Exercise sheet 5

1. Let G be a finite abelian group. For any subsets A and B of G, we denote

$$r_{A,-B}(x) = |\{(a,b) \in A \times B \mid a - b = x\}|.$$

(a) Show that for any sets A and B, we have

$$\sum_{x \in G} r_{A,-B}(x)^2 = \sum_{x \in G} r_{A,-A}(x) r_{B,-B}(x).$$

(b) We assume from now on that A is a Sidon set in G. Prove that

$$\sum_{x \in G} r_{A,-A}(x) r_{B,-B}(x) \leqslant |A||B| + |B|^2 - |B|.$$

(c) Deduce from the previous questions that

$$\sum_{x \in G} \Big(r_{A,-B}(x) - \frac{|A||B|}{|G|} \Big)^2 \leqslant |B|(|A| - 1) + \frac{|B|^2(|G| - |A|^2)}{|G|}.$$

(d) Let also C be a subset of G and define

$$N = |\{(b,c) \in B \times C \mid b + c \in A\}|.$$

Show that

$$N - \frac{|A||B||C|}{|G|} = \sum_{c \in C} \Big(r_{A,-B}(c) - \frac{|A||B|}{|G|} \Big).$$

(e) Deduce that

$$N - \frac{|A||B||C|}{|G|} \leqslant |C|^{1/2} \Big(|B|(|A| - 1) + \frac{|B|^2(|G| - |A|^2}{|G|} \Big)^{1/2}.$$

(f) Define δ by $|A| = |G|^{\frac{1}{2}} - \delta$. Show that

$$N = \frac{|A||B||C|}{|G|} + \theta(|B||C|\sqrt{|G|})^{1/2},$$

where

$$\theta \leqslant 1 + \frac{|B|}{|G|} \max(0, \delta), \qquad \theta \leqslant 1 + \frac{|C|}{|G|} \max(0, \delta).$$

(g) Show that

$$|C|\,|A \cap B| \leqslant |\{(x,y) \in -C \times (B+C) \mid x+y \in A\}|.$$

(h) Deduce that

$$|A \cap B| \leqslant \frac{|B+C||A|}{|G|} + \theta\Big(\frac{|B+C|}{|C|}\Big)^{1/2}|G|^{1/4}.$$

(a) Observe that

$$\begin{aligned}
\sum_{x \in G} r_{A,-B}(x)^2 &= \sum_{x \in G} |\{(a,b) \in A \times B | a-b=x\}|^2 \\
&= |\{(a_1,b_1),(a_2,b_2) \in A \times B | a_1-b_1=a_2-b_2\}| \\
&= \sum_{x \in G} |\{(a_1,a_2) \in A \times A, (b_1,b_2) \in B \times B | a_1-a_2=b_1-b_2=x\}| \\
&= \sum_{x \in G} r_{A,-A}(x) r_{B,-B}(x).
\end{aligned}$$

(b) If A is a Sidon set, then $r_{A,-A}(x) \leqslant 1$, for all $x \in G$. Thus,

$$\begin{aligned}
\sum_{x \in G} r_{A,-A}(x) r_{B,-B}(x) &= r_{A,-A}(0) r_{B,-B}(0) + \sum_{x \in G \setminus \{0\}} r_{A,-A}(x) r_{B,-B}(x) \\
&\leqslant |A||B| + |B|(|B|-1).
\end{aligned}$$

(c)

$$\begin{aligned}
\sum_{x \in G}\left(r_{A,-B}(x) - \frac{|A||B|}{|G|}\right)^2 &= \sum_{x \in G} r_{A.-B}(x)^2 - 2\frac{|A||B|}{|G|}\sum_{x \in G} r_{A,-B}(x) + \left(\frac{|A||B|}{|G|}\right)^2 \\
&\leqslant |A||B| + |B|^2 - |B| - \frac{|B|^2|A|^2}{|G|} \\
&= |B|(|A|-1) + |B|^2\left(\frac{|G|-|A|^2}{|G|}\right)
\end{aligned}$$

