#A75 INTEGERS 16 (2016)

ON TRIPLING CONSTANT OF MULTIPLICATIVE SUBGROUPS

I.D. Shkredov[1]
Steklov Mathematical Institute, ul. Gubkina, 8, Moscow, Russia
IITP RAS, Bolshoy Karetny per. 19, Moscow, Russia
ilya.shkredov@gmail.com

Received: 4/17/15, Revised: 8/4/16, Accepted: 10/23/16, Published: 11/11/16

Abstract
We prove that any multiplicative subgroup Γ of the prime field $\mathbb{F}_p$ with $|\Gamma| < \sqrt{p}$ satisfies $|3\Gamma| \gg \frac{|\Gamma|^2}{\log|\Gamma|}$. Also, we obtain a bound for the multiplicative energy of any nonzero shift of Γ, namely $\mathsf{E}^{\times}(\Gamma + x) \ll |\Gamma|^2 \log|\Gamma|$, where $x \neq 0$ is arbitrary.

1. Introduction

Let p be a prime number, $\mathbb{F}_p$ be the finite field, and $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Also, let $\Gamma \subseteq \mathbb{F}_p^*$ be an arbitrary multiplicative subgroup. Such subgroups were studied by various authors (see the references in [7]). One of the interesting questions is the determination of the *additive* structure of multiplicative subgroups see, e.g., [1, 3, 4, 5, 10, 11, 12, 14]. In particular, what can we say about the size of sumsets of subgroups, that is, about the sets of the form

$$2\Gamma = \Gamma + \Gamma := \{\gamma_1 + \gamma_2 \ : \ \gamma_1, \gamma_2 \in \Gamma\}\,?$$

There is a well–known conjecture that the sumset 2Γ contains $\mathbb{F}_p^*$, provided $|\Gamma| > p^{1/2+\varepsilon}$, where $\varepsilon > 0$ is any number and $p \geq p(\varepsilon)$ is large enough. In this article we study the bigger set $3\Gamma = \Gamma + \Gamma + \Gamma$, instead of 2Γ. Let us formulate the main result of our paper.

Theorem 1. *Let p be a prime number, $\Gamma \subset \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| < \sqrt{p}$. Then*

$$|3\Gamma| \gg \frac{|\Gamma|^2}{\log|\Gamma|}\,.$$

[1]This work was supported by grant Russian Scientific Foundation RSF 14–11–00433.

It is interesting to compare Theorem 1 with a result of A.A. Glibichuk who obtained in [4] that $|4\Gamma| > p/2$ provided $|\Gamma| > \sqrt{p}$, as well as with a result from [12], which asserts that

$$\mathbb{F}_p^* \subseteq 5\Gamma\,, \quad \text{if} \quad -1 \in \Gamma \quad \text{and} \quad |\Gamma| \gg \sqrt{p} \cdot \log^{1/3} p\,.$$

Let us say a few words about the proof. In [9] O. Roche–Newton obtained that for any set A from $\mathbb{R}$ there are $a, b \in A$ such that

$$|(A+a)(A+b)| \gg \frac{|A|^2}{\log |A|}\,. \tag{1}$$

More precisely, it was proved in [9] that the common multiplicative energy (see the definition in Section 2) of $A+a$ and $A+b$ is small:

$$\mathsf{E}^\times(A+a, A+b) \ll |A|^2 \log |A|\,. \tag{2}$$

The proof used the Szemerédi–Trotter Theorem from the incidence geometry. Roche–Newton calculated the number of collinear triples in the Cartesian product $A \times A$ in two different ways and comparing these two estimates gives (2). In our arguments, we use Stepanov's method [15] in the form of Mit'kin [8] (see also [6] and [7]), which allows us to get (1), (2) for A being any multiplicative subgroup of size less than $\sqrt{p}$. It is easy to see that such an analog of (1) implies Theorem 1. Notice also that in the case of a multiplicative subgroup A, bound (2) is equivalent to

$$\mathsf{E}^\times(A+1) \ll |A|^2 \log |A|$$

because $A + a = a(A+1)$, $A+b = b(A+1)$, $a, b \in A$. Thus the method allows us to obtain a good upper bound for the multiplicative energy of $A+1$ (and actually of any shift $A+x$, $x \in \mathbb{F}_p^*$, see Theorem 2 of Section 4).

