EXAMPLES SHEET, APPLICATIONS OF COMMUTATIVE HARMONIC ANALYSIS

TOM SANDERS

Exercises with daggers (†) are harder, which is not to say that the others are not. Answers and comments on some of the questions appear at the end.

1. † Show that Proposition 1.5 is best possible up to the implied constant. That is, show that there is a set $A \subset \{1, \ldots, N\}$ of size $\Omega(\sqrt{N})$ containing no additive quadruples all of whose elements are distinct.

2. Suppose that $I = [0, 1]$ and $S \subset (0, \epsilon)$ is open. Show that

$$\|1_I * f_S - 1_I\|_{L^1(\mathbb{R})} = O(\epsilon).$$

3. Show that the map

$$\phi : \mathbb{R} \to \mathbb{R}; x \mapsto \begin{cases} \exp(-1/x) & \text{if } x > 0 \\ 0 & \text{otherwise.} \end{cases}$$

is infinitely differentiable. Since $\phi(1/2) \neq 0$ it follows that $x \mapsto \phi(x)\phi(1 - x)$ is a bump function.

4. Considering $1_{\{1,\ldots,N\}}$ as an element of $\ell^1(\mathbb{Z})$, write down an expression for the convolution of functions $1_{\{1,\ldots,N\}} * 1_{\{1,\ldots,N\}}$.

5. † Considering $1_{\{1,\ldots,N\}}$ as an element of $\ell^1(\mathbb{Q}_{>0})$, show that

$$1_{\{1,\ldots,N\}} * 1_{\{1,\ldots,N\}}(x) = O(x^{o(1)}).$$

6. Prove the nesting of the $L^p(X)$-norms and $\ell^p(X)$-norms. Show that in the first case equality holds if and only if the function is constant, and in the latter if and only if the function is a δ-function, meaning that it is supported on exactly one point of the domain.

7. Check that you believe the basic facts about convolution in Lemma 2.7.

8. Prove that

$$\nu(\{x : |f(x)| \geqslant \epsilon\}) \leqslant \epsilon^{-p} \|f\|_{L^p(\nu)}^p,$$

for all $f \in L^p(\nu)$. (The case $p = 2$ is Chebychev's inequality.)

Last updated: 5th August, 2013.

9. Show that Young's inequality, Proposition 2.12, can be improved using an example other than (a scalar multiple of) $f = g = 1_G$. Which (finite) groups is this possible for? Give as wide a class as you can of extremal functions when the triple of indices (p, q, r) is not internal.

10. Prove the version of Young's inequality for measures in Proposition 2.13.

11. Suppose that p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is endowed with counting measure, $A \subset \mathbb{Z}/p\mathbb{Z}$ and $\lambda_1, \dots, \lambda_r \in (\mathbb{Z}/p\mathbb{Z})^*$. Show that the number of solutions to $\lambda_1 x_1 + \cdots + \lambda_r x_r = x_{r+1}$ with $x_1, \dots, x_{r+1} \in A$ is

$$\langle 1_{\lambda_1 A} * \cdots * 1_{\lambda_r A}, 1_A \rangle_{\ell^2(\mathbb{Z}/p\mathbb{Z})}.$$

What if p is not prime?

12. Suppose that $A \subset \{1, \dots, N\}$ as in Proposition 1.5. Let $\phi : \mathbb{Z} \to \mathbb{Z}/(2N-1)\mathbb{Z}$ by the usual projection. Then show that $(x, y, z, w) \in A^4$ is an additive quadruple if and only if $(\phi(x), \phi(y), \phi(z), \phi(w)) \in \phi(A)^4$ is an additive quadruple. In light of this use convolution of finite Abelian groups to reprove Proposition 1.5.

13. Suppose that N is a natural and $\mathbb{Z}/N\mathbb{Z}$ is endowed with counting measure. Describe the operators M_f with respect to the standard basis, that is the orthonormal basis of functions $(1_{\{k+N\mathbb{Z}\}})_{k=1}^N$

14. Check that you believe the generalised Parseval identity, that is if $\{e_1, \dots, e_N\}$ is an orthonormal basis for a finite dimensional Hilbert space H then

$$\|v\|^2 = \sum_{i=1}^N |\langle v, e_i \rangle|^2 \text{ for all } v \in H.$$

15. Verify the orthogonality relations for characters directly. That is, show that

$$\int \gamma(x)\overline{\lambda(x)} d\mu(x) = \begin{cases} \mu(G) & \text{if } \gamma = \lambda \\ 0 & \text{otherwise} \end{cases}$$

for $\gamma, \lambda \in \widehat{G}$, and

$$\int \gamma(x)\overline{\gamma(y)} d\mu^*(\gamma) = \begin{cases} \mu^*(\widehat{G}) & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

for $x, y \in G$. By a dimension argument, or otherwise, conclude from these that $|\widehat{G}| \leqslant |G|$.

16. Prove the structure theorem for finite Abelian groups, that if G is such then there are naturals $d_1 | d_2 | \dots | d_r$ such that

$$G \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z}).$$

17. Show that if $G = (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})$ and $r \in G$ then

$$(x_1, \ldots, x_n) \mapsto \exp(2\pi i(\sum_{i=1}^{n} x_i r_i/d_i))$$

is a well-defined character on G, and different rs determine different characters.

18. Use the previous three questions to conclude that if G is a finite Abelian group then $\widehat{G} \cong G$.

19. Derive Parseval's theorem and the inversion formula directly from the previous results.

20. Prove that $\|\widehat{f}\|_{L^\infty(\mu^*)} \geqslant \|f\|_{L^1(\mu)}/\sqrt{|G|}$. Can you do any better?

21. Prove the Hausdorff-Young inequality that $\|\widehat{f}\|_{L^p(\mu^*)} \leqslant \|f\|_{L^{p'}(\mu)}$ for all even integers $p \geqslant 2$ using Young's inequality. Note by duality that this this is equivalent to $\|f\|_{L^p(\mu)} \leqslant \|\widehat{f}\|_{L^{p'}(\mu^*)}$ for the same values of p. It turns out that both inequalities are true for every $p \geqslant 2$.

