Arithmetic progressions in multiplicative groups of finite fields *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

Let G be a multiplicative subgroup of the prime field $\mathbb{F}_p$ of size $|G| > p^{1-\kappa}$ and r an arbitrarily fixed positive integer. Assuming $\kappa = \kappa(r) > 0$ and p large enough, it is shown that any proportional subset $A \subset G$ contains non-trivial arithmetic progressions of length r. The main ingredient is the Szemerédi-Green-Tao theorem.

Introduction.

We denote by $\mathbb{F}_p$ the prime field with p elements and $\mathbb{F}_p^*$ its multiplicative group. The main result in this paper is the following.

Theorem 1. *Given $r \in \mathbb{Z}^+$, there is some $\kappa = \frac{1}{r\,2^{r+1}} > 0$ such that the following holds. Let $\delta > 0$, p a sufficiently large prime and $G < \mathbb{F}_p^*$ a subgroup of size*

$$|G| > p^{1-\kappa}.$$

Then any subset $A \subset G$ satisfying $|A| > \delta|G|$ contains non-trivial r-progressions.

The proof is based on the extension of Szemerédi's theorem for pseudo-random weights due to Green and Tao, which is also a key ingredient in their

*2010 *Mathematics Subject Classification.*Primary 11B25.
†*Key words.* arithmetic progressions, characters, exponential sums.
‡Research partially financed by the NSF Grants DMS 1600154.

proof of arithmetic progressions in the primes. (See [8].) In §.2 we will recall the precise statement of that result and the various underlying concepts.

The next point is that a multiplicative group behaves like a pseudo-random object (for the relevant notaion of pseudo-randomness). The latter fact is established by rather straightforward applications of Weil's theorem for character sums with polynomial argument. As an introductory result, we illustrate its use by proving

Proposition 2. *Let $r \in \mathbb{Z}_+$ be fixed, p large enough and $G < \mathbb{F}_p^*$ a multiplicative group of size*

$$|G| > c_r p^{1-\frac{1}{2r}} \tag{0.1}$$

Then G contains $c_r\big(\frac{|G|}{p}\big)^r p|G|$ many non-trivial $r+1$-progressions.

Taking $r = 2$, condition (0.1) becomes

$$|G| > cp^{\frac{3}{4}} \tag{0.2}$$

ensuring G to contain non-trivial triplets $a, a+b, a+2b$ in arithmetic progression. This last result is simple and well-known, but though one could conjecture a condition of the form $|G| > cp^{\frac{1}{2}}$ to suffice, still the best available in this direction. (See [1] for instance.)

Concerning three-term arithmetic progressions in general sets, we recall Sanders' result [19] which provides the strongest form of Roth's theorem to date and, in the setting of subsets of $\mathbb{F}_q^n$, q fixed, the solution to the cap set problem due to Ellenberg and Gijswijt [11]. In negative direction, Behrend's lower bound of $r_3(n)$ has been slightly improved by Elkin [10]. (See also [3], [6], [16], [17], [18], [21].)

It is also natural to expect that when r is large, a condition of the type $|G| > p^{1-\epsilon_r}$ with $\epsilon_r \to 0$ as $r \to \infty$ should be necessary for Proposition 2 to hold. We are not able to show that and could only establish the following.

Proposition 3. *There is a function $\eta_r \to 0$ as $r \to \infty$ and arbitrarily large primes p for which there is a subgroup $G < \mathbb{F}_p^*$ containing no r-progressions and*

$$|G| > p^{\frac{1}{2}-\eta_r}. \tag{0.3}$$

The argument is closely related to a construction in [4]. We note that a more satisfactory result would be (0.3) with exponent $1-\eta_r$ but $\frac{1}{2}-\eta_r$ seems the limit of the method.

Related to additive shifts of multiplicative subgroups of prime fields, we should also mention the paper of Shkredov and Vyugin [20], generalizing results of Konyagin, Heath-Brown and Garcia, Voloch. (See [13], [14], [15].)

