Additive structures in multiplicative subgroups

I. D. Shkredov

Steklov Mathematical Institute

Multiplicative subgroups

- p be a prime number, $\Gamma \subseteq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be a multiplicative subgroup.
- $t = |\Gamma|$, t divides $p-1$, $n = \frac{p-1}{t}$.

Structure

$$\Gamma = \{1, g^n, g^{2n}, \dots, g^{(t-1)n}\},$$

where g is a primitive root, i.e.

$$\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} = \{1, g, g^2, \dots, g^{p-2}\}.$$

$$\Gamma = \{x^n \ : \ x \in \mathbb{F}_p^*\} = \{x \in \mathbb{F}_p^* \ : \ x^t \equiv 1 \pmod p\}.$$

Uniform distribution

Definition

Γ is *uniformly distributed* if for any $\delta \in (0,1]$ and any segment Δ, $|\Delta| = \delta p$ the following holds

$$|\Gamma \cap \Delta| = \frac{|\Gamma|}{p-1} \cdot |\Delta| + o_\delta(p)\,, \quad p \to \infty\,.$$

Here $\frac{|\Gamma|}{p-1}$ is the density of Γ in $\mathbb{F}_p^*$.

If $t = |\Gamma| \geq p^{1/4+\varepsilon}$ then Γ is uniformly distributed (Konyagin).

Small subgroups

Theorem (Bourgain–Glibichuk–Konyagin, 2006)

Let $\varepsilon \in (0,1)$. If

$$|\Gamma| \geq p^{\varepsilon} \quad (\text{ or } |\Gamma| \geq p^{\frac{C}{\log\log p}})$$

then Γ is uniformly distributed.

Sum–product phenomenon

For any $A \subseteq \mathbb{F}_p$, $|A| \leq p^{1-\delta}$, we have

$$\max\{|A \cdot A|, |A+A|\} \geq c_1 |A|^{1+\varepsilon},$$

where $c_1 > 0$ is an absolute constant, $\varepsilon = \varepsilon(\delta) > 0$.

Additive properties of subgroups : sumsets

If Γ is a random set, $|\Gamma| \le \sqrt{p}$ then

$$|\Gamma \pm \Gamma| \ge |\Gamma|^{2-\varepsilon}, \quad \varepsilon > 0\,.$$

Theorem (Garcia–Voloch, 1988)

Suppose that $|\Gamma| = O(p^{3/4})$. Then

$$|\Gamma \pm \Gamma| \ge c_1 |\Gamma|^{4/3}\,.$$

Theorem (Heath–Brown and Konyagin, 2000)

Suppose that $|\Gamma| = O(p^{2/3})$. Then

$$|\Gamma \pm \Gamma| \ge c_2 |\Gamma|^{3/2}\,.$$

Theorem (Shkredov–Vyugin, 2010)

Suppose that $|\Gamma| = O(p^{1/2})$. Then

$$|\Gamma - \Gamma| \geq c_3 \frac{|\Gamma|^{5/3}}{\log^{1/2} |\Gamma|} .$$

For subgroups $|\Gamma| > p^{1/2}$ there are better results (the same method) **Schoen–Shkredov, 2010**. Applications to sum–product problems in $\mathbb{R}$, $\mathbb{C}$.

Additive properties of subgroups : expanding property

Theorem (Schoen–Shkredov, 2011)

Let $A \subseteq \Gamma$ be an arbitrary set, and $|\Gamma| = O(p^{2/3})$. Then

$$|A+\Gamma| \ge |A| \cdot \frac{|\Gamma|^3}{\mathsf{E}(\Gamma)} \ge c|A||\Gamma|^{1/2}, \quad c > 0 \,.$$

More generally, for any sets $A^{(x)} \subseteq \Gamma$, $x \in B$, $B \subseteq \Gamma$

$$\left| \bigcup_{x\in B} (x + A^{(x)}) \right| \ge \frac{|\Gamma|}{|B|\mathsf{E}(\Gamma)} \cdot \left(\sum_{x \in B} |A^{(x)}| \right)^2$$

Theorem (Shkredov–Vyugin, 2011)

Let $P \subseteq \Gamma$ be an arbitrary *progression*, and $|\Gamma| = O(p^{2/3})$. Then

$$|\Gamma + P| \geq c|\Gamma||P|^{1-o(1)}, \quad c > 0\,.$$

Higher dimensional generalizations.
Certainly, the result is best possible.

Additive properties of subgroups : intersections

Theorem (Garcia–Voloch, 1988)

If

$$|\Gamma| < \frac{p-1}{(p-1)^{1/4}+1}$$

then for any nonzero s

$$|\Gamma \bigcap (\Gamma + s)| \le 4|\Gamma|^{2/3} .$$

We generalize the result. Our generalization has found some cryptographic applications (Bourgain–Garaev–Konyagin–Shparlinski, 2011–2012).