22. Suppose that $G = (\mathbb{Z}/2\mathbb{Z})^{2n}$ is endowed with Haar probability measure and $S \subset G$ is the set of vectors with exactly n non-zero entries in them. Show that

$$\widehat{1_S}(\gamma) = \begin{cases} \binom{n}{s}\binom{2n}{2s}^{-1}(-1)^s\mathbb{P}_G(S) & \text{if } |\gamma| = 2s; \\ 0 & \text{otherwise.} \end{cases}$$

23. Suppose that $G = \mathbb{Z}/N\mathbb{Z}$ is endowed with Haar counting measure and $I \subset G$ is a symmetric interval about 0_G of length $2M+1$. Show that

$$\widehat{1_I}(r) = \frac{\sin(\pi(2M+1)r/N)}{\sin(\pi r/N)}$$

where r corresponds to the character $x \mapsto \exp(2\pi i r x/N)$.

24. Using Parseval's theorem and the result of Exercise 23 with $N = 2(2M+1)$ or otherwise solve the Bassel problem. That is to say prove that

$$\sum_{r=1}^{\infty} \frac{1}{r^2} = \frac{\pi^2}{6}.$$

In this discrete setting the details of this are developed by Sisask in [Sis08].

25. Suppose that $G = \mathbb{Z}/N\mathbb{Z}$ is endowed with Haar probability measure and write $G^* := \{r + N\mathbb{Z} : (r, N) = 1\}$. By definition we have $|G^*| = \phi(N)$; show that

$$\widehat{1_{G^*}}(r) = \frac{\mu(N/(N,r))}{\phi(N/(N,r))}$$

where (a,b) is the highest common factor of a and b and r is the character $x \mapsto \exp(2\pi i r x/N)$. When G is endowed with Haar counting measure the sums $\widehat{1_{G^*}}(r)$ are called Ramanujan sums and are denoted $c_N(r)$.

26. Suppose that $G = \mathbb{Z}/N\mathbb{Z}$, $I \subset G$ is an interval of size δN and X is chosen uniformly at random from G^*.[2] Then
$$\mathbb{P}(X \in I) = \delta + o(1).$$

27. If $A \subset G$ has size $\delta_G(A) = k$, how large and small can $\mathbb{P}_{\widehat{G}}(A^\perp)$ possibly be in terms of k?

28. Given $A \subset G$ non-empty, we write ν_A for the measure on $\widehat{G}$ assigning mass $\mu(A)^{-1}|\widehat{1_A}(\gamma)|^2$ to $\gamma \in \widehat{G}$. Show that
$$d(x,y) := \|\phi_{G,\widehat{G}}(x) - \phi_{G,\widehat{G}}(y)\|_{L^2(\nu_A)}$$
is a metric on G. How are the balls $\{x : d(x,1) \leqslant \epsilon\}$ related to the sets $\{x : 1_A * 1_{-A}(x) \geqslant (1-\delta)\mu(A)\}$?

29. Suppose that G is endowed with Haar probability measure and $A \subset G$ has density α. Find an upper estimate for $\mathbb{P}_G(\{x : 1_A * 1_A(x) > c\alpha\})$. Is there an interesting lower estimate? What if $c < \alpha$? Suppose that you know $\|1_A * 1_A\|_{L^2(G)}^2 \geqslant \eta\alpha^3$. Does that help? What if $\eta > 2c$?

30. Show that if $|A - A| < 1.5|A|$ then $A - A$ is a subgroup of G.

31. Prove that $\|f\|_{A(G)} := \sup\{|\langle f, g\rangle_{L^2(\mu)}| : \|\widehat{g}\|_{L^\infty(\mu^*)} \leqslant 1\}$ is an algebra norm, that is, it is a norm such that $\|fg\|_{A(G)} \leqslant \|f\|_{A(G)}\|g\|_{A(G)}$. Show that $\|f\|_{A(G)} = \|\widehat{f}\|_{L^1(\mu^*)}$, and that it is independent of the particular normalisation of Haar measure used. Show, further, that $\|f\|_{L^\infty(G)} \leqslant \|f\|_{A(G)}$.

32. We say that $\nu \in M(G)$ is idempotent if $\nu * \nu = \nu$. Show that $\nu \in M(G)$ is idempotent if and only if $\widehat{\nu} = 1_A$ for some $A \subset G$, and note that $\|\nu\| = \|1_A\|_{A(G)}$.

33. Show that if ν is idempotent then $\nu \equiv 0$ or else $\|\nu\| \geqslant 1$. Show that if $\|\nu\| = 1$ then $\widehat{\nu} = 1_W$ where W is a coset in $\widehat{G}$.

34. † Establish a robust version of the result in Exercise 33, *i.e.* show that if $\nu \in M(G)$ is idempotent and non-trivial with $\|\nu\| \leqslant 1 + \eta$ for sufficiently small η then $\widehat{\nu} = 1_W$ where W is a coset in $\widehat{G}$.

35. Give an example of an idempotent measure $\nu \in M(G)$ with $\widehat{\nu} \neq 1_W$ for any coset W in $\widehat{G}$ and such that $\|\nu\| < 2$.

[2]See Exercise 25 for a definition of G^*.

36. Which functions f are idempotent (meaning $f * f = f$) and have $\|f\|_{L^p(\mu)} \leqslant 1$ for some $p > 1$? Prove $\|f\|_{L^\infty(\mu)} \leqslant 1$ using Young's inequality.

37. Prove the spectral radius formula. That is prove that

$$\|\nu^{(k)}\|^{1/k} := \|\overbrace{\nu * \cdots * \nu}^{k\text{-fold}}\|^{1/k} \to \|\widehat{\nu}\|_{\ell^\infty(\widehat{G})},$$

as $k \to \infty$ where $\nu \in M(G)$. (The limit on the right is called the spectral radius of the operator M_ν.)

38. Show that if $G = \mathbb{Z}/N\mathbb{Z}$ and $A = \{0, 1\}$ then the associated random walk requires $\Omega(|G|^2)$ steps before $\tau(\mu_k, \mu_G) \leqslant 1/10$.

