Combinatorial problems in finite fields and Sidon sets

Javier Cilleruelo

ICMAT-Universidad Autónoma de Madrid

4th Workshop on Fourier Analysis and Related Fields
Budapest, Hungary, 26-30 August, 2013.

In this talk we present a simple combinatorial method to study some combinatorial problems in finite fields.

1. Equations in finite fields

Sarkozy studied the number of solutions of the following equations in $\mathbb{F}_q$:

(1) $a + b = cd, \qquad a \in A,\ b \in B,\ c \in C, d \in D$

(2) $ab + 1 = cd, \qquad a \in A,\ b \in B,\ c \in C, d \in D$

Theorem (Sarkozy, 2005)

If N is the number of solutions of the equation (1) or (2), then

$$\left| N - \frac{|A||B||C||D|}{q} \right| \ll \left(|A||B||C||D|\right)^{1/2} q^{1/2}$$

The proof use estimates of exponential sums and he asked for an algebraic combinatorial proof of these results.

2. Incidence of points and lines in $\mathbb{F}_q \times \mathbb{F}_q$

Let P be a set of points and L a set of lines in $\mathbb{F}_q \times \mathbb{F}_q$. We denote by $\mathcal{I}(P, L)$ the number of incidences between P and L.

$$\mathcal{I}(P, L) = |\{(p, l) : \ p \in P, \ l \in L, \ p \in l\}|$$

Theorem (Vinh)

$$\mathcal{I}(P, L) \leq \frac{|P||L|}{q} + \sqrt{|P||L|q}.$$

3. Sum-product estimates in finite fields

Theorem (Garaev, 2007)

For any $A_1, A_2, A_3 \subset \mathbb{F}_q$ we have

$$(*) \qquad |A_1 + A_2||A_1 A_3| \gg \min(|A_1|q, |A_1|^2|A_2||A_3|/q).$$

He asked for a combinatorial proof of this estimate.

Solymosi (2010) gave a different proof of this result using the spectral graph method.

$$(*) \qquad \Longrightarrow \max(|A+A|, |AA|) \gg \min(\sqrt{|A|q}, |A|^2/\sqrt{q}),$$

which is optimal when $|A| \gg p^{2/3}$.

Sidon sets

Definition: A set $A \subset (G,+)$ is a **Sidon** set if all the differences $a-a'$, $a \neq a'$ are distinct.

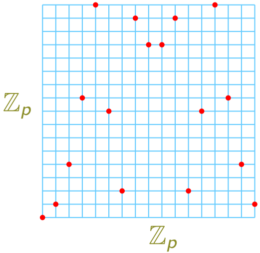
$$|A|(|A|-1) \leq |G|-1 \implies |A| \leq \sqrt{|G|-3/4}+1/2$$

The interesting Sidon sets are those with

$$|A| = \sqrt{|G|} - \delta$$

and small δ.

- The set $A = \{(x, x^2),\ x \in \mathbb{Z}_q\}$ is a Sidon set in $G = \mathbb{F}_q \times \mathbb{F}_q$ with q elements.

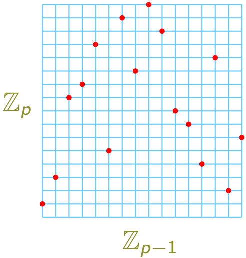


$$|A| = |G|^{1/2} - \delta, \quad \delta = 0.$$

- Let g be a generator of $\mathbb{F}_q$. The set

$$A = \{(\log_g x, x),\ x \in \mathbb{F}_q^*\}$$

is a Sidon set in $G = \mathbb{Z}_{q-1} \times \mathbb{F}_q$ with $q-1$ elements.

