Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **10** (2016), 325–331. doi:10.2298/AADM160827019S

AN ADDITIVE PROBLEM IN FINITE CYCLIC RINGS

Nguyen Minh Sang, Pham Van Thang, Le Anh Vinh

Let q be a prime power, and $\mathbb{F}_q$ be the finite field of order q. In this short note, by using methods from spectral graph theory, we give sufficient conditions to guarantee that

$$\mathbb{F}_q \setminus \{0\} \subseteq \{a_1 u_1^{x_1} + \cdots + a_d u_d^{x_d} : 1 \leq x_i \leq M_i, 1 \leq i \leq d\},$$

where a_i and u_i are non-zero elements in $\mathbb{F}_q$, and M_i are integers. This result generalizes a recent result given by Cilleruelo and Zumalacárregui (2014). Using the same techniques, we extend this result in the setting of the finite cyclic ring.

1. INTRODUCTION

Let p be a large prime and g a primitive root modulo p. Andrew Odlyzko asked for which values of M the set

$$\mathcal{A} := \{g^x - g^y \pmod p \colon 1 \leq x, y \leq M\}$$

contains every residue class modulo p. He also conjectured that one can take M to be as small as $p^{1/2+\epsilon}$, for any fixed $\epsilon > 0$ and p large enough in terms of ϵ. The first result was given by Rudnik and Zaharescu in [**13**] by using standard methods of characters sums. More precisely, they proved that if $M \geq cp^{3/4} \log p$ for some $c > 0$, then $\mathbb{F}_p \subseteq \mathcal{A}$. This result was improved to $10p^{3/4}$ by Garaev in [**7**] and independently by Konyagin in [**12**]. García [**8**] reduced the constant c to $2^{5/4}$. By using a combinatorial approach, Cilleruelo [**4**] improved the constant to $\sqrt{2} + \epsilon$ for p large enough in terms of $\epsilon > 0$.

2010 Mathematics Subject Classification. 11N69, (11A07, 11N25).
Keywords and Phrases. Primitive roots, finite fields, difference sets.

In [**5**] Cilleruelo and Zumalacárregui generalized this problem to arbitrary finite fields $\mathbb{F}_q$ and for elements of large multiplicative order by employing character sum techniques and properties of Sidon sets as follows.

Theorem 1.1 (Cilleruelo and Zumalacárregui, [**5**]). *Let u_1 and u_2 be two non-zero elements of $\mathbb{F}_q$. Suppose that*

$$\min\left\{\mathtt{ord}_{\mathbb{F}_q^*}(u_1), \lfloor M_1/2\rfloor\right\} \cdot \min\left\{\mathtt{ord}_{\mathbb{F}_q^*}(u_2), \lfloor M_2/2\rfloor\right\} \geq q^{3/2}$$

then

$$\mathbb{F}_q^* \subseteq \left\{u_1^x + u_2^y \colon 1 \leq x \leq M_1, 1 \leq y \leq M_2\right\},$$

and

$$\mathbb{F}_q^* \subseteq \left\{u_1^x - u_2^y \colon 1 \leq x \leq M_1, 1 \leq y \leq M_2\right\},$$

where $\mathbb{F}_q^* := \mathbb{F}_p \setminus \{0\}$, and $\mathtt{ord}_{\mathbb{F}_q^*}(u_i)$ is the order of u_i in $\mathbb{F}_q^*$.

Note that 0 may not belong to these sets, for instance, if q is a prime, $q \equiv 3 \mod 4$, and $\mathtt{ord}_{\mathbb{F}_q^*}(u_i) = (q-1)/2$, then the elements $u_1^x + u_2^y$ are sum of two squares and 0 is not of this form, see [**5**] for more details.

In this short note, we present a graph-theoretic proof of a generalization of Theorem 1.1 as follows.

Theorem 1.2. *Let $u_1, \ldots, u_d$ be d non-zero elements in $\mathbb{F}_q$. Suppose that*

$$\prod_{i=1}^{d} \min\left\{\mathtt{ord}_{\mathbb{F}_q^*}(u_i), \lfloor M_i/2\rfloor\right\} \geq \sqrt{2} q^{\frac{d+1}{2}},$$

then for any d-tuple $(a_1, \ldots, a_d)$ in $(\mathbb{F}_q^*)^d$ we have

$$\mathbb{F}_q^* \subseteq \left\{a_1 u_1^{x_1} + \cdots + a_d u_d^{x_d} \colon 1 \leq x_i \leq M_i,\ 1 \leq i \leq d\right\}.$$

Using the same techniques, we extend Theorem 1.2 in the setting of the finite cyclic ring $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$, where $q = p^r$ is a prime power.