39. Show that if $A \subset (\mathbb{Z}/2\mathbb{Z})^n$ contains the identity then A has spectral gap $\Omega(|A|^{-1})$. On the other hand if the random walk associated to A converges to the uniform distribution on $(\mathbb{Z}/2\mathbb{Z})^n$ show that $|A| \geqslant n + 1$. It follows from the bound (3.9) (in the notes) that if $A = \{0_G, e_1, \ldots, e_n\}$ where e_i are the canonical basis vectors then the random walk will have achieved 'good convergence' to the uniform distribution in $O(n^2)$ steps.

40. Suppose that $G = (\mathbb{Z}/2\mathbb{Z})^n$ and $A = \{0_G, e_1, \ldots, e_n\}$ as in Exercise 39. By examining $\|f_0 * \mu_A^{(k)} - 1\|_{\ell^2(G)}$ directly for a probability mass functions f_0 show that we have achieved 'good convergence' to the uniform distribution in $O(n \log n)$ steps. It turns out that this is the correct order of magnitude.

41. Explain why if $A \subset \mathbb{Z}/p\mathbb{Z}$ has size $2m + 1$ then

$$\sum_{a \in A} (1 - \operatorname{Re}\exp(2\pi i a/p)) \geqslant \sum_{|n| \leqslant m} (1 - \operatorname{Re}\exp(2\pi i n/p)).$$

Hence, or otherwise, show that if $A \subset \mathbb{Z}/p\mathbb{Z}$ contains the identity and has density α then A has spectral gap $\Omega(\alpha^2)$.

42. Use the ideas in Example 41 to give another proof that if G is an Abelian group and $A \subset G$ contains the identity then A has spectral gap $\Omega(|A|/|G|^2)$.

43. Show that if $A \subset G$ contains 0_G then A has spectral gap equal to the Rayleigh quotient

$$\sup\left\{\frac{\|M_{\mu_A} f\|_{L^2(G)}}{\|f\|_{L^2(G)}} : \langle f, 1\rangle_{L^2(G)} = 0\right\}$$

44. Given $A \subset G$ generating G which is endowed with counting measure, the edge isoperimetric number or Cheeger constant of A is defined to be

$$h(A) := \min\left\{\frac{\langle 1_S * \widetilde{1_{G\setminus S}}, 1_A\rangle_{\ell^2(G)}}{|S|} : S \subset G, |S| \leqslant |G|/2\right\}.$$

Prove that

$$h(A)/|A| \leqslant \min\left\{\frac{|S+A|}{|S|} : S \subset G, |S| \leqslant |G|/2\right\} \leqslant h(A).$$

This relates the edge isoperimetric number to the vertex isoperimetric number.

45. Given $A \subset G$ generating G we define $\lambda_2 := \sup_{\gamma \neq 0_{\widehat{G}}} \operatorname{Re}\widehat{\mu_A}(\gamma)$. (There is no modulus sign.) As mentioned in the notes the usual definition of spectral gap is $1-\lambda_2$. Show that A has spectral gap (in the sense of the lecture notes) at most $1-\lambda_2$; give an example of a set A (generating G and containing 0_G) such that $1-\lambda_2 = \Omega(1)$ and for which the spectral gap tends to 0 as $|G| \to \infty$.

46. Using the definitions of Exercises 44 and 45 prove the Cheeger-Alon-Milman inequality for Cayley graphs on Abelian groups. That is, prove that

$$|A|(1-\lambda_2) \leqslant h(A) \leqslant |A|\sqrt{2(1-\lambda_2)}.$$

47. Use the probabilistic method to show that there is a set $A \subset \{1,\dots,N\}$ containing no non-trivial three-term progressions such that $|A| = \Omega(N^{1/2})$.

48. Show that there is a set $A \subset \{1,\dots,N\}$ of size $|A| = \Omega(1)$ such that A contains no solutions to $x+y=z$.

49. Suppose that $A \subset G := (\mathbb{Z}/2\mathbb{Z})^n$ has density at least $1/2-\epsilon$ and contains no sums $x+y=z$. Show that there is some $V \leqslant G$ with $\mathbb{P}_G(A\triangle(G\backslash V)) = O(\epsilon)$.

50. Show that if $A \subset (\mathbb{Z}/3\mathbb{Z})^m$ and $B \subset (\mathbb{Z}/3\mathbb{Z})^n$ do not contain any non-trivial three-term arithmetic progressions then $A \times B$ does not contain any non-trivial three-term arithmetic progressions. Hence, or otherwise, show that there is a set $A \subset (\mathbb{Z}/3\mathbb{Z})^n$ such that $|A| \geqslant 2^n$ not containing any non-trivial three-term arithmetic progressions.

51. Given an example of a group G and Bohr set $\operatorname{Bohr}(\Gamma,\delta)$ of rank k such that

$$\mathbb{P}_G(\operatorname{Bohr}(\Gamma,\delta)) \sim (\delta/\pi)^k.$$

52. Suppose that $G = \mathbb{Z}/N\mathbb{Z}$ and $\Gamma = \{\gamma^{2^r} : 0 \leqslant r \leqslant k-1\}$ where γ generates $\widehat{G}$. Show that

$$\mathbb{P}_G(\operatorname{Bohr}(\Gamma,\delta)) = \Omega(2^{-k}\delta).$$

53. Show that if $G = \mathbb{Z}/p\mathbb{Z}$ for some prime p and Γ is size k then $\operatorname{Bohr}(\Gamma,\delta)$ contains an arithmetic progression of length $\delta p^{1/k}(1-o_{\delta\to 0}(1))/\pi$

54. Suppose that p and q are primes with $p \sim q$, $N := pq$, $G := \mathbb{Z}/N\mathbb{Z}$ and let $\gamma(x) := \exp(2\pi i x/q)$. Show that any arithmetic progression in $\operatorname{Bohr}(\{\gamma\},1/4)$ has length $O(\sqrt{N})$.

55. Show that for $G = \mathbb{Z}/p\mathbb{Z}$ for p a prime and $\delta \in (0,1]$ there is a Bohr set $\mathrm{Bohr}(\Gamma,\delta)$ of rank k such that the longest arithmetic progression in $\mathrm{Bohr}(\Gamma,\delta)$ is $O(\delta p^{1/k})$.