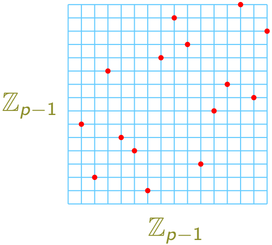


$$|A| = |G|^{1/2} - \delta, \quad \delta = 1/2 - o(1).$$

- Let g_1, g_2 be generators of $\mathbb{F}_q$. The set

$$A = \{(x,y),\ x,y \in \mathbb{Z}_{q-1},\ g_1^x + g_2^y = 1\}$$

is a Sidon set in $G = \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ with $q-2$ elements.



$$|A| = |G|^{1/2} - \delta, \quad \delta = 1.$$

The main theorem

Theorem (C.,2012)

Let A be a Sidon set in a finite abelian group G with $|A| = \sqrt{|G|} - \delta$. Then, for all $B, B' \subset G$ we have

$$|\{(b, b') \in B \times B' : \; b + b' \in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

for some θ with $|\theta| \leq 1 + \max(0, \delta)\frac{|B|}{|G|}$.

We will apply this theorem to the three Sidon sets above. For the Sidon sets in the examples we have that $0 \leq \delta \leq 1$.

In applications we have $|B| = o(|G|)$, so $|\theta| \leq 1 + o(1)$.

$$|\{(b,b')\in B\times B' :\ b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Corollary

For any $U, V \subset \mathbb{F}_q \times \mathbb{F}_q$ let $N(U,V)$ be the number of solutions of the equation

$$x_3 + x_4 = (x_1+x_2)^2, \qquad (x_1,x_3)\in U,\ (x_2,x_4)\in V.$$

We have

$$\left| N - \frac{|U||V|}{q} \right| \le \sqrt{q|U||V|}.$$

Proof: We consider the set $A = \{(x,x^2) :\ x \in \mathbb{F}_q\}$ and the sets

$$B = \{(x_1,x_3)\in U\} \qquad B' = \{(x_2,x_4)\in V\}.$$

It is clear that $(x_1,x_3)+(x_2,x_4)\in A \iff x_3+x_4=(x_1+x_2)^2$. Thus

$$N(U,V) = |\{(b,b')\in B\times B' :\ b+b'\in A\}|$$

Corollary

For any $A_1, A_2, A_3, A_4 \subset \mathbb{F}_q$ *let* N *be the number of solutions of the equation*

$$x_1 + x_2 = (x_3 + x_4)^2, \qquad x_i \in A_i$$

$$\left| N - \frac{|A_1||A_2||A_3||A_4|}{q} \right| \le \sqrt{q|A_1||A_2||A_3||A_4|}.$$

Corollary

For any $A_1, A_2 \subset \mathbb{F}_q$ *let* N *be the number of solutions of the equation*

$$x_1 + x_2 = z^2, \qquad x_1 \in A_1,\ x_2 \in A_2,\ z \in \mathbb{F}_q.$$

$$|N - |A_1||A_2|| \le \sqrt{q|A_1||A_2|}.$$

Corollary (Shkredov)

Let $A_1, A_2 \subset \mathbb{F}_q,\ |A_1||A_2| > 2q$. *Then there exist* $x, y \in \mathbb{F}_q$ *such that*

$$x + y \in A_1,\ xy \in A_2.$$

$$|\{(b,b')\in B\times B' : \; b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Corollary (Sarkozy)

For any $U, V \subset \mathbb{F}_q^* \times \mathbb{F}_q$ let $N(U,V)$ be the number of solutions of the equation

$$x_1x_2 = x_3 + x_4, \qquad (x_1,x_3)\in U,\; (x_2,x_4)\in V.$$

We have

$$\left| N - \frac{|U||V|}{q} \right| \ll \sqrt{q|U||V|}.$$

Proof: We consider the set $A = \{(\log x, x) : \; x \in \mathbb{F}_q^*\}$ and the sets

$$B = \{(\log x_1, x_3) : \; (x_1,x_3)\in U\} \qquad B' = \{(\log x_2, x_4) : \; (x_2,x_4)\in V\}.$$

It is clear that $(\log x_1, x_3) + (\log x_2, x_4) \in A \iff x_1x_2 = x_3 + x_4$. Thus

$$N(U,V) = |\{(b,b')\in B\times B' : \; b+b'\in A\}|$$

$$|\{(b,b')\in B\times B':\ b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Corollary (Sarközy)