Theorem 1.3. *Let $u_1, \ldots, u_d$ be d elements in $\mathbb{Z}_q^*$, where $\mathbb{Z}_q^*$ is the set of units in $\mathbb{Z}_q$. Suppose that*

$$\prod_{i=1}^{d} \min\left\{\mathtt{ord}_{\mathbb{Z}_q^*}(u_i), \lfloor M_i/2\rfloor\right\} \geq \sqrt{2r} p^{\frac{d(2r-1)+1}{2}},$$

then for any d-tuple $(a_1, \ldots, a_d)$ in $(\mathbb{Z}_q^*)^d$ we have

$$\mathbb{Z}_q^* \subseteq \left\{a_1 u_1^{x_1} + \cdots + a_d u_d^{x_d} \colon 1 \leq x_i \leq M_i,\ 1 \leq i \leq d\right\},$$

where $\mathtt{ord}_{\mathbb{Z}_q^*}(u_i)$ is the order of u_i in the cyclic group $\mathbb{Z}_q^*$.

If we want the sum-set to cover the whole ring $\mathbb{Z}_q$, we need a stronger condition as in the following theorem.

Theorem 1.4. *Let $u_1, \dots, u_d$ be d elements in $\mathbb{Z}_q^*$. Suppose that*

$$\sqrt{\min\left\{\mathtt{ord}_{\mathbb{Z}_q^*}(u_1), M_1\right\}} \prod_{i=2}^{d} \min\left\{\mathtt{ord}_{\mathbb{Z}_q^*}(u_i), \lfloor M_i/2 \rfloor\right\} \geq \sqrt{2r} p^{\frac{d(2r-1)+1}{2}},$$

then for any d-tuple $(a_1, \dots, a_d)$ in $(\mathbb{Z}_q^*)^d$ we have

$$\mathbb{Z}_q \subseteq \{a_1 u_1^{x_1} + \cdots + a_d u_d^{x_d} : 1 \leq x_i \leq M_i,\ 1 \leq i \leq d\}.$$

Note that the bound of Theorem 1.4 is only effective in the case $d > r + 1$.

We remark here that our approach in this paper and character sum techniques in [**5**] have been the main tools to deal with problems with large restricted sets. Many results obtained by Fourier analytic methods can be proved by using our techniques and vice versa. The interested reader can find a detailed discussion on the relation between these methods in [**19**].

There is also a series of papers dealing with similar problems in recent years, for example, see [**6, 9, 10, 11, 14**] and references therein.

The rest of this paper is organized as follows: In Section 2, we recall some properties of pseudo-random graphs, and the spectrum of product graphs, sum-product graphs over finite fields and finite cyclic rings. The proofs of Theorems 1.2, 1.3 and 1.4 are presented in Section 3.

2. PROPERTIES OF PSEUDO-RANDOM GRAPHS

For a graph G of order n, let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the second eigenvalue of G. A graph $G = (V, E)$ is called an (n, k, λ)-graph if it is k-regular, has n vertices, and the second eigenvalue of G is at most λ. Since G is a k-regular graph, k is an eigenvalue of its adjacency matrix with the all-one eigenvector $\mathbf{1}$. If the graph G is connected, the eigenvalue k has multiplicity one. Furthermore, if G is not bipartite, for any other eigenvalue θ of G, we have $|\theta| < k$. Let $\mathbf{v}_\theta$ denote the corresponding eigenvector of θ. We will make use of the trick that $\mathbf{v}_\theta \in \mathbf{1}^\perp$, so $J\mathbf{v}_\theta = 0$ where J is the all-one matrix of size $n \times n$ (see [**3**] for more background on spectral graph theory).

It is well known (see [**2**, Chapter 9] for more details) that if λ is much smaller than the degree k, then G has certain random-like properties. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs (u, w) such that $u \in U$, $w \in W$, and (u, w) is an edge of G. We recall the following well-known fact (see, for example, [**2**]).