56. Show that if G is endowed with Haar counting measure and $A \subset G$ has size $\epsilon \log |G|$ then

$$\sup_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)| \geqslant (1 - o_{\epsilon\to 0}(1))|A|.$$

57. Give an example of a set $A \subset \{1,\dots,N\}$ of density α such that $A+A+A$ does not contain an arithmetic progression of length longer than $N^{o_{\alpha\to 0}(1)}$.

58. Convince yourself that the proof of Theorem 4.10 can be adapted to show that if $A \subset (\mathbb{Z}/3\mathbb{Z})^n$ has density α then $A+A+A$ contains an affine subspace (translate of a subspace) of co-dimension $O(\alpha^{-3})$. The co-dimension of $V \leqslant (\mathbb{Z}/3\mathbb{Z})^n$ is $n - \dim V$ when V is considered as a subspace of $(\mathbb{Z}/3\mathbb{Z})^n$ which is, in turn, considered as a vector space over $\mathbb{Z}/3\mathbb{Z}$.

59. Use the proof of the Roth-Meshulam theorem to improve the above and show that if $A \subset (\mathbb{Z}/3\mathbb{Z})^n$ has density α then $A+A+A$ contains an affine subspace of co-dimension $O(\alpha^{-1})$.

60. Show that if $G = \mathbb{Z}/p\mathbb{Z}$ for some prime p then $Q := \{x^2 \pmod p : x \in \mathbb{Z}\}$ has $|\widehat{1_Q}(\gamma)| \lesssim \sqrt{|Q|}$ whenever γ is non-trivial.

61. Show that if X is a real random variable on a finite probability space then the map $X \mapsto \|X\|$ where $\|X\|$ is the smallest non-negative constant such that

$$\mathbb{E}\exp(\lambda X) \leqslant \exp(\|X\|^2\lambda^2/2) \text{ for all } \lambda \in \mathbb{R}$$

is a norm.

62. Show that for random variables $X_1,\dots,X_n$ with $\mathbb{E}\sum_i X_i = 0$ we have

$$\mathbb{E}|\sum_i X_i|^p \leqslant O(p)^{p/2} n^{p/2-1} \sum_{k=1}^n \mathbb{E}|X_i|^p.$$

63. Show that if a random variable X has $\|X\|_{L^p(\mathbb{P})} \leqslant C\|X\|_{L^2(\mathbb{P})}$ for some $p > 2$ then $\|X\|_{L^2(\mathbb{P})} \leqslant C^{1/(p-2)}\|X\|_{L^1(\mathbb{P})}$.

64. Suppose that A is an independent subset of $G := (\mathbb{Z}/2\mathbb{Z})^n$. How large is $nA := \{a_1 + \dots + a_n : a_1,\dots,a_n \in A\}$ in terms of n and the size of A?

65. Suppose that we pick $x_1, \dots, x_k$ uniformly and independently at random from G. Show that if[3] $k = \log_3 |G| - \omega_{|G|\to\infty}(1)$ then w.h.p. $\{x_1, \dots, x_k\}$ is dissociated and if $k \geqslant \log_2 |G|$ then w.h.p. $\{x_1, \dots, x_k\}$ is not dissociated.

66. Suppose that $A \subset G$ is maximal dissociated. Show that the spectral gap of A is $\Omega(1/|A|^2)$ and hence that the random walk associated to A will have achieved 'good convergence' to the uniform distribution on G in $O(\log^3 |G|)$ steps.

67. Suppose that $k \in \mathbb{N}$ and $S \subset G$. We say that S is *k-dissociated* if

$$\sum_{s \in S} \epsilon_s s = 0_G \text{ and } \epsilon \in \{-1, 0, 1\}^S \text{ with } \|\epsilon\|_{\ell^1(S)} \leqslant k \Rightarrow \epsilon \equiv 0,$$

and write

$$\mathrm{Span}_k(S) := \{\sum_{s \in S} \epsilon_s s : \epsilon \in \{-1, 0, 1\}^S \text{ and } \|\epsilon\|_{\ell^1(S)} \leqslant k\}.$$

Show that if $S \subset T$ is maximal k-dissociated then $T \subset \mathrm{Span}_k(S)$.

68. Suppose that $G = (\mathbb{Z}/2\mathbb{Z})^n$ and suppose that $\Gamma \subset \widehat{G}$ is $2k$-dissociated. Prove that

$$\|f^\vee\|_{L^{2k}(G)} = O(\sqrt{k}\|f\|_{\ell^2(\Gamma)}) \text{ for all } f \in \ell^2(\Gamma).$$

This can be useful because begin $2k$-dissociated is a weaker condition than being dissociated. The extension of this to finite Abelian groups is proved by Shkredov in [Shk08].

69. Suppose that Γ is a dissociated set of characters on G. By considering the product

$$\prod_{\gamma \in \Gamma} (1 + \mathrm{Re}\,\gamma)$$

or otherwise show that for all $\lambda \in \widehat{G}$ we have

$$|\{\epsilon \in \{-1, 0, 1\}^\Gamma : \|\epsilon\|_{\ell^1(\Gamma)} = r \text{ and } \sum_{\gamma \in \Gamma} \epsilon_\gamma \gamma = \lambda\}| \leqslant 2^r.$$

This is a result of Rider [Rid66].

70. †† A set of characters Γ on G is said to be C-Sidon if to every $\omega \in \ell^\infty(\Gamma)$ with $\|\omega\|_{\ell^\infty(\Gamma)} \leqslant 1$ there is some measure μ_ω such that

$$\widehat{\mu_\omega}|_\Gamma = \omega \text{ and } \|\mu_\omega\| \leqslant C.$$

Prove that dissociated sets are $O(1)$-Sidon. (You may wish to use the result of Exercise 69.)

71. † Show that if Γ is C-Sidon and $p \in [2, \infty)$ then

$$\|f^\vee\|_{L^p(G)} = O(C\sqrt{p}\|f\|_{\ell^2(\Gamma)}) \text{ for all } f \in \ell^2(\Gamma).$$

[3]Here $\omega_{|G|\to\infty}(1)$ denotes a quantity which tends to infinity as $|G| \to \infty$.

