DOI: 10.4153/S0008414X25000136

Canad. J. Math. Vol. **00** (0), 2025 pp. 1–41
http://dx.doi.org/10.4153/xxxx

Multiplicative structure of shifted multiplicative subgroups and its applications to Diophantine tuples

Seoyoung Kim, Chi Hoi Yip and Semin Yoo

Abstract. **In this paper, we investigate the multiplicative structure of a shifted multiplicative subgroup and its connections with additive combinatorics and the theory of Diophantine equations. Among many new results, we highlight our main contributions as follows. First, we show that if a nontrivial shift of a multiplicative subgroup G contains a product set AB, then $|A||B|$ is essentially bounded by $|G|$, refining a well-known consequence of a classical result by Vinogradov. Second, we provide a sharper upper bound of $M_k(n)$, the largest size of a set such that each pairwise product of its elements is n less than a k-th power, refining the recent result of Dixit, Kim, and Murty. One main ingredient in our proof is the first non-trivial upper bound on the maximum size of a generalized Diophantine tuple over a finite field. In addition, we determine the maximum size of an infinite family of generalized Diophantine tuples over finite fields with square order, which is of independent interest. We also make significant progress towards a conjecture of Sárközy on the multiplicative decompositions of shifted multiplicative subgroups. In particular, we prove that for almost all primes p, the set $\{x^2-1 : x \in \mathbb{F}_p^*\} \setminus \{0\}$ cannot be decomposed as the product of two sets in $\mathbb{F}_p$ non-trivially.**

1 Introduction

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. Let G be a multiplicative subgroup of $\mathbb{F}_q$. While G itself has a "perfect" multiplicative structure, it is natural to ask if a (non-trivial additive) shift of G still possesses some multiplicative structure. Indeed, as a fundamental question in additive combinatorics, this question has drawn the attention of many researchers and it is closely related to many questions in number theory. For example, a classical result of Vinogradov [36] states that for a prime p and an integer n such that $p \nmid n$, if $A, B \subset \{1, 2, \dots, p-1\}$, then

$$\left| \sum_{a \in A,\, b \in B} \left(\frac{ab+n}{p} \right) \right| \leq \sqrt{p|A||B|}. \tag{1.1}$$

More generally, inequality (1.1) extends to all nontrivial multiplicative characters over all finite fields; see Proposition 3.1. Inequality (1.1) leads an estimate on the size of a product set contains in the set of shifted squares: if $A, B \subset \mathbb{F}_p^*$, $\lambda \in \mathbb{F}_p^*$, and G is the subgroup of $\mathbb{F}_p^*$ of index 2 such that $AB \subset (G+\lambda)$, then

$$|A||B| < (1+o(1))p. \tag{1.2}$$

2020 Mathematics Subject Classification: Primary 11B30, 11D72; Secondary 11D45, 11N36, 11L40.
Keywords: Diophantine tuples, shifted multiplicative subgroup, multiplicative decomposition.

For more recent works related to this question and its connection with other problems, we refer to [17, 27, 31, 37] and references therein. An *analogue* of this question over integers is closely related to the well-studied Diophantine tuples and their generalizations; see Subsection 1.1.

In this paper, we study the multiplicative structure of a shifted multiplicative subgroup following the spirit of the aforementioned works and discuss a few new applications in additive combinatorics and Diophantine equations. More precisely, one of our contributions is the following theorem.

***Theorem* 1.1** *Let $d \mid (q-1)$ with $d \geq 2$. Let $S_d = \{x^d : x \in \mathbb{F}_q^*\}$. Let $A, B \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$ with $|A|, |B| \geq 2$. Assume further that $\binom{|A|-1+\frac{q-1}{d}}{|A|} \not\equiv 0 \pmod{p}$ if $q \neq p$. If $AB + \lambda \subset S_d \cup \{0\}$, then*

$$|A||B| \leq |S_d| + |B \cap (-\lambda A^{-1})| + |A| - 1.$$

Moreover, when $\lambda \in S_d$, we have a stronger upper bound:

$$|A||B| \leq |S_d| + |B \cap (-\lambda A^{-1})| - 1.$$

Clearly, Theorem 1.1 improves inequality (1.2) implied by Vinogradov's estimate (1.1) when $d = 2$, and the generalization of inequality (1.2) by Gyarmati [17, Theorem 8] for general d, where the upper bound is given by $(\sqrt{p}+2)^2$ when $q = p$ is a prime. We remark that in general the condition on the binomial coefficient in the statement of Theorem 1.1 cannot be dropped when q is not a prime; see Theorem 1.6.

The proof of Theorem 1.1 is based on Stepanov's method [35], and is motivated by a recent breakthrough of Hanson and Petridis [21]. In fact, Theorem 1.1 can be viewed as a multiplicative analog of their results. Going beyond the perspective of these multiplicative analogs, we provide new insights into the application of Stepanov's method. For example, our technique applies to all finite fields while their technique only works over prime fields. We also prove a similar result for restricted product sets (see Theorem 4.2), whereas their technique appears to only lead to a weaker bound; see Remark 4.3.

Besides Theorem 1.1, we also provide three novel applications of Theorem 1.1 and its variants. These applications significantly improve on many previous results in the literature. Unsurprisingly, to achieve these applications, we need additional tools and insights from Diophantine approximation, sieve methods, additive combinatorics, and character sums. From here, we briefly mention what applications are about. In Subsection 1.1, we improve the upper bound of generalized Diophantine tuples over integers. Interestingly, Theorem 1.1 is closely related to a bipartite version of Diophantine tuples over finite fields. This new perspective yields a substantial improvement in the result of generalized Diophantine tuples over integers. In Subsection 1.2, we obtain the first nontrivial upper bounds on generalized Diophantine tuples and strong Diophantine tuples over finite fields. Moreover, some of our new bounds are sharp. Last but not least, in Subsection 1.3, we make significant progress towards a conjecture of Sárközy [31] on multiplicative decompositions of shifted multiplicative subgroups. We elaborate on the context of these applications in the next subsections.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

1.1 Diophantine tuples over integers

A set $\{a_1, a_2, \ldots, a_m\}$ of distinct positive integers is a *Diophantine m-tuple* if the product of any two distinct elements in the set is one less than a square. The first known example of integral Diophantine 4-tuples is $\{1, 3, 8, 120\}$ which was studied by Fermat. The Diophantine 4-tuple was extended by Euler to the rational 5-tuple $\{1, 3, 8, 120, \frac{777480}{8288641}\}$, and it had been conjectured that there is no Diophantine 5-tuple. The difficulty of extending Diophantine tuples can be explained by its connection to the problem of finding integral points on elliptic curves: if $\{a, b, c\}$ forms a Diophantine 3-tuple, in order to find a positive integer d such that $\{a, b, c, d\}$ is a Diophantine 4-tuple, we need to solve the following simultaneous equation for d:

$$ad + 1 = s^2, \quad bd + 1 = t^2, \quad cd + 1 = r^2.$$

This is related to the problem of finding an integral point (d, str) on the following elliptic curve

$$y^2 = (ax + 1)(bx + 1)(cx + 1).$$

From this, we can deduce that there are no infinite Diophantine m-tuples by Siegel's theorem on integral points. On the other hand, Siegel's theorem is not sufficient to give an upper bound on the size of Diophantine tuples due to its ineffectivity. In the same vein, finding a Diophantine tuple of size greater than or equal to 5 is related to the problem of finding integral points on hyperelliptic curves of genus $g \geq 2$. Despite the aforementioned difficulties, the conjecture on the non-existence of Diophantine 5-tuples was recently proved to be true in the sequel of important papers by Dujella [9], and He, Togbé, and Ziegler [22].

The definition of Diophantine m-tuples has been generalized and studied in various contexts. We refer to the recent book of Dujella [10] for a thorough list of known results on the topic and their reference. In this paper, we focus on the following generalization of Diophantine tuples: for each $n \geq 1$ and $k \geq 2$, we call a set $\{a_1, a_2, \ldots, a_m\}$ of distinct positive integers a *Diophantine m-tuple with property $D_k(n)$* if the product of any two distinct elements is n less than a k-th power. We write

$$M_k(n) = \sup\{|A|\colon A \subset \mathbb{N} \text{ satisfies the property } D_k(n)\}.$$

Similar to the classical case, the problem of finding $M_k(n)$ for $k \geq 3$ and $n \geq 1$ is related to the problem of counting the number of integral points of the superelliptic curve

$$y^k = f(x) = (a_1x + n)(a_2x + n)(a_3x + n)$$

The theorem of Faltings [13] guarantees that the above curve has only finitely many integral points, and this, in turn, implies that a set with property $D_k(n)$ must be finite. The known upper bounds for the number of integral points depend on the coefficients of $f(x)$. The Caporaso-Harris-Mazur conjecture [6] implies that $M_k(n)$ is uniformly bounded, independent of n. For other conditional bounds, we refer the readers to Subsection 2.4.

Unconditionally, in [4], Bugeaud and Dujella [4, Corollary 4] showed that $M_3(1) \leq 7$, $M_k(1) \leq 5$ for $k \in \{4, 5\}$, $M_k(1) \leq 4$ for $6 \leq k \leq 176$, and the uniform bound

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

$M_k(1) \leq 3$ for any $k \geq 177$ [1]. On the other hand, the best-known upper bound on $M_2(n)$ is $(2+o(1))\log n$, due to the second author [39]. Very recently, Dixit, Murty, and the first author [7] studied the size of a generalized Diophantine m-tuple with property $D_k(n)$, improving the previously best-known upper bound $M_3(n) \leq 2|n|^{17} + 6$ and $M_k(n) \leq 2|n|^5+3$ for $k \geq 5$ given by Bérczes, Dujella, Hajdu and Luca [2] when $n \to \infty$. They showed that if k is fixed and $n \to \infty$, then $M_k(n) \ll_k \log n$. Following their proof in [7], the bound can be more explicitly expressed as $M_k(n) \leq (3\phi(k) + o(1))\log n$ when $k \geq 3$ is fixed, $n \to \infty$, and ϕ is the Euler phi function. Note that their upper bound on $M_k(n)$ is perhaps not desirable. Indeed, it is natural to expect that $M_k(n)$ would decrease if n is fixed, and k increases, since k-th powers become sparser. Instead, our new upper bounds on $M_k(n)$ support this heuristic.

In this paper, we provide a significant improvement on the upper bound of $M_k(n)$ by using a novel combination of Stepanov's method and Gallagher's larger sieve inequality. In order to state our first result, we define the following constant

$$\eta_k = \min_{\mathcal{I}} \frac{|\mathcal{I}|}{T_{\mathcal{I}}^2} \tag{1.3}$$

for each $k \geq 2$, where the minimum is taken over all nonempty subsets $\mathcal{I}$ of the set

$$\{1 \leq i \leq k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\},$$

and $T_{\mathcal{I}} = \sum_{i\in\mathcal{I}} \sqrt{\gcd(i-1,k)}$.

***Theorem* 1.2** *There is a constant $c' > 0$, such that as $n \to \infty$,*

$$M_k(n) \leq \left(\frac{2k}{k-2} + o(1)\right)\eta_k\phi(k)\log n, \tag{1.4}$$

holds uniformly for positive integers $k, n \geq 3$ such that $\log k \leq c'\sqrt{\log\log n}$.

The constant η_k is essentially computed via the optimal collection of "admissible" residue classes when applying Gallagher's larger sieve (see Section 5). Note that when $\mathcal{I} = \{1\}$, we have $T_{\mathcal{I}} = \sqrt{k}$, and hence we have $\eta_k \leq \frac{1}{k}$. In particular, if $k \geq 3$ is fixed and $n \to \infty$, inequality (1.4) implies the upper bound

$$M_k(n) \leq \frac{(2+o(1))\phi(k)}{k-2}\log n, \tag{1.5}$$

which already improves the best-known upper bound $M_k(n) \leq (3\phi(k) + o(1))\log n$ of [7] that we mentioned earlier substantially. In Appendix A, we illustrate the bound in inequality (1.4): for $2 \leq k \leq 1001$, we compute the suggested upper bound

$$\nu_k = \frac{2k}{k-2}\eta_k\phi(k)$$

of $\gamma_k = \limsup_{n\to\infty} \frac{M_k(n)}{\log n}$. From Figure A.1, one can compare the bound of $M_k(n)$ in Theorem 1.2 with the bound in [7]. From inequality (1.5), we see γ_k is uniformly

[1] As pointed out by [2], there was a minor inaccuracy in the original proof of [4, Corollary 4], but it only affected the upper bound on $M_5(1)$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

bounded by 6. Table A.2 illustrates better upper bounds on γ_k for $2 \le k \le 201$. In particular, we use a simple greedy algorithm to determine η_k for a fixed k. We also refer to Subsection 5.3 for a simple upper bound on η_k, which well approximates η_k empirically.

At first glance, Theorem 1.2 improves the bound in [7] of $M_k(n)$ by only a constant multiplicative factor when k is fixed. Nevertheless, note that Theorem 1.2 holds uniformly for k and n as long as $\log k \le c'\sqrt{\log\log n}$. Thus, when k is assumed to be a function of n which increases as n increases, we can break the "$\log n$ barrier" in [7], that is, $M_k(n) = O_k(\log n)$, and provide a *dramatic* improvement.

***Theorem* 1.3** *There is $k = k(n)$ such that $\log k \asymp \sqrt{\log\log n}$, and*

$$M_k(n) \ll \exp\left(-\frac{c''(\log\log n)^{1/4}}{\log\log\log n}\right)\log n,$$

where $c'' > 0$ is an absolute constant.

The proofs of Theorem 1.2 and Theorem 1.3 require the study of (generalized) Diophantine tuples over finite fields, which we discuss below.

1.2 Diophantine tuples over finite fields

A *Diophantine m-tuple with property $D_d(\lambda, \mathbb{F}_q)$* is a set $\{a_1, \dots, a_m\}$ of m distinct elements in $\mathbb{F}_q^*$ such that $a_i a_j + \lambda$ is a d-th power in $\mathbb{F}_q^*$ or 0 whenever $i \ne j$. Moreover, we also define the strong Diophantine tuples in finite fields motivated by Dujella and Petričević [11]: a *strong Diophantine m-tuple with property $SD_d(\lambda, \mathbb{F}_q)$* is a set $\{a_1, \dots, a_m\}$ of m distinct elements in $\mathbb{F}_q^*$ such that $a_i a_j + \lambda$ is a d-th power in $\mathbb{F}_q^*$ or 0 for any choice of i and j. Unlike the natural analog for the classical Diophantine tuples (of property $D_2(1)$), it makes sense to talk about the strong Diophantine tuples in $\mathbb{F}_q$. The strong generalized Diophantine tuples with property $D_k(n)$ in for general k and n are also meaningful to study: the problem of counting the explicit size of the strong generalized Diophantine tuples with property $D_k(n)$ involves the problem of counting solutions of the equations appearing in the statement of Pillai's conjecture. Theorem 1.2 can be improved for strong generalized Diophantine tuples with property $D_k(n)$; see Theorem 5.2.