Lemma 2.5 (Corollary 9.2.5, [**2**])**.** *Let $G = (V, E)$ be an (n, k, λ)-graph. For any two sets $B, C \subset V$, we have*

$$\left| e(B, C) - \frac{k|B||C|}{n} \right| \leq \lambda \sqrt{|B||C|}.$$

2.1. Product graphs over finite fields

For any $\lambda \in \mathbb{F}_q$, we define the product graph $\mathcal{P}_{\mathbb{F}_q,n}(\lambda)$ as follows. The vertex set of the product graph is the set $V\left(\mathcal{P}_{\mathbb{F}_q,n}(\lambda)\right) = \mathbb{F}_q^n \backslash (0,\ldots,0)$. Two vertices $\mathbf{a}$ and $\mathbf{b}$ in $V\left(\mathcal{P}_{\mathbb{F}_q,n}(\lambda)\right)$ are connected by an edge, $(\mathbf{a},\mathbf{b}) \in E\left(\mathcal{P}_{\mathbb{F}_q,n}(\lambda)\right)$, if and only if $\mathbf{a}\cdot\mathbf{b} := a_1b_1 + \cdots + a_nb_n = \lambda$. When $\lambda = 0$, the graph is the Erdős-Rényi graph, which has several interesting applications, for example, see [**1, 15, 18**]. We now study the product graph when $\lambda \in \mathbb{F}_q^*$.

Theorem 2.6 (Theorem 8.1, [**16**]). *For any $n \geq 2$ and $\lambda \in \mathbb{F}_q^*$, the product graph, $\mathcal{P}_{\mathbb{F}_q,n}(\lambda)$, is a*

$$\left(q^n - 1, q^{n-1}, \sqrt{2q^{n-1}}\right)\text{-graph.}$$

2.2. Product graphs over finite rings

Suppose that $q = p^r$ for some odd prime p and $r \geq 1$. We identify $\mathbb{Z}_q$ with $\{0,1,\ldots,q-1\}$, then $p\mathbb{Z}_{p^{r-1}}$ is the set of nonunits in $\mathbb{Z}_q$. For any $\lambda \in \mathbb{Z}_q^*$, the product graph $\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)$ is defined as follows. The vertex set of the product graph $\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)$ is the set $V\left(\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)\right) = \mathbb{Z}_q^n \setminus (p\mathbb{Z}_{p^{r-1}})^n$. Two vertices $\mathbf{a} = (a_1,\ldots,a_n)$, $\mathbf{b} = (b_1,\ldots,b_n)$ in $V\left(\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)\right)$ are connected by an edge $(\mathbf{a},\mathbf{b}) \in E\left(\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)\right)$ if and only if $\mathbf{a}\cdot\mathbf{b} := a_1b_1 + \cdots + a_nb_n = \lambda$.

Theorem 2.7 (Theorem 3.1, [**17**]). *The product graph $\mathcal{P}_{\mathbb{Z}_q,n}(\lambda)$ is a*

$$\left(p^{rn} - p^{n(r-1)}, p^{r(n-1)}, \sqrt{2rp^{(n-1)(2r-1)}}\right)\text{-graph.}$$

2.3. Sum-product graphs over finite rings

The sum-product graph $\mathcal{SP}_{q,n}$ is defined as follows. The vertex set of the sum-product graph $\mathcal{SP}_{q,n}$ is the set $V(\mathcal{SP}_{q,n}) = \mathbb{Z}_q \times \mathbb{Z}_q^n$. Two vertices $U = (a,\mathbf{b})$ and $V = (c,\mathbf{d}) \in V(\mathcal{SP}_{q,n})$ are connected by an edge, $(U,V) \in E(\mathcal{SP}_{q,n})$, if and only if $a + c = \mathbf{b}\cdot\mathbf{d}$.

Theorem 2.8 (Theorem 4.1, [**17**]). *The sum-product graph, $\mathcal{SP}_{q,n}$, is a*

$$\left(q^{n+1}, q^n, \sqrt{2rp^{n(2r-1)}}\right) - \textit{graph.}$$

3. PROOFS OF THEOREMS 1.2, 1.3, AND 1.4

Proof of Theorem 1.2. For any $1 \leq i \leq d$, let $t_i := \min\left\{\mathtt{ord}_{\mathbb{F}_q^*}(u_i), \lfloor M_i/2 \rfloor\right\}$, and

$$\mathcal{A} := \left\{(a_1u_1^{x_1},\ldots,a_du_d^{x_d})\colon 1 \leq x_i \leq t_i,\ 1 \leq i \leq d\right\},$$
$$\mathcal{B} := \left\{(u_1^{x_1},\ldots,u_d^{x_d})\colon 1 \leq x_i \leq t_i,\ 1 \leq i \leq d\right\}.$$