72. Show that if Γ is C-Sidon then $|\Gamma| = O(C^2 \log |G|)$.

73. Show that if $A \subset G$ then $2A - 2A := \{a_0 + a_1 - a_2 - a_3 : a_0, a_1, a_2, a_3 \in A\}$ contains a Bohr set of rank $O(\alpha^{-1} \log \alpha^{-1})$ and width $\Omega(\alpha^{O(1)})$. This result is called Bogolyubov's theorem.

74. Prove Chang's theorem for functions. That is suppose that $f \in L^2(G)$ and Γ is a dissociated subset of $\{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \epsilon \|f\|_{L^1(G)}\}$. Then

$$|\Gamma| = O(\epsilon^{-2} \log(\|f\|_{L^2(G)}^2 \|f\|_{L^1(G)}^{-2})).$$

75. Use the version of Khintchine's inequality with good constants (Theorem 5.9) to show that if $g \in \ell^2(\widehat{G})$ has $\|g\|_{\ell^2(\widehat{G})} = 1$ then there is some $h \in L^2(G)$ such that $\widehat{h} = g$ and $\|h\|_{L^2(G)}^2 / \|h\|_{L^1(G)}^2 \leqslant 2$. This shows that unless $\|h\|_{L^2(G)}^2 / \|h\|_{L^1(G)}^2 \to \infty$ we cannot expect any additional structure in the large spectrum of L^2-functions.

76. Suppose that G is endowed with Haar counting measure and $A \subset G$ has $|A+A| \leqslant K|A|$. By considering $f = 1_{A+A} * 1_{-A}$ or otherwise show that $A \subset \operatorname{Span}(S)$ for some set S with $|S| = O(K \log |A|)$.

77. By using Khintchine's inequality for $p > 4$ prove the following refinement of the claim in the proof of Theorem 5.20. Given $k \in \ell^2(\widehat{G})$ and $\eta \in (0, 1/2]$ there is some choice of signs ϵ on the support of k (meaning $\epsilon : \operatorname{supp} k \to \{-1, 1\}$) and a function g with

$$\|\widehat{g} - \epsilon k\|_{\ell^2(\widehat{G})} \leqslant \eta \|k\|_{\ell^2(\widehat{G})} \text{ and } \|g\|_{L^\infty(G)} = O(\sqrt{\log \eta^{-1}} \|k\|_{\ell^2(\widehat{G})}).$$

Comments and solutions

1. First it should be remarked that this question was set by mistake: the intention was for the probabilistic method (or, equivalently, the greedy algorithm) to be used, and in that case one gets a set A with $|A| = \Omega(N^{1/3})$.

One picks the set A by taking $x \in \{1, \ldots, N\}$ independently at random with probability δ. There are $O(N^3)$ additive quadruples in $\{1, \ldots, N\}$ with all entries distinct. Let B be the set of such quadruples occurring in A, then we have

$$\mathbb{E}|B| = O(\delta^4 N^3) \text{ and } \mathbb{E}|A| = \delta N.$$

It follows that we can pick $\delta = \Omega(N^{2/3})$ such that

$$\mathbb{E}(|A| - 2|B|) \geqslant \delta N/2.$$

Hence there is a choice of elements of A such that $|A| - 2|B| \geqslant \delta N/2$, and so $|A| \geqslant \delta N/2$ and $|B| \leqslant |A|/2$. We let A' be the set A with one element in each quadruple in B removed from A. As a result of this A' has no quadruples with all elements distinct and $|A'| \geqslant |A|/2 \geqslant \delta N/4 = \Omega(N^{1/3})$ as required.

To construct a larger set we make use of the parabola. Suppose that p is an odd prime and put $A' := \{(x, x^2 \pmod p) : 1 \leqslant x \leqslant p\}$. We unwrap this construction into $\{1, ..., N\}$. Let p be an odd prime with $\sqrt{N} < 4p \leqslant 2\sqrt{N}$, which can be done by Bertrand's postulate[1] provided N is a sufficiently large (absolute) constant. Let $A := \{x + 2py : (x, y) \in A'\}$, which is a subset of $\{1, \ldots, N\}$ since $2p^2 + p \leqslant 4p^2 \leqslant N$, and if $x', y', z', w' \in A$ then

$$x' + y' = z' + w' \implies x + y = z + w \text{ and } x^2 + y^2 \equiv z^2 + w^2 \pmod p$$

If $z \neq x$ then

$$x^2 - z^2 \equiv w^2 - y^2 \pmod p \implies x + z \equiv w + y \pmod p \text{ on division by } x - z = w - y$$

which in turn implies that $x = w$. Hence A contains no non-degenerate additive quadruples and $|A| = p = \Omega(N)$.

This construction can be tightened up as in Singer [Sin38] but see also [HL63] for some details.

5. This question is about proving the estimate $\tau(x) = O(x^{o(1)})$ for the divisor function. (Equivalently this means proving $\tau(x) = O_\epsilon(x^\epsilon)$ for all $\epsilon > 0$.) We write $n = \prod_{i=1}^r p_i^{e_i}$ where the p_i are primes and the e_i are naturals using the Fundamental Theorem of Arithmetic. We divide the factors into two classes:

$$L := \{i : p_i \geqslant \exp(\epsilon^{-1})\} \text{ and } S := \{i : p_i < \exp(\epsilon^{-1})\}.$$

Now,

$$1 + e_i \leqslant \exp(e_i) \leqslant p_i^{\epsilon e_i} \text{ for all } i \in L,$$

while

$$1 + e_i \leqslant (\epsilon/\log 2)^{-1}(1 + \epsilon e_i \log 2) \leqslant (\epsilon/\log 2)^{-1} 2^{\epsilon e_i} \leqslant (\epsilon/\log 2)^{-1} p_i^{\epsilon e_i} \text{ for all } i.$$

[1]See footnote 25 of the notes.