The generalizations of Diophantine tuples over finite fields are of independent interest. Perhaps the most interesting question to explore is the exact analog of estimating $M_k(n)$ as discussed in Subsection 1.1. Indeed, estimating the size of the largest Diophantine tuple with property $SD_d(\lambda, \mathbb{F}_q)$ or with property $D_d(\lambda, \mathbb{F}_q)$ is of particular interest for the application of Diophantine tuples (over integers) as discussed in [1, 7, 8, 16, 24]. Similarly, we denote

$$MSD_d(\lambda, \mathbb{F}_q) = \sup\{|A|\colon A \subset \mathbb{F}_q^* \text{ satisfies property } SD_d(\lambda, \mathbb{F}_q)\}, \quad \text{and}$$
$$MD_d(\lambda, \mathbb{F}_q) = \sup\{|A|\colon A \subset \mathbb{F}_q^* \text{ satisfies property } D_d(\lambda, \mathbb{F}_q)\}.$$

Note that when $\lambda = 0$, it is trivial that $MSD_d(\lambda, \mathbb{F}_q) = MD_d(\lambda, \mathbb{F}_q) = \frac{q-1}{d}$. Thus, we always assume $\lambda \ne 0$ throughout the paper. In Section 3, we give an upper bound

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

$\sqrt{q} + O(1)$ of $MSD_d(\lambda, \mathbb{F}_q)$ and $MD_d(\lambda, \mathbb{F}_q)$. More precisely, we prove the following proposition using a double character sum estimate. We refer to the bounds in the following proposition as the "trivial" upper bound.

Proposition* 1.4** ***(Trivial upper bound) *Let $d \geq 2$ and let $q \equiv 1 \pmod{d}$ be a prime power. Let $A \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$. Then $MSD_d(\lambda, \mathbb{F}_q) \leq \frac{\sqrt{4q-3}+1}{2}$ and $MD_d(\lambda, \mathbb{F}_q) \leq \sqrt{q - \frac{11}{4}} + \frac{5}{2}$.*

For the case $q = p$, similar bounds of Proposition 1.4 are known previously in [1, 7, 17]. On the other hand, Proposition 1.4 gives an almost optimal bound of $MSD_d(\lambda, \mathbb{F}_q)$ and $MD_d(\lambda, \mathbb{F}_q)$ when q is a square (Theorem 1.6). Our next theorem improves the trivial upper bounds in Proposition 1.4 by a multiplicative constant factor $\sqrt{1/d}$ or $\sqrt{2/d}$ when $q = p$ is a prime.

***Theorem* 1.5** *Let $d \geq 2$. Let $p \equiv 1 \pmod{d}$ be a prime and let $\lambda \in \mathbb{F}_p^*$. Then*

(1) *$MSD_d(\lambda, \mathbb{F}_p) \leq \sqrt{(p-1)/d} + 1$. Moreover, if λ is a d-th power in $\mathbb{F}_p^*$, then we have a stronger upper bound:*

$$MSD_d(\lambda, \mathbb{F}_p) \leq \sqrt{\frac{p-1}{d} - \frac{3}{4}} + \frac{1}{2}.$$

(2) *$MD_d(\lambda, \mathbb{F}_p) \leq \sqrt{2(p-1)/d} + 4$.*

We remark that our new bound on $MSD_d(\lambda, \mathbb{F}_p)$ is sometimes sharp. For example, we get a tight bound for a prime $p \in \{5, 7, 11, 13, 17, 23, 31, 37, 41, 53, 59, 61, 113\}$ when $d = 2$ and $\lambda = 1$. See also Theorem 4.7 and Remark 4.8 for a generalization of Theorem 1.5 over general finite fields with non-square order under some extra assumptions.

Nevertheless, in the case of finite fields of square order, we improve Proposition 1.4 by a little bit under some minor assumptions; see Theorem 4.5. Surprisingly, this tiny improvement turns out to be sharp for many *infinite families* of (q, d, λ). Equivalently, we determine $MD_d(\lambda, \mathbb{F}_q)$ and $MSD_d(\lambda, \mathbb{F}_q)$ *exactly* in those families. In the following theorem, we give a sufficient condition so that $MD_d(\lambda, \mathbb{F}_q)$ and $MSD_d(\lambda, \mathbb{F}_q)$ can be determined explicitly.

***Theorem* 1.6** *Let q be a prime power and a square, $d \geq 2$, and $d \mid (\sqrt{q}+1)$. Let $S_d = \{x^d : x \in \mathbb{F}_q^*\}$. Suppose that there is $\alpha \in \mathbb{F}_q$ such that $\alpha^2 \in S_d$ and $\lambda \in \alpha^2 \mathbb{F}_{\sqrt{q}}^*$ (for example, if $\alpha = 1$ and $\lambda \in \mathbb{F}_{\sqrt{q}}^*$). Suppose further that $r \leq (p-1)\sqrt{q}$, where r is the remainder of $\frac{q-1}{d}$ divided by $p\sqrt{q}$. Then $MSD_d(\lambda, \mathbb{F}_q) = \sqrt{q} - 1$. If $q \geq 25$ and $d \geq 3$, then we have the stronger conclusion that $MD_d(\lambda, \mathbb{F}_q) = \sqrt{q} - 1$.*

Under the assumptions on Theorem 1.6, $\alpha \mathbb{F}_{\sqrt{q}}^*$ satisfies the required property $SD_d(\lambda, \mathbb{F}_q)$ and $D_d(\lambda, \mathbb{F}_q)$. Compared to Theorem 1.5, it is tempting to conjecture that such an algebraic construction (which is unique to finite fields with proper prime power

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

order) is the optimal one with the required property. Given Proposition 1.4, to show such construction is optimal, it suffices to rule out the possibility of a Diophantine tuple with property $SD_d(\lambda, \mathbb{F}_q)$ and $D_d(\lambda, \mathbb{F}_q)$ of size $\sqrt{q}$. While this seems easy, it turned out that this requires non-trivial efforts.

Next, we give concrete examples where Theorem 1.6 applies.

Example 1.7 Note that a Diophantine tuple with property $SD_2(1, \mathbb{F}_q)$ corresponds to a strong Diophantine tuple over $\mathbb{F}_q$. If q is an odd square, Theorem 1.6 implies that the largest size of a strong Diophantine tuple over $\mathbb{F}_q$ is given by $\sqrt{q} - 1$, which is achieved by $\mathbb{F}^*_{\sqrt{q}}$. Note that in this case we have $r = \frac{p\sqrt{q}-1}{2} < (p-1)\sqrt{q}$.

We also consider the case that $d = 3, d \mid (\sqrt{q}+1)$, and $\lambda = 1$. In this case, Theorem 1.6 also applies. Note that $3 \mid (\sqrt{q}+1)$ implies that $p \equiv 2 \pmod 3$, in which case the base-p representation of $\frac{q-1}{3}$ only contains the digit $\frac{p-2}{3}$ and $\frac{2p-1}{3}$, so that the condition $r \le (p-1)\sqrt{q}$ holds.

One key ingredient of the proof of Theorem 1.5 and Theorem 1.6 is Theorem 1.1. Indeed, Theorem 1.1 can also be viewed as on an upper bound of a bipartite version of Diophantine tuples over finite fields. For the applications to strong Diophantine tuples, Theorem 1.1 is sufficient. On the other hand, to obtain upper bounds on Diophantine tuples (which are not necessarily strong Diophantine tuples), we also need a version of Theorem 1.1 for restricted product sets, which can be found as Theorem 4.2. Indeed, Theorem 1.1 alone only implies a weaker bound of the form $2\sqrt{p/d}$ for $MSD_d(\lambda, \mathbb{F}_p)$; see Remark 4.3.

1.3 Multiplicative decompositions of shifted multiplicative subgroups

A well-known conjecture of Sárközy [30] asserts that the set of nonzero squares $S_2 = \{x^2 : x \in \mathbb{F}_p^*\} \subset \mathbb{F}_p$ cannot be written as $S_2 = A + B$, where $A, B \subset \mathbb{F}_p$ and $|A|, |B| \ge 2$, provided that p is a sufficiently large prime. This conjecture essentially predicts that the set of quadratic residues in a prime field cannot have a rich additive structure. Similarly, one expects that any non-trivial shift of S_2 cannot have a rich multiplicative structure. Indeed, this can be made precise via another interesting conjecture of Sárközy [31], which we make progress in the current paper.

***Conjecture* 1.8 (*Sárközy*)** *If p is a sufficiently large prime and $\lambda \in \mathbb{F}_p^*$, then the shifted subgroup $(S_2 - \lambda) \setminus \{0\}$ cannot be written as the product AB, where $A, B \subset \mathbb{F}_p^*$ and $|A|, |B| \ge 2$. In other words, $(S_2 - \lambda) \setminus \{0\}$ has no non-trivial multiplicative decomposition.*

We note that it is necessary to take out the element 0 from the shifted subgroup, for otherwise one can always decompose $S_2 - \lambda$ as $\{0, 1\} \cdot (S_2 - \lambda)$. It appears that this problem concerning multiplicative decompositions is more difficult than the one concerning additive decompositions stated previously, given that it might depend on the parameter λ. Inspired by Conjecture 1.8, we formulate the following more general conjecture for any proper multiplicative subgroup. For simplicity, we denote $S_d = S_d(\mathbb{F}_q) = \{x^d : x \in \mathbb{F}_q^*\}$ to be the set of d-th powers in $\mathbb{F}_q^*$, equivalently, the subgroup of $\mathbb{F}_q^*$ with order $\frac{q-1}{d}$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

***Conjecture* 1.9** *Let $d \geq 2$. If $q \equiv 1 \pmod{d}$ is a sufficiently large prime power, then for any $\lambda \in \mathbb{F}_q^*$, $(S_d - \lambda) \setminus \{0\}$ does not admit a non-trivial multiplicative decomposition, that is, there do not exist two sets $A, B \subset \mathbb{F}_q^*$ with $|A|, |B| \geq 2$, such that $(S_d - \lambda) \setminus \{0\} = AB$.*

Conjecture 1.9 predicts that a shifted multiplicative subgroup of a finite field admits a non-trivial multiplicative decomposition only when it has a small size. We remark that the integer version of Conjecture 1.9, namely, for each $k \geq 2$, a non-trivial shift of k-th powers in integers has no non-trivial multiplicative decomposition, has been proved and strengthened in a series of papers by Hajdu and Sárközy [18, 19, 20]. On the other hand, to the best knowledge of the authors, Conjecture 1.9 appears to be much harder and no partial progress has been made. For the analog of Conjecture 1.9 on the additive decomposition of multiplicative subgroups, we refer to recent papers [21, 31, 33, 38] for an extensive discussion on partial progress.

Our main contribution to Conjecture 1.9 is the following two results. The first one is a corollary of Theorem 1.1.

***Corollary* 1.10** *Let $d \geq 2$ and p be a prime such that $d \mid (p-1)$. Let $\lambda \in S_d$. If $(S_d - \lambda) \setminus \{0\}$ can be multiplicative decomposed as the product of two sets $A, B \subset \mathbb{F}_p^*$ with $|A|, |B| \geq 2$, then we must have $|A||B| = |S_d| - 1$, that is, all products ab are distinct. In other words, A, B are multiplicatively co-Sidon.*

In particular, Corollary 1.10 confirms Conjecture 1.9 under the assumption that q is a prime, $\lambda \in S_d$, and $|S_d| - 1$ is a prime. The second result provides a partial answer to Conjecture 1.9 asymptotically.

***Theorem* 1.11** *Let $d \geq 2$ be fixed and n be a positive integer. As $x \to \infty$, the number of primes $p \leq x$ such that $p \equiv 1 \pmod{d}$ and $(S_d(\mathbb{F}_p) - n) \setminus \{0\}$ has no non-trivial multiplicative decomposition is at least*

$$\left(\frac{1}{[\mathbb{Q}(e^{2\pi i/d}, n^{1/d}) : \mathbb{Q}]} - o(1)\right)\pi(x).$$

In particular, by setting $n = 1$ and $d = 2$, our result has the following significant implication to Sárközy's conjecture [31]: for almost all odd primes p, the shifted multiplicative subgroup $(S_2(\mathbb{F}_p) - 1) \setminus \{0\}$ has no non-trivial multiplicative decomposition. In other words, if $\lambda = 1$, then Sárközy's conjecture holds for almost all primes p; see Theorem 6.1 for a precise statement.

Some partial progress has been made for Conjecture 1.9 when the multiplicative decomposition is assumed to have special forms [31, 33]. We also make progress in this direction in Subsection 6.2. In particular, in Theorem 6.6, we confirm the ternary version of Conjecture 1.9 in a strong sense, which generalizes [31, Theorem 2].

Notations. We follow standard notations from analytic number theory. We use π and θ to denote the standard prime-counting functions. We adopt standard asymptotic notations $O, o, \asymp$. We also follow the Vinogradov notation $\ll$: we write $X \ll Y$ if there is an absolute constant $C > 0$ so that $|X| \leq CY$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Throughout the paper, let p be a prime and q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We always assume that $d \mid (q-1)$ with $d \geq 2$, and denote $S_d(\mathbb{F}_q) = \{x^d : x \in \mathbb{F}_q^*\}$ to be the subgroup of $\mathbb{F}_q^*$ with order $\frac{q-1}{d}$. If q is assumed to be fixed, for brevity, we simply write S_d instead of $S_d(\mathbb{F}_q)$.

We also need some notations for arithmetic operations among sets. Given two sets A and B, we write the *product set* $AB = \{ab : a \in A, b \in B\}$, and the *sumset* $A + B = \{a + b : a \in A, b \in B\}$. Given the definition of Diophantine tuples, it is also useful to define the *restricted product set* of A, that is, $A\hat{\times}A = \{ab : a, b \in A, a \neq b\}$.

Structure of the paper. In Section 2, we introduce more background. In Section 3, using Gauss sums and Weil's bound, we give an upper bound on the size of the set which satisfies various multiplicative properties based on character sum estimates. In particular, we prove Proposition 1.4. In Section 4, we first prove Theorem 1.1 using Stepanov's method. At the end of the section, we deduce applications of Theorem 1.1 to Diophantine tuples and prove Theorem 1.5 and Theorem 1.6. Via Gallagher's larger sieve inequality and other tools from analytic number theory, in Section 5, we prove Theorem 1.2 and Theorem 1.3. In Section 6, we study multiplicative decompositions and prove Theorem 1.11.