We now prove that $|\mathcal{A}|, |\mathcal{B}| \geq \prod_{i=1}^{d} t_i$. Since $(a_1, \ldots, a_d) \in \left(\mathbb{F}_q^*\right)^d$, we obtain $|\mathcal{A}| = |\mathcal{B}|$. It suffices to indicate that all elements in $\mathcal{B}$ are distinct. If there exist two points $(u_1^{x_1}, \ldots, u_d^{x_d})$ and $(u_1^{y_1}, \ldots, u_d^{y_d})$ in $\mathcal{B}$ satisfying

$$(u_1^{x_1}, \ldots, u_d^{x_d}) = (u_1^{y_1}, \ldots, u_d^{y_d}), \text{ with } (x_1, \ldots, x_d) \neq (y_1, \ldots, y_d),$$

then, without loss of generality, we assume that $x_1 \neq y_1$ which implies that

$$u_1^{|x_1 - y_1|} = 1.$$

So, $\mathtt{ord}_{\mathbb{F}_q}(u_1) \leq |x_1 - y_1|$. On the other hand, since $1 \leq x_1, y_1 \leq t_1$, $0 \leq |x_1 - y_1| < t_1$. This leads to a contradiction since $t_1 \leq \mathtt{ord}_{\mathbb{F}_q}(u_i)$. In short, all elements in $\mathcal{B}$ are distinct, and $|\mathcal{B}| \geq \prod_{i=1}^{d} t_i$. For any fixed $\lambda \in \mathbb{F}_q^*$, the equation

$$a_1 u_1^{x_1} + \cdots + a_d u_d^{x_d} = \lambda \tag{3.1}$$

has at least one solution $(x_1, \ldots, x_d)$ with $1 \leq x_i \leq M_i$ for all $1 \leq i \leq d$, if and only if there exists an edge between $\mathcal{A}$ and $\mathcal{B}$ in the product graph $\mathcal{P}_{\mathbb{F}_q,d}(\lambda)$. It follows from Lemma 2.5 and Theorem 2.6 that there exists at least one edge between $\mathcal{A}$ and $\mathcal{B}$ when $|\mathcal{A}||\mathcal{B}| \geq 2q^{d+1}$. Hence if $\prod_{i=1}^{d} t_i \geq \sqrt{2} q^{(d+1)/2}$, then for any $\lambda \in \mathbb{F}_q^*$, the equation (3.1) has at least one solution, which completes the proof of theorem.

Proof of Theorem 1.3. First we note that since q is an odd prime power, $\mathbb{Z}_q^*$ is a cyclic group of order $p^r - p^{r-1}$. Therefore, by using the same arguments as in the proof of Theorem 1.2, Theorem 1.3 follows from Lemma 2.5 and Theorem 2.7.

Proof of Theorem 1.4. First we set

$$t_i := \begin{cases} \min\{\mathtt{ord}_{\mathbb{F}_q^*}(u_1), M_1\}, & i = 1 \\ \min\{\mathtt{ord}_{\mathbb{F}_q^*}(u_i), \lfloor M_i/2 \rfloor\}, & i \geq 2 \end{cases}$$

For a fixed $\lambda \in \mathbb{Z}_q$, we define

$$\mathcal{A} := \left\{(\lambda, a_2 u_2^{x_2}, \ldots, a_d u_d^{x_d}) \colon 1 \leq x_i \leq t_i,\ 2 \leq i \leq d\right\},$$

and

$$\mathcal{B} := \left\{(-a_1 u_1^{x_1}, u_2^{x_2}, \ldots, u_d^{x_d}) \colon\ 1 \leq x_1 \leq \min\{\mathtt{ord}_{\mathbb{Z}_q^*}(u_1), M_1\}, 1 \leq x_i \leq t_i,\ 2 \leq i \leq d\right\}.$$

We can consider $\mathcal{A}$ and $\mathcal{B}$ as two vertex sets in the sum-product graph $\mathcal{SP}_{q,d}$. By using the same arguments as in the proof of Theorem 1.2, we obtain $|\mathcal{A}||\mathcal{B}| \geq t_1 \prod_{i=2}^{d} t_i^2$. Therefore, it follows from Lemma 2.5 and Theorem 2.8 that if

$$\sqrt{t_1} \prod_{i=2}^{d} t_i \geq \sqrt{2r} p^{\frac{d(2r-1)+1}{2}},$$

then there exists at least an edge between $\mathcal{A}$ and $\mathcal{B}$. Thus, the equation (3.1) has at least one solution for any fixed $\lambda \in \mathbb{Z}_q$. This concludes the proof of the theorem.