It follows that

$$\begin{aligned}\tau(n)=\prod_{i=1}^{r}(1+e_i) &= \prod_{i\in L}(1+e_i).\prod_{i\in S}(1+e_i)\\ &\leqslant \prod_{i} p_i^{\epsilon e_i}.\prod_{i\in S}(\epsilon/\log 2)^{-1}\\ &\leqslant n^{\epsilon}(\epsilon\log 2)^{-\exp(\epsilon^{-1})}=\exp(\exp(O(\epsilon^{-1})))n^{\epsilon}\end{aligned}$$

since $|S|\leqslant\exp(\epsilon^{-1})$. The required result is proved.

17. The point of this remark is not to do this question but to explicitly pick out some particular dual groups. If $G=\mathbb{Z}/N\mathbb{Z}$ then the characters on G all have the form

$$x\mapsto\exp(2\pi ixr/N)\text{ as }r\text{ ranges }\mathbb{Z}/N\mathbb{Z}.$$

On the other hand if $G=\mathbb{F}_2^n$ then the characters are called *Walsh functions* and have the form

$$r\mapsto(-1)^{r.x}\text{ where }r.x=r_1x_1+\cdots+r_nx_n$$

and r ranges $\mathbb{F}_2^n$. The quantity $r.x$, while *not* an inner product, is quite like an inner product and algebraically it behaves in the same way.

As a final example we consider $G=\mathbb{F}_3^n$ where the characters have the form

$$r\mapsto\omega^{r.x}\text{ where }1+\omega+\omega^2=0$$

and r ranges $\mathbb{F}_3^n$.

In the first instance if N is prime then G has no non-trivial subgroups and the annihilators are consequently not interesting. This is in marked contrast to $\mathbb{F}_2^n$ and $\mathbb{F}_3^n$ which both have a rich subgroups structure.

33. (*This solution is due to Ines Marušić.*)

Let $\nu\in M(G)$ be an idempotent measure. Then either $\nu\equiv 0$ or $\|\nu\|\geqslant 1$. Indeed, by applying the algebra inequality for measures ($\|\rho_1*\rho_2\|\leqslant\|\rho_1\|\|\rho_2\|$ for all $\rho_1,\rho_2\in M(G)$) we get:

$$\|\nu\|=\|\nu*\nu\| \quad\leqslant\quad \|\nu\|^2.$$

Hence, if $\nu\not\equiv 0$, then $\|\nu\|>0$ which implies $\|\nu\|\geqslant 1$.

Given $\nu\not\equiv 0$ there is some $x\in G$ such that $|\nu(\{x\})|>0$. Hence, if we write S for the set $\{x\in G:|\nu(\{x\})|>0\}$, we conclude that S is nonempty. Suppose that $z\in G$ is such that

$|\nu(\{z\})| = \max_{x\in G}|\nu(\{x\})|$. We now have:

$$\begin{aligned} |\nu(\{z\})| = |\nu * \nu(\{z\})| &= \left|\sum_{x\in G}\nu(\{z-x\})\nu(\{x\})\right| \\ &= \left|\sum_{x\in S}\nu(\{z-x\})\nu(\{x\})\right| \\ &\leqslant \sum_{x\in S}|\nu(\{z\})||\nu(\{x\})| = |\nu(\{z\})|\|\nu\| = |\nu(\{z\})|. \end{aligned}$$

We conclude that we must have equality in the above inequality and so $\nu(\{z-x\})\nu(\{x\})$ has the same sign and $|\nu(\{z-x\})| = |\nu(\{z\})|$ for all $x \in S$. We shall now see that S is a subgroup. Write

$$M := \{z \in S : |\nu(\{z\})| = \max_{x\in G}|\nu(\{x\})|\},$$

and note that we showed that if $z \in M$ then $z-S \subset M$. On the other hand $M \subset S$ whence $M - M = M$ and since it is non-empty we conclude that M is a subgroup. But $z - S \subset M$ and so $|M| \geqslant |S|$; since $S \subset M$ we conclude that $M = S$ and so S is a subgroup.

We have shown that $\nu = c\mu_S$ where S is a subgroup and c is a function on S of modulus 1 with $c(z-x)c(x)$ constant for all $x \in S$ and given $z \in S$. This tells us that

$$c(x+y)c(0_G) = c(x)c(y) \text{ for all } x, y \in S,$$

and so $c(x) = c\gamma(x)$ for some character γ and constant c. By idempotence $c^2 = c$ and so $c = 1$ since $\nu \not\equiv 0$ and we conclude that $\nu = \gamma\mu_S$ which gives the required result on taking the Fourier transform.

34. We start by using Exercise 32 and let A be such that $1_A = \widehat{\nu}$. We now think of f defined by $f(x) := \nu(\{x\})$ as being a function in $\ell^1(G)$ so that $\widehat{\nu} = \widehat{f}$ and $\|f\|_{\ell^1(G)} = \|\nu\| \leqslant 1+\eta$. Then

$$\mathbb{P}_{\widehat{G}}(A) = \mathbb{E}_{\gamma\in\widehat{G}}|1_A(\gamma)|^2 = \sum_{x\in G}|f(x)|^2 \leqslant \left(\sum_{x\in G}|f(x)|^4\right)^{1/3}\left(\sum_{x\in G}|f(x)|\right)^{2/3}$$

by Hölder's inequality. It follows that

$$\mathbb{P}_G(A)^3/(1+\eta)^2 \leqslant \|f\|_{\ell^4(G)}^4 = \mathbb{E}1_A * 1_{-A}(x)^2$$

where the last equality is Parseval's theorem and the fact that $\widehat{|f|^2} = \widehat{f} * \widehat{\overline{f}} = 1_A * 1_{-A}$. Now follow the argument from (3.6) of the notes to conclude that there is some coset of a subgroup H such that

$$\mathbb{P}_G(A \triangle (\gamma + H)) = O(\eta^{1/2}\mathbb{P}_G(A)).$$

We separate the ℓ^1-mass of f into two parts:

$$\|f\|_{\ell^1(G)} = \sum_{x\in H^\perp}|f(x)| + \sum_{x\notin H^\perp}|f(x)|.$$

Of course,

$$\sum_{x\in H^\perp}|f(x)| = \sum_{x\in G}|f(x)1_{H^\perp}(x)| = \|1_A * \mu_H\|_{A(G)} \geqslant \|1_A * \mu_H\|_{\ell^\infty(G)} \geqslant (1 - O(\eta^{1/2});$$

and

$$\sum_{x\notin H^\perp}|f(x)| = \sum_{x\in G}|f(x)(1-1_{H^\perp})(x)| = \|1_A - 1_A * \mu_H\|_{A(G)} \geqslant \|1_A - 1_A * \mu_H\|_{\ell^\infty(G)}.$$

We conclude that

$$\|1_A - 1_A * \mu_H\|_{\ell^\infty(G)} \leqslant 1 + \eta - (1 - O(\eta^{1/2})) = O(\eta^{1/2}).$$

Thus, if $\gamma' \in \gamma + H$ we conclude $\gamma' \in A$ and conversely, so that $A = \gamma + H$ and we are done.