2 Background

2.1 Stepanov's method

We first describe Stepanov's method [35]. If we can construct a low degree *non-zero* auxiliary polynomial that vanishes on each element of a set A with high multiplicity, then we can give an upper bound on $|A|$ based on the degree of the polynomial. It turns out that the most challenging part of our proofs is to show that the auxiliary polynomial constructed is *not identically zero*.

To check that each root has a high multiplicity, standard derivatives might not work since we are working in a field with characteristic p. To resolve this issue, we need the following notation of derivatives, known as the *Hasse derivatives* or *hyper-derivatives*; see [26, Section 6.4].

***Definition* 2.1** Let $c_0, c_1, \ldots c_d \in \mathbb{F}_q$. If n is a non-negative integer, then the *n-th hyper-derivative* of $f(x) = \sum_{j=0}^{d} c_j x^j$ is

$$E^{(n)}(f) = \sum_{j=0}^{d} \binom{j}{n} c_j x^{j-n},$$

where we follow the standard convention that $\binom{j}{n} = 0$ for $j < n$, so that the n-th hyper-derivative is a polynomial.

Following the definition, we have $E^{(0)} f = f$. We also need the next three lemmas.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

***Lemma* 2.2** *([26, Lemma 6.47])* *If $f, g \in \mathbb{F}_q[x]$, then*

$$E^{(n)}(fg) = \sum_{k=0}^{n} E^{(k)}(f)E^{(n-k)}(g).$$

***Lemma* 2.3** *([26, Corollary 6.48])* *Let n, d be positive integers. If $a \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$, then we have*

$$E^{(n)}\left((ax+c)^d\right) = a^n \binom{d}{n} (ax+c)^{d-n}. \tag{2.1}$$

***Lemma* 2.4** *([26, Lemma 6.51])* *Let f be a non-zero polynomial in $\mathbb{F}_q[x]$. If c is a root of $E^{(k)}(f)$ for $k = 0, 1, \ldots, m-1$, then c is a root of multiplicity at least m.*

2.2 Gallagher's larger sieve inequality

In this subsection, we introduce Gallagher's larger sieve inequality and provide necessary estimations from it. Gallagher's larger sieve inequality will be one of the main ingredients for the proof of Theorem 1.2. In 1971, Gallagher [15] discovered the following sieve inequality.

***Theorem* 2.5** (Gallagher's larger sieve inequality) *Let N be a natural number and $A \subset \{1, 2, \ldots, N\}$. Let $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $A_p = A \pmod p$. For any $1 < Q \leq N$, we have*

$$|A| \leq \frac{\sum\limits_{p \leq Q, p \in \mathcal{P}} \log p - \log N}{\sum\limits_{p \leq Q, p \in \mathcal{P}} \frac{\log p}{|A_p|} - \log N}, \tag{2.2}$$

provided that the denominator is positive.

As a preparation to apply Gallagher's larger sieve in our proof, we need to establish a few estimates related to primes in arithmetic progressions. For $(a, k) = 1$, we follow the standard notation

$$\theta(x; k, a) = \sum_{\substack{p \leq x \\ p \equiv a \bmod k}} \log p.$$

For our purposes, $\log k$ could be as large as $\sqrt{\log\log x}$ (for example, see Theorem 1.2), and we need the Siegel-Walfisz theorem to estimate $\theta(x; k, a)$.

***Lemma* 2.6** *([28, Corollary 11.21])* *Let $A > 0$ be a constant. There is a constant $c_1 > 0$ such that*

$$\theta(Q; k, a) = \frac{Q}{\phi(k)} + O_A\left(Q \exp(-c_1\sqrt{\log Q})\right)$$

holds uniformly for $k \leq (\log Q)^A$ and $(a, k) = 1$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

A standard application of partial summation with Lemma 2.6 leads to the following corollary.

***Corollary* 2.7** *There is a constant $c > 0$, such that*

$$\sum_{\substack{p \le Q \\ p \equiv a \bmod k}} \frac{\log p}{\sqrt{p}} = \frac{2\sqrt{Q}}{\phi(k)} + O\left(\sqrt{Q}\exp(-c\sqrt{\log Q})\right)$$

holds uniformly for $k \le \log Q$ and $(a, k) = 1$.

We also need the following lemma.

***Lemma* 2.8** *([1, page 72]) Let n be a positive integer. Then*

$$\sum_{p \mid n} \frac{\log p}{\sqrt{p}} \ll (\log n)^{1/2}.$$

2.3 An effective estimate for $M_k(n, \frac{k}{k-2})$

Following [7], for each real number $L > 0$, we write

$$M_k(n; L) := \sup\{|S \cap [n^L, \infty)| : S \text{ satisfies property } D_k(n)\}.$$

It is shown in [7] that $M_k(n, 3) \ll_k 1$ as $n \to \infty$. For our application, we show a stronger result that $M_k(n, \frac{k}{k-2}) \ll_k 1$ and we will make this estimate explicit and effective. We follow the proof in [7] closely and prove the following proposition, which will be used later in the proof of Theorem 1.2.

***Proposition* 2.9** *If $k \ge 3$ and $n > (2ke)^{k^2}$, then $M_k(n, \frac{k}{k-2}) \ll \log k \log\log k$, where the implicit constant is absolute.*

Let $k \ge 3$. Let $m = M_k(n, \frac{k}{k-2})$ and $A = \{a_1, a_2, \dots, a_m\}$ be a generalized m-tuple with property $D_k(n)$ and $n^{\frac{k}{k-2}} < a_1 < a_2 < \cdots < a_m$. Consider the system of equations

$$\begin{cases} a_1 x + n = u^k \\ a_2 x + n = v^k. \end{cases} \tag{2.3}$$

Clearly, for each $i \ge 3$, $x = a_i$ is a solution to this system, and we denote u_i, v_i so that $a_1 a_i + n = u_i^k$ and $a_2 a_i + n = v_i^k$. Let $\alpha := (a_1/a_2)^{1/k}$.

The following lemma is a generalization of [7, Lemma 3.1], showing that u_i/v_i provides a "good" rational approximation to α if n is large. Note that in [7, Lemma 3.1], it was further assumed that k is odd and $L = 3$. Nevertheless, an almost identical proof works, and we skip the proof.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

***Lemma* 2.10** *Let*

$$c(k) := \prod_{j=1}^{\lfloor (k-1)/2 \rfloor} \left(\sin \frac{2\pi j}{k}\right)^2.$$

Assume that $n > (2/c(k))^{(k-2)/2}$. *Then for each* $3 \le i \le m$, *we have*

$$\left|\frac{u_i}{v_i} - \alpha\right| \le \frac{a_2}{2v_i^k}. \tag{2.4}$$

***Corollary* 2.11** *Assume that* $n > (2/c(k))^{(k-2)/2}$. *Then* $v_i \ge a_2^4$ *for each* $14 \le i \le m$ *and*

$$\left|\frac{u_i}{v_i} - \alpha\right| < \frac{1}{v_i^{k-1/2}}. \tag{2.5}$$

Proof Let $2 \le i \le m-3$. Applying the gap principle from [7, Lemma 2.4] to $a_i, a_{i+1}, a_{i+2}, a_{i+3}$, we have

$$a_{i+1}a_{i+3} \ge k^k n^{-k} (a_i a_{i+2})^{k-1} \ge k^k n^{-k} (a_i a_{i+1})^{k-1}.$$

It follows that

$$a_{i+3} \ge a_i^{k-1} a_{i+1}^{k-2} n^{-k} \ge a_i^{k-1}.$$

In particular $a_{14} \ge a_2^{(k-1)^4} \ge a_2^{4k}$. Thus, if $i \ge 14$, then $v_i \ge a_i^{1/k} \ge a_{14}^{1/k} \ge a_2^4$ and inequality (2.5) follows from Lemma 2.10. ∎

Now we are ready to prove Proposition 2.9. Recall we have the inequality $\sin x \ge \frac{2x}{\pi}$ for $x \in [0, \frac{\pi}{2}]$, and the inequality $s! \ge (s/e)^s$ for all positive integers s. It follows that

$$\sqrt{c(k)} = \prod_{j=1}^{(k-1)/2} \sin \frac{2\pi j}{k} = \prod_{j=1}^{(k-1)/2} \sin \frac{\pi j}{k} \ge \prod_{j=1}^{(k-1)/2} \frac{2j}{k} = \frac{((k-1)/2)!}{(k/2)^{(k-1)/2}} \ge \left(\frac{k-1}{ke}\right)^{(k-1)/2}$$

when k is odd, and

$$(c(k))^{1/4} = \sqrt{\prod_{j=1}^{(k-2)/2} \sin \frac{2\pi j}{k}} = \prod_{j=1}^{\lfloor k/4 \rfloor} \sin \frac{\pi j}{k/2} \ge \prod_{j=1}^{\lfloor k/4 \rfloor} \frac{4j}{k} = \frac{(\lfloor k/4 \rfloor)!}{(k/4)^{\lfloor k/4 \rfloor}} \ge \left(\frac{4\lfloor k/4 \rfloor}{ke}\right)^{\lfloor k/4 \rfloor}$$

when k is even. Thus, when $k \ge 3$, we always have

$$\frac{2}{c(k)} \le 2\left(\frac{ke}{k-2}\right)^k \le 2(ke)^k.$$

Therefore, when $n > (2ke)^{k^2}$, we can apply Lemma 2.10. Note that the absolute height of α is $H(\alpha) \le a_2^{1/k}$. Since $k \ge 3$, for $14 \le i \le m$, Lemma 2.10 implies that

$$\left|\frac{u_i}{v_i} - \alpha\right| \le \frac{1}{v_i^{k-1/2}} \le \frac{1}{v_i^{2.5}};$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

moreover, $\max(u_i, v_i) = v_i > a_2^{1/k} \geq \max(H(\alpha), 2)$. Therefore, we can apply the quantitative Roth's theorem due to Evertse [12] (see also [7, Theorem 2.2]) to conclude that

$$m \leq 13 + 2^{28} \log(2k) \log(2 \log 2k) \ll \log k \log \log k,$$

where the implicit constant is absolute.

2.4 Implications of the Paley graph conjecture

The Paley graph conjecture on double character sums implies many results of the present paper related to the estimation of character sums. We record the statement of the conjecture (see for example [7, 16]).

***Conjecture* 2.12 (*Paley graph conjecture*)** *Let $\epsilon > 0$ be a real number. Then there is $p_0 = p_0(\epsilon)$ and $\delta = \delta(\epsilon) > 0$ such that for any prime $p > p_0$, any $A, B \subseteq \mathbb{F}_p$ with $|A|, |B| > p^{\epsilon}$, and any non-trivial multiplicative character χ of $\mathbb{F}_p$, the following inequality holds:*

$$\left| \sum_{a \in A,\, b \in B} \chi(a+b) \right| \leq p^{-\delta} |A||B|.$$

The connection between the Paley graph conjecture and the problem of bounding the size of Diophantine tuples was first observed by Güloğlu and Murty in [16]. Let $d \geq 2$ be fixed, $\lambda \in \mathbb{F}_p^*$, where $p \equiv 1 \pmod{d}$ is a prime. The Paley graph conjecture trivially implies $MD_d(\lambda, \mathbb{F}_p) = p^{o(1)}$ and $MSD_d(\lambda, \mathbb{F}_p) = p^{o(1)}$ as $p \to \infty$. Also, the bound on $M_k(n)$ in Theorem 1.2 can be improved to $(\log n)^{o(1)}$ (see [7], [16]) when k is fixed and $n \to \infty$. Furthermore, the Paley graph conjecture also immediately implies Sárközy's conjecture (Conjecture 1.8) in view of Proposition 3.4. However, the Paley graph conjecture itself remains widely open, and our results are unconditional. We refer to [32] and the references therein for recent progress on the Paley graph conjecture assuming A, B have small doubling.

3 Preliminary estimations for product sets in shifted multiplicative subgroups

3.1 Character sum estimate and the square root upper bound

The purpose of this subsection is to prove Proposition 1.4 by establishing an upper bound on the double character sum in Proposition 3.1 using basic properties of characters and Gauss sums. For any prime p, and any $x \in \mathbb{F}_p$, we follow the standard notation that $e_p(x) = \exp(2\pi i x/p)$, where we embed $\mathbb{F}_p$ into $\mathbb{Z}$. We refer the reader to [26, Chapter 5] for more results related to Gauss sums and character sums.

We refer to [1, Section 2] for a historical discussion of Vinogradov's inequality (1.1). Gyarmati [17, Theorem 7] and Becker and Murty [1, Proposition 2.7] independently showed that the Legendre symbol in inequality (1.1) can be replaced with any non-trivial Dirichlet character modulo p. For our purposes, we extend Vinogradov's inequality (1.1) to all finite fields $\mathbb{F}_q$ and all nontrivial multiplicative characters χ of $\mathbb{F}_q$, with a slightly improved upper bound.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

***Proposition* 3.1** *Let χ be a non-trivial multiplicative character of $\mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^*$. For any $A, B \subset \mathbb{F}_q^*$, we have*

$$\left| \sum_{a\in A,\, b\in B} \chi(ab+\lambda) \right| \le \sqrt{q|A||B|}\left(1 - \frac{\max\{|A|,|B|\}}{q}\right)^{1/2}.$$

Before proving Proposition 3.1, we need some preliminary estimates. Let χ be a multiplicative character of $\mathbb{F}_q$; then the Gauss sum associated to χ is defined to be

$$G(\chi) = \sum_{c\in\mathbb{F}_q} \chi(c) e_p\big(\mathrm{Tr}_{\mathbb{F}_q}(c)\big),$$

where $\mathrm{Tr}_{\mathbb{F}_q} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace map.

***Lemma* 3.2** *([26, Theorem 5.12]) Let χ be a multiplicative character of $\mathbb{F}_q$. Then for any $a \in \mathbb{F}_q$,*

$$\overline{\chi(a)} = \frac{1}{G(\chi)} \sum_{c\in\mathbb{F}_q} \chi(c) e_p\big(\mathrm{Tr}_{\mathbb{F}_q}(ac)\big).$$

Now we are ready to prove Proposition 3.1.

