \eta_i \eta_j + \sum_{i=1}^n d_i \eta_i$$

where $c_{i,j}, d_i$ take values in an additive group Z, and $\eta_1, \ldots, \eta_n$ are independent uniformly distributed random ± 1 signs.

One can now ask under what conditions one can establish upper bounds on the concentration of the random variable Q. In the special case when the c_{ij} are identically zero, we know from Corollary 7.13 that Q will not concentrate at a single point as soon as many of the d_i are non-zero. One can then hope to establish a similar result for the quadratic component, namely that Q will not concentrate at a single point as soon as many of the c_{ij} are non-zero. We give a sample result of this form as follows:

Proposition 7.33 *[64] Let Z be either torsion-free or finite of odd order. Let the notation be as above, and suppose that for at least k values of i, we have $c_{i,j} \neq 0$ for at least l values of j. Then for any $x \in Z$ we have $\mathbf{P}(Q = x) = O(\min(k, l)^{-1/8})$.*

Proof Without loss of generality we may take $k \leq l$. A greedy algorithm argument shows that we can find a set $A \subset [1, n]$ of cardinality $\lfloor (k+1)/2 \rfloor$, such that for each $i \in A$ we have $c_{i,j} \neq 0$ for at least $\lfloor (l+1)/2 \rfloor$ values of $j \in [1, n] \backslash A$. The basic idea is to view the quadratic object Q as a linear expression $\sum_j X_j \eta_j$, where the X_j are themselves linear expressions of $\eta_1, \ldots, \eta_n$, so that one can obtain a quadratic non-concentration result from two applications of the linear non-concentration result. However there is a "coupling" problem, arising from the fact that the X_j and η_j do not behave independently. This however can be resolved via the following *decoupling inequality*

$$\begin{aligned} \mathbf{P}(E(X,Y)) &\leq \mathbf{P}(E(X,Y) \wedge E(X,Y'))^{1/2} \\ &\leq \mathbf{P}(E(X,Y) \wedge E(X,Y') \wedge E(X',Y) \wedge E(X',Y'))^{1/4} \end{aligned} \quad (7.13)$$

whenever X, Y, X', Y' are independent random variables taking finitely many values, with X, X' having the same distribution and Y, Y' having the same distribution, and $E(X, Y)$ is any event depending only on X and Y. The proof of this inequality follows from two applications of the Cauchy–Schwarz inequality and is left as an exercise. We apply this inequality with $X := (\eta_i)_{i \in A}$ and $Y := (\eta_j)_{j \in [1,n] \backslash A}$, writing Q as $Q(X, Y)$, to obtain

$$\mathbf{P}(Q(X,Y) = x) \leq \mathbf{P}(Q(X,Y) = Q(X,Y') = Q(X',Y) = Q(X',Y') = x)^{1/4}$$

where $X' = (\eta'_1, \ldots, \eta'_{n/2})$ and $Y' = (\eta'_{n/2+1}, \ldots, \eta'_n)$ are identical independent copies of X and Y. In particular we have

$$\mathbf{P}(Q(X,Y) = x) \leq \mathbf{P}(Q(X,Y) - Q(X,Y') - Q(X',Y) + Q(X',Y') = 0)^{1/4}.$$

On the other hand, we have the factorization

$$\begin{aligned} Q(X,Y) - Q(X,Y') - Q(X',Y) + Q(X',Y') &= \sum_{i \in A} \sum_{j \in B} c_{ij} (\eta_i - \eta'_i)(\eta_j - \eta'_j) \\ &= \sum_{i \in A} v_i \eta_i^{(1/2)} \end{aligned}$$

where $v_i := \sum_{j \in B} 4c_{ij}\eta_j^{(1/2)}$ and $\eta_i^{(1/2)} = (\eta_i - \eta_i')/2$. Observe that the $\eta_i^{(1/2)}$ are all independent and have the distribution of $\eta^{(1/2)}$ (i.e. they equal 0 with probability $1/2$, and ± 1 with probability $1/4$ each). Also we make the crucial observation that the $(v_i)_{i \in A}$ and $(\eta_i^{(1/2)})_{i \in A}$ are *independent*.