The point about this question is that idempotence is very rigid: there is a genuine step in the norm of idempotent measures between 1 and $1 + \Omega(1)$. This is a consequence of this result and the fact that $\|\gamma\mu_{H^\perp}\| = 1$ for any $\gamma \in \widehat{G}$ and $H \leqslant \widehat{G}$.

35. The idea here was to consider $\nu = \delta_{0_G} - \mu_V$ where $V \leqslant G$ is a subgroup of size greater than 2. Then $\widehat{\nu} = 1_{\widehat{G}} - 1_{V^\perp}$ which is an indicator function of a set and hence idempotent. Moreover,

$$\|\nu\| = 1 - \frac{1}{|V|} + (|V|-1)\frac{1}{|V|} = 2 - \frac{2}{|V|} < 2.$$

On the other hand $1_{\widehat{G}\backslash V^\perp} \neq 1_W$ for any coset W in $\widehat{G}$ since $|\widehat{G}| > |\widehat{G}\backslash V^\perp| > |\widehat{G}|(1-1/2)$ and so $|\widehat{G}\backslash V^\perp|$ does not divide $\widehat{G}$ and so is not a coset of a subgroup by Lagrange's theorem. (Note that if $|V|$ has size 2 then $\widehat{G}\backslash V^\perp$ *is* a coset of a subgroup, it is the 'other' coset of $V^\perp$.)

46. The usual lower bound is half of that given and follows from noting that

$$h(A) \geqslant \frac{|G|}{2}\min\left\{\frac{\langle 1_S * \widetilde{1_{G\backslash S}}, 1_A\rangle_{\ell^2(G)}}{|S||G\backslash S|} : S \subset G\right\}.$$

In our simpler setting the stronger bound given also holds.

The upper bound is rather harder than the lower bound. To get some intuition it may be helpful to first consider a weaker argument. One can begin by supposing that γ is such that $\operatorname{Re}\widehat{\mu_A}(\gamma) = \lambda_2 =: 1 - \epsilon$ and let

$$S := \{x \in G : |\gamma(x) - 1| \leqslant \sqrt{2}\} \text{ and } I := \{x \in G : |\gamma(x) - 1| < \delta\}$$

for some δ to be optimised later. Then

$$\mu_A(A\backslash I)\delta^2/2 \leqslant \int \operatorname{Re}(1 - \gamma(x))d\mu_A(x) = \epsilon.$$

On the other hand by construction we have

$$1_S * 1_S(x) \geqslant (1 - O(\delta))|S| \text{ for all } x \in I,$$

and we conclude that

$$\langle 1_S * 1_S, 1_A \rangle \geqslant (1 - O(\delta))|S|(1 - O(\epsilon\delta^{-2}))|A|.$$

Optimising by taking $\delta = \epsilon^{1/3}$ tells us that

$$\langle 1_S * 1_S, 1_A \rangle \geqslant (1 - O(\epsilon^{1/3}))|A||S|$$

and, of course, $|S| \leqslant |G|/2$. It follows that $h(A) = O(\epsilon^{1/3})$. The weakness with this argument is that while the map $x \mapsto \gamma(x)$ *is* measure preserving, the map $x \mapsto \operatorname{Re}\gamma(x)$ is *not* measure preserving. (At least this is true with the obvious measures on S^1 and $[-1, 1]$ respectively.) To get the actual inequality which says that $h(A) \leqslant \sqrt{2\epsilon}$ we have to remedy this problem.

It may be helpful to first prove that

$$\sum_{x,y} |\operatorname{Re}\gamma(x) - \operatorname{Re}\gamma(y)| 1_A(x - y) \leqslant |G|\sqrt{2|A|(|A| - \widehat{1_A}(\gamma))},$$

and then find a lower bound for

$$B := \sum_{x,y} |\operatorname{Re}\gamma(x) - \operatorname{Re}\gamma(y)| 1_A(x - y).$$

To do this is not trivial because of the modulus signs. It may be helpful to start by writing $1 = c_0 \geqslant c_1 \geqslant \ldots \geqslant c_R$ for the values taken by $\operatorname{Re}\gamma(x)$ and $S_i := \{x \in G : \operatorname{Re}\gamma(x) \geqslant c_i\}$, so that

$$\operatorname{Re}\gamma(x) = \sum_i (1_{S_i}(x) - 1_{S_{i-1}}(x))c_i = \sum_i 1_{S_i}(x)(c_i - c_{i+1}).$$

Then

$$\begin{aligned} B &= 2\sum_{x,y:\operatorname{Re}\gamma(x)\geqslant\operatorname{Re}\gamma(y)} |\operatorname{Re}\gamma(x) - \operatorname{Re}\gamma(y)| 1_A(x - y) \\ &\geqslant 2\sum_i \sum_{x,y} (c_i - c_{i+1}) 1_{S_i}(x) 1_{G\setminus S_i}(y) 1_A(x - y) \\ &\geqslant 2h(A)\left(\sum_{i:|S_i|\leqslant|G|/2} (c_i - c_{i+1})|S_i| + \sum_{i:|S_i|>|G|/2} (c_i - c_{i+1})(|G| - |S_i|)\right). \end{aligned}$$

From here the result is fairly straightforward.