Proof By Lemma 3.2, we can write

$$\begin{aligned}\sum_{a\in A,\, b\in B} \overline{\chi(ab+\lambda)} &= \sum_{a\in A,\, b\in B} \overline{\chi(b)}\overline{\chi(a+\lambda b^{-1})} \\ &= \frac{1}{G(\chi)} \sum_{c\in\mathbb{F}_q} \chi(c) \sum_{a\in A,\, b\in B} \overline{\chi(b)} e_p\big(\mathrm{Tr}((a+\lambda b^{-1})c)\big).\end{aligned}$$

It is well-known that $|G(\chi)| = \sqrt{q}$ (see for example [26, Theorem 5.11]). Since $|\chi(c)| = 1$ for each $c \in \mathbb{F}_q^*$, we can apply the triangle inequality and Cauchy-Schwarz inequality to obtain

$$\begin{aligned}\left| \sum_{a\in A,\, b\in B} \chi(ab+\lambda) \right| &\le \frac{1}{\sqrt{q}} \sum_{c\in\mathbb{F}_q^*} \left| \sum_{a\in A,\, b\in B} \overline{\chi(b)} e_p\big(\mathrm{Tr}((a+\lambda b^{-1})c)\big) \right| \\ &\le \frac{1}{\sqrt{q}} \left(\sum_{c\in\mathbb{F}_q^*} \left| \sum_{a\in A} e_p\big(\mathrm{Tr}(ac)\big) \right|^2 \right)^{1/2} \left(\sum_{c\in\mathbb{F}_q^*} \left| \sum_{b\in B} \overline{\chi(b)} e_p\big(\mathrm{Tr}(b^{-1}c)\big) \right|^2 \right)^{1/2}.\end{aligned}$$

By orthogonality relations, we have

$$\sum_{c\in\mathbb{F}_q^*} \left| \sum_{a\in A} e_p\big(\mathrm{Tr}(ac)\big) \right|^2 = q|A| - |A|^2, \quad \sum_{c\in\mathbb{F}_q^*} \left| \sum_{b\in B} \overline{\chi(b)} e_p\big(\mathrm{Tr}(b^{-1}c)\big) \right|^2 \le q|B|.$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Thus, we have

$$\left|\sum_{a\in A,\, b\in B}\chi(ab+\lambda)\right| \le \sqrt{q|A||B|}\left(1-\frac{|A|}{q}\right)^{1/2}.$$

By switching the roles of A and B, we obtain the required character sum estimate. ∎

Let $d \mid (q-1)$ such that $d \ge 2$ and denote $S_d = \{x^d : x \in \mathbb{F}_q^*\}$ with order $\frac{q-1}{d}$. Then we prove Proposition 1.4.

Proof Let χ be a multiplicative character of order d.

Let $A \subset \mathbb{F}_q^*$ with property $SD_d(\lambda, \mathbb{F}_q)$, that is, $AA + \lambda \subset S_d \cup \{0\}$. Note that $\chi(ab+\lambda) = 1$ for each $a, b \in A$, unless $ab + \lambda = 0$. Note that given $a \in A$, there is at most one $b \in A$ such that $ab + \lambda = 0$. Therefore, by Proposition 3.1, we have

$$|A|^2 - |A| \le \left|\sum_{a,b\in A}\chi(ab+\lambda)\right| \le \sqrt{q}|A|\left(1-\frac{|A|}{q}\right)^{1/2}.$$

It follows that

$$(|A|-1)^2 \le q - |A| \implies |A| \le \frac{\sqrt{4q-3}+1}{2}.$$

Next we work under the weaker assumption $A\hat{\times}A + \lambda \subset S_d \cup \{0\}$. In this case, note that $\chi(ab+\lambda) = 1$ for each $a, b \in A$ such that $a \ne b$, unless $ab+\lambda = 0$. Proposition 3.1 then implies that

$$|A|^2 - 3|A| \le \left|\sum_{a,b\in A}\chi(ab+\lambda)\right| \le \sqrt{q}|A|\left(1-\frac{|A|}{q}\right)^{1/2}$$

and it follows that $|A| \le \sqrt{q-\frac{11}{4}} + \frac{5}{2}$. ∎

3.2 Estimates on $|A|$ and $|B|$ if $AB = (S_d - \lambda)\setminus\{0\}$

Let $A, B \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$. In this subsection, we provide several useful estimates on $|A|$ and $|B|$ when $AB = (S_d - \lambda)\setminus\{0\}$, which will be used in Section 6.

We need to use the following lemma, due to Karatsuba [23].

***Lemma* 3.3** *Let $A, B \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$. Then for any non-trivial multiplicative character χ of $\mathbb{F}_q$ and any positive integer ν, we have*

$$\sum_{\substack{a\in A\\ b\in B}}\chi(ab+\lambda) \ll_\nu |A|^{(2\nu-1)/2\nu}(|B|^{1/2}q^{1/2\nu} + |B|q^{1/4\nu}).$$

The following proposition improves and generalizes [31, Theorem 1]. It also improves [33, Lemma 17] (see Remark 3.7).

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

***Proposition* 3.4** *Let $\epsilon > 0$. Let $d \mid (q-1)$ such that $2 \le d \le q^{1/2-\epsilon}$ and $\lambda \in \mathbb{F}_q^*$. If $AB = (S_d - \lambda) \setminus \{0\}$ for some $A, B \subset \mathbb{F}_q^*$ with $|A|, |B| \ge 2$, then*

$$\frac{\sqrt{q}}{d} \ll \min\{|A|, |B|\} \le \max\{|A|, |B|\} \ll q^{1/2}.$$

Proof Let $A, B \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$ such that $AB = (S_d - \lambda) \setminus \{0\}$ with $|A|, |B| \ge 2$. Without loss of generality, we assume that $|A| \ge |B|$. We first establish a weaker lower bound that $|B| \gg q^{\epsilon/2}$.

When $d = 2$, Sárközy [31] has shown that $|B| \gg \frac{\sqrt{q}}{3 \log q}$. While he only proved this estimate when $q = p$ is a prime [31, Theorem 1], it is clear that the same proof extends to all finite fields $\mathbb{F}_q$.

Next, assume that $d \ge 3$. Let $B = \{b_1, b_2, \dots, b_k\}$ and $|B| = k$. Since $AB \subset S_d - \lambda$, we have $AB + \lambda \subset S_d$. Let χ be a multiplicative character of $\mathbb{F}_q$ with order d. Then it follows that for each $a \in A$, we have $\chi(a + \lambda b_i^{-1}) = 1/\chi(b_i)$ for each $1 \le i \le k$. Therefore, by a well-known consequence of Weil's bound (see for example [26, Exercise 5.66]),

$$|A| \le \frac{q}{d^k} + \left(k - 1 - \frac{k}{d} + \frac{1}{d^k}\right)\sqrt{q} + \frac{k}{d} < \frac{q}{d^k} + k\sqrt{q}.$$

On the other hand, since $AB = (S_d - \lambda) \setminus \{0\}$, we have

$$|A||B| \ge |AB| \ge |S_d| - 1 = \frac{q-1}{d} - 1.$$

Combining the above two inequalities, we obtain that

$$\frac{2q}{d^2} + k^2\sqrt{q} \ge \frac{kq}{d^k} + k^2\sqrt{q} > |A||B| \ge \frac{q-1}{d} - 1.$$

Since $d \ge 3$, it follows that $k^2\sqrt{q} \gg \frac{q}{d}$ and thus

$$|B| = k \gg \frac{q^{1/4}}{\sqrt{d}} \gg q^{\epsilon/2}.$$

Let $\nu = \lceil 2/\epsilon \rceil$. By Lemma 3.3, and as $|B| \gg q^{1/\nu}$, we have

$$|A||B| = \sum_{\substack{a \in A \\ b \in B}} \chi(ab+\lambda) \ll |A|^{(2\nu-1)/2\nu}(|B|^{1/2}q^{1/2\nu} + |B|q^{1/4\nu}) \ll |A|^{(2\nu-1)/2\nu}|B|q^{1/4\nu}.$$

It follows that $|A| \ll q^{1/2}$. Thus, $|B| \gg |S_d|/|A| \gg q^{1/2}/d$. ∎

Remark 3.5 We remark that the same method could be used to refine a similar result for the additive decomposition of multiplicative subgroups, which improves a result of Shparlinski [34, Theorem 6.1] (moreover, our proof appears to be much simpler than his proof). More precisely, we can prove the following:

Let $\epsilon > 0$. Let $d \mid (q-1)$ such that $2 \le d \le q^{1/2-\epsilon}$. If $A + B = S_d$ for some $A, B \subset \mathbb{F}_q$ with $|A|, |B| \ge 2$, then

$$\frac{\sqrt{q}}{d} \ll \min\{|A|, |B|\} \le \max\{|A|, |B|\} \ll q^{1/2}.$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Note that Proposition 3.4 only applies to multiplicative subgroups $G = S_d$ with $|G| > \sqrt{q}$. When $q = p$ is a prime, and G is a non-trivial multiplicative subgroup of $\mathbb{F}_p$ (in particular, $|G| < \sqrt{p}$ is allowed), we have the following estimate, due to Shkredov [33].

Lemma 3.6 *If G is a proper multiplicative subgroup of $\mathbb{F}_p$ such that $AB = (G - \lambda) \setminus \{0\}$ for some $A, B \subset \mathbb{F}_p^*$ with $|A|, |B| \geq 2$ and some $\lambda \in \mathbb{F}_p^*$, then*

$$|G|^{1/2+o(1)} = \min\{|A|, |B|\} \leq \max\{|A|, |B|\} = |G|^{1/2+o(1)}$$

as $|G| \to \infty$.

Proof If $0 \in G-\lambda$, let $A' = A \cup \{0\}$; otherwise, let $A' = A$. Then we have $A'B = G-\lambda$, or equivalently, $A'/(B^{-1}) = G-\lambda$. Note that $|A' \setminus \{0\}| = |A| \geq 2$ and $|B^{-1}| = |B| \geq 2$, thus, the lemma then follows immediately from [33, Lemma 17]. ∎

Remark 3.7 Let $AB = (S_d - \lambda) \setminus \{0\}$, where $A, B \subset \mathbb{F}_p^*$ with $|A|, |B| \geq 2$ and $\lambda \in \mathbb{F}_p^*$. When d is a constant, and $p \to \infty$, Proposition 3.4 is better than Lemma 3.6. Indeed, in [33, Lemma 17], Shkredov showed that $\max\{|A|, |B|\} \ll \sqrt{p} \log p$, while Proposition 3.4 showed the stronger result that $\max\{|A|, |B|\} \ll \sqrt{p}$, removing the $\log p$ factor. This stronger bound would be crucial in proving results related to multiplicative decompositions (for example, Theorem 6.1). Instead, Lemma 3.6 will be useful for applications in ternary decompositions (Theorem 6.6).

Remark 3.8 Lemma 3.6 fails to extend to $\mathbb{F}_q$, where q is a proper prime power. Let $q = r^2$ be a square, $G = \mathbb{F}_r^*$, and $\lambda = -1$. Let A be a subset of $\mathbb{F}_r^*$ with size $\lfloor (r-1)/2 \rfloor$. Let $B = \mathbb{F}_r^* \setminus A^{-1}$. Then we have $AB = \mathbb{F}_r^* \setminus \{1\} = (G+1) \setminus \{0\}$ while $|A|, |B| \gg |G|$.

Remark 3.9 Let $d \geq 2$ be fixed. Let $q \equiv 1 \pmod{d}$ be a prime power and let $\lambda \in \mathbb{F}_q^*$, we define $N(q, \lambda)$ be the total number of pairs (A, B) of sets $A, B \subseteq \mathbb{F}_q$ with $|A|, |B| \geq 2$ such that $AB = (S_d - \lambda) \setminus \{0\}$. Note that Conjecture 1.9 implies $N(q, \lambda) = 0$ when q is sufficiently large, but it seems out of reach in general. Instead, one can find a non-trivial upper bound of $N(q, \lambda)$. Using Proposition 3.4 and following the same strategy of the proof in [3, Theorem 1], we have a non-trivial upper bound of $N(q, \lambda)$ as follows:

$$N(q, \lambda) \leq \exp\left(O(q^{1/2})\right).$$

We also note that by using Corollary 1.10, we confirmed $N(q, \lambda) = 0$ if q is a prime, $\lambda \in S_d$, and $|S_d| - 1$ is a prime. In addition, Theorem 1.11 gives the same result for $N(p, n)$ asymptotically for a subset of primes p with lower density at least $\frac{1}{[\mathbb{Q}(e^{2\pi i/d}, n^{1/d}):\mathbb{Q}]}$.

4 Products and restricted products in shifted multiplicative subgroups

In this section, we use Stepanov's method to study product sets and restricted product sets that are contained in shifted multiplicative subgroups. Our proofs are inspired by

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Stepanov's original paper [35], and the recent breakthrough of Hanson and Pertidis [21], together with its extensions and applications developed by the second author [38, 40].

Throughout the section, we assume $d \geq 2$ and $q \equiv 1 \pmod{d}$ is a prime power. Recall that $S_d = S_d(\mathbb{F}_q) = \{x^d : x \in \mathbb{F}_q^*\}$.

4.1 Product set in a shifted multiplicative subgroup

In this subsection, we prove Theorem 1.1, which can be viewed as the bipartite version of Diophantine tuples over finite fields. As a corollary of Theorem 1.1, we prove Corollary 1.10. Besides it, Theorem 1.1 will be also repeatedly used to prove several of our main results in the present paper.

Proof Let $r = |B \cap (-\lambda A^{-1})|$. Let $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_m\}$ such that $b_{r+1}, \ldots, b_m \notin (-\lambda A^{-1})$. Since $AB + \lambda \subset S_d \cup \{0\}$, we have

$$(a_i b_j + \lambda)^{\frac{q-1}{d}+1} = a_i b_j + \lambda$$

for each $1 \leq i \leq n$ and $1 \leq j \leq m$. This simple observation will be used repeatedly in the following computation.