2. Notation

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ be two functions. Define

$$(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y) g(x-y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbb{F}_p} f(y) g(y+x)\,. \tag{3}$$

Replacing the addition by the multiplication, one can define the *multiplicative convolution* of two functions f and g. Write $\mathsf{E}^+(A, B)$ for the *additive energy* of two sets $A, B \subseteq \mathbb{F}_p$ (see, e.g., [16]), that is,

$$\mathsf{E}^+(A,B) = |\{a_1 + b_1 = a_2 + b_2 \ : \ a_1, a_2 \in A,\, b_1, b_2 \in B\}|\,.$$

If $A = B$ we simply write $\mathsf{E}^+(A)$ instead of $\mathsf{E}^+(A, A)$. Clearly,

$$\mathsf{E}^+(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x) . \quad (4)$$

Denote by $|S|$ the cardinality of a set $S \subseteq \mathbb{F}_p$. Notice that by the Cauchy–Schwarz inequality one has

$$\mathsf{E}^+(A, B) \le \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\} , \quad (5)$$

and

$$\mathsf{E}^+(A, B)^2 \le \mathsf{E}^+(A)\mathsf{E}^+(B) . \quad (6)$$

In the same way define the *multiplicative energy* of two sets $A, B \subseteq \mathbb{F}_p$

$$\mathsf{E}^\times(A, B) = |\{a_1 b_1 = a_2 b_2 \ : \ a_1, a_2 \in A, \, b_1, b_2 \in B\}| \ .$$

Certainly, multiplicative energy $\mathsf{E}^\times(A, B)$ can be expressed in terms of multiplicative convolutions, similar to (4).

Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. A set $Q \subseteq \mathbb{F}_p^*$ is called Γ*–invariant* if $Q\Gamma = Q$. All logarithms are base 2. Signs $\ll$ and $\gg$ are the usual Vinogradov's symbols, so $a \ll b$ means $a = O(b)$ and $a \gg b$ is equivalent to $b = O(a)$.

3. On Sumsets of Multiplicative Subgroups

In this section we have to deal with the quantity (here T stands for *collinear triples*)

$$\mathsf{T}(A, B, C, D) := \sum_{c \in C, \, d \in D} \mathsf{E}^\times(A - c, B - d) . \quad (7)$$

Because $\mathsf{E}^\times(A - c, B - b) \ge |A||B|$, it follows that $\mathsf{T}(A, B, C, D) \ge |A||B||C||D|$. It turns out that there is the same upper bound for T up to logarithmic factors in the case of A, B, C, D equal some cosets of a multiplicative subgroup. The proof is based on the following lemma of Mit'kin [8], see also [13].

Lemma 1. *Let $p > 2$ be a prime number, Γ, Π be subgroups of $\mathbb{F}_p^*$, M_Γ, M_Π be sets of distinct coset representatives of Γ and Π, respectively. For an arbitrary set $\Theta \subset M_\Gamma \times M_\Pi$ such that $(|\Gamma||\Pi|)^2|\Theta| < p^3$ and $|\Theta| \le 33^{-3}|\Gamma||\Pi|$, we have*

$$\sum_{(u,v) \in \Theta} \Big|\{(x, y) \in \Gamma \times \Pi : ux + vy = 1\}\Big| \ll (|\Gamma||\Pi||\Theta|^2)^{1/3} . \quad (8)$$

Using the lemma above, we prove the main technical result of this section. The proof is in spirit of [9].

Proposition 1. *Let p be a prime number, Γ, Π be subgroups of $\mathbb{F}_p^*$. Suppose that $|\Gamma||\Pi| < p$. Then*

$$\sum_{\gamma\in\Gamma,\, \pi\in\Pi} \mathsf{E}^{\times}(\Gamma-\gamma, \Pi-\pi) \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma||\Pi|(|\Gamma|^2 + |\Pi|^2)\,. \quad (9)$$

Proof. Consider the equation

$$(a-b)(a'-c') = (a-c)(a'-b')\,, \quad a,b,c \in \Gamma\,, \quad a',b',c' \in \Pi\,. \quad (10)$$

Clearly, the number of solutions to the equation is

$$\mathsf{T}(\Gamma,\Pi,\Gamma,\Pi) = \sum_{\gamma\in\Gamma,\, \pi\in\Pi} \mathsf{E}^{\times}(\Gamma-\gamma, \Pi-\pi)\,.$$

One can assume that products in (10) are nonzero and $b \neq c$ because otherwise we have at most $O(|\Gamma|^3|\Pi| + |\Gamma||\Pi|^3 + |\Pi|^2|\Gamma|^2)$ number of solutions. Denote by σ the remaining number of solutions.