Notations. We recall that the notation $U = O(V)$ is equivalent to the inequality $|U| \leq cV$ with some constant $c > 0$, while with the notation $U = o(V)$, in the above inequality, the constant c goes to 0. We denote by $\mathrm{ht}F(x)$ the *height* of the polynomial $F(x)$, which is the max of the modulus of the coefficients of $F(x)$. For a set G, $\mathbb{I}_G$ is the indicator function of G. By $\mathbb{E}(f \mid x \in S)$, we mean the average of $f(x)$ over $x \in S$. The constant c_r is a constant depending on r and may vary even within the same context.

1 Arithmetic progressions in multiplicative groups.

In this section we will prove Proposition 2.

First we note that the progression $a, a+b, \dots, a+rb \in G$ is equivalent to that $a \in G$ and $1 + a^{-1}b, \dots, 1 + ra^{-1}b \in G$. Hence we will analyze

$$\sum_{x \in \mathbb{F}_p} \mathbb{I}_G(1+x)\mathbb{I}_G(1+2x)\dots\mathbb{I}_G(1+rx) \tag{1.1}$$

Using the representation

$$\mathbb{I}_G = \frac{|G|}{p-1} \sum_{\chi \equiv 1 \text{ on G}} \chi, \tag{1.2}$$

we write

$$\mathbb{I}_G = \frac{|G|}{p-1}\Bigg(\chi_0 + \sum_{\substack{\chi \neq \chi_0 \\ \chi = 1 \text{ on G}}} \chi\Bigg). \tag{1.3}$$

So we write (1.1) as

$$\left(\frac{|G|}{p-1}\right)^r (p + \mathcal{A}), \tag{1.4}$$

where

$$|\mathcal{A}| \leq \left(\frac{p-1}{|G|}\right)^r \max \left| \sum_{x \in \mathbb{F}_p} \chi_1(1+x)\dots\chi_r(1+rx) \right| \tag{1.5}$$

with max taken over all r-tuples $\chi_1, \dots, \chi_r$ of multiplicative characters which are 1 on G and at least one of them non-trivial.

We now bound the sum in (1.5). For the r-tuple $\chi_1, \dots, \chi_r$ obtaining the max, let $I = \{s \in [1, r] : \ \chi_s \neq \chi_0\}$. Assume $\mathcal{Y}$ generates $\widehat{\mathbb{F}_p^*}$ and let $\chi = \mathcal{Y}^{|G|}$. Then $\chi_s = \chi^{j_s}$, where $j_s < \frac{p-1}{|G|}$. Hence

$$\sum_{x \in \mathbb{F}_p} \prod_{s \in I} \chi_s(1 + sx) = \sum_{x \in \mathbb{F}_p} \mathcal{Y}(f(x))$$

with

$$f(x) = \prod_{s \in I} (1 + sx)^{j_s |G|}.$$

Since $\mathcal{Y}$ is of order $p-1$ and $f(x)$ is not a $p-1$-power, Weil's theorem implies

$$\left| \sum_{x \in \mathbb{F}_p} \mathcal{Y}(f(x)) \right| < |I| \sqrt{p}. \tag{1.6}$$

Assume $|G| > c_r p^{1 - \frac{1}{2r}}$. It follows that (1.4) and hence (1.1) is bounded below by

$$\left(\frac{|G|}{p-1} \right)^r p - r\sqrt{p} > c_r \left(\frac{|G|}{p-1} \right)^r p. \tag{1.7}$$

Therefore, G contains at least $c_r \left(\frac{|G|}{p}\right)^r p|G|$ many non-trivial $r+1$-progressions.

Remark 1.1. We note that if $G \subset \mathbb{F}_p^*$ is a random set, then the expected size of (1.1) would also be $\left(\frac{|G|}{p-1}\right)^r p$. So the above observation indicates a random behavior of sufficiently large multiplicative group in terms of r-progressions. (This point of view will be exploited further in the next section.)

2 Progressions in large subsets of multiplicative groups.

An interesting problem is the following.

How large can $G \subset \mathbb{F}_p^*$ be without containing an r-progression?

In this section we will prove Theorem 1. We will use the Green-Tao extension of Szemerédi's theorem for large subsets of pseudo-random sets. (See Theorem 2.2 in [9].)