Let $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$ be the unique solution of the following system of equations:

$$\begin{cases} \sum_{i=1}^n c_i = 1 \\ \sum_{i=1}^n c_i a_i^j = 0, \quad 1 \leq j \leq n-1 \end{cases}. \tag{4.1}$$

This is justified by the invertibility of the coefficient matrix of the system (a Vandermonde matrix). We claim that $\sum_{i=1}^n c_i a_i^n \neq 0$. Suppose otherwise that $\sum_{i=1}^n c_i a_i^n = 0$, then $c_i = 0$ for all i, violating the assumption $\sum_{i=1}^n c_i = 1$ in equation (4.1). Indeed, the generalized Vandermonde matrix $(a_i^j)_{1\leq i\leq n, 1\leq j\leq n}$ is non-singular since it has determinant

$$a_1 a_2 \ldots a_n \prod_{i<j} (a_j - a_i) \neq 0.$$

Consider the following auxiliary polynomial

$$f(x) = -\lambda^{n-1} + \sum_{i=1}^n c_i (a_i x + \lambda)^{n-1+\frac{q-1}{d}} \in \mathbb{F}_q[x]. \tag{4.2}$$

Note that $n = |A| \leq |S_d \cup \{0\}| \leq \frac{q-1}{d} + 1$. Thus, if $q = p$ is a prime, then $n - 1 + \frac{p-1}{d} \leq \frac{2(p-1)}{d} \leq p - 1$ and thus the condition $\binom{n-1+\frac{q-1}{d}}{n} \not\equiv 0 \pmod{p}$ is automatically satisfied. Then f is a non-zero polynomial since the coefficient of x^n in f is

$$\binom{n-1+\frac{q-1}{d}}{n} \cdot \lambda^{\frac{q-1}{d}-1} \cdot \sum_{i=1}^n c_i a_i^n \neq 0$$

by the assumption on the binomial coefficient. Also, it is clear that the degree of f is at most $n - 1 + \frac{q-1}{d}$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Next, we compute the derivatives of f on B. For each $1 \le j \le m$, system (4.1) implies that

$$E^{(0)} f(b_j) = -\lambda^{n-1} + \sum_{i=1}^{n} c_i (a_i b_j + \lambda)^{n-1} = -\lambda^{n-1} + \sum_{\ell=0}^{n-1} \binom{n-1}{\ell} \lambda^{n-1-\ell} \left(\sum_{i=1}^{n} c_i a_i^{\ell} \right) b_j^{\ell} = 0.$$

For each $1 \le j \le m$ and $1 \le k \le n-2$, we have that

$$\begin{aligned} E^{(k)} f(b_j) &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{i=1}^{n} c_i a_i^k (a_i b_j + \lambda)^{n-1+\frac{q-1}{d}-k} \\ &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{i=1}^{n} c_i a_i^k (a_i b_j + \lambda)^{n-1-k} \\ &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{\ell=0}^{n-1-k} \binom{n-1-k}{\ell} \lambda^{n-1-k-\ell} \left(\sum_{i=1}^{n} c_i a_i^{k+\ell} \right) b_j^{\ell} = 0, \end{aligned}$$

where we use Lemma 2.3 and the assumptions in system (4.1).

For each $r+1 \le j \le m$, by the assumption, $b_j \notin (-\lambda A^{-1})$, that is, $a_i b_j + \lambda \ne 0$ for each $1 \le i \le n$. Thus, for each $r+1 \le j \le m$, we additionally have

$$E^{(n-1)} f(b_j) = \binom{n-1+\frac{q-1}{d}}{n-1} \sum_{i=1}^{n} c_i a_i^{n-1} (a_i b_j + \lambda)^{\frac{q-1}{d}} = \binom{n-1+\frac{q-1}{d}}{n-1} \sum_{i=1}^{n} c_i a_i^{n-1} = 0.$$

Therefore, Lemma 2.4 allows us to conclude that each of $b_1, b_2, \dots b_r$ is a root of f with multiplicity at least $n-1$, and each of $b_{r+1}, b_{r+2}, \dots b_m$ is a root of f with multiplicity at least n. It follows that

$$r(n-1) + (m-r)n = mn - r \le \deg f \le \frac{q-1}{d} + n - 1.$$

Finally, assuming that $\lambda \in S_d$. In this case,

$$f(0) = -\lambda^{n-1} + \lambda^{n-1+\frac{q-1}{d}} \sum_{i=1}^{n} c_i = -\lambda^{n-1} + \lambda^{n-1} = 0.$$

And the coefficient of x^j of f is 0 for each $1 \le j \le n-1$ by the assumptions on c_i's. It follows that 0 is also a root of f with multiplicity n. Since $0 \notin B$, we have the stronger estimate that $mn - r + n \le \frac{q-1}{d} + n - 1$. ∎

Remark 4.1 More generally, one can study the same question if $AB + \lambda$ is instead contained in a coset of S_d. However, note that this more general case can be always reduced to the special case studied in Theorem 1.1. Indeed, if $AB + \lambda \subset \xi S_d \cup \{0\}$ with $\xi \in \mathbb{F}_q^*$, then $A'B + \lambda/\xi \subset S_d \cup \{0\}$, where $A' = A/\xi$.

Next, we prove Corollary 1.10, an important corollary of Theorem 1.1. It would be crucial for proving results in Section 6.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Proof Since $0 \notin AB + \lambda$, we have $B \cap (-\lambda A^{-1}) = \emptyset$, thus Theorem 1.1 implies that $|A||B| \leq |S_d| - 1$. On the other hand, since $(S_d - \lambda) \setminus \{0\} = AB$, it follows that $|A||B| \geq |AB| = |(S_d - \lambda) \setminus \{0\}| = |S_d| - 1$. Therefore, we have $|A||B| = |AB| = |S_d| - 1$. ∎

4.2 Restricted product set in a shifted multiplicative subgroup

Recall that $A' \subset \mathbb{F}_q^*$ has property $D_d(\lambda, \mathbb{F}_q)$ if and only if $ab + \lambda \in S_d \cup \{0\}$ for each $a, b \in A'$ such that $a \neq b$. In other words, $A' \hat{\times} A' + \lambda \subset S_d \cup \{0\}$. Thus, in this subsection, we are led to study restricted product sets and we establish the following restricted product analog of Theorem 1.1. In the next subsection, Theorem 1.1 and Theorem 4.2 will be applied together to prove Theorem 1.5 in the case that q is a prime and Theorem 1.6 in the case that q is a square.

***Theorem* 4.2** *Let $d \geq 2$ and let $q \equiv 1 \pmod{d}$ be a prime power. Let $A' \subset \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_q^*$. If $A' \hat{\times} A' + \lambda \subset S_d \cup \{0\}$ while $A'A' + \lambda \not\subset S_d \cup \{0\}$, then $|A'| \leq \sqrt{2(q-1)/d} + 4$.*

The proof of Theorem 4.2 is similar to Theorem 1.1, but it is more delicate. In particular, the choice of the auxiliary polynomial (4.4) needs to be modified from that of the proof (4.2) of Theorem 1.1. In view of Theorem 1.1, we can further assume that $A'A' + \lambda \not\subset S_d \cup \{0\}$, for otherwise we already have a good bound on $|A'|$; we refer to Subsection 4.3 for details. It turns out that this additional assumption (which we get for free) is crucial in our proof since it guarantees that the auxiliary polynomial we constructed is not identically zero.

Proof Since $A'A' + \lambda \not\subset S_d \cup \{0\}$, there is $b \in A'$ such that $b^2 + \lambda \not\subset S_d \cup \{0\}$. Let $A'' = A' \setminus \{-\lambda/b\}$. If $|A''| = 1$, then we are done. Otherwise, if $|A''|$ is even, let $A = A''$; if $|A''|$ is odd, let $A = A'' \setminus \{b'\}$, where $b' \in A''$ is an arbitrary element such that $b' \neq b$. Then we have $b \in A$ and $|A|$ is even. Note that $|A| \geq |A'| - 2$, thus it suffices to show $|A| \leq \sqrt{2(q-1)/d} + 2$.

Let $|A| = n$, where n is even. Write $A = \{a_1, a_2, \ldots, a_n\}$. Without loss of generality, we may assume that $a_1 = b$. Let $m = n/2 - 1$. Let $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$ be the unique solution of the following system of equations:

$$\begin{cases} \sum_{i=1}^n c_i a_i^j = 0, & -m \leq j \leq m \\ \sum_{i=1}^n c_i a_i^{m+1} = 1. \end{cases} \tag{4.3}$$

Indeed, that coefficient matrix of the system is the generalized Vandermonde matrix $(a_i^j)_{1 \leq i \leq n, -m \leq j \leq m+1}$, which is non-singular since it has nonzero determinant $(a_1 a_2 \ldots a_n)^{-m} \prod_{i<j}(a_j - a_i) \neq 0$. Note that $c_1 \neq 0$; for otherwise $c_1 = 0$ and we must have $c_1 = c_2 = \ldots = c_n = 0$ in view of the first $n - 1$ equations in system (4.3), which contradicts the last equation in system (4.3).

Consider the following auxiliary polynomial

$$f(x) = \sum_{i=1}^n c_i (a_i x + \lambda)^{m + \frac{q-1}{d}} (a_i^{-1} x - 1)^m \in \mathbb{F}_q[x]. \tag{4.4}$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

It is clear that the degree of f is at most $2m + \frac{q-1}{d}$. Since $A\hat{\times}A + \lambda \subset S_d \cup \{0\}$, we have

$$(a_i a_j + \lambda)^{\frac{q-1}{d}+1}(a_i^{-1}a_j - 1) = (a_i a_j + \lambda)(a_i^{-1}a_j - 1)$$

for each $1 \le i, j \le n$. This simple observation will be used repeatedly in the following computation.

First, we claim that for each $0 \le k_1 < m$, $0 \le k_2 < m$, and $1 \le j \le n$, we have

$$\sum_{i=1}^{n} c_i E^{(k_1)}[(a_i x + \lambda)^{m+\frac{q-1}{d}}](a_j) \cdot E^{(k_2)}[(a_i^{-1}x - 1)^m](a_j) = 0. \tag{4.5}$$

Indeed, by Lemma 2.3, we have

$$\begin{aligned}
&\sum_{i=1}^{n} c_i E^{(k_1)}[(a_i x + \lambda)^{m+\frac{q-1}{d}}](a_j) \cdot E^{(k_2)}[(a_i^{-1}x - 1)^m](a_j) \\
&= \binom{m+\frac{q-1}{d}}{k_1}\binom{m}{k_2}\left(\sum_{i=1}^{n} c_i a_i^{k_1-k_2}(a_j a_i + \lambda)^{m-k_1}(a_i^{-1}a_j - 1)^{m-k_2}\right) \\
&= \binom{m+\frac{q-1}{d}}{k_1}\binom{m}{k_2}\sum_{\ell_1=0}^{m-k_1}\sum_{\ell_2=0}^{m-k_2}\binom{m-k_1}{\ell_1}\binom{m-k_2}{\ell_2}\left(\sum_{i=1}^{n} c_i a_i^{k_1-k_2}(a_j a_i)^{\ell_1}\lambda^{m-k_1-\ell_1}(a_i^{-1}a_j)^{\ell_2}(-1)^{m-k_2-\ell_2}\right) \\
&= \binom{m+\frac{q-1}{d}}{k_1}\binom{m}{k_2}\sum_{\ell_1=0}^{m-k_1}\sum_{\ell_2=0}^{m-k_2}\binom{m-k_1}{\ell_1}\binom{m-k_2}{\ell_2}a_j^{\ell_1+\ell_2}\lambda^{m-k_1-\ell_1}(-1)^{m-k_2-\ell_2}\left(\sum_{i=1}^{n} c_i a_i^{(k_1+\ell_1)-(k_2+\ell_2)}\right).
\end{aligned}$$

Note that in the exponent of the last summand, we always have $0 \le k_1 + \ell_1 \le m$ and $0 \le k_2 + \ell_2 \le m$ so that $-m \le (k_1 + \ell_1) - (k_2 + \ell_2) \le m$, and thus

$$\sum_{i=1}^{n} c_i a_i^{(k_1+\ell_1)-(k_2+\ell_2)} = 0$$

by the assumptions in system (4.3). This proves the claim.

Then, for each $1 \le j \le n$ and $0 \le r \le m-1$, we apply Lemma 2.2 and equation (4.5) in the above claim to obtain that

$$E^{(r)}f(a_j) = \sum_{i=1}^{n} c_i\left(\sum_{k=0}^{r} E^{(k)}[(a_i x + \lambda)^{m+\frac{q-1}{d}}](a_j) \cdot E^{(r-k)}[(a_i^{-1}x - 1)^m](a_j)\right) = 0.$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Similarly, using Lemma 2.2, Lemma 2.3, system (4.3), and equation (4.5), we can compute

$$\begin{aligned}
E^{(m)}f(a_1) &= \sum_{i=1}^{n} c_i \left(\sum_{k=0}^{m} E^{(k)}[(a_i x+\lambda)^{m+\frac{q-1}{d}}](a_1) \cdot E^{(m-k)}[(a_i^{-1}x-1)^m](a_1) \right) \\
&= \sum_{i=1}^{n} c_i \left(E^{(0)}[(a_i x+\lambda)^{m+\frac{q-1}{d}}](a_1) \cdot E^{(m)}[(a_i^{-1}x-1)^m](a_1) \right) \\
&\quad + \sum_{i=1}^{n} c_i \left(E^{(m)}[(a_i x+\lambda)^{m+\frac{q-1}{d}}](a_1) \cdot E^{(0)}[(a_i^{-1}x-1)^m](a_1) \right) \\
&= \sum_{i=1}^{n} c_i (a_1 a_i+\lambda)^{m+\frac{q-1}{d}} a_i^{-m} + \binom{m+\frac{q-1}{d}}{m} \left(\sum_{i=1}^{n} c_i a_i^m (a_1 a_i+\lambda)^{\frac{q-1}{d}} (a_i^{-1}a_1-1)^m \right).
\end{aligned}$$

Since $a_1 a_i + \lambda \neq 0$ for each $1 \leq i \leq n$, we have $(a_1 a_i+\lambda)^{\frac{q-1}{d}} = 1$ for $i > 1$, and thus

$$(a_1 a_i+\lambda)^{\frac{q-1}{d}}(a_i^{-1}a_1-1) = a_i^{-1}a_1 - 1$$

for all i. Since $a_1^2 + \lambda \notin S_d \cup \{0\}$, we have

$$(a_1^2+\lambda)^m \left((a_1^2+\lambda)^{\frac{q-1}{d}} - 1 \right) \neq 0.$$

Putting these altogether into the computation of $E^{(m)}f(a_1)$, we have

$$\begin{aligned}
E^{(m)}f(a_1) &= \sum_{i=1}^{n} c_i (a_1 a_i+\lambda)^{m+\frac{q-1}{d}} a_i^{-m} + \binom{m+\frac{q-1}{d}}{m} \sum_{i=1}^{n} c_i a_i^m (a_i^{-1}a_1-1)^m \\
&= c_1 a_1^{-m} \left((a_1^2+\lambda)^{m+\frac{q-1}{d}} - (a_1^2+\lambda)^m \right) + \sum_{i=1}^{n} c_i (a_1 a_i+\lambda)^m a_i^{-m} \\
&\quad + \binom{m+\frac{q-1}{d}}{m} \sum_{k=0}^{m} \binom{m}{k} a_1^{m-k} (-1)^k \left(\sum_{i=1}^{n} c_i a_i^k \right) \\
&= c_1 a_1^{-m} (a_1^2+\lambda)^m \left((a_1^2+\lambda)^{\frac{q-1}{d}} - 1 \right) + \sum_{k=0}^{m} \binom{m}{k} a_1^k \lambda^{m-k} \left(\sum_{i=1}^{n} c_i a_i^{k-m} \right) \\
&= c_1 a_1^{-m} (a_1^2+\lambda)^m \left((a_1^2+\lambda)^{\frac{q-1}{d}} - 1 \right) \neq 0,
\end{aligned}$$

where we used the fact $c_1 \neq 0$. In particular, f is not identically zero.

