Appendix: Arithmetic progressions in multiplicative groups of finite fields *†

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

In this appendix, we show that a generalized arithmetic progression cannot contain a large subset of elements which are sufficiently separated and too close to the unit circle.

Given $\xi_0, \xi_1, \dots, \xi_r \in \mathbb{C}$, a *symmetric generalized arithmetic progression* P *of rank* r is

$$P = \{\xi_0 + n_1\xi_1 + \cdots + n_r\xi_r : |n_i| < M \quad \text{for } i = 1, \dots, r\}. \tag{1}$$

We say a set $S \subset \mathbb{C}$ is δ*-separated* if for any $s_1, s_2 \in S$, $|s_1 - s_2| \geq \delta$, and S is ε*-close to the unit circle* if for all $s \in S$, $1 - \varepsilon < |s| < 1 + \varepsilon$.

Precisely, our result is the following

Theorem 1. *Given* r*, there is a constant* C_r *with the following property. Let* $P \subset \mathbb{C}$ *be a* r*-progression as in* (1)*. Let* $0 < \delta < 1$ *and* $\varepsilon < N^{-C_r}\delta^{C_r}$*. Let* $S \subset P$ *be a subset consisting of elements which are* δ*-separated and* ε*-close to the unit circle. Then*

$$|S| < \exp\left(C_r \frac{\log M}{\log\log M}\right).$$

In this appendix, C_r is a constant depending on r and may vary even within

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

the same context.
We denote the set of the coefficient vectors of S by

$$\mathcal{E} = \left\{ \bar{n} = (n_1, \ldots, n_r) \in \mathbb{Z}^r : |n_i| < M, \left| |\xi_0 + \sum_{i=1}^{r} n_i \xi_i|^2 - 1 \right| < \varepsilon \right\}.$$

Fix $\bar{m} \in \mathcal{E}$. Hence

$$\left| \sum_{i=1}^{r} (n_i - m_i)\xi_i \right| \leq 2\sqrt{1+\varepsilon} \quad \text{for all } \bar{n} \in \mathcal{E}. \tag{2}$$

Let $\langle \mathcal{E} \rangle$ be the vector space generated by $\mathcal{E}$. We assume $\dim\langle \mathcal{E} \rangle = r$, since otherwise we may reduce the rank of P without significantly changing the size of P (see Chapter 3 in [4]). Therefore, we can take r independent vectors $\bar{n}^{(1)}, \cdots, \bar{n}^{(r)} \in \mathcal{E}$ and use Cramer's rule to solve $\xi_1, \cdots, \xi_r$ in the following system of r equations.

$$\begin{gathered}
(n_1^{(1)} - m_1)\xi_1 + \cdots + (n_r^{(1)} - m_r)\xi_r = c^{(1)} \\
\cdots \\
\cdots \\
\cdots \\
(n_1^{(r)} - m_1)\xi_1 + \cdots + (n_r^{(r)} - m_r)\xi_r = c^{(r)}
\end{gathered}$$

where $|c^{(1)}|, \cdots, |c^{(r)}| \leq 2\sqrt{1+\varepsilon} < 3$.

We obtain a bound

$$|\xi_1|, \ldots, |\xi_r| \leq 3r! M^{r-1}, \tag{3}$$

and hence

$$|\xi_0| < \sum_i |n_i \xi_i| + 1 + \varepsilon < (3r)r! M^r. \tag{4}$$

Next, assume that $||\geq 2$. Then the separation assumption means that for any $\bar{m}, \bar{n} \in \mathcal{E}$ with $\bar{m} \neq \bar{n}$ we have $|\sum_{i=1}^{r} (m_i - n_i)\xi_i| > \delta$. Thus,

$$\max\{|\xi_1|, \ldots, |\xi_r|\} > \frac{\delta}{2rM}. \tag{5}$$

Without loss of generality, assume that the maximum above is attained by $|\xi_1|$.

Lemma 2. *There exist $z_0, z_1, \ldots, z_r, w_0, w_1, \ldots, w_r \in \mathbb{C}$ with $z_1 \neq 0$ such that for any $\bar{n} \in \mathcal{E}$*

$$\Big(z_0 + \sum_{i=1}^{r} n_i z_i\Big)\Big(w_0 + \sum_{i=1}^{r} n_i w_i\Big) = 1.$$

We next conclude our result using this lemma.

Proof of Theorem 1.

Let $A = \{z_0 + \sum_{i=1}^{r} n_i z_i : \bar{n} \in \mathcal{E}\}$.

Applying Proposition 3 in [2] to the mixed progression

$$\{n_0 z_0 + n_0 w_0 + \sum_{i=1}^{r} n_i z_i + \sum_{i=1}^{r} n_i' w_i : |n_0|, |n_0'| < 2 \text{ and } |n_i|, |n_i'| < M\},$$

we have

$$|A| \leq \exp(D_r \log M / \log\log M),$$

for some positive constant D_r.