Theorem GT. *Let $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ be a pseudo-random weight, and let $r \in \mathbb{Z}^+$. Then for any $\delta > 0$, there is $c_r(\delta) > 0$ satisfying the following property. For any $f : \mathbb{Z}_N \to \mathbb{R}$ such that*

$$0 \leq f(x) \leq \nu(x), \forall x \quad \text{and} \quad \mathbb{E}(f \mid \mathbb{Z}_N) \geq \delta, \tag{2.1}$$

we have

$$\mathbb{E}(f(x)f(x+t)\dots f(x+rt) \mid x, t \in \mathbb{Z}_N) \geq c_r(\delta) - o(1). \tag{2.2}$$

(Note that here the notation $\mathbb{E}$ refers to the normalized sum.)

In order to apply this result, one will need to verify that under appropriate assumptions, $\mathbb{I}_G$ for $G \subset \mathbb{F}_p^*$, satisfies the required pseudo-randomness conditions.

We call that ν is a pseudo-random weight if ν satisfies the following two conditions.

(1). *Condition on linear forms.*

Let m_0, t and $L \in \mathbb{Z}$ be constants depending on r only. Let $m \leq m_0$ be an integer and $\psi_1, \dots, \psi_m : \mathbb{Z}_N^t \to \mathbb{Z}_N$ be functions of the form

$$\psi_i(\mathbf{x}) = b_i + \sum_{j=1}^{t} L_{i,j} x_j, \tag{2.3}$$

where $\mathbf{x} = (x_1, \dots, x_t)$, $b_i \in \mathbb{Z}$, $|L_{i,j}| \leq L$ and the m vectors $(L_{i,j})_{1 \leq j \leq t} \in \mathbb{Z}^t$ are pairwisely non-collinear.

Then

$$\mathbb{E}\big(\nu(\psi_1(\mathbf{x}))\dots\nu(\psi_m(\mathbf{x}))\big| \, \mathbf{x} \in \mathbb{Z}_N^t) = 1 + o(1). \tag{2.4}$$

(2). *Condition of correlations.*

Let $q_0 \in \mathbb{Z}$ be a constant. Then there exists $\tau : \mathbb{Z}_N \to \mathbb{R}^+$ satisfying

$$\text{for all} \quad \ell \geq 1, \mathbb{E}(\tau^\ell(x) \mid x \in \mathbb{Z}_N) = O_\ell(1) \tag{2.5}$$

such that for all $q \leq q_0$ and $h_1, \dots, h_q \in \mathbb{Z}_N$ (not necessarily distinct), we have

$$\mathbb{E}\big(\nu(x+h_1)\nu(x+h_2)\dots\nu(x+h_q) \mid x \in \mathbb{Z}_N\big) \leq \sum_{1 \leq i \leq j \leq q} \tau(h_i - h_j). \tag{2.6}$$

Remark 2.1. As Y. Zhao pointed out that in his paper [5] with D. Conlon and J. Fox, they showed that in applying Theorem GT one only needs to verify the m_0-linear forms condition (with $m_0 = r\,2^{r-1}$), and that the correlation condition is actually unnecessary.

Proof of Theorem 1. In our application of Theorem GT, $\mathbb{Z}_N$ will be $\mathbb{F}_p$ with additive structure and $\nu = \frac{p-1}{|G|}\mathbb{I}_G$. We will verify the condition on linear forms above by using Weil's theorem.

Using the representation (1.3), we have

$$\begin{aligned} \nu = \frac{p-1}{|G|}\mathbb{I}_G &= \frac{p-1}{|G|}\,\frac{|G|}{p-1}\sum_{\chi=1 \text{ on G}} \chi \\ &= \chi_0 + \sum_{\substack{\chi\neq \chi_0\\ \chi=1 \text{ on G}}} \chi. \end{aligned} \tag{2.7}$$