In conclusion, f is a non-zero polynomial with degree at most $\frac{q-1}{d} + 2m$, and Lemma 2.4 implies that each of $a_1, a_2, \ldots a_n$ is a root of f with multiplicity at least m. Recall that $m = n/2 - 1$. It follows that

$$\frac{n(n-2)}{2} = mn \leq \deg f \leq \frac{q-1}{d} + 2m = \frac{q-1}{d} + n - 2,$$

that is, we have $(n-2)^2 \leq \frac{2(q-1)}{d}$. Therefore, $n \leq \sqrt{2(q-1)/d} + 2$. This finishes the proof. ∎

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

4.3 Applications to generalized Diophantine tuples over finite fields

In this subsection, we illustrate how to apply Theorem 1.1 and Theorem 4.2 for obtaining improved upper bounds on the size of a generalized Diophantine tuple or a strong generalized Diophantine tuple over $\mathbb{F}_q$, when $q = p$ is a prime and q is a square.

Proof (1) Let $A \subset \mathbb{F}_p^*$ with property $SD_d(\lambda, \mathbb{F}_p)$, that is, $AA + \lambda \subset S_d \cup \{0\}$. Theorem 1.1 implies that

$$|A|^2 \le |S_d| + |A \cap (-\lambda A^{-1})| + |A| - 1 \le |S_d| + 2|A| - 1.$$

It follows that $(|A| - 1)^2 \le |S_d|$. If $\lambda \in S_d$, we have a stronger upper bound:

$$|A|^2 \le |S_d| + |A \cap (-\lambda A^{-1})| - 1 \le |S_d| + |A| - 1.$$

It follows that $(|A| - \frac{1}{2})^2 \le |S_d| - \frac{3}{4}$.

(2) Let $A \subset \mathbb{F}_p^*$ with property $D_d(\lambda, \mathbb{F}_p)$, that is, $A\hat{\times}A + \lambda \subset S_d \cup \{0\}$. If $AA + \lambda \subset S_d \cup \{0\}$, then (1) implies that $|A| \le \sqrt{p/d} + 1$ and we are done. If $AA + \lambda \not\subset S_d \cup \{0\}$, then Theorem 4.2 implies the required upper bound. ∎

Remark 4.3 Theorem 1.1 can be used to deduce a weaker upper bound of the form $2\sqrt{p/d} + O(1)$ for Theorem 1.5 (2). Let $A \subset \mathbb{F}_p^*$ such that $A\hat{\times}A + \lambda \subset S_d \cup \{0\}$. We can write $A = B \sqcup C$ such that $|B|$ and $|C|$ differ by at most 1. Note that since B and C are disjoint, we have $BC + \lambda \subset A\hat{\times}A + \lambda \subset S_d \cup \{0\}$ and thus Theorem 1.1 implies that $|B||C| \le p/d + |B| + |C|$, which further implies that $|A| \le 2\sqrt{p/d} + O(1)$. Note that such a weaker upper bound is worse than the trivial upper bound from character sums (Proposition 1.4) when $d = 2, 3$, and this is one of our main motivations for establishing the bound $\sqrt{2p/d} + O(1)$ in Theorem 1.5 (2).

Next, we consider the case q is a square. First we establish a non-trivial upper bound on $MSD_d(\lambda, \mathbb{F}_q)$ and $MD_d(\lambda, \mathbb{F}_q)$ under some minor assumption. While these new bounds only improve the trivial upper bound from character sums (Proposition 1.4) slightly, we will see these new bounds are sometimes sharp in the proof of Theorem 1.6. To achieve our goal, we need the following special case of Kummer's theorem [25].

***Lemma* 4.4** *Let p be a prime and m, n be positive integers. If there is no carry between the addition of m and n in base-p, then $\binom{m+n}{n}$ is not divisible by p.*

***Theorem* 4.5** *Let q be a prime power and a square, and let $\lambda \in \mathbb{F}_q^*$.*

(1) *Let $d \ge 2$ be a divisor of $(q-1)$. Let r be the remainder of $\frac{q-1}{d}$ divided by $p\sqrt{q}$. If $r \le (p-1)\sqrt{q}$, then $MSD_d(\lambda, \mathbb{F}_q) \le \sqrt{q} - 1$.*
(2) *Let $q \ge 25$ and let $d \ge 3$ be a divisor of $(q-1)$. Let r be the remainder of $\frac{q-1}{d}$ divided by $p\sqrt{q}$. If $r \le (p-1)\sqrt{q}$, then $MD_d(\lambda, \mathbb{F}_q) \le \sqrt{q} - 1$.*

Proof (1) Since $r \le (p-1)\sqrt{q}$, there is no carry between the addition of $r - 1$ and $\sqrt{q}$ in base-p. Thus, there is no carry between the addition of $\frac{q-1}{d} - 1$ and $\sqrt{q}$ in base-p. It

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

follows from Lemma 4.4 that

$$\binom{\sqrt{q}-1+\frac{q-1}{d}}{\sqrt{q}} \not\equiv 0 \pmod{p}.$$

Let $A \subset \mathbb{F}_q^*$ with property $SD_d(\lambda, \mathbb{F}_q)$ such that $|A| = MSD_d(\lambda, \mathbb{F}_q)$. Note that Proposition 1.4 implies that $|A| \leq \sqrt{q}$. For the sake of contradiction, assume that $|A| = \sqrt{q}$. Note that $AA + \lambda \subset S_d \cup \{0\}$ and

$$\binom{|A|-1+\frac{q-1}{d}}{|A|} = \binom{\sqrt{q}-1+\frac{q-1}{d}}{\sqrt{q}} \not\equiv 0 \pmod{p},$$

it follows from Theorem 1.1 that

$$|A|^2 \leq |S_d| + |A \cap (-\lambda A^{-1})| + |A| - 1 \leq |S_d| + 2|A| - 1,$$

that is, $|A| \leq \sqrt{|S_d|} + 1 < \sqrt{q}$, a contradiction. This completes the proof.

(2) Let $A \subset \mathbb{F}_q^*$ with property $D_d(\lambda, \mathbb{F}_q)$ such that $|A| = MD_d(\lambda, \mathbb{F}_q)$. Then $A\hat{\times}A + \lambda \subset S_d \cup \{0\}$. If $AA+\lambda \subset S_d \cup \{0\}$, we just apply (1). Next assume that $AA+\lambda \not\subset S_d \cup \{0\}$, then Theorem 4.2 implies that

$$|A| \leq \sqrt{\frac{2(q-1)}{d}} + 4 \leq \sqrt{\frac{2(q-1)}{3}} + 4 \leq \sqrt{q} - 1,$$

provided that $q \geq 738$. When $25 \leq q \leq 737$, we have used SageMath to verify the theorem. ∎

Now we are ready to prove Theorem 1.6, which determines the maximum size of an infinitely family of generalized Diophantine tuples and strong generalized Diophantine tuples over finite fields.

Proof In both cases, the upper bound $\sqrt{q} - 1$ follows from Theorem 4.5. To show that $\sqrt{q} - 1$ is a lower bound, we observe that $A = \alpha\mathbb{F}_{\sqrt{q}}^*$ has property $SD_d(\lambda, \mathbb{F}_q)$ (and therefore $D_d(\lambda, \mathbb{F}_q)$). Indeed, $AA + \lambda = \alpha^2\mathbb{F}_{\sqrt{q}}^* + \lambda \subset \alpha^2\mathbb{F}_{\sqrt{q}} \subset S_d \cup \{0\}$ since $\alpha^2 \in S_d$ and $\mathbb{F}_{\sqrt{q}}^* \subset S_d$ (from the assumption $d \mid (\sqrt{q} + 1)$). ∎

Remark 4.6 Our SageMath code indicates that the last statement of Theorem 1.6 does not hold when $d = 2$ and $q = 9, 25, 49$, when $d = 3$ and $q = 4, 16$, and when $d = 4$ and $q = 9$. We conjecture the same statement holds for $d = 2$, provided that q is sufficiently large.

So far we have only considered special cases of applying Theorem 1.1. In general, to apply Theorem 1.1, the assumption on the binomial coefficient in the statement of Theorem 1.1 might be tricky to analyze. However, if the base-p representation of $\frac{q-1}{d}$ behaves "nicely" (for example, if the order of p modulo d is small, then the base-p representation is periodic with a small period), then it is still convenient to apply Theorem 1.1. As a further illustration, we prove the following theorem. Note that the new bound is of the same shape as that in Theorem 1.5 (2), so it can be viewed as a generalization

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

of Theorem 1.5 (2) as changing a prime p to an arbitrary power of p, provided that $d \mid (p-1)$.

***Theorem* 4.7** *Let $d \geq 2$, and let q be a power of p such that $d \mid (p-1)$. Then $MD_d(\lambda, \mathbb{F}_q) \leq \sqrt{2(q-1)/d} + 4$ for any $\lambda \in \mathbb{F}_q^*$.*

Proof Let $B \subset \mathbb{F}_q^*$ with property $D_d(\lambda, \mathbb{F}_q)$, that is, $B\hat{\times}B + \lambda \subset S_d \cup \{0\}$. If $BB + \lambda \nsubseteq S_d \cup \{0\}$, we are done by Theorem 4.2. Thus, we may assume that $BB + \lambda \subset S_d \cup \{0\}$. It suffices to show $|B| \leq \sqrt{2(q-1)/d} + 4$. To achieve that, we try to find an arbitrary subset A of B such that $\binom{|A|-1+\frac{q-1}{d}}{|A|} \not\equiv 0 \pmod{p}$ and $|A|$ is as large as possible. With such a subset A, we have $AB + \lambda \subset S_d \cup \{0\}$ so that we can apply Theorem 1.1. In the rest of the proof, we aim to find such an A with $|A| \geq |B|/2$ so that, from Theorem 1.1, we can deduce

$$\frac{|B|^2}{2} \leq \frac{q-1}{d} + 2|B| - 1 \implies |B| \leq \sqrt{\frac{2(q-1)}{d} + 2} + 2 < \sqrt{\frac{2(q-1)}{d}} + 4.$$

Write $|B| - 1 = (c_k, c_{k-1}, \ldots, c_1, c_0)_p$ in base-p, that is, $|B| - 1 = \sum_{i=0}^{k} c_i p^i$ with $0 \leq c_i \leq p-1$ for each $0 \leq i \leq k$ and $c_k \geq 1$. Next, we construct A according to the size of c_k.

Case 1. $c_k \leq p - 1 - \frac{p-1}{d}$. In this case, let A be an arbitrary subset of B with $|A| - 1 = (c_k, 0, \ldots, 0)_p$, that is, $|A| = c_k p^k + 1$. It is easy to verify that $\binom{|A|-1+\frac{q-1}{d}}{|A|} \not\equiv 0 \pmod{p}$ using Lemma 4.4. Since $|B| \leq (c_k + 1)p^k$, it also follows readily that $|A| \geq |B|/2$.

Case 2. $c_k > p - 1 - \frac{p-1}{d}$. In this case, let A be an arbitrary subset of B with

$$|A| - 1 = \left(\frac{(d-1)(p-1)}{d}, \frac{(d-1)(p-1)}{d}, \ldots, \frac{(d-1)(p-1)}{d} \right)_p,$$

that is, $|A| = \frac{(d-1)(p-1)}{d} \cdot \sum_{i=0}^{k} p^i + 1$. Again, it is easy to verify that $\binom{|A|-1+\frac{q-1}{d}}{|A|} \not\equiv 0 \pmod{p}$ using Lemma 4.4. Since $d \geq 2$, it follows that $2|A| \geq (p-1)\sum_{i=0}^{k} p^i + 2 = p^{k+1} + 1 > |B|$. ∎

***Remark* 4.8** Under the same assumption, the proof of Theorem 4.7 can be refined to obtain improved upper bounds on $MSD_d(\lambda, \mathbb{F}_q)$. In particular, if $d, r \geq 2$ are fixed, and $p \equiv 1 \pmod{d}$ is a prime, then as $p \to \infty$, we can show that $MSD_d(\lambda, \mathbb{F}_{p^{2r-1}}) \leq (1 + o(1))\sqrt{p^{2r-1}/d}$ uniformly among $\lambda \in \mathbb{F}_{p^{2r-1}}^*$. Indeed, if $B \subset \mathbb{F}_q^*$ with property $D_d(\lambda, \mathbb{F}_q)$ with $q = p^{2r-1}$ and $\lambda \in \mathbb{F}_q^*$, then we can assume without loss of generality that $\sqrt{q/d} < |B|$. Otherwise, we are done. Note that $|B| < \sqrt{q} + O(1)$ by Proposition 1.4. Following the notations used in the proof of Theorem 4.7, we have $\sqrt{p/d} - 1 \leq c_k \leq \sqrt{p}$ and thus we are always in Case 1, and the same construction of A gives $|A| = (1 - o(1))|B|$ as $p \to \infty$. Thus, Theorem 1.1 gives $|B| \leq (1 + o(1))\sqrt{q/d}$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

5 Improved upper bounds on the largest size of generalized Diophantine tuples over integers

5.1 Proof of Theorem 1.2

In this subsection, we improve the upper bounds on the largest size of generalized Diophantine tuples with property $D_k(n)$. We first recall that for each $n \geq 1$ and $k \geq 2$,

$$M_k(n) = \sup\{|A| : A \text{ satisfies property } D_k(n)\}.$$

For $k \geq 2$, we defined the constant in the introduction

$$\eta_k = \min_{\mathcal{I}} \frac{|\mathcal{I}|}{T_{\mathcal{I}}^2}, \tag{5.1}$$

where the minimum is taken over all nonempty subset $\mathcal{I}$ of

$$\{1 \leq i \leq k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\},$$

and

$$T_{\mathcal{I}} = \sum_{i \in \mathcal{I}} \sqrt{\gcd(i-1,k)}. \tag{5.2}$$

Here is the proof of our main theorem, Theorem 1.2.

Proof Let $A = \{a_1, a_2, \ldots, a_m\}$ be a generalized Diophantine m-tuple with property $D_k(n)$ and $k \geq 3$. Given the assumption that $\log k = O(\sqrt{\log\log n})$, Proposition 2.9 implies that the contribution of a_i with $a_i > n^{\frac{k}{k-2}}$ is $|A \cap (n^{\frac{k}{k-2}}, \infty)| = O(\log k \log\log k)$ is negligible. Thus, we can assume that $A \subset [1, n^{\frac{k}{k-2}}]$. Let $\mathcal{I}$ be a nonempty subset of $\{1 \leq i \leq k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\}$, such that the ratio $|\mathcal{I}|/T_{\mathcal{I}}^2$ in equation (5.1) is minimized by $\mathcal{I}$. In other words, we have $\eta_k = |\mathcal{I}|/T_{\mathcal{I}}^2$, where

$$T = T_{\mathcal{I}} = \sum_{i \in \mathcal{I}} \sqrt{\gcd(i-1,k)}.$$

To apply the Gallagher sieve inequality (Theorem 2.5), we set $N = n^{\frac{k}{k-2}}$ and define the set of primes

$$\mathcal{P} = \{p : p \equiv i \pmod{k} \text{ for some } i \in \mathcal{I}\} \setminus \{p : p \mid n\}.$$

For each prime $p \in \mathcal{P}$, denote by A_p the image of $A \pmod{p}$ and let $A_p^* = A_p \setminus \{0\}$.