We next partition $\mathcal{E}$ as

$$\mathcal{E} = \bigcup_{a \in A} \mathcal{E}_a, \text{ where } \mathcal{E}_a = \Big\{\bar{n} \in \mathcal{E} : z_0 + \sum_{i=1}^{r} n_i z_i = a\Big\}.$$

Let S be as in Theorem 1, we write

$$S = \Big\{\xi_0 + \sum_{i=1}^{r} n_i \xi_i : \bar{n} \in \mathcal{E}\Big\} = \bigcup_{a \in A} S_a, \tag{6}$$

where

$$S_a := \{\xi_0 + \sum_{i=1}^{r} n_i \xi_i : \bar{n} \in \mathcal{E}_a\}.$$

Notice that $S_a \subset P_a := \{\xi_0 + \sum_{i=1}^{r} n_i \xi_i \in P : z_0 + \sum_{i=1}^{r} n_i z_i = a\}$. The gain here is that P_a is contained in a progression of rank at most $r-1$, so by induction

$$|S_a| \leq \exp(C_{r-1} \log M / \log\log M).$$

It thus follows from (6) that

$$|S| \leq \exp(C_r \log M / \log\log M),$$

for some appropriately chosen constant sequence C_r, completing the proof. $\square$

We now prove Lemma 2. We will use the following effective form of Nullstellensatz [3].

Theorem KPS *Let* $g, f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ *with* $\deg g, \deg f_i \leq d$ *for all* i*, and* $\log(ht(f_i)) \leq H$*. Then there exist* $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ *and positive integers* b, l *such that*

$$b\ g^l = \sum_{i=1}^{s} g_i f_i$$

where

$$l \leq D = \max_{1 \leq i \leq s}\{\deg g_i\} \leq 4nd^n$$

as well as

$$\max_{1 \leq i \leq s}\{\log|b|, \log(ht(g_i))\} \leq 4n(n+1)d^n\big[H + \log s + (n+7)d\log(n+1)\big].$$

Here ht(.) is the height function.

Remark. Theorem 1 in [3] is stated for the case that $f_1, \cdots, f_s$ has no common zero. However, the standard proof of Nullstellensatz gives the above statement. (For example, see [1].)

Now define the function P over $\bar{n} \in \mathcal{E}$ as

$$P_{\bar{n}}(z_0, z_1, \ldots, z_r, w_0, w_1, \ldots, w_r) = \big(z_0 + \sum_{i=1}^{r} n_i z_i\big)\big(w_0 + \sum_{i=1}^{r} n_i w_i\big).$$

Assume that the claim does not hold, then by Theorem KPS, with $n = 2r+2, s = |\mathcal{E}| \leq (2M)^r, d = 2, H \leq 2\log M$ we have

$$bz_1^l = \sum_{\bar{n} \in \mathcal{E}} P_{\bar{n}} Q_{\bar{n}}, \tag{7}$$

where $b \in \mathbb{Z}\backslash\{0\}$, $Q_{\bar{n}} \in \mathbb{Z}[z_0, \ldots, z_r, w_0, \ldots, w_r]$ such that

- $\deg(Q_{\bar{n}}), l \leq D \leq C'_r$
- the coefficients of $Q_{\bar{n}}$ are bounded by $M^{C'_r}$.

Now replacing $z_0, \ldots, z_r$ and $w_0, \ldots, w_r$ by $\xi_0, \ldots, \xi_r$ and $\bar{\xi_0}, \ldots, \bar{\xi_r}$ in (7), we have

$$|\xi_1|^l \leq \sum_{\bar{n} \in \mathcal{E}} |P_{\bar{n}}(\xi_0, \ldots, \xi_r, \bar{\xi_0}, \ldots, \bar{\xi_d})| \; |Q_{\bar{n}}(\xi_0, \ldots, \xi_r, \bar{\xi_0}, \ldots, \bar{\xi_d})|.$$

By (3), (4), (5), we then have

$$\left(\frac{\delta}{2rM}\right)^l \leq DM^{C'_r}(3r!rM^r)^D \sum_{\bar{n} \in \mathcal{E}} |P_{\bar{n}}(\xi_0, \ldots, \xi_r, \bar{\xi_0}, \ldots, \bar{\xi_r})|.$$

On the other hand, by definition, $|P_{\bar{n}}(\xi_0, \ldots, \xi_r, \bar{\xi_0}, \ldots, \bar{\xi_r})| \leq \varepsilon$ for any $\bar{n} \in \mathcal{E}$. It thus follows that

$$\left(\frac{\delta}{2rM}\right)^l \leq \left(\frac{\delta}{2rM}\right)^D \leq M^{C''_r}\varepsilon.$$

However, this is impossible with the choice of ε from Theorem 1.

References

[1] E. Bombieri, J. Bourgain and S. V. Konyagin, Roots of Polynomials in Subgroups of forumla and Applications to Congruences, Int Math Res Notices, 5, 802-834 (2009).

[2] M.-C. Chang, Factorization in generalized arithmetic progressions and application to the Erdős-Szemerédi sum-product problems, Geom. Funct. Anal. 13 (4), 720-736 (2003).

[3] T. Krick, L. M. Pardo and M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J., 109, 521598 (2001).

[4] T. Tao and V. Vu, Additive Combinatorics, Cambridge Univ. Press, 2006.