Take a parameter $\tau \geq 2$ and define

$$\Theta_\tau := \{(u,v) \in M_\Gamma \times M_\Pi \ :\ |\{(x,y) \in \Gamma\times\Pi : ux+vy=1\}| \geq \tau\}\,.$$

In other words, Θ_τ counts the number of lines $l_{u,v} = \{(x,y) : ux+vy=1\}$, $(u,v) \in M_\Gamma \times M_\Pi$ having the intersection with $\Gamma\times\Pi$ greater than τ. Obviously, if $(u,v) \equiv (u',v') \mod (\Gamma\times\Pi)$, then the intersections of lines $l_{u,v}$ and $l_{u',v'}$ with $\Gamma\times\Pi$ coincide. By Lemma 1, we have $|\Theta_\tau| \ll |\Gamma||\Pi|\tau^{-3}$, provided $(|\Gamma||\Pi|)^2|\Theta_\tau| < p^3$ and $|\Theta_\tau| \leq 33^{-3}|\Gamma||\Pi|$. Thus

$$q_\tau := \{(u,v) \ :\ |\{(x,y) \in \Gamma\times\Pi : ux+vy=1\}| \geq \tau\} \ll |\Gamma|^2|\Pi|^2\tau^{-3}\,, \quad (11)$$

provided $(|\Gamma||\Pi|)^2|\Theta_\tau| < p^3$ and $|\Theta_\tau| \leq 33^{-3}|\Gamma||\Pi|$. The number of all lines intersecting $\Gamma\times\Pi$ by at least two points does not exceed $|\Gamma|^2|\Pi|^2$. Thus, splitting Θ_τ into smaller sets if its required, we get upper bound (11) for q_τ with possibly bigger absolute constant, provided the only condition $(|\Gamma||\Pi|)^2|\Theta_\tau| < p^3$ holds. The assumption $|\Gamma||\Pi| < p$ implies the last inequality.

It is easy to see that for any tuple (a,a',b,b',c,c') satisfying (10), the points (a,a'), (b,b'), (c,c') lie on the same line and these points are pairwise distinct. Clearly, the number of such triples belonging the lines that have the form $ux+vy=0$ and intersect $\Gamma\times\Pi$ does not exceed $(|\Gamma||\Pi|)^2$, so it is negligible. Thus, using (11), we see that the remaining part of the quantity σ is less than

$$\sum_{u,v} |l_{u,v} \cap (\Gamma\times\Pi)|^3 \ll \sum_{j\geq 1} \sum_{u,v:\ 2^{j-1} < |l_{u,v}\cap(\Gamma\times\Pi)| \leq 2^j} |l_{u,v}\cap(\Gamma\times\Pi)|^3 \ll$$

$$\ll \sum_{j\geq 1} 2^{3j} \cdot |\Gamma|^2|\Pi|^2 2^{-3j} \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\})\,.$$

This completes the proof. $\square$

Remark 1. A careful analysis of the proof gives that one can assume that a, b, c belong to different cosets of Γ and a', b', c' are from different cosets of Π (it will be three Cartesian products of cosets instead of one in this case). In particular, the following holds

$$\sum_{\gamma\in\xi\Gamma,\, \pi\in\eta\Pi} \mathsf{E}^{\times}(\Gamma-\gamma, \Pi-\pi) \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma||\Pi|(|\Gamma|^2+|\Pi|^2)\,, \quad (12)$$

where $\xi, \eta \in \mathbb{F}_p^*$ are arbitrary. Of course, one can permute Γ to $\xi\Gamma$ and Π to $\eta\Pi$ in formula (12).

Proposition 1 allows us to prove new results on sumsets of subgroups, which improve some bounds from [3], see Lemma 7.3 and also Lemma 7.4.