(d)

$$\begin{aligned}
\sum_{c \in C} r_{A,-B}(c) &= \sum_{c \in C} |\{(a,b) \in A \times B | a-b=c\}| \\
&= \sum_{c \in C} |\{(a,b) \in A \times B | a=b+c\}| \\
&= N.
\end{aligned}$$

(e) From item c) and Cauchy's Schwartz we have

$$\sum_{c\in C}\left(r_{A,-B}(c)-\frac{|A||B|}{|G|}\right)\leqslant |C|^{1/2}\left(\sum_{c\in C}\left(r_{A,-B}(c)-\frac{|A||B|}{|G|}\right)^2\right)^{1/2}$$
$$\leqslant |C|^{1/2}\left(|B|(|A|-1)+|B|^2\left(\frac{|G|-|A|^2}{|G|}\right)\right)^{1/2}.$$

(f) Setting $|A|=|G|^{1/2}-\delta$ in the previous inequality we have

$$N-\frac{|A||B||C|}{|G|}\leqslant |C|^{1/2}\left(|B|(|G|^{1/2}-\delta-1)+|B|^2\left(\frac{|G|-(|G|^{1/2}-\delta)^2}{|G|}\right)\right)^{1/2}$$
$$\leqslant |C|^{1/2}|B|^{1/2}|G|^{1/4}\left(1-\frac{\delta}{|G|^{1/2}}-\frac{1}{|G|^{1/2}}+\frac{|B|\delta(2|G|^{1/2}-\delta)}{|G|^{3/2}}\right)^{1/2}.$$

If $\delta\geqslant 0$ then it holds that

$$1-\frac{\delta}{|G|^{1/2}}-\frac{1}{|G|^{1/2}}+\frac{|B|\delta(2|G|^{1/2}-\delta)}{|G|^{3/2}}\leqslant 1+2\frac{|B|}{|G|},$$

and for $\delta<0$ we get

$$\frac{|\delta|}{|G|^{1/2}}-\frac{1}{|G|^{1/2}}-\frac{|B||\delta|2}{|G|}-\frac{\delta^1|B|}{|G|^{3/2}}\leqslant 0$$
$$|G||\delta|\leqslant |G|+2|B||\delta||G|^{1/2}-\delta^2|B|\leqslant 0.$$

So, from d), the symmetry of the problem for B and C and the observations above we conclude the result.

(g) Consider the map $f: C\times A\cap B\to |\{(x,y)\in -C\times(B+C)|x+y\in A\}$, $f(c,b)=(c,-c+b)$.
Observe that the map is well-defined because $c-c+b=b\in A\cap B\subset A$, and it is injective. If $(x,y)\in(Im)(f)$ then $b=x+y$ and $c=y-b$.

(h) From f) we have

$$|\{(x,y)\in -C\times(B+C)|x+y\in A\}|\leqslant\frac{|C||B+C||A|}{|G|}\theta(|B+C||C||G|^{1/2})^{1/2}.$$

Using the equality from the item above we conclude the result.

2. Let p be a prime number. Let $P\subset\mathbf{F}_p^2$ be a set of points and L a set of affine lines in $\mathbf{F}_p^2$. Assume that all lines are given by an equation $y=ax+b$ with $a\neq 0$ and that all $(u,v)\in P$ satisfy $u\neq 0$.

(a) Find a large Sidon subset $A \subset \mathbf{F}_p^\times \times \mathbf{F}_p$ and subsets B, $C \subset \mathbf{F}_p^\times \times \mathbf{F}_p$ such that

$$|\{(b,c) \in B \times C \mid b + c \in A\}| = |\{(p,\ell) \in P \times L \mid p \in \ell\}|.$$

(Hint: write the equations of the lines in the form $y = ax + b$ and the coordinates of the points as (u,v), and interpret the equation $au + b = v$.)

(b) Deduce from this and from the previous exercise that

$$|\{(p,\ell) \in P \times L \mid p \in \ell\}| = \frac{|P||L|}{p} + O(p^{1/2}\sqrt{|P||L|}).$$

(c) When is this result interesting?