Theorem (Shkredov–Vyugin, 2010)

Let $k \geq 2$, and $s_1, \ldots, s_{k-1} \neq 0$ be different residuals. Suppose that

$$1 \ll_k |\Gamma| \ll_k p^{1-\beta_k}\,.$$

Then

$$|\Gamma \bigcap (\Gamma + s_1) \bigcap \cdots \bigcap (\Gamma + s_{k-1})| \ll |\Gamma|^{1/2+\alpha_k}\,,$$

where $\alpha_k, \beta_k \to 0$, $k \to \infty$.

For $\Gamma =$ quadratic residuals
changing RHS to p^{ε}, $\varepsilon > 0$ implies Vinogradov conjecture.

About the proof

Theorem (Shkredov–Vyugin, 2010, again)

Let $k \geq 1$, and $\mu_1, \dots, \mu_k \neq 0$ be different residuals. Suppose that

$$1 \ll_k |\Gamma| \ll_k p^{1-\beta_k} .$$

Then

$$|\Gamma \bigcap (\Gamma + \mu_1) \bigcap \dots \bigcap (\Gamma + \mu_k)| \ll |\Gamma|^{1/2+\alpha_k} ,$$

where $\alpha_k, \beta_k \to 0$, $k \to \infty$.

Proof : Stepanov's method.

We want to estimate the cardinality of the set

$$\mathcal{E} = \Gamma \bigcap (\Gamma + \mu_1) \bigcap \dots \bigcap (\Gamma + \mu_k)\,.$$

Construct a polynomial Ψ s.t.

- Ψ is nonzero.
- $\Psi(x)$ has root of order D at any $x \in \mathcal{E}$.

Then

$$|\mathcal{E}| \le \frac{\deg \Psi}{D}\,.$$

We know that

$$\Gamma = \{x \in \mathbb{F}_p^* \ : \ x^t = 1\} , \quad t = |\Gamma| . \tag{1}$$

Put

$$\Psi(x) = \sum_{\vec{a}=(a_0,a_1,\dots,a_k)} \lambda_{\vec{a}} x^{a_0 t} (x-\mu_1)^{a_1 t} \dots (x-\mu_k)^{a_k t} .$$

By (1) we know that

$$x^{a_0 t} = (x-\mu_1)^{a_1 t} = \dots = (x-\mu_k)^{a_k t} = 1$$

at any $x \in \mathcal{E} = \Gamma \bigcap (\Gamma + \mu_1) \bigcap \dots \bigcap (\Gamma + \mu_k)$.

Thus $\Psi(x)$ has small degree.

Further for any $n < D$

$$[X(X-\mu_1)\dots(X-\mu_k)]^n \left(\frac{d}{dX}\right)^n X^{a_0 t}(X-\mu_1)^{a_1 t}\dots(X-\mu_k)^{a_k t}\Big|_{X=x}$$

$$= P_{n,\vec{a}}(x)\,, \quad \forall x \in \mathcal{E}\,.$$

We have

- ◦ Any $P_{n,\vec{a}}(x)$ has small degree.
- ◦ Coefficients of $P_{n,\vec{a}}(x)$ are linear forms on $\lambda_{\vec{a}}$.

Taking large number of $\lambda_{\vec{a}}$ we make all $P_{n,\vec{a}}(x)$ identically zero.

Why $\Psi(x)$ is nonzero? Recall that

$$\Psi(x) = \sum_{\vec{a}} \lambda_{\vec{a}} x^{a_0 t} (x-\mu_1)^{a_1 t} \dots (x-\mu_k)^{a_k t} .$$

If $\Psi(x) = 0$ then there is a polynomial

$$\sum_{\vec{b}} \lambda_{\vec{b}} c_{\vec{b}} x^{b_0 t} (x-\mu_1)^{b_1 t} \dots (x-\mu_{k-1})^{b_{k-1} t}$$

which is divided by $(x-\mu_k)^t$.

In the case of small k one can apply the unicity theorem in $\mathbb{F}_p[x]$.

We use more quantitative method.

Put

$$\Phi_i(x) = x^{b_{0,i}t}(x-\mu_1)^{b_{1,i}t}\dots(x-\mu_{k-1})^{b_{k-1,i}t}\,, \quad i = 1, 2, \dots, l\,.$$

and consider Wronskian

$$W(\Phi_1, \dots, \Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi_1'(x) & \Phi_2'(x) & \dots & \Phi_l'(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l-1)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}.$$

If a linear combination of $\Phi_{\vec{a}}(x)$ is divided by $(x-\mu_k)^t$ then $W(\Phi_1, \dots, \Phi_l)$ is divided by $(x-\mu_k)^{t-(l-1)}$.

Lemma 1

Suppose that $W(\Phi_1(x), \dots, \Phi_l(x)) = 0$ and $\deg W < p$. Then $\Phi_1(x), \dots, \Phi_l(x)$ are linearly dependent.