Corollary 1. *Let p be a prime number, $\Gamma \subset \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| < \sqrt{p}$. Then*

$$\left|\left\{ \frac{a \pm b}{a \pm c} \;:\; a, b, c \in \Gamma \right\}\right| \gg \frac{|\Gamma|^2}{\log|\Gamma|}\,,$$

and for any $X \subseteq \Gamma$ one has

$$|2\Gamma + X| \gg \frac{|X|^2}{\log|\Gamma|}\,.$$

In particular,

$$|3\Gamma| \gg \frac{|\Gamma|^2}{\log|\Gamma|}\,.$$

Proof. The first estimate follows from the Cauchy–Schwarz inequality and the interpretation of the quantity $\mathsf{T}(\Gamma, \Pi, \Gamma, \Pi)$ for $\Gamma = \Pi$ as the number of solutions to (12) with $\xi = \pm 1$, $\eta = \pm 1$. To get the second estimate one applies (12) with parameters $\Gamma = \Gamma$, $\Pi = \Gamma$, $\xi = \eta = -1$. We find $\gamma_1, \gamma_2 \in \Gamma$ such that

$$\mathsf{E}^{\times}(\Gamma + \gamma_1, \Gamma + \gamma_2) \ll |\Gamma|^2 \log|\Gamma|$$

because by formula (7) and Proposition 1 one has

$$|\Gamma|^2 \min_{\gamma_1,\gamma_2\in\Gamma} \mathsf{E}^{\times}(\Gamma+\gamma_1, \Gamma+\gamma_2) \le \sum_{\gamma_1,\gamma_2\in\Gamma} \mathsf{E}^{\times}(\Gamma+\gamma_1, \Gamma+\gamma_2) = \mathsf{T}(\Gamma, \Gamma, -\Gamma, -\Gamma) \ll |\Gamma|^4 \log|\Gamma|\,.$$

By the Cauchy–Schwarz inequality (5), we get

$$|(\Gamma+\gamma_1)(X+\gamma_2)| \cdot \mathsf{E}^{\times}(\Gamma+\gamma_1, \Gamma+\gamma_2) \ge |(\Gamma+\gamma_1)(X+\gamma_2)| \cdot \mathsf{E}^{\times}(\Gamma+\gamma_1, X+\gamma_2) \ge |\Gamma|^2|X|^2\,.$$

Notice that $(\Gamma + \gamma_1)(X + \gamma_2) \subseteq 2\Gamma + \gamma_1 X + \gamma_1\gamma_2$. Moreover, $|2\Gamma + \gamma_1 X + \gamma_1\gamma_2| = |2\Gamma + X|$. Hence

$$|2\Gamma + X| \ge |(\Gamma + \gamma_1)(X + \gamma_2)| \gg \frac{|X|^2}{\log|\Gamma|}$$

as required. $\square$

We are going to apply the method of this section to the problems concerning decompositions of multiplicative subgroups in the future paper.

4. Generalizations

First of all, we derive a consequence of Proposition 1 concerning multiplicative energies of shifts of subgroups.

Theorem 2. *Let p be a prime number, and let Γ, Π be multiplicative subgroups of $\mathbb{F}_p^*$. Suppose that $|\Gamma||\Pi| < p$. Then for any $x, y \neq 0$ one has*

$$\mathsf{E}^{\times}(\Gamma + x, \Pi + y) \ll |\Gamma||\Pi| \log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma|^2 + |\Pi|^2 .$$

Proof. Since $x, y \neq 0$, it follows that $x \in \xi\Gamma$, $y \in \eta\Pi$ and $\xi, \eta \neq 0$. Further it is easy to see that

$$\mathsf{E}^{\times}(\Gamma + x, \Pi + y) = \mathsf{E}^{\times}(\xi^{-1}\Gamma + \gamma, \eta^{-1}\Pi + \pi)$$

for *any* $\gamma \in \Gamma$ and $\pi \in \Pi$. Thus all energies in the left–hand side of formula (12) coincide. This completes the proof. $\square$

Corollary 2. *Let p be a prime number, and let Γ be a multiplicative subgroup of $\mathbb{F}_p^*$, $|\Gamma| < \sqrt{p}$, and Q be Γ–invariant set. Then*

$$\mathsf{E}^{\times}(\Gamma + x, Q + y) \ll |Q|^2 \log |\Gamma| ,$$

where $x, y \in \mathbb{F}_p^*$ are arbitrary.