Let $p \in \mathcal{P}$. We can naturally view A_p^* as a subset of $\mathbb{F}_p^*$. Since A has property $D_k(n)$, it follows that $A_p^* \hat{\times} A_p^* + n \subset \{x^k : x \in \mathbb{F}_p^*\} \cup \{0\}$. Note that $\{x^k : x \in \mathbb{F}_p^*\}$ is the multiplicative subgroup of $\mathbb{F}_p^*$ with order $\frac{p-1}{\gcd(p-1,k)}$. Since $\gcd(p-1,k) > 1$ and $p \nmid n$, Theorem 1.5 (2) implies that

$$|A_p| \leq |A_p^*| + 1 \leq \sqrt{\frac{2(p-1)}{\gcd(p-1,k)}} + 5.$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Set $Q = 2(\frac{\phi(k)\log N}{T})^2$. Applying Gallagher's larger sieve, we obtain that

$$|A| \le \frac{\sum_{p\in\mathcal{P},p\le Q}\log p - \log N}{\sum_{p\in\mathcal{P},p\le Q}\frac{\log p}{|A_p|} - \log N}. \tag{5.3}$$

Let c be the constant from Corollary 2.7. For the numerator on the right-hand side of inequality (5.3), we have

$$\begin{aligned}\sum_{p\in\mathcal{P},p\le Q}\log p - \log N &\le \sum_{i\in\mathcal{I}}\Bigg(\sum_{\substack{p\equiv i \bmod k,\\ p\le Q}}\log p\Bigg) - \log N\\ &= \frac{|\mathcal{I}|Q}{\phi(k)} + O\Big(|\mathcal{I}|Q\exp(-c\sqrt{\log Q})\Big) - \log N.\end{aligned}$$

Next, we estimate the denominator on the right-hand side of inequality (5.3). Note that $|\mathcal{I}| \le T = \sum_{i\in\mathcal{I}}\sqrt{\gcd(i-1,k)}$. Then we have $T \le |\mathcal{I}|\sqrt{k} \le \phi(k)\sqrt{k}$, and so $\phi(k)/T \ge 1/\sqrt{k}$. Since $k = (\log N)^{o(1)}$, we deduce $Q > 2(\log N)^{2-o(1)}$. Thus we have $k = Q^{o(1)}$. This, together with Corollary 2.7 and Lemma 2.8, deduces that for each $i \in \mathcal{I}$,

$$\begin{aligned}\sum_{\substack{p\in\mathcal{P},p\le Q\\ p\equiv i \bmod k}}\frac{\log p}{|A_p|} &\ge \sum_{\substack{p\in\mathcal{P},p\le Q\\ p\equiv i \bmod k}}\frac{\log p}{\sqrt{\frac{2(p-1)}{\gcd(i-1,k)}}+5}\\ &= \sum_{\substack{p\le Q\\ p\equiv i \bmod k}}\frac{\log p}{\sqrt{\frac{2p}{\gcd(i-1,k)}}} + O\Bigg(\sum_{p\le Q}\frac{k\log p}{p}\Bigg) + O\Bigg(\sum_{p\mid n}\frac{\sqrt{k}\log p}{\sqrt{p}}\Bigg)\\ &= \sqrt{\frac{\gcd(i-1,k)}{2}}\sum_{\substack{p\le Q\\ p\equiv i \bmod k}}\frac{\log p}{\sqrt{p}} + O(k\log Q) + O(k(\log n)^{1/2})\\ &= \frac{\sqrt{2Q\gcd(i-1,k)}}{\phi(k)} + O\left(\sqrt{Q}\sqrt{\gcd(i-1,k)}\exp(-c\sqrt{\log Q})\right).\end{aligned}$$

Thus we have

$$\begin{aligned}|A| &\le \frac{\sum_{p\in\mathcal{P},p\le Q}\log p - \log N}{\sum_{p\in\mathcal{P},p\le Q}\frac{\log p}{|A_p|} - \log N}\\ &\le \frac{\frac{|\mathcal{I}|Q}{\phi(k)} + O(|\mathcal{I}|Q\exp(-c\sqrt{\log Q})) - \log N}{\sum_{i\in\mathcal{I}}\left(\sum_{\substack{p\in\mathcal{P},p\le Q\\ p\equiv i \bmod k}}\frac{\log p}{|A_p|}\right) - \log N}\\ &\le \frac{\frac{|\mathcal{I}|Q}{\phi(k)} + O(|\mathcal{I}|Q\exp(-c\sqrt{\log Q})) - \log N}{\frac{T\sqrt{2Q}}{\phi(k)} + O\left(T\sqrt{Q}\exp(-c\sqrt{\log Q})\right) - \log N}.\end{aligned}$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Finally, recall that $Q = 2(\frac{\phi(k)\log N}{T})^2$. It follows that

$$|A| \le \frac{2|\mathcal{I}|\phi(k)(\frac{\log N}{T})^2 + O\left(|\mathcal{I}|(\frac{\phi(k)\log N}{T})^2 \exp\left(-c\sqrt{\log(\frac{\phi(k)\log N}{T})}\right)\right)}{2\log N + O\left(\phi(k)\log N \exp\left(-c\sqrt{\log(\frac{\phi(k)\log N}{T})}\right)\right) - \log N}$$
$$= \frac{\frac{2|\mathcal{I}|\phi(k)}{T^2}\log N + O\left(\frac{|\mathcal{I}|\phi(k)^2\log N}{T^2} \exp\left(-c\sqrt{\log(\frac{\phi(k)\log N}{T})}\right)\right)}{1 + O\left(\phi(k)\exp\left(-c\sqrt{\log(\frac{\phi(k)\log N}{T})}\right)\right)}.$$

Recall that $N = n^{\frac{k}{k-2}}$. Thus, to obtain our desired result, we need to show

$$|A| \le \frac{(1+o(1))\frac{2|\mathcal{I}|\phi(k)}{T^2}\log N}{1-o(1)},$$

and it suffices to show that

$$\phi(k)\exp\left(-c\sqrt{\log(\frac{\phi(k)\log N}{T})}\right) = o(1),$$

as $N \to \infty$, or equivalently,

$$\log k - c\sqrt{\log\frac{\phi(k)}{T} + \log\log N} \to -\infty,$$

as $N \to \infty$. We notice that $\phi(k)/T \ge 1/\sqrt{k}$. Let $c' = c/2$. Then the assumption $\log k \le c'\sqrt{\log\log n} < c'\sqrt{\log\log N}$ implies

$$\log\log N + \log\frac{\phi(k)}{T} \ge \log\log N - \frac{1}{2}\log k = (1-o(1))\log\log N,$$

and

$$\log k - c\sqrt{\log\frac{\phi(k)}{T} + \log\log N} \le -(c'-o(1))\log\log N \to -\infty,$$

as required. ∎

Remark 5.1 Note that when $\mathcal{I} = \{1\}$, that is to say, when we only consider primes p such that $p \equiv 1 \pmod k$ for applying the Gallagher inequality, the condition $p \equiv 1 \pmod k$ guarantees that the k-th powers are indeed k-th powers modulo p. We have $T = T_{\mathcal{I}} = \sqrt{k}$, thus we trivially have $\eta_k \le \frac{1}{k}$ in view of equation (5.1). In particular, if k is fixed and $n \to \infty$, Theorem 1.2 implies that

$$M_k(n) \le \frac{(2+o(1))\phi(k)}{k-2}\log n, \tag{5.4}$$

which already provides a substantial improvement on the best-known upper bound $M_k(n) \le (3\phi(k)+o(1))\log n$ whenever $k \ge 3$ given in [7]. Moreover, note that $\frac{\phi(k)}{k}$ can be as small as $O(\frac{1}{\log\log k})$ when k is the product of distinct primes [28, Theorem 2.9].

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Thus, in view of Theorem 1.2, the inequality (5.4) already shows there is $k = k(n)$ such that $\log k \asymp \sqrt{\log\log n}$ and

$$M_k(n) \ll \frac{\log n}{\log\log k} \ll \frac{\log n}{\log\log\log n}. \tag{5.5}$$

Note that (5.5) already breaks the $\log n$ barrier. On the other hand, we can still use other primes p such that $\gcd(p-1,k) > 1$ for which k-th powers are in fact $\gcd(k,p-1)$-th powers modulo p when we apply the Gallagher sieve inequality. We can take advantage of the improvement on the upper bound of $M_k(n)$. In the next two subsections, we further provide a significant improvement on inequality (5.5).

Next, we define a *strong Diophantine m-tuple with property $SD_k(n)$* to be a set $\{a_1,\dots,a_m\}$ of m distinct positive integers such that $a_i a_j + n$ is a k-th power for any choice of i and j. We have a stronger upper bound for the size of a strong Diophantine tuple with property $SD_k(n)$. We define

$$MS_k(n) = \sup\{|A|\colon A \subset \mathbb{N} \text{ satisfies the property } SD_k(n)\}.$$

***Theorem* 5.2** *There is a constant $c' > 0$, such that as $n \to \infty$,*

$$MS_k(n) \le \left(\frac{k}{k-2} + o(1)\right)\eta_k \phi(k)\log n,$$

holds uniformly for positive integers $k, n \ge 3$ such that $\log k \le c'\sqrt{\log\log n}$. Moreover, if k is even, under the same assumption (including the case $k = 2$), we have the stronger bound

$$MS_k(n) \le \min\{\big(1 + o(1)\big)\eta_k \phi(k)\log n, \tau(n)\},$$

where $\tau(n)$ is the number of divisors of n.

Proof The proof is very similar to the proof of Theorem 1.2 and we follow all the notations and steps as in the proof of Theorem 1.2, apart from the minor modifications stated below.

We prove the first part. For each $p \in \mathcal{P}$, we have the stronger upper bound that $|A_p| \le \sqrt{\frac{(p-1)}{\gcd(p-1,k)}} + 2$ by Theorem 1.5 (2). To optimize the upper bound obtained from Gallagher's larger sieve, we instead set $Q = (\frac{\phi(k)\log N}{T})^2$.

Next, we assume that k is even and prove the second part. Notice that for each $x \in A$, there is a positive integer y, such that $x^2 + n = y^2$. Thus, $|A|$ is bounded by the number of positive integral solutions to the equation $x^2 + n = y^2$, which is at most $\tau(n)$. On the other hand, this also implies that all the elements in A are at most n. Thus, we can set $N = n$ instead and obtain the stronger upper bound. ∎

5.2 Proof of Theorem 1.3

In this subsection, by finding a more refined upper bound on η_k in equation (5.1), we show that the same approach significantly improves the upper bound of $M_k(n)$ in inequality (5.5) when k is the product of the first few distinct primes.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

We label all the primes in increasing order so that $2 = p_1 < p_2 < \cdots < p_\ell < \cdots$. Let $P_\ell = \prod_{i=1}^{\ell} p_i$ be the product of first ℓ primes. Let $\mathcal{I}_1 = \{1\}$. For $\ell \geq 1$, we define $\mathcal{I}_{\ell+1}$ inductively:

$$\mathcal{I}_{\ell+1} = \{i + jP_\ell : i \in \mathcal{I}_\ell, 0 \leq j < p_{\ell+1}, p_{\ell+1} \nmid (i + jP_\ell)\}. \tag{5.6}$$

We note that $\mathcal{I}_\ell \subset \mathcal{I}_{\ell+1}$ for any $\ell \geq 1$. Also, it is clear that

$$|\mathcal{I}_{\ell+1}| = |\mathcal{I}_\ell|(p_{\ell+1} - 1). \tag{5.7}$$

***Lemma* 5.3** *Following the above definitions, we have*

$$\mathcal{I}_\ell \subset \{1 \leq x \leq P_\ell : \gcd(x, P_\ell) = 1, \gcd(x - 1, P_\ell) > 1\}. \tag{5.8}$$

Proof We give an inductive proof. When $\ell = 1$, the inclusion (5.8) holds. We assume that (5.8) holds for some $\ell \geq 1$. Let $x = i + jP_\ell \in \mathcal{I}_{\ell+1}$. By the assumption, we have $\gcd(i, P_\ell) = 1$, and it follows that $\gcd(x, P_{\ell+1}) = \gcd(x, P_\ell)\gcd(x, p_{\ell+1}) = \gcd(i, P_\ell)\gcd(x, p_{\ell+1}) = 1$. This proves the claim. ∎

Furthermore, we introduce the following notation which is similar to the previously introduced on equation (5.2). For each $\ell \geq 1$, we let

$$T_\ell = \sum_{y \in \mathcal{I}_\ell} \sqrt{\gcd(y - 1, P_\ell)}.$$

Note that $T_1 = \sqrt{2}$. We also establish a recurrence relation on the sequence.

***Lemma* 5.4** *The sequence $(T_\ell)_{\ell \geq 1}$ satisfies the recurrence relation*

$$T_{\ell+1} = T_\ell(p_{\ell+1} - 2 + \sqrt{p_{\ell+1}}). \tag{5.9}$$

Proof We have

$$\begin{aligned} T_{\ell+1} &= \sum_{i \in \mathcal{I}_\ell} \sum_{\substack{0 \leq j < p_{\ell+1} \\ p_{\ell+1} \nmid (i + jP_\ell)}} \sqrt{\gcd(i + jP_\ell - 1, P_{\ell+1})} \\ &= \sum_{i \in \mathcal{I}_\ell} \sum_{\substack{0 \leq j < p_{\ell+1} \\ p_{\ell+1} \nmid (i + jP_\ell)}} \sqrt{\gcd(i + jP_\ell - 1, P_\ell)}\sqrt{\gcd(i + jP_\ell - 1, p_{\ell+1})} \\ &= \sum_{i \in \mathcal{I}_\ell} \sqrt{\gcd(i - 1, P_\ell)}\left(\sum_{\substack{0 \leq j < p_{\ell+1} \\ p_{\ell+1} \nmid (i + jP_\ell)}} \sqrt{\gcd(i + jP_\ell - 1, p_{\ell+1})} \right). \end{aligned}$$

It is easy to show that the inner sum consists of $(p_{\ell+1} - 2)$ many 1 and a single $\sqrt{p_{\ell+1}}$. It follows that

$$T_{\ell+1} = (p_{\ell+1} - 2 + \sqrt{p_{\ell+1}}) \sum_{i \in \mathcal{I}_\ell} \sqrt{\gcd(i - 1, P_\ell)} = T_\ell(p_{\ell+1} - 2 + \sqrt{p_{\ell+1}}),$$

proving the lemma. ∎

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

We are now ready to prove Theorem 1.3.