Acknowledgements. The authors would like to thank two anonymous referees for valuable comments and suggestions which improved the presentation of this paper considerably.

The second listed author was partially supported by Swiss National Science Foundation grants 200020-162884 and 200020-144531. The research of the third listed author is funded by the National Foundation for Science and Technology Development Project. 101.99-2013.21.

REFERENCES

1. N. Alon, M. Krivelevich: *Constructive bounds for a Ramsey-type problems.* Graphs Combin., **13** (1997), 217–225.
2. N. Alon, J. H. Spencer: *The probabilistic method*, 2nd ed. Willey-Interscience, 2000.
3. A. Brouwer, W. Haemers: *Spectra of Graphs.* Springer, New York, 2012.
4. J. Cilleruelo: *Combinatorial problems in finite fields and Sidon sets.* Combinatorica, **32** (5) (2012), 497–511.
5. J. Cilleruelo, A. Zumalacárregui: *An additive problem in finite fields with powers of elements of large multiplicative order.* Rev. Mat. Complut., **27** (2014), 501–508.
6. C. Elsholtz: *Almost all primes have a hamming weight.* Bull. Aust. Math. Soc., 2016.
7. M. Z. Garaev, K.-L. Kueh: *Distribution of special sequences modulo a large prime.* Int. J. Math. Math. Sci., **50**, (2003), 3189–3194.
8. C. V. García: *A note on an additive problem with powers of a primitive root.* Bol. Soc. Mat. Mex. (3), **11** (1) (2005), 1–4.
9. D. Hart, A. Iosevich: *Sums and products in finite fields*: *An integral geometric viewpoint.* Radon transforms, geometry, and wavelets **464** (2008), 129–135.
10. D. Hart, A. Iosevich, D. Koh, M. Rudnev: *Averages over hyperplanes, sum–product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture.* Trans. Amer. Math. Soc., **363** (6) (2011), 3255–3275.
11. D. Hart, A. Iosevich, J. Solymosi: *Sum-product estimates in finite fields via Kloosterman sums.* IMRN-International Mathematics Research Notices, 2007 (7), rnm007.
12. S. V. Konyagin: *Bounds of exponential sums over subgroups and Gauss sums.* In: 4th International Conference Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State University, pp. 86–114. Moscow (2002).
13. Z. Rudnik, A. Zaharescu: *The distribution of spacings between small powers of a primitive root.* Israel J. Math., **120** (200), 271–287.
14. I. E. Shparlinski: *On the solvability of bilinear equations in finite fields.* Glasg. Math. J., **50** (3) (2008), 523–529.
15. P. V. Thang, L. A. Vinh: *Erdős-Rényi graph, Szemerédi-Trotter type theorem, and sum-product estimates over finite rings.* Forum Math., **27** (1) (2015), 331-342.
16. L. A. Vinh: *The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs.* Forum Math., **26** (1) (2014), 141–175.

17. L. A. Vinh: *Product graphs, Sum-product graphs and sum-product estimate over finite rings.* Forum Math., **27** (3) (2015), 1639–1655.

18. L. A. Vinh: *A Szemerédi-Trotter type theorem and sum-product estimate over finite fields.* Eur. J. Comb., **32** (8) (2011), 1177–1181.

19. L. A. Vinh: *On the sum of the squared multiplicities of the distances in a point set over finite spaces.* Appl. Anal. Discrete Math., **7** (2013), 106–118.

Hanoi University of Science,
Vietnam National University
Viet Nam
E-mail: sangnmkhtnhn@gmail.com

Department of Mathematics,
EPF Lausanne
Switzerland
E-mail: thang.pham@epfl.ch

University of Education,
Vietnam National University
Viet Nam
E-mail: vinhla@vnu.edu.vn

(Received Jaunary 29, 2016)
(Revised August 23, 2016)