Proof. Split the set Q into cosets over Γ, that is, write $Q = \bigsqcup_{j=1}^s \xi_j \Gamma$, $s = |Q|/|\Gamma|$. Then using the Cauchy–Schwartz inequality, we obtain

$$\mathsf{E}^{\times}(\Gamma + x, Q + y) = \sum_{i,j=1}^{s} \sum_{z} ((\Gamma + x) \circ (\Gamma + x))(z)((\xi_i\Gamma + y) \circ (\xi_j\Gamma + y))(z) =$$

$$= \sum_{i,j=1}^{s} \sum_{z} ((\Gamma + x) \circ (\xi_i\Gamma + y))(z)((\Gamma + x) \circ (\xi_j\Gamma + y))(z) \leq$$

$$\leq \sum_{i,j=1}^{s} (\mathsf{E}^{+}(\Gamma + x, \xi_i\Gamma + y))^{\frac{1}{2}} (\mathsf{E}^{+}(\Gamma + x, \xi_j\Gamma + y))^{\frac{1}{2}} = \left(\sum_{i=1}^{s} \mathsf{E}^{+}(\Gamma + x, \xi_i\Gamma + y))^{\frac{1}{2}} \right)^2$$

$$\leq s \sum_{i=1}^{s} \mathsf{E}^{+}(\Gamma + x, \xi_i\Gamma + y) .$$

Now applying the last bound, as well as Theorem 2 (see Remark 1), we have

$$\mathsf{E}^{\times}(\Gamma+x, Q+y) \ll s^2|\Gamma|^2 \log|\Gamma| = |Q|^2 \log|\Gamma|$$

as required. $\square$

It is interesting to compare the last theorem with results of [2] and [17] which give a pointwise bound for the multiplicative convolution of characteristic functions of multiplicative subgroups in contrary to our average estimate.

Using formula

$$\mathsf{E}^{+}(\Gamma) = \mathsf{E}^{\times}(\Gamma, \Gamma+1)$$

for an arbitrary subgroup Γ ($\gamma_1(\gamma_2+1) = \gamma'_1(\gamma'_2+1) \Leftrightarrow \gamma_1\gamma_2 + \gamma_1 = \gamma'_1\gamma'_2 + \gamma'_1 \Leftrightarrow \tilde{\gamma}_1 + \tilde{\gamma}_2 = \tilde{\gamma}'_1 + \tilde{\gamma}'_2$ for any $\gamma_j, \gamma'_j, \tilde{\gamma}_j, \tilde{\gamma}'_j$ from Γ), we derive by the Cauchy–Schwarz inequality and Theorem 2 that $\mathsf{E}^{+}(\Gamma) \ll |\Gamma|^{5/2} \log^{1/2}|\Gamma|$. Indeed, by (5), (6)

$$\mathsf{E}^{+}(\Gamma)^2 = (\mathsf{E}^{\times}(\Gamma, \Gamma+1))^2 \le \mathsf{E}^{\times}(\Gamma)\mathsf{E}^{\times}(\Gamma+1) \ll \mathsf{E}^{\times}(\Gamma)|\Gamma|^2\log|\Gamma| \le |\Gamma|^5 \log|\Gamma|\,.$$

This coincides with Konyagin's bound [6] up to logarithmic factors.

Let us prove a generalization of Proposition 1 and Theorem 2.

In the proof we need the notion of incidences between points and lines. Let $\mathbb{F}_q$, $q=p^n$, be a finite field. Suppose that we have a subset $\mathcal{P}$ of $\mathbb{F}_q \times \mathbb{F}_q$ which we call the set of points and also we have some set of lines $\mathcal{L}$. The number of *incidences* between points $\mathcal{P}$ and lines $\mathcal{L}$ is

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

A trivial upper bound for the quantity $\mathcal{I}(\mathcal{P}, \mathcal{L})$ can be found in [16], see Section 8.2, namely,

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) \ll \min\{|\mathcal{P}||\mathcal{L}|^{1/2} + |\mathcal{L}|, |\mathcal{P}|^{1/2}|\mathcal{L}| + |\mathcal{P}|\}\,. \tag{13}$$

Theorem 3. *Let p be a prime number, Γ, Π be multiplicative subgroups of $\mathbb{F}_p^*$. Suppose that $|\Gamma||\Pi| < p$ and Q_1 is Γ–invariant, Q_2 is Π–invariant sets. Then*

$$\mathsf{T}(Q_1, Q_2, Q_1, Q_2) \ll \frac{|Q_1|^3|Q_2|^3}{|\Gamma||\Pi|} \log^2(\min\{|Q_1|, |Q_2|\}) + |Q_1||Q_2|(|Q_1|^2 + |Q_2|^2)\,. \tag{14}$$