For any $U, V \subset \mathbb{F}_q^* \times \mathbb{F}_q^*$ let $N(U,V)$ be the number of solutions of the equation

$$x_1x_2 - x_3x_4 = 1, \qquad (x_1,x_3)\in U,\ (x_2,x_4)\in V.$$

We have

$$\left| N - \frac{|U||V|}{q} \right| \ll \sqrt{q|U||V|}.$$

Proof: We consider the set $A = \{(x,y):\ g^x - g^y = 1\}$ and the sets

$$B = \{(\log x_1, \log x_3):\ (x_1,x_3)\in U\} \qquad B' = \{(\log x_2, \log x_4):\ (x_2,x_4)\in V\}.$$

It is clear that $(\log x_1, \log x_3) + (\log x_2, \log x_4) \in A \iff x_1x_2 - x_3x_4 = 1$. Thus

$$N(U,V) = |\{(b,b')\in B\times B':\ b+b'\in A\}|$$

$$|\{(b,b')\in B\times B':\ b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Theorem (Vinh)

$\mathcal{I}(P,L) = \frac{|P||L|}{q} + O\left(\sqrt{|P||L|q}\right).$

Proof: Let

$$\begin{aligned} L &= \{y = \lambda_i x + \mu_i :\ 1 \le i \le |L|\} \\ P &= \{(p_j, q_j) :\ 1 \le j \le |P|\} \end{aligned}$$

We consider the Sidon set $A = \{(\log x, x) :\ x \in \mathbb{F}_q^*\}$ and the sets

$$\begin{aligned} B &= \{b = (\log \lambda_i, -\mu_i) :\ 1 \le i \le |L|\} \\ B' &= \{b' = (\log p_j, q_j) :\ 1 \le j \le |P|\} \end{aligned}$$

We observe that
$b + b' \in A \iff \lambda_i p_j = q_j - \mu_i \iff (p_j, q_j) \in y = \lambda_i x + \mu_i$

$$\mathcal{I}(P,L) = \frac{q-1}{(q-1)q}|P||L| + \theta(|P||L|)^{1/2}((q-1)q)^{1/4} = \frac{|P||L|}{q} + O(\sqrt{|P||L|q})$$

$$|\{(b,b')\in B\times B':\ b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Corollary

Let A be a Sidon set in a finite abelian group G with $|A| = \sqrt{|G|}-\delta$. Then, for all $B, B' \subset G$ we have

$$|A\cap B| \le \frac{|B+B'||A|}{|G|} + \theta\left(\frac{|B+B'|}{|B'|}\right)^{1/2}|G|^{1/4}$$

for some θ with $|\theta| \le 1+\max(0,\delta)\frac{|B|}{|G|}$.

Proof:

$$\begin{aligned}
|B'||A\cap B| &= |\{(-b', b+b'):\ b'\in B',\ b\in B,\ -b'+(b+b')\in A\}| \\
&\le |\{(-b', b'')\in(-B')\times(B+B'),\ -b'+b''\in A\}| \\
&\le \frac{|A||B'||B+B'|}{|G|} + \theta\sqrt{|B'||B+B'|}|G|^{1/4}.
\end{aligned}$$

$$|A\cap B| \le \frac{|B+B'||A|}{|G|} + \theta\left(\frac{|B+B'|}{|B'|}\right)^{1/2}|G|^{1/4}$$

Theorem (Garaev, 2007)

Let $A_1, A_2, A_3 \in \mathbb{F}_q$. We have

$$|A_1A_2||A_1+A_3| \gg \min(|A_1|q, |A_1|^2|A_2||A_3|/q).$$

Proof: We consider the Sidon set $A = \{(\log x, x) : \ x \in \mathbb{F}_q\}$ and the sets

$$\begin{aligned} B &= (\log A_1) \times A_1 \\ B' &= (\log A_2) \times A_3 \end{aligned}$$