Lemma 2

Suppose that $W(\Phi_1(x), \dots, \Phi_l(x)) = 0$. Then $\Phi_1(x), \dots, \Phi_l(x)$ are linearly dependent provided by

$$\sum_{j=1}^{n} \deg \Phi_j \le Cp\,, \quad C > 0\,.$$

If

$$\Phi_i(x) = x^{b_{0,i}t}(x-\mu_1)^{b_{1,i}t}\dots(x-\mu_{k-1})^{b_{k-1,i}t}$$

$$W(\Phi_1,\dots,\Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi'_1(x) & \Phi'_2(x) & \dots & \Phi'_l(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l-1)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}.$$

then $W(\Phi_1,\dots,\Phi_l)$ is divided by

$$\Psi_s(x) = (x-\alpha_s)^{\left(t\sum_{i=1}^{l} b_{k,i}\right)-\frac{1}{2}l(l-1)}, \quad s = 1,\dots,k-1\,.$$

Comparing the degrees of $W(\Phi_1, \dots, \Phi_l)$ and

$$\prod_{s=0}^{k-1} \Psi_s(x)\,,$$

we obtain a contradiction.
Thus

$$\Psi(x) = \sum_{\vec{a}} \lambda_{\vec{a}} x^{a_0 t} (x-\mu_1)^{a_1 t} \dots (x-\mu_k)^{a_k t}\,.$$

is nonzero provided that not all $\lambda_{\vec{a}}$ are zero.

Work in progress ...

Theorem (Shkredov–Vyugin, 2012–??, work in progress)

$$|\Gamma \bigcap (\Gamma + s_1) \bigcap \dots \bigcap (\Gamma + s_{k-1})| \ll_k |\Gamma|^{\gamma_k} \,,$$

where $\gamma_k \to 0$, $k \to \infty$.
For any $|\Gamma| = O(\sqrt{p})$

$$|\Gamma \pm \Gamma| \ge c|\Gamma|^{2-\varepsilon} \,, \quad c, \varepsilon > 0 \,.$$

Unfortunately, for small subgroups.

Quadratic residuals and sumsets

$$R = \{x^2 \ : \ x \in \mathbb{F}_p^*\}\,, \quad |R| = \frac{p-1}{2}\,.$$

Paley Graph conjecture

Let $A, B \subseteq \mathbb{F}_p$, $|A|, |B| > p^\varepsilon$. Then

$$A + B \subsetneq R\,. \tag{2}$$

Karatsuba proved (2) for

$$|A| > p^{\varepsilon_1} \quad \text{and} \quad |B| > p^{1/2+\varepsilon_2}\,.$$

Karatsuba conjecture

Let $A, B \subseteq \mathbb{F}_p$, $|A|, |B| \sim p^{1/2}$. Then

$$A + B \subsetneq R\,.$$

Chang's results for specific A and B.

Sárközy Theorem

Theorem (Sárközy, 2012)

Let $R = A + B$, $|A|, |B| \geq 2$. Then

$$\frac{p^{1/2}}{3 \log p} < |A|, |B| < p^{1/2} \log p \,.$$

Actually (Shkredov, 2012)

$$\frac{p^{1/2}}{12} < |A|, |B| < 12p^{1/2} \,.$$

The proof uses Weil's bounds for exponential sums with Legendre symbols.

Perfect difference sets

Definition

A set A is called a *perfect difference set* if the number of the solutions of the equation

$$a_1 - a_2 = x \qquad a_1, a_2 \in A$$

does not depend on nonzero x.

For example, if $p \equiv -1 \pmod 4$ then R is a perfect difference set.

The main idea

Replace the family $\{e^{\frac{-2\pi i\lambda x}{p}}\}_{\lambda\in\mathbb{F}_p}$ and Fourier transform

$$f \to \hat{f}(\lambda) = \sum_x f(x) e^{\frac{-2\pi i\lambda x}{p}}$$

by the family

$$\{\chi(x+\lambda) - \frac{1}{\sqrt{p}}\}, \quad \lambda \in \mathbb{F}_p$$

and the transform

$$f \to \tilde{f}(\lambda) = \sum_x f(x) \left(\chi(x+\lambda) - \frac{1}{\sqrt{p}} \right),$$

$$A \dot{+} A = \{a_1 + a_2 \ : \ a_1 \neq a_2 \, , a_1, a_2 \in A\} \, .$$

Example

$A \dot{+} A = R$ and A is a *perfect difference set*:
(a) $p = 3$, $A = \{0, 1\}$.
(b) $p = 7$, $A = \{3, 5, 6\}$.
(c) $p = 13$, $A = \{0, 1, 3, 9\}$, $A = \{0, 4, 10, 12\}$.
Here $p = n^2 + n + 1$, $|A| = n + 1$, $n = q^s$, q is a prime number or 1.

Singer's Theorem

Let $n = q^s$, q is a prime number or 1. Then there is a perfect difference set $A \subseteq \mathbb{Z}/(n^2+n+1)\mathbb{Z}$, $|A| = n+1$.

In other words the number of the solutions of the equation

$$a_1 - a_2 = x \qquad a_1, a_2 \in A$$

equals 1 for all nonzero $x \in \mathbb{Z}/(n^2+n+1)\mathbb{Z}$.

Theorem (Shkredov, 2012, work in progress)

- $R = A + A$ iff $p = 3$, $A = \{2\}$.
- $R = A \dot{+} A$ then A is from example above.

Similar results for $R \approx A + A$ that is $|R \triangle (A + A)|$ small.
If $R \approx A \dot{+} A$ then A is "close" to a perfect difference set.

Thank you for your attention!