49. The important point here is that the density is very large indeed. We write α for the density of A and note that by hypothesis

$$0 = \langle 1_A * 1_A, 1_A \rangle_{L^2(G)} = \sum_{\gamma\in\widehat{G}} \widehat{1_A}(\gamma)^3.$$

Since $G = (\mathbb{Z}/2\mathbb{Z})^n$ all the characters are real and so $\widehat{1_A}$ is real. Moreover $\widehat{1_A}(0_{\widehat{G}}) = \alpha$ as usual and so

$$-\alpha^3 = \sum_{\gamma\neq 0_{\widehat{G}}} \widehat{1_A}(\gamma)^3.$$

It follows that there is some $\gamma \neq 0_{\widehat{G}}$ such that

$$\widehat{1_A}(\gamma) < 0 \text{ and } |\widehat{1_A}(\gamma)| \geqslant \alpha^3/(\sum_{\gamma \neq 0_{\widehat{G}}} |\widehat{1_A}(\gamma)|^2) \geqslant \alpha^3/(\alpha - \alpha^2) - = \alpha(1 - O(\epsilon)),$$

since $\alpha = 1/2 - \epsilon$. On the other hand

$$\widehat{1_A}(\gamma) = \frac{|A \cap \ker \gamma|}{|G|} - \frac{|A \cap (G \setminus \ker \gamma)|}{|G|},$$

and so

$$|A \cap \ker \gamma| - |A \cap (G \setminus \ker \gamma)| \leqslant -|A|(1 - O(\epsilon)).$$

Of course

$$|A \cap \ker \gamma| + |A \cap (G \setminus \ker \gamma)| = |A|,$$

and so the result follows on setting $V := \ker \gamma$.

54. The point of this exercise is that the power of p in Lemma 4.9 cannot be improved for general cyclic groups. This is to be compared with Exercise 53 which gives a stronger bound than Lemma 4.9 using a simplification of that argument; this stronger bound does *not* extend to general cyclic groups.

55. The basic idea is to find a Bohr set whose size roughly matches the lower bound of Lemma 4.8, in particular such that for some $\eta = \Omega(p^{1/k})$ we have $\mathrm{Bohr}(\Gamma, \eta) = \{0_G\}$. Given such a Bohr set suppose that we have an arithmetic progression of length L in $\mathrm{Bohr}(\Gamma, \delta)$. Then there is a centred progression of length L in $\mathrm{Bohr}(\Gamma, 2\delta)$ by the triangle inequality. Say this progression has common difference $d \neq 0_G$, and note that

$$|\gamma_i(kd) - 1| \leqslant 2\delta \text{ for all } |k| \leqslant L/2 \text{ and } i \in \{1, \ldots, k\}.$$

If δ is smaller than some absolute constant this implies that

$$|\gamma_i(d) - 1| = O(\delta/L) \text{ for all } i \in \{1, \ldots, k\},$$

and so $d \in \mathrm{Bohr}(\Gamma, O(\delta/L))$. We can pick $L = O(\delta p^{1/k})$ large enough that this forces a contradiction and the result is proved.

It remains to find a Bohr set of the right size. To do this pick $\gamma_1, \ldots, \gamma_k$ independently and uniformly at random from $\widehat{G}$ and put $\Gamma := \{\gamma_1, \ldots, \gamma_k\}$. Then

$$\begin{aligned} \mathbb{E}\mathbb{P}_G(\mathrm{Bohr}(\Gamma, \eta)) &= \frac{1}{|G|} + \mathbb{E}\mathbb{E}_{x \in G} 1_{G \setminus \{0_G\}}(x) \prod_{i=1}^{k} 1_{\{z : |1 - \gamma_i(z)| \leqslant \eta\}}(x) \\ &= \frac{1}{|G|} + \mathbb{E}_{x \in G} \prod_{i=1}^{k} (O(\eta) + O(1/p)) \end{aligned}$$

We can pick $\eta = \Omega(p^{1/k})$ such that this mean is strictly less than $2/p$, hence there is a choice of characters with the required property.

66. The reader may wish to compare this exercise with Exercise 39. First note that if $A \subset G$ is maximal dissociated then $G \subset \mathrm{Span}(A)$ by Lemma 5.12. It follows that $3^{|A|} \geqslant |G|$ and so $|A| \geqslant \log_3 |G|$. On the other hand since A is dissociated we have $2^{|A|} \leqslant |G|$ and so $|A| = \Theta(\log |G|)$.

We now examine a Bohr set in $\widehat{G}$ using Pontryagin duality:

$$\mathrm{Bohr}(A, 1/10|A|) = \{\gamma \in \widehat{G} : |\gamma(x) - 1| \leqslant 1/10|A|\}.$$

Since $G \subset \mathrm{Span}(A)$ we see by the triangle inequality that if $\gamma \in \mathrm{Bohr}(A, 1/10|A|)$ then $|1 - \gamma(y)| \leqslant 1/10$ for all $y \in G$. It follows that $\gamma = 0_{\widehat{G}}$. We conclude that for all $\gamma \neq 0_{\widehat{G}}$ we have

$$|\widehat{1_A}(\gamma) - |A|| \geqslant \sup_{x \in A} |\gamma(x) - 1| \geqslant 1/10|A|,$$

from which the claimed bound follows.

Combining the above with our earlier result (3.9) we see that for every initial distribution μ_0 on G the random walk associated to A will have achieved 'good convergence' to the uniform distribution on G in $O(\log^3 |G|)$ steps which is much faster than the trivial estimates.

References

[HL63] H. Halberstam and R. R. Laxton. On perfect difference sets. *Quart. J. Math. Oxford Ser. (2)*, 14:86–90, 1963.

[Rid66] D. Rider. Gap series on groups and spheres. *Canad. J. Math.*, 18:389–398, 1966.

[Shk08] I. D. Shkredov. On sets of large trigonometric sums. *Izv. Ross. Akad. Nauk Ser. Mat.*, 72(1):161–182, 2008.

[Sin38] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[Sis08] O. Sisask. An additive combinatorial take on zeta constants. Available at `www.maths.qmul.ac.uk/~olof`, 2008.

Mathematical Institute, University of Oxford, 24-29 St. Giles', Oxford OX1 3LB, England

E-mail address: `tom.sanders@maths.ox.ac.uk`