Since $(\log a_1, a_1) \in A$ for all $a_1 \in A_1$ we have that $|A \cap B| = |A_1|$. We observe also that $|B+B'| = |A_1A_2||A_1+A_3|$. Lemma above implies that

$$|A_1| \le \frac{|A_1A_2||A_1+A_3|}{q} + \theta\sqrt{q\frac{|A_1A_2||A_1+A_3|}{|A_2||A_3|}}.$$

$|A \cap B| \le \frac{|B+B'||A|}{|G|} + \theta \left(\frac{|B+B'|}{|B'|}\right)^{1/2} |G|^{1/4}$

Theorem (Garaev-Shen)

Let $A_1, A_2, A_3 \in \mathbb{F}_q$. We have

$$|(A_1+1)A_2||A_1A_3| \gg \min(|A_1|q, |A_1|^2|A_2||A_3|/q).$$

Proof: We consider the Sidon set $A = \{(x,y): \; g^x - g^y = 1\}$ and the sets

$$\begin{aligned} B &= (\log(A_1+1)) \times \log A_1 \\ B' &= (\log A_2) \times \log A_3 \end{aligned}$$

Since $(\log(a_1+1), \log a_1) \in A$ for all $a_1 \in A_1$ we have that $|A \cap B| = |A_1|$. We observe also that $|B+B'| = |(A_1+1)A_2||A_1A_3|$. Lemma above implies that

$$|A_1| \le \frac{|(A_1+1)A_2||A_1A_3|}{q} + \theta\sqrt{q\frac{|(A_1+1)A_2||A_1A_3|}{|A_2||A_3|}}$$

$|A \cap B| \leq \frac{|B+B'||A|}{|G|} + \theta \left(\frac{|B+B'|}{|B'|}\right)^{1/2} |G|^{1/4}$

Theorem (Solymosi, 2008)

Let $p(x)$ be a quadratic polynomial. For all $X \subset \mathbb{F}_q$ we have

$$|X + p(X)| \gg \min(\sqrt{|X|q}, |X|^2/\sqrt{q}).$$

Proof: We consider the Sidon set $A = \{(x, p(x)) : \ x \in \mathbb{F}_q\}$ and the sets

$$\begin{aligned} B &= X \times p(X) \\ B' &= p(X) \times X \end{aligned}$$

Since $(x, p(x)) \in A$ for all $x \in X$ we have that $|A \cap B| = |X|$. We observe also that $|B + B'| = |X + p(X)|^2$. Lemma above implies that

$$|X| \leq \frac{|X + p(X)|^2}{q} + O\left(\frac{|X + p(X)|}{|X|}\sqrt{q}\right)$$

$|A \cap B| \leq \frac{|B+B'||A|}{|G|} + \theta \left(\frac{|B+B'|}{|B'|} \right)^{1/2} |G|^{1/4}$

Theorem (Solymosi, 2008)

Let $p(x)$ be a quadratic polynomial. For all $X \subset \mathbb{F}_q$ we have

$$\max(|X+X|, |p(X)+p(X)|) \gg \min(\sqrt{|X|q}, |X|^2/\sqrt{q}).$$

Proof: We consider the Sidon set $A = \{(x, p(x)) : x \in \mathbb{F}_q\}$ and the sets

$$\begin{aligned} B &= X \times p(X) \\ B' &= X \times p(X) \end{aligned}$$

Since $(x, p(x)) \in A$ for all $x \in X$ we have that $|A \cap B| = |X|$. We observe also that $|B + B'| = |X + X||p(X) + p(X)|$. Lemma above implies that

$$|X| \leq \frac{|X+X||p(X)+p(X)|}{q} + O\left(\frac{\sqrt{|X+X||p(X)+p(X)|}}{|X|} \sqrt{q} \right)$$

The main theorem

Theorem (C.,2012)

Let A be a Sidon set in a finite abelian group G with $|A| = \sqrt{|G|} - \delta$. Then, for all $B, B' \subset G$ we have

$$|\{(b, b') \in B \times B' : \; b + b' \in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

for some θ with $|\theta| \leq 1 + \max(0, \delta)\frac{|B|}{|G|}$.