Proof. Let $L = \log(\min\{|Q_1|, |Q_2|\})$. We use the arguments of Proposition 1 and interpret the quantity $\mathsf{T}(Q_1, Q_2, Q_1, Q_2)$ as the number of collinear triples in $Q_1 \times Q_2$ in particular. The term $|Q_1||Q_2|(|Q_1|^2 + |Q_2|^2) + |Q_1|^2|Q_2|^2$ in (14) corresponds to degenerate triples (vertical, horizontal and lying on exceptional lines) and appears similarly as in the proof of Proposition 1. Thus, we are considering the set of lines (pairs)

$$\mathcal{L}_\tau := \{(u,v) \;:\; |\{(x,y) \in Q_1 \times Q_2 : ux + vy = 1\}| \ge \tau\}$$

intersecting $Q_1 \times Q_2$ in at least $\tau \geq 3$ distinct points and we want to obtain a good upper bound for the size of the set to estimate the number of collinear triples. Let $Q_1 \times Q_2 = \bigsqcup_{i=1}^{s} C_i$, where C_i are products of the corresponding cosets, $s = |Q_1||Q_2||\Gamma|^{-1}|\Pi|^{-1}$. Taking a line $l \in \mathcal{L}_\tau$ and using the diadic Dirichlet principle, we find a number $\Delta(l)$ such that

$$\tau \leq |l \cap (Q_1 \times Q_2)| \leq \sum_{i=1}^{s} |l \cap C_i| \leq 2 \sum_{i \,:\, |l \cap C_i| \geq \tau (2s)^{-1}} |l \cap C_i| \ll L \Delta(l) |\Omega_\Delta(l)|\,,$$

where

$$\Omega_\Delta(l) = \{ i \;:\; \Delta < |l \cap C_i| \leq 2\Delta \}\,,$$

and $\Delta(l) \geq 2^{-1} \max\{\tau s^{-1}, 1\}$. The number $\Delta(l)$ depends on l, but using the diadic Dirichlet principle again, we find a set $\mathcal{L}'_\tau \subseteq \mathcal{L}_\tau$, $|\mathcal{L}'_\tau| \gg |\mathcal{L}_\tau| L^{-1}$ with some fixed $\Delta \geq \max\{\tau s^{-1}, 1\}$. After that, applying the arguments of Proposition 1, we see

$$|\mathcal{L}_\tau| L^{-1} \ll |\mathcal{L}'_\tau| \ll \frac{|\Gamma|^2 |\Pi|^2}{\Delta^3} \ll \frac{|\Gamma|^2 |\Pi|^2 s^3}{\tau^3}$$

and we have obtained (14).

Let us give another proof. Take the same family of the lines $\mathcal{L}'_\tau$ and consider a smaller family of points $\mathcal{P}' := \bigcup_{l \in \mathcal{L}'_\tau} \bigsqcup_{i \in \Omega_\Delta(l)} C_i$. Using Lemma 1, as well as the arguments of the proof of Proposition 1 again, we see that any line meets at most $|\Gamma||\Pi|\Delta^{-3}$ cells C_i. In other words, $|\Omega_\Delta(l)| \ll |\Gamma||\Pi|\Delta^{-3}$. Let us calculate the number of incidences $I(\mathcal{L}'_\tau, \mathcal{P}')$ between lines from $\mathcal{L}'_\tau$ and points $\mathcal{P}'$. On the one hand, any line from $\mathcal{L}'_\tau$ contains at least $\Delta |\Omega_\Delta(l)| \gg \tau L^{-1}$ number of points. Thus

$$I(\mathcal{L}'_\tau, \mathcal{P}') \gg \Delta |\mathcal{L}'_\tau| |\Omega_\Delta(l)| \gg |\mathcal{L}'_\tau| \tau L^{-1}\,.$$

On the other hand, by estimate (13), we get

$$I(\mathcal{L}'_\tau, \mathcal{P}') \leq \sum_{i=1}^{s} I(\mathcal{L}'_\tau, \mathcal{P}' \cap C_i) \leq \sum_{i=1}^{s} \left(|\mathcal{P}' \cap C_i| |L_i|^{1/2} + |L_i| \right)\,,$$

where by L_i we denote the lines from $\mathcal{L}'_\tau$, intersecting C_i. Clearly, $|\mathcal{P}' \cap C_i| = |\Gamma||\Pi|$. Further since any line l meets at most $|\Omega_\Delta(l)| \ll |\Gamma||\Pi|\Delta^{-3}$ cells C_i, we see that

$$\sum_{i=1}^{s} |L_i| \ll |\mathcal{L}'_\tau| \cdot |\Gamma||\Pi|\Delta^{-3}\,.$$