In (2.4), the trivial character χ_0 contributes for 1 and the additional contribution may be bounded as in §1 by

$$\left(\frac{p-1}{|G|}\right)^m p^{-t} \max\left|\sum_{\mathbf{x}\in\mathbb{F}_p^t} \chi_1(\psi_1(\mathbf{x}))\dots\chi_m(\psi_m(\mathbf{x}))\right| \tag{2.8}$$

with max taken over all m-tuples $\chi_1,\dots,\chi_m$, which are 1 on G and not all χ_0. For the m-tuples $\chi_1,\dots,\chi_m$ obtaining the max, let $I=\{s\in[1,m]: \chi_s\neq\chi_0\}$, hence $\chi_s=\mathcal{Y}^{j_s|G|}$, with $j_s<\frac{p-1}{|G|}$ for $s\in I$. We obtain

$$\sum_{\mathbf{x}\in\mathbb{F}_p^t} \chi_1(\psi_1(\mathbf{x}))\dots\chi_m(\psi_m(\mathbf{x})) = \sum_{\mathbf{x}\in\mathbb{F}_p^t} \mathcal{Y}\Big(\prod_{s\in I}\psi_s(\mathbf{x})^{j_s|G|}\Big) \tag{2.9}$$

To introduce a new variable z, we perform a shift $\mathbf{x}\mapsto\mathbf{x}+z\mathbf{a}$, where $\mathbf{a}\in\{1,\dots,m\}^t$ may be chosen such that

$$\sum_{j=1}^t L_{s,j}a_j \neq 0, \quad \text{for } s=1,\dots,m. \tag{2.10}$$

Recall that $|L_{s,j}|\le L$ and the m vectors $(L_{s,j})_{j=1,\dots,t}\in\mathbb{Z}^t$ are pairwisely non-collinear. Hence we may choose $\mathbf{a}$ as above to fulfill (2.10) and moreover $\sum_{j=1}^t L_{s,j}a_j \not\equiv 0 \pmod p$. We estimate (2.9) as

$$\frac{1}{p}\sum_{\mathbf{x}\in\mathbb{F}_p^t}\left|\sum_{z=0}^{p-1}\mathcal{Y}(f_{\mathbf{x}}(z))\right|, \tag{2.11}$$

where

$$f_{\mathbf{x}}(z)=\prod_{s\in I}\Big(\big(\sum_j L_{s,j}a_j\big)z+\psi_s(\mathbf{x})\Big)^{j_s|G|}. \tag{2.12}$$

Clearly, $f_{\mathbf{x}}(z)$ will not be a $(p-1)$-power of a polynomial, if the following expressions

$$\frac{\psi_s(\mathbf{x})}{\sum_j L_{s,j}a_j},\quad s\in I \tag{2.13}$$

are pairwisely distinct.

To estimate the double sum in (2.11), we write $\sum_{\mathbf{x}\in\mathbb{F}_p^t}$ as $\sum^{(1)}+\sum^{(2)}$, where $\sum^{(1)}$ is over those $\mathbf{x}\in\mathbb{F}_p^t$ for which (2.13) are pairwisely distinct and $\sum^{(2)}$ over the other $\mathbf{x}$.

By Weil's theorem

$$\frac{1}{p}\sum{}^{(1)}\Big|\sum_{z=0}^{p-1}\mathcal{Y}(f_{\mathbf{x}}(z))\Big|\le |I|\,p^{t-1}\sqrt{p}. \tag{2.14}$$

For $\sum^{(2)}$ we estimate trivially.

$$\begin{aligned}&\frac{1}{p}\sum{}^{(2)}\Big|\sum_{z=0}^{p-1}\mathcal{Y}(f_{\mathbf{x}}(z))\Big|\\ \le&\sum_{\substack{s,s'\in I\\ s\neq s'}}\left|\left\{\mathbf{x}\in\mathbb{F}_p^t:\frac{\psi_s(\mathbf{x})}{\sum_j L_{s,j}a_j}=\frac{\psi_{s'}(\mathbf{x})}{\sum_j L_{s',j}a_j}\right\}\right|\end{aligned} \tag{2.15}$$

Since $(L_{s,j})_{1\le j\le t}$ and $(L_{s',j})_{1\le j\le t}$ are not collinear (and bounded), there is some j_0 such that

$$\frac{L_{s,j_0}}{\sum L_{s,j}a_j}-\frac{L_{s',j_0}}{\sum L_{s',j}a_j}\in\mathbb{F}_p^*.$$