(a) We consider the set $A = \{(x,x) : x \in \mathbf{F}_p^\times\} \subset \mathbf{F}_p^\times \times \mathbf{F}_p$, endowed with the operation $(x,x) + (y,y) = (xy, x+y)$. This set is shown to be a Sidon set in the Example 2.3.9 in the lecture notes.

Let $B = \{a, -b), \text{ for } l : y = ax + b \in L\}$ and $C = P$. We observe that $((a,-b),(u,v)) \in B \times C$ is such that $(a,-b) + (u,v) \in A$ if and only if $au = -b + v \Leftrightarrow v = au + b$, therefore

$$|\{(b,c) \in B \times C \mid b + c \in A\}| = |\{(p,\ell) \in P \times L \mid p \in \ell\}|.$$

(b) Observe that $|B| = |P|$, $|C| = |L|$, $|A| = p - 1$ and $|G| = p(p-1)$. Therefore, using 1f) we get

$$\begin{aligned} |\{(b,c) \in B \times C | b + c \in A\}| &= \frac{|A||B||C|}{|G|} + \theta(|B||C|\sqrt{|G|})^{1/2} \\ &= \frac{|P||L|}{p} + \theta(\sqrt{|P||L|}(p(p-1))^{1/4}) \\ &= \frac{|P||L|}{p} + O(p^{1/2}\sqrt{|P||L|}). \end{aligned}$$

(c) We want

$$\begin{aligned} \frac{|P||L|}{p} &\gg p^{1/2}\sqrt{|P||L|} \Leftrightarrow \\ \sqrt{|P||L|} &\gg p^{3/2} \Leftrightarrow \\ |P||L| &\gg p^3. \end{aligned}$$

3. Let p be a prime number. Let A_1, A_2 be subsets of $\mathbf{F}_p^\times$ and $A_3 \subset \mathbf{F}_p$. Let $G = \mathbf{F}_p^\times \times \mathbf{F}_p$ and consider the subsets

$$B = \{(x,x) \mid x \in A_1\} \subset G, \qquad C = A_2 \times A_3 \subset G.$$

(a) Show that $|B \star C| \leqslant |A_1 A_2||A_1 + A_3|$, where $\star$ refers to the group law in G.

(b) Find a large Sidon set $A \subset G$ such that $|A \cap B| = |B|$.

(c) Deduce that there exists a constant $c > 0$ such that

$$\max(|A_1 A_2|, |A_1 + A_3|) \geqslant c \min((|A_1|p)^{1/2}, |A_1|(|A_2||A_3|p^{-1})^{1/2}).$$

(d) When does this result imply a non-trivial bound for the classical sum-product problem in $\mathbf{F}_p$?

Note: the results in these exercises are due to Cilleruelo, the last one recovering a previous result of Garaev.

1. Observe that

$$|B \star C| = |\{(a_1 a_2, a_1 + a_3) \in a_i \in A_i, i = 1, 2, 3\}| \leqslant |A_1 A_2||A_1 + A_3|.$$

2. As 2a), we consider $A = \{(x, x) : x \in \mathbf{F}_p^\times\} \subset \mathbf{F}_p^\times \times \mathbf{F}_p$.

3. We use 1h) and3a)

$$|A_1| = |A \cap B| \leqslant \frac{|B + C||A|}{|G|} + \theta \left(\frac{|B + C|\sqrt{|G|}}{|C|} \right)^{1/2}$$
$$\leqslant \frac{|A_1 A_2||A_1 + A_3|}{p} + \theta \sqrt{\frac{|A_1 A_2|A_1 + A_3|p}{|A_2||A_3|}}.$$

Denote by $x = |A_1 A_2|A_1 + A_3|$ and observe that

$$p|A_1| \leqslant x + \frac{\theta p^{3/2}}{\sqrt{|A_1|A_3|}} x^{1/2},$$

therefore we can conclude that

$$\max(|A_1 A_2|, |A_1 + A_3|) \leqslant \sqrt{|A_1 A_2||A_1 + A_3|} \geqslant \min\left(\sqrt{p|A_1|}, \frac{|A_1|\sqrt{|A_1||A_3|}}{p^{1/2}} \right).$$