Proof of the main theorem

$$|\{(b,b') \in B \times B' : \; b + b' \in A\}| = \sum_{b' \in B} r_{A-B}(b').$$

i) $\sum_{x \in G} r_{A-B}(x) = |A||B|$

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

iii) $\sum_{x \in G} \left(r_{A-B}(x) - \frac{|A||B|}{|G|} \right)^2 = \sum_{x \in G} r_{A-A}(x) r_{B-B}(x) - \frac{|A|^2|B|^2}{|G|}$

$$\begin{aligned} E &= |\{(b,b') \in B \times B' : \; b + b' \in A\}| - \frac{|A|}{|G|}|B||B'| \\ &= \sum_{b' \in B'} \left(r_{A-B}(b') - \frac{|A||B|}{|G|} \right) \end{aligned}$$

$$
\begin{aligned}
E^2 &\leq \sum_{b' \in B'} 1 \sum_{b' \in B'} \left(r_{A-B}(b') - \frac{|A||B|}{|G|} \right)^2 \\
&\leq |B'| \sum_{x \in G} \left(r_{A-B}(x) - \frac{|A||B|}{|G|} \right)^2 \\
\text{by iii)} \rightsquigarrow \quad &= |B'| \left(\sum_{x \in G} r_{A-A}(x) r_{B-B}(x) - \frac{|A|^2|B|^2}{|G|} \right) \\
\text{(A is a Sidon set)} \rightsquigarrow \quad &\leq |B'| \left(|A||B| + \sum_{x \neq 0} r_{B-B}(x) - \frac{|A|^2|B|^2}{|G|} \right) \\
&= |B'| \left(|A||B| + |B|^2 - |B| - \frac{|A|^2|B|^2}{|G|} \right) \\
(|A| = |G|^{1/2} - \delta) \rightsquigarrow \quad &= |B||B'| \left(|G|^{1/2} - \delta - 1 + |B| \frac{2\delta |G|^{1/2} - \delta^2}{|G|} \right) \\
&\leq |B||B'||G|^{1/2} \left(1 + 2\max(0, \delta) \frac{|B|}{|G|} \right)
\end{aligned}
$$

The equation $g^x - g^y = \lambda$

Let g be a generator of $\mathbb{F}_p$ and let M the smallest positive integer such that

$$\{g^x - g^y : \ 1 \le x, y \le M\} = \mathbb{F}_p.$$

In other words, M is the smallest integer such that the equation

$$g^x - g^y = \lambda, \ 1 \le x, y \le M$$

has solutions for any $\lambda \in \mathbb{F}_p$.

- $M \ll p^{3/4} \log p$ (Rudnick and Zaharescu, 2000)
- $M \le Cp^{3/4}$ (Garaev and Khue, Konyagin, Shkredov, 2003)
- $M \le 2^{5/4} p^{3/4}$ (García, 2005)
- $M \le 2p^{3/4}$ (Garaev-García, personal communication)
- $M \le (\sqrt{2} + o(1))p^{3/4}$ (C., 2012)

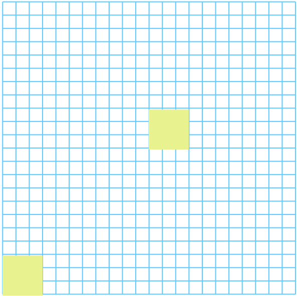
$$|\{(b,b')\in B\times B':\ b+b'\in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Proof: Suppose that the equation $g^x - g^y = \lambda,\ 1\le x,y\le M$ has not solutions. We consider the Sidon set

$$A = \{(x,y):\ g^x - g^y = \lambda\}$$

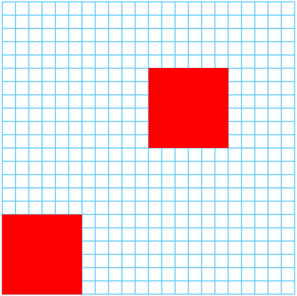
Since $(x,y)\in A \iff (y,x)+(\frac{p-1}{2},\frac{p-2}{2})\in A$, the set in red color does not contains elements of A.