This shows that (2.15) is bounded by r^2p^{t-1}. Therefore, we proved that (2.11) is bounded by $rp^{t-\frac{1}{2}}$, and (2.8) is bounded by

$$c_r\frac{(p-1)^m}{|G|^m\sqrt{p}}, \tag{2.16}$$

which is bounded by $p^{-\frac{1}{4}}$, assuming

$$|G|>p^{1-\frac{1}{4m_0}}.\quad\square \tag{2.17}$$

3 Construction of large multiplicative groups with no r-progressions.

In this section we will prove Proposition 3. Our argument is very similar to the proof of Theorem 39 in [4], where it is shown that there is a subset $\Delta \subset \mathcal{P}_T = \{p : p \text{ is a prime, and } p \le T\}$, $|\Delta| < \delta \frac{T}{\log T}$ with $\delta = \delta(r) \to 0$ as $r \to \infty$ and such that for any $p \in \mathcal{P}_T \setminus \Delta$ and any $t \in \mathbb{Z}$

$$\max\big(\mathrm{ord}_p(t+1), \dots, \mathrm{ord}_p(t+r)\big) > T^{\frac{1}{2}-\delta}. \tag{3.1}$$

Obviously, (3.1) implies that

$$\mathrm{ord}_p\langle t+1, \dots, t+r\rangle > T^{\frac{1}{2}-\delta}, \tag{3.2}$$

which is the only relevant property for us.

As in §1, if $a, a+b, \dots, a+rb \in G \subset \mathbb{F}_p^*$, and $b \in F_p^*$, then $1+t, 1+2t, \dots, 1+rt \in G, t \equiv a^{-1}b \pmod p$ and hence we obtain $t \in \mathbb{Z}, t \not\equiv 0 \pmod p$ such that

$$\mathrm{ord}_p\langle 1+t, \dots, 1+rt\rangle \le |G|.$$

Thus our purpose is to ensure that for all $t \not\equiv 0 \pmod p$ such that

$$\mathrm{ord}_p\langle 1+t, \dots, 1+rt\rangle > p^{\frac{1}{2}-\delta}, \tag{3.3}$$

with p such that $p-1$ has a divisor d in the interval $[p^{\frac{1}{2}-\eta}, p^{\frac{1}{2}-\delta}]$. Then the subgroup $G < \mathbb{F}_p^*$ of order d will have no $(r+1)$-progression. Assuming (3.3) holds for all $p \in \mathcal{P}_T \setminus \Delta$ with $|\Delta| < \delta\frac{T}{\log T}$, it will then suffice (taking $\eta = c\delta$) to invoke

Lemma 3.1. *Let notations be as above. Then*

$$\Big|\big\{p \in \mathcal{P}_T : p-1 \text{ has a prime divisor in the interval } [T^{\frac{1}{2}-\eta}, T^{\frac{1}{2}-\frac{\eta}{2}}]\big\}\Big| > c\eta\frac{T}{\log T}. \tag{3.4}$$

Proof. In Bombieri-Vinogradov theorem, taking

$$Q = T^{\frac{1}{2}}\big(\log T\big)^{-10} \tag{3.5}$$

we have

$$\sum_{q \le Q}\left|\psi(T; q, 1) - \frac{T}{\phi(q)}\right| = O\big(T^{\frac{1}{2}}Q\big(\log T\big)^5\big) < cT\big(\log T\big)^{-5}, \tag{3.6}$$

where $\phi(q)$ is the Euler's totient function and

$$\psi(T;q,1) = \sum_{\substack{n\le T\\ n\equiv 1 \mod q}} \Lambda(n),$$

$\Lambda(n)$ being the von Mangoldt function. Denote

$$\Omega = \left\{ q \in \left[T^{\frac{1}{2}-\eta}, T^{\frac{1}{2}-\frac{\eta}{2}}\right] \cap \mathcal{P} : \psi(T;q,1) < \frac{T}{2\phi(q)} \right\}.$$

Let $[2^k, 2^{k+1}] \subset [T^{\frac{1}{2}-\eta}, T^{\frac{1}{2}-\frac{\eta}{2}}] := I$. From (3.6),

$$\left|\Omega \cap [2^k, 2^{k+1}]\right| \frac{T}{2^{k+1}} < c\, T\big(\log T\big)^{-5},$$

hence

$$\left|\Omega \cap [2^k, 2^{k+1}]\right| < c\frac{2^k}{\big(\log T\big)^5} < \frac{1}{100}\left|\mathcal{P} \cap [2^k, 2^{k+1}]\right|. \tag{3.7}$$