Proof For each n, we choose $k = k(n) = P_\ell$, where $\ell = \ell(n)$ is the largest integer such that $\log P_\ell < c'\sqrt{\log\log n}$. It follows that $\log k = \log P_\ell \asymp \sqrt{\log\log n}$. Thus, using equations (5.7) and (5.9), we have

$$\eta_k \phi(k) \le \frac{|\mathcal{I}_\ell|\phi(P_\ell)}{T_\ell^2} = \prod_{p \le p_\ell} \frac{(p-1)^2}{(p-2+\sqrt{p})^2}.$$

Note that for each prime p, it is easy to verify that $\frac{p-1}{p-2+\sqrt{p}} \le 1 - \frac{1}{\sqrt{p}}$. Recall that the inequality $e^x \ge 1+x$ holds for all real x, and a standard application of partial summation gives

$$\sum_{p \le x} \frac{1}{\sqrt{p}} = \frac{2\sqrt{x}}{\log x} + O\left(\frac{\sqrt{x}}{\log^2 x}\right).$$

Also, the prime number theorem implies that

$$\log P_\ell = \sum_{p \le p_\ell} \log p = \theta(p_\ell) = (1+o(1))p_\ell$$

and thus $p_\ell = (1+o(1))\log P_\ell$. Putting the above estimates altogether, we have

$$\begin{aligned}\eta_k \phi(k) &\le \prod_{p \le p_\ell} \left(1 - \frac{1}{\sqrt{p}}\right)^2 \le \exp\left(-2\sum_{p \le p_\ell} \frac{1}{\sqrt{p}}\right) \\ &= \exp\left(-\frac{(4+o(1))\sqrt{p_\ell}}{\log p_\ell}\right) = \exp\left(-\frac{(4+o(1))\sqrt{\log P_\ell}}{\log\log P_\ell}\right) \\ &\le \exp\left(-\frac{c''(\log\log n)^{1/4}}{\log\log\log n}\right).\end{aligned}$$

for some absolute constant $c'' > 0$. It follows from Theorem 1.2 that

$$M_k(n) \ll \eta_k \phi(k) \log n \ll \exp\left(-\frac{c''(\log\log n)^{1/4}}{\log\log\log n}\right)\log n.$$

■

5.3 An upper bound on η_k

In this subsection, we deduce a simple upper bound of η_k. It turns out that this upper bound well approximates η_k empirically.

***Theorem* 5.5** *For any $k \ge 2$, we have*

$$\eta_k \le \mu_k,$$

where $\mu_k = R_k \cdot \min\{\beta(p^\alpha) : p^\alpha || k\}$ with

$$R_k = \prod_{p^\alpha || k} \frac{(p-1)p^{\alpha-1}}{\left(p^\alpha - p^{\alpha-1} - p^{(\alpha-1)/2} + p^{\alpha-1/2}\right)^2},$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

and

$$\beta(p^\alpha) = \frac{\left(p^\alpha - p^{\alpha-1} - p^{(\alpha-1)/2} + p^{\alpha-1/2}\right)^2}{(p-1)\left(-p^{(\alpha-1)/2} + p^{\alpha-1} + p^{\alpha-1/2}\right)^2}.$$

Proof We denote $k = \prod_{j=1}^{\ell} p_j^{\alpha_j}$, where $p_1, p_2, \ldots, p_\ell$ are distinct primes factors of k such that

$$\beta(p_\ell^{\alpha_\ell}) = \min\{\beta(p^\alpha) : p^\alpha \mid\mid k\}.$$

Define

$$\mathcal{I} = \{1 \le i \le k : \gcd(k,i) = 1, i \equiv 1 \pmod{p_\ell}\}, \quad T_{\mathcal{I}} = \sum_{i \in \mathcal{I}} \sqrt{\gcd(i-1,k)}.$$

Then $\mathcal{I}$ is obviously a subset of the set $\{1 \le i \le k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\}$ consisting of residue classes that can be used in Gallagher's larger sieve in the proof of Theorem 1.2. (In particular, when $p_\ell = 2$, $\mathcal{I}$ consists of all the available residue classes with $|\mathcal{I}| = \phi(k)$.) In view of the definition of η_k, it suffices to show that

$$\frac{|\mathcal{I}|}{T_{\mathcal{I}}^2} = \mu_k = R_k \cdot \beta(p_\ell^{\alpha_\ell}).$$

We first compute the size of $\mathcal{I}$. Equivalently, we can write

$$\mathcal{I} = \{1 \le i \le k : i \not\equiv 0 \pmod{p_j} \text{ for each } 1 \le j < \ell, \text{ and } i \equiv 1 \pmod{p_\ell}\},$$

and hence, we deduce $|\mathcal{I}| = \prod_{j=1}^{\ell-1}(p_j - 1)p_j^{\alpha_j - 1} \cdot p_\ell^{\alpha_\ell - 1}$. In order to compute $T_{\mathcal{I}}$, we first count the number of solutions to $v_{p_j}(i-1) = s$ over $1 \le i \le p_j^{\alpha_j}$ such that $p_j \nmid i$ for $0 \le s \le \alpha_j$ separately, and then use the Chinese remainder theorem. Set

$$C_{j,s} = \{1 \le i \le p_j^{\alpha_j} : i \not\equiv 0 \pmod{p_j},\ v_{p_j}(i-1) = s\}, \quad \text{for } 0 \le s \le \alpha_j,\ j < \ell;$$
$$C_{\ell,s} = \{1 \le i \le p_\ell^{\alpha_\ell} : i \equiv 1 \pmod{p_\ell},\ v_{p_\ell}(i-1) = s\}, \quad \text{for } 0 \le s \le \alpha_\ell.$$

Note that

$$|C_{j,s}| = \phi(p_j^{\alpha_j - s}), \qquad \text{for } 0 < s \le \alpha_j,\ j < \ell;$$
$$|C_{j,0}| = \phi(p_j^{\alpha_j}) - p_j^{\alpha_j - 1}, \qquad \text{for } j < \ell;$$
$$|C_{\ell,s}| = \phi(p_\ell^{\alpha_\ell - s}), \qquad \text{for } 0 < s \le \alpha_\ell,$$

and $|C_{\ell,0}| = 0$. It follows that

$$T_{\mathcal{I}} = \sum_{i \in \mathcal{I}} \sqrt{\gcd(i-1,k)} = \sum_{d \mid k} \sqrt{d} \sum_{\substack{i \in \mathcal{I}, \\ \gcd(i-1,k) = d}} 1 = \prod_{j=1}^{\ell} \left(\sum_{s=0}^{\alpha_j} \sqrt{p_j^s} |C_{j,s}| \right).$$

For each $1 \le j \le \ell - 1$, we calculate

$$\sum_{s=0}^{\alpha_j} \sqrt{p_j^s} |C_{j,s}| = \phi(p_j^{\alpha_j}) - p_j^{\alpha_j - 1} + \sum_{s=1}^{\alpha_j} \sqrt{p_j^s} \phi(p_j^{\alpha_j - s}) = p_j^{\alpha_j} - p_j^{\alpha_j - 1} - p_j^{(\alpha_j - 1)/2} + p_j^{\alpha_j - 1/2}.$$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Similarly, we have

$$\sum_{s=0}^{\alpha_\ell} \sqrt{p_\ell^s}|C_{\ell,s}| = \sum_{s=1}^{\alpha_\ell} \sqrt{p_\ell^s}\phi(p_\ell^{\alpha_\ell - s}) = -p_\ell^{(\alpha_\ell-1)/2} + p_\ell^{\alpha_\ell - 1} + p_\ell^{\alpha_\ell - 1/2}.$$

Putting these all together, we compute

$$T_{\mathcal{I}} = \prod_{j=1}^{\ell-1} \left[p_j^{\alpha_j} - p_j^{\alpha_j-1} - p_j^{(\alpha_j-1)/2} + p_j^{\alpha_j-1/2} \right] \cdot \left(- p_\ell^{(\alpha_\ell-1)/2} + p_\ell^{\alpha_\ell-1} + p_\ell^{\alpha_\ell-1/2} \right).$$

Hence,

$$\frac{|\mathcal{I}|}{T_{\mathcal{I}}^2} = \prod_{j=1}^{\ell-1} \frac{(p_j-1)p_j^{\alpha_j-1}}{\left(p_j^{\alpha_j} - p_j^{\alpha_j-1} - p_j^{(\alpha_j-1)/2} + p_j^{\alpha_j-1/2}\right)^2} \cdot \frac{p_\ell^{\alpha_\ell-1}}{\left(- p_\ell^{(\alpha_\ell-1)/2} + p_\ell^{\alpha_\ell-1} + p_\ell^{\alpha_\ell-1/2}\right)^2}.$$

■

Therefore, Theorem 1.2 implies

***Corollary* 5.6** *There is a constant $c' > 0$, such that as $n \to \infty$,*

$$M_k(n) \le \left(\frac{2k}{k-2} + o(1) \right) \mu_k \phi(k) \log n,$$

holds uniformly for positive integers $k, n \ge 3$ such that $\log k \le c' \sqrt{\log \log n}$.

***Remark* 5.7** Our computations indicate that when $2 \le k \le 100{,}000$, the inequality $\mu_k \le 2\eta_k$ holds for all but 501 of them. This numerical evidence suggests that μ_k provides a good approximation for η_k for a generic k. Note that the computational complexity for computing μ_k is the same as that of the prime factorization of k: a naive algorithm takes $O(\sqrt{k})$ time. The best theoretical algorithm has running time $O\big(\exp((\log k)^{1/3+o(1)})\big)$ using the general number field sieve [5]. On the other hand, computing η_k requires $O(k \log k)$ time; we refer to Appendix A for an algorithm and some computational results.

6 Multiplicative decompositions of shifted multiplicative subgroups

In this section, we present our contributions to Conjecture 1.9. In particular, we make significant progress towards Sárközy's conjecture (Conjecture 1.8). We recall $S_d = S_d(\mathbb{F}_q) = \{x^d : x \in \mathbb{F}_q^*\}$.

6.1 Applications to Sárközy's conjecture

In this subsection, we show that for almost all primes $p \equiv 1 \pmod{d}$, the set $(S_d(\mathbb{F}_p) - 1) \setminus \{0\}$ cannot be decomposed as the product of two sets non-trivially. This confirms

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

the truth of Sárközy's conjecture (Conjecture 1.8) as well as the truth of its generalization in the generic case (Conjecture 1.9) when the shift of the subgroup is given by $\lambda = 1$.

***Theorem* 6.1** *Let $d \geq 2$ be fixed. As $x \to \infty$, the number of primes $p \leq x$ such that $p \equiv 1 \pmod{d}$ and $(S_d(\mathbb{F}_p) - 1) \setminus \{0\}$ can be decomposed as the product of two sets non-trivially (that is, it can be written as the product of two subsets of $\mathbb{F}_p^*$ with size at least 2) is $o(\pi(x))$.*

Proof Let $\mathcal{P}_d$ be the set of primes p such that $p \equiv 1 \pmod{d}$ and $(S_d(\mathbb{F}_p) - 1) \setminus \{0\}$ admits a non-trivial multiplicative decomposition. By the prime number theorem for arithmetic progressions, it suffices to show that $|\mathcal{P}_d \cap [0, x]| = o(x/\log x)$.

Let $p \in \mathcal{P}_d$. Then we can write $(S_d - 1) \setminus \{0\}$ as the product of two sets $A, B \subset \mathbb{F}_p^*$ such that $|A|, |B| \geq 2$. Then Corollary 1.10 implies that $|A||B| = \frac{p-1}{d} - 1$, that is,

$$d|A||B| = p - (d + 1). \tag{6.1}$$

On the other hand, Proposition 3.4 implies that we can find an absolute constant $C_d \in (0, 1)$ such that

$$C_d\sqrt{p} < \min\{|A|, |B|\} < \sqrt{p}.$$

It follows that $p - (d + 1)$ has a divisor in the interval $(C_d\sqrt{p}, \sqrt{p})$. To summarize, if $p \in \mathcal{P}_d$, then we have $\tau(p - (d + 1); C_d\sqrt{p}, \sqrt{p}) \geq 1$, where $\tau(n; y, z)$ denotes the number of divisors of n in the interval $(y, z]$. Now, we use results by Ford [14, Theorem 6] on the distribution of shift primes with a divisor in a given interval. Denote

$$H(x, y, z) = \#\{1 \leq n \leq x : \tau(n; y, z) \geq 1\}; \tag{6.2}$$

$$P_d(x, y, z) = \#\{p \leq x : \tau(p - (d + 1); y, z) \geq 1\}. \tag{6.3}$$

Setting $y = C_d\sqrt{x}/2$ and $z = \sqrt{x}$, [14, Theorem 6] and [14, Theorem 1, third case of (v)] imply that

$$P_d(x, y, z) \ll \frac{H(x, y, z)}{\log x} \ll \frac{x}{\log x} u^{\delta} \left(\log \frac{2}{u}\right)^{-3/2}$$

where $\delta = 1 - \frac{1+\log\log 2}{\log 2}$ and $u = \log(C_d/2)/\log y$. It follows that as $x \to \infty$, we have $P_d(x, y, z) = o(x/\log x)$. Therefore, we have

$$\#\{p \in \mathcal{P}_d : x/2 \leq p \leq x\} \leq \#\{x/2 \leq p \leq x : \tau(p-(d+1); C_d\sqrt{x}/2, \sqrt{x}) \geq 1\} = o(x/\log x).$$

We conclude that as $x \to \infty$,

$$\begin{aligned} |\mathcal{P}_d \cap [0, x]| &= O(\sqrt{x}) + \#\{p \in \mathcal{P}_d : \sqrt{x} \leq p \leq x\} \\ &= O(\sqrt{x}) + \sum_{0 \leq j \leq (\log_2 x)/2} o\left(\frac{x/2^j}{\log(x/2^j)}\right) \\ &= O(\sqrt{x}) + \left(\sum_{0 \leq j \leq (\log_2 x)/2} \frac{1}{2^j}\right) o\left(\frac{x}{\log x}\right) = o\left(\frac{x}{\log x}\right). \end{aligned}$$

■

Using a similar argument, we can prove Theorem 1.11:

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Proof Consider the family of primes p such that $p \equiv 1 \pmod{d}$ and n is a d-th power modulo p. By a standard application of the Chebotarev density theorem, the density of such primes is given by