It now suffices to show that

$$\mathbf{P}\left(\sum_{i \in A} v_i \eta_i^{(1/2)} = 0\right) = O\left(\frac{1}{k^{1/2}}\right).$$

For each $i \in A$, we have the easy bound

$$\mathbf{E}(\mathbf{I}(v_i = 0)) = \mathbf{P}(v_i = 0) \leq \frac{3}{4}$$

as can be seen by conditioning all the η_j except for a single j for which $c_{i,j} \neq 0$. From Corollary 7.13 we also have

$$\mathbf{E}(\mathbf{I}(v_i = 0)) = \mathbf{P}(v_i = 0) \leq O\left(\frac{1}{\sqrt{l}}\right).$$

By linearity of expectation we thus have

$$\mathbf{E}\left(\sum_{i \in A} \mathbf{I}(v_i = 0)\right) \leq |A| \min\left(\frac{3}{4}, O\left(\frac{1}{\sqrt{l}}\right)\right).$$

In particular by Markov's inequality we have

$$\mathbf{P}\left(\sum_{i \in A} \mathbf{I}(v_i = 0) \leq \frac{7}{8}|A|\right) \leq \min\left(\frac{6}{7}, O\left(\frac{1}{\sqrt{l}}\right)\right);$$

since $|A| = \Omega(k)$, we conclude

$$\mathbf{P}(|\{1 \leq i \leq n/2 : v_i \neq 0\}| = \Omega(k)\}|) \geq \max\left(\frac{1}{7}, 1 - O\left(\frac{1}{\sqrt{l}}\right)\right).$$

Now if we condition on the above event (call it E), then the distribution and independence of the $\eta_i^{(1/2)}$ remain unaffected. Thus we may apply Corollary 7.13 again to obtain

$$\mathbf{P}\left(\sum_{i \in A} v_i \eta_i^{(1/2)} = 0 | E\right) = O\left(\frac{1}{\sqrt{k}}\right);$$

we also have the crude upper bound of $\frac{3}{4}$ as before. Thus

$$\mathbf{P}\left(\sum_{i \in A} v_i \eta_i^{(1/2)} \neq 0 | E\right) = \max\left(\frac{1}{4}, 1 - O\left(\frac{1}{\sqrt{k}}\right)\right).$$

Combining this with the estimate on $\mathbf{P}(E)$ and Bayes' formula, we obtain the claim. □

In [64] this estimate was used, together with some techniques from the preceding section, to obtain

Theorem 7.34 *[64] Let M_n be a random symmetric $n \times n$ matrix whose entries are random uniformly distributed signs ± 1, and with the entries in the upper triangular half being independent. (The entries in the strictly lower triangular half are of course determined from the upper half by symmetry.) Then* $\mathbf{P}(\det(M_n) = 0) = O_\varepsilon(n^{-1/8+\varepsilon})$ *for any $\varepsilon > 0$.*

Exercises

7.6.1 Give examples that show that for arbitrary $k, l \geq 1$, there exists Q obeying the hypothesis in Proposition 7.33 with $\mathbf{P}(Q = 0) = \Omega(\min(k, l)^{-1/2})$. Thus, except for the exponent $1/8$ and for absolute constants, the conclusion in Proposition 7.33 is best possible.

7.6.2 Obtain a generalization of Proposition 7.33 to polynomials of degree d in $\eta_1, \ldots, \eta_n$, with $1/8$ replaced by an exponent depending on d.

7.6.3 Improve the constant $1/8$ in Proposition 7.33 to $1/4$.

7.6.4 (Meshulam, private communication) Find a quadratic form $Q = \sum_{1 \leq i,j \leq n} c_{ij} \xi_i \xi_j$, where $c_{ij} \neq 0$ for all i, j and ξ_i are i.i.d Bernoulli random variables, such that

$$\mathbf{P}(Q = 0) \geq (2 - o(1)) \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n}.$$

Compare this to the linear case (Corollary 7.4).