Clearly, (3.7) and the prime number theorem imply that

$$\begin{aligned} \sum_{\substack{q\notin\Omega\\ q\in I\cap\mathcal{P}}} \frac{1}{q} &= \sum_{(\frac{1}{2}-\eta)\log T<k<(\frac{1}{2}-\frac{\eta}{2})\log T} \quad \sum_{\substack{q\notin\Omega\\ q\in[2^k,2^{k+1}]\cap\mathcal{P}}} \frac{1}{q} \\ &< \sum_{(\frac{1}{2}-\eta)\log T<k<(\frac{1}{2}-\frac{\eta}{2})\log T} \frac{1}{2^k} \left|\mathcal{P} \cap [2^k, 2^{k+1}]\right| < 2\eta. \end{aligned}$$

Let $\sigma < 2\eta$ be a parameter (to be specified). From the preceding, there is a subset $S \subset I \cap \mathcal{P}$, $S \cap \Omega = \emptyset$, such that

$$\sigma < \sum_{q\in S} \frac{1}{q} < 2\sigma, \tag{3.8}$$

and since $S \cap \Omega = \emptyset$, we have for all $q \in S$

$$|A_q| \ge \frac{T}{2\big(\log T\big)q}, \quad \text{where } A_q := \{p < T : p \equiv 1 \pmod q\}. \tag{3.9}$$

From the inclusion/exclusion principle and the Brun-Titchmarsh theorem, the left hand side of (3.4) is at least

$$\begin{aligned}\left|\bigcup_{q\in S} A_q\right| &\geq \sum_{q\in S}|A_q| - \sum_{\substack{q_1,q_2\in S\\ q_1\neq q_2}} |A_{q_1q_2}| \\ &\geq \frac{T}{2\log T}\sum_{q\in S}\frac{1}{q} - \sum_{\substack{q_1,q_2\in S\\ q_1\neq q_2}}\left\{\frac{2T}{\phi(q_1q_2)\log\frac{T}{q_1q_2}}\left(1+O\Big(\frac{1}{\log\frac{T}{q_1q_2}}\Big)\right)\right\}\end{aligned} \tag{3.10}$$

Since $\phi(q_1q_2) = (q_1-1)(q_2-1)$, and $q_1q_2 \leq T^{1-\eta}$ for $q_1 \neq q_2$ in S, (3.10) is bounded below by

$$\begin{aligned}&\frac{T}{\log T}\left(\frac{1}{2}\sum_{q\in S}\frac{1}{q} - \frac{3}{\eta}\Big(\sum_{q\in S}\frac{1}{q}\Big)^2\right)\\ =\ &\frac{T}{\log T}\left(\frac{\sigma}{2} - \frac{3}{\eta}\sigma^2\right) > c\,\eta\frac{T}{\log T}\end{aligned}$$

for some small $c > 0$ and appropriate choice of σ. □

Returning to the proof of Theorem 39 in [4], a key ingredient is Lemma 17 (in [4]) depending on a result from [7] on additive relations in multiplicative subgroups of $\mathbb{C}^*$. Keeping (3.3) in mind, the appropriate variant of Lemma 17 we will need is the following.

Lemma 3.2. *Let $z \in \mathbb{C}^*$ and $r \in \mathbb{Z}_+$ be sufficiently large. Consider the set $\mathcal{A} = \{1 + sz : 1 \leq s \leq r\} \subset \mathbb{C}$. Then there is a multiplicative independent subset $\mathcal{A}_0 \subset \mathcal{A}$ of size*

$$|\mathcal{A}_0| > c\log r. \tag{3.11}$$

The proof is the same as Lemma 17 in [4]. Note that one distinction is that we have to assume $z \neq 0$, which will also lead to a small modification in the proof of Theorem 39 in [4], in order to establish (3.3). Thus

Lemma 3.3. *There is a subset $\Delta \subset \mathcal{P}_T$, $|\Delta| = o\big(\frac{T}{\log T}\big)$ such that every $p \in \mathcal{P}_T \setminus \Delta$ has the following property.*
If $t \in \mathbb{Z}, t \not\equiv 0 \pmod p$, then

$$\mathrm{ord}_p\langle 1+t, \ldots, 1+rt\rangle > p^{\frac{1}{2}-\delta}, \tag{3.12}$$

where $\delta = \delta(r)$.