Using the estimate $|\Omega_\Delta(l)|\Delta \gg \tau L^{-1}$, the Cauchy–Schwarz inequality and the lower bound for $I(\mathcal{L}'_\tau, \mathcal{P}')$, we obtain

$$|\mathcal{L}_\tau| L^{-1} \ll |\mathcal{L}'_\tau| \ll \frac{L |\Gamma|^2 |\Pi|^2 s}{\Delta \tau} \ll \frac{L |\Gamma|^2 |\Pi|^2 s}{\tau \max\{1, \tau s^{-1}\}}\,.$$

After some calculations we have (14). This completes the proof. $\square$

Remark 2. Considering $\mathsf{T}(Q_1, Q_2, \xi Q_1, \eta Q_2)$, where $\xi \neq 0, 1$ or $\eta \neq 0, 1$ one can reduce the term $|Q_1||Q_2|(|Q_1|^2 + |Q_2|^2)$ in formula (14) of Theorem 3 sometimes. For example, if Γ is a subgroup, Q is Γ–invariant set, then the corresponding error term in $\mathsf{T}(\Gamma, Q, \xi\Gamma, Q)$, $\xi \neq 0, 1$ is $O(|\Gamma|^3|Q| + |\Gamma|^2|Q|^2)$, and thus it is negligible.

References

[1] T. Cochrain, C. Pinner. Sum–product estimates applied to Waring's problem mod p, *Integers* **8**, A46 (2008), 1–18.

[2] P. Corvaja, U. Zannier. Greatest common divisors of $u - 1$, $v - 1$ in positive characteristic and rational points on curves over finite fields, *J. Eur. Math. Soc.* **15** (2013), 1927–1942.

[3] T. Cochrain, D. Hart, C. Pinner, C. Spencer. Waring's number for large subgroups of double–struck $\mathbb{Z}_p$, *Acta Arithmetica* **163**:4 (2014), 309–325.

[4] A. A. Glibichuk. Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem, *Mat. Zametki* **79** (2006), 384–395; translation in: *Math. Notes* **79** (2006), 356–365.

[5] D. Hart. A note on sumsets of subgroups in $\mathbb{Z}_p^*$, *Acta Arithmetica* **161** (2013), 387–395.

[6] S. V. Konyagin. Estimates for trigonometric sums and for Gaussian sums, *IV International conference "Modern problems of number theory and its applications". Part 3* (2002), 86–114.

[7] S. V. Konyagin, I. Shparlinski, *Character sums with exponential functions*, Cambridge University Press, Cambridge, 1999.

[8] D. A. Mit'kin. Estimation of the total number of the rational points on a set of curves in a simple finite field, *Chebyshevsky sbornik* **4**:4 (2003), 94–102.

[9] O. Roche–Newton. A short proof of a near–optimal cardinality estimate for the product of a sum set, *Proceedings of the 31st Symposium on Computational Geometry* (2015), 74–80.

[10] T. Schoen, I. D. Shkredov. Additive properties of multiplicative subgroups of $\mathbb{F}_p$, *Quart. J. Math.* **63**:3 (2012), 713–722.

[11] I. D. Shkredov. Some new inequalities in additive combinatorics, *Moscow J. Combin. Number Theory* **3** (2013), 237–288.

[12] I. D. Shkredov. On exponential sums over multiplicative subgroups of medium size, *Finite Fields and Their Applications* **30** (2014), 72–87.

[13] I. D. Shkredov, E. Solodkova, I. Vyugin. Intersections of Shifts of Multiplicative Subgroups, *Mat. Zametki* **100**:2 (2016), 3–12.

[14] I. D. Shkredov, I. V. Vyugin. On additive shifts of multiplicative subgroups, *Mat. Sbornik* **203**:6 (2012), 81–100.

[15] S. A. Stepanov. On the number of points on hyperelliptic curve over prime finite field, *Izv. Akad. Nauk SSSR Ser.Mat.* **33** (1969), 1171–1181.

[16] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, Cambridge, 2006.

[17] I. Vyugin, S. Makarichev. On the number of solutions of polynomial equation over $\mathbb{F}_p$, arXiv:1504.01354v1 [math.NT] 26 Mar 2015.