B



$M/2$

$B+B$



M

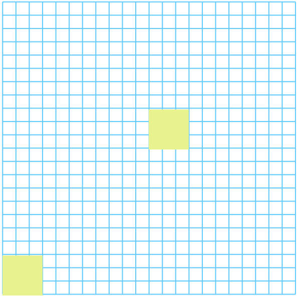
$$|\{(b,b') \in B \times B' :\ b + b' \in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}$$

Proof:

$$\frac{|A|}{|G|}|B||B'| \leq (1+o(1))(|B||B'|)^{1/2}|G|^{1/4} \implies M \leq (\sqrt{2}+o(1))p^{3/4}$$

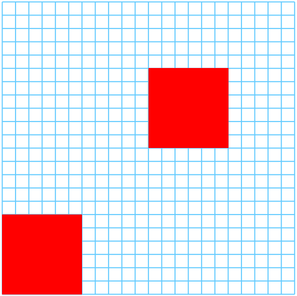
$$|B| = |B'| \sim M^2/2, \quad |A| = p-2, \quad |G| = (p-1)^2$$

B



$M/2$

$B+B$



M

Let $J(M)$ the number of solutions of

$$g^x - g^y = 1,\ 1 \le x, y \le M.$$

Theorem (Folklore)

$$J(M) = \frac{M^2}{p} + O(\sqrt{p}\log^2 p).$$

In particular, $J(M) \sim M^2/p$ *in the range* $Mp^{-3/4}\log^{-1} p \to \infty$.

Theorem (Garaev, 2006)

$$J(M) = \frac{M^2}{p} + O\left(M^{2/3}\log^{2/3}(Mp^{-3/4}+2) + \sqrt{p}\right).$$

In particular, $J(M) \sim M^2/p$ *in the range* $Mp^{-3/4} \to \infty$.

Theorem (C., 2012)

$$J(M) = \frac{M^2}{p} + O\left(\sqrt{p}e^{O(\sqrt{\log(Mp^{-3/4}+2)})}\right).$$

Let $I(M)$ be the number of solutions of

$$xy = 1, \qquad 1 \leq x, y \leq M.$$

Theorem (Folklore)

$$I(M) = \frac{M^2}{p} + O(\sqrt{p}\log^2 p).$$

In particular, $I(M) \sim M^2/p$ *in the range* $Mp^{-3/4}\log^{-1} p \to \infty$.

Theorem (Garaev, 2006)

$$I(M) = \frac{M^2}{p} + O\left(\sqrt{p}\log^2(pM^{-3/4}+2)\right).$$

In particular, $I(M) \sim M^2/p$ *in the range* $Mp^{-3/4} \to \infty$.

Saving the logarithm in the threshold

Theorem (C.-Zumalacárregui, 2013)

Let $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ be a finite abelian group and $B \subset G$ a k-dimensional box. For any subset $A \subset G$ we have

$$|A \cap B| = \frac{|A||B|}{|G|} + O_k\left(m(A)\log^k\left(\frac{|A||B|}{m(A)|G|} + 2\right)\right)$$

where

$$m(A) = \max_{\chi \neq \chi_0}\left|\sum_{a \in A} \chi(a)\right|.$$

In the interesting applications $m(A) \ll |A|^{1/2}$ holds. It is the case when A is a Sidon set with $|A| = |G|^{1/2} + O(1)$.