Proof. The basic strategy is the same as that of Theorem 39 in [4].

We fix an integer $r_0 = [\log r]$, let

$$\delta = \delta(r) = \frac{100}{r_0}, \tag{3.13}$$

and choose $u \in \mathbb{Z}_+$ such that

$$u^{r_0} = cT^{\frac{1}{2}-\delta} \quad \text{and} \quad \frac{1}{2}T^{\frac{1}{2}-\delta} < u^{r_0} < 2T^{\frac{1}{2}-\delta}. \tag{3.14}$$

Let $\mathcal{E}$ be the collection of all subsets $E \subset \{1, \dots, r\}, |E| = r_0$.

Next, given any two subsets $E_1, E_2 \subset \{1, \dots r\}$, $E_1 \cap E_2 = \emptyset$, $0 < |E_1| + |E_2| \le r_0$, and exponents $\tilde{u} = (u_s)_{s \in E_1 \cup E_2}, 1 \le u_s \le u$, we introduce the polynomial

$$F = F_{E_1, E_2, \tilde{u}}(x) = \prod_{s \in E_1} (1 + sx)^{u_s} - \prod_{s \in E_2} (1 + sx)^{u_s} \in \mathbb{Z}[x]. \tag{3.15}$$

Note that x is always a factor of $F(x)$. Clearly $\deg F(x) \le r_0 u$, $\mathrm{ht} F(x) \le r^{\,2r_0 u}$, and there are at most $2^{r_0}\binom{r}{r_0}u^{r_0}$ such polynomials.

Denote by $\mathcal{F} \subset \mathbb{Z}[x]$ the collection of all irreducible factors $f(x) \in \mathbb{Z}[x]$ and $f(x) \ne x$ extracted from all polynomials of the form (3.15). Hence

$$|\mathcal{F}| \le r_0 2^{r_0} \binom{r}{r_0} u^{r_0+1}. \tag{3.16}$$

Next, if $f, g \in \mathcal{F}, f \not\sim g$, (i.e. f and g are not proportional) then the resultant of f, g satisfies

$$\mathrm{Res}(f, g) \in \mathbb{Z} \setminus \{0\} \quad \text{and} \quad |\mathrm{Res}(f, g)| < r^{2(r_0 u)^2}. \tag{3.17}$$

From (3.16)

$$B = \prod_{\substack{f, g \in \mathcal{F} \\ f \not\sim g}} \mathrm{Res}(f, g) \ \in \mathbb{Z} \setminus \{0\} \tag{3.18}$$

satisfies

$$|B| < r^{\,2r_0^4\, 4^{r_0} \binom{r}{r_0}^2 u^{2r_0+4}} < r^{\,r^{2r_0}\, u^{2r_0+4}}. \tag{3.19}$$

By (3.14) and (3.13), for T sufficiently large, we can bound the exponent in (3.19) as

$$r^{2r_0}\ u^{2r_0+4} < r^{2r_0}T^{1-2\delta+\frac{2}{r_0}} < T^{1-\delta} = o\left(\frac{T}{\log T}\right).$$

Therefore, there is a set $\Delta \subset \mathcal{P}_T$ of primes $p \leq T$, with $|\Delta| = o\big(\frac{T}{\log T}\big)$ such that $(p, B) = 1$ for all $p \in \mathcal{P}_T \setminus \Delta$.

Now, take $p \in \mathcal{P}_T \setminus \Delta$ and suppose there exists some $t \in \mathbb{Z},\ t \not\equiv 0 \pmod p$ such that

$$\mathrm{ord}_p\langle 1+t, \dots, 1+rt\rangle < u^{r_0}.$$

Then, for all $E \in \mathcal{E}$, there are $E_1, E_2 \subset E,\ E_1 \cap E_2 = \emptyset,\ |E_1| + |E_2| \geq 1$ and $\tilde{u} = (u_s)_{s\in E_1\cup E_2}$ such that $F_{E_1,E_2,\tilde{u}}(t) \equiv 0 \pmod p$. Hence there is a factor $f_E(x)$ of $F_{E_1,E_2,\tilde{u}}(x)$ such that $f_E(t) \equiv 0 \pmod p$. Since $t \not\equiv 0 \pmod p$, $f_E(x) \neq x$. For all $E, F \in \mathcal{E}$, since $f_E(x), f_F(x)$ have common root $t \pmod p$

$$\mathrm{Res}(f_E, f_F) \equiv 0 \pmod p. \tag{3.20}$$

If $f_E \neq cf_F$, then $\mathrm{Res}(f_E, f_F)|B$, contradicting $(B, p) = 1$. Thus $f_E = cf_F$ for all $E, F \in \mathcal{E}$ and hence have a common root $z \in \mathcal{C}^*$. But by Lemma 3.2, there is a set $E \in \mathcal{E}$ such that $\{1 + sz : s \in E\}$ are multiplicatively independent, implying $F_{E_1,E_2,\tilde{u}}(z) \neq 0, f_E(z) \neq 0$, which is a contradiction. □

4

Ackonwledgement. The author would like to thank Yufei Zhao for bringing her attention to [5]. The author would also like to thank the referees for careful reading, which improved an earlier version of the paper.

References

[1] N. Alon, J. Bourgain, *Additive Patterns in Multiplicative Subgroups*, Geom. Funct. Anal. 24(3), 721-739, (2014).

[2] M. Bateman and N. Katz, *New bounds on cap sets*, J. Amer. Math. Soc. 25(2), 585-613,(2012).

[3] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Natl. Acad. Sci. USA, 32(12), 331-332, (1946).

[4] J. Bourgain,M. Z. Garaev, S. V. Konyagin, I. Shparlinski, *Multiplicative congruences with variables from short intervals*, J. Anal. Math. 124(1), 117-147, (2014).

[5] D. Conlon, J. Fox, and Y. Zhao, *A relative Szemerdi theorem*, Geom. Funct. Anal. 25, 733762, (2015).

[6] E. Croot, V. Lev, and P. P. Pach, *Progression-free sets in* $\mathbb{Z}_n^4$ *are exponentially small*, preprint, (2016). arXiv:1605.01506.

[7] J.-H. Evertse, H. Schlickewei, W. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2), 155, 807-836, (2002).

[8] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2), 167(2), 481-547, (2008).

[9] B. Host, *Arithmetic progressions in primes*, Séminaire Bourbaki 47, 229-246 (2004/2005).

[10] M. Elkin, *An improved construction of progression free sets*, Israel J. Math. 184, 93-128, (2011).

[11] J. Ellenberg, D. Gijswijt, *On large subsets of* $\mathbb{F}_q^n$ *with no three-term arithmetic progression*, preprint, (2016). arXiv:1605.09223.

[12] P. Frankl, R. L. Graham, V. Rödl, *On Subsets of Abelian Groups with No 3-Term Arithmetic Progression*, J. Combin. Theory Ser. A 45, 157-161, (1987).

[13] A. Garcia, J.F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30, 345-356, (1988).

[14] D. R. Heath-Brown, S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronns exponential sum*, Quart. J. Math. 51, 221-235, (2000).

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

[16] R. Meshulam, *On subsets of finite abelian groups with no 3-term arithmetic progressions*, J. Combin. Theory Ser. A 71(1), 168-172, (1995).

[17] K. Roth, *On certain sets of integers*, J. Lond. Math. Soc. (2), 28, 245-252, (1953).

[18] R. Salem, D. Spencer, *On sets of integers which contain no three in arithmetic progression*, Proc. Natl. Acad. Sci. USA, 28, 561-563, (1942).

[19] T. Sanders, *On Roth's theorem on progressions*, Ann. of Math. (2), 174 (1), 619-636, (2011).

[20] I. Shkredov, I. Vyugin, *On additive shifts of multiplicative subgroups*, Mat. Sb. 203(6), 81-100, (2012).

[21] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 27, 299-345, (1975).