Applications

$$|A \cap B| = \frac{|A||B|}{|G|} + O_k\left(m(A)\log^k\left(\frac{|A||B|}{m(A)|G|} + 2\right)\right)$$

Take $A = \{(x, y) : \ g^x - g^y = 1\}, \ G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ and

$$B = [1, M] \times [1, M].$$

It is easy to check that $m(A) \leq \sqrt{p}$. Theorem above implies that if $J(M)$ is the number of solutions of

$$g^x - g^y = 1, \qquad 1 \leq x, y \leq M$$

then

$$J(M) = |A \cap B| = \frac{M^2}{p} + O\left(\sqrt{p}\log^2(Mp^{-3/4} + 2)\right)$$

Proof

Lemma

Let G be a finite abelian group. For any $A, B, C \subset G$ we have

$$|\{(b,c) \in B \times C : \ b+c \in A\}| = \frac{|A||B||C|}{|G|} + \theta \frac{m(A)}{|G|} \sum_{\chi \neq \chi_0} \left| \sum_{b \in B} \chi(b) \right| \left| \sum_{b' \in B'} \chi(b') \right|$$

for some $|\theta| \leq 1$.

Proof:

$$\begin{aligned} |\{(b,c) \in B \times C : \ b+c \in A\}| &= \frac{1}{|G|} \sum_{\chi} \sum_{a \in A, b \in B, c \in C} \chi(b+c-a) \\ &= \frac{|A||B||C|}{|G|} + Error \end{aligned}$$

Proof

Lemma

Let G be a finite abelian group. For any $A, B, C \subset G$ we have

$$|\{(b,c) \in B \times C :\ b+c \in A\}| = \frac{|A||B||C|}{|G|} + \theta \frac{m(A)}{|G|} \sum_{\chi \neq \chi_0} \left| \sum_{b \in B} \chi(b) \right| \left| \sum_{b' \in B'} \chi(b') \right|$$

for some $|\theta| \leq 1$.

Proof:

$$\begin{aligned}
|Error| &= \left| \frac{1}{|G|} \sum_{\chi \neq \chi_0} \sum_{a \in A, b \in B, c \in C} \chi(b + c - a) \right| \\
&\leq \frac{1}{|G|} \sum_{\chi \neq \chi_0} \left| \sum_{a \in A} \chi(a) \right| \left| \sum_{b \in B} \chi(b) \right| \left| \sum_{b' \in B'} \chi(b') \right| \\
&\leq \frac{m(A)}{|G|} \sum_{\chi \neq \chi_0} \left| \sum_{b \in B} \chi(b) \right| \left| \sum_{b' \in B'} \chi(b') \right|
\end{aligned}$$

Proof

$$B = \prod_{i=1}^{k} [H_i + 1, H_i + M_i]$$

We consider two approximations of B, say B', B'', and a suitable small box C such that

$$B'' + C \subset B \subset B' + C$$

$$C = \prod_{i=1}^{k} [0, m_i]$$

$$\frac{|(b'', c) \in B'' \times C : \ b'' + c \in A\}|}{|C|} \leq |A \cap B| \leq \frac{|(b', c) \in B' \times C : \ b' + c \in A\}|}{|C|}$$

Proof

For $\alpha = (\alpha_1, \ldots, \alpha_k) \in G$ we write

$$\chi_\alpha(x_1, \ldots, x_k) = e\left(\frac{\alpha_1 x_1}{n_1} + \cdots + \frac{\alpha_k x_k}{n_k}\right).$$

$$\sum_{c \in C} \chi_\alpha(c) = \prod_{i=1}^{k} \left(\sum_{c_i=0}^{m_i} e\left(\frac{\alpha_i c_i}{n_i}\right)\right)$$

$$\left|\sum_{c \in C} \chi_\alpha(c)\right| = \prod_{i=1}^{k} \min\left(\frac{4n_i}{|\alpha_i|}, m_i + 1\right)$$

$$\sum_{\alpha} \left|\sum_{b' \in B'} \chi_\alpha(b')\right| \left|\sum_{c \in C} \chi_\alpha(c)\right| \leq \prod_{i=1}^{k} \left(\sum_{0 \leq \alpha_i \leq n_i/2} \min(\tfrac{8n_i}{\alpha_i}, 4M_i) \min(\tfrac{4n_i}{\alpha_i}, m_i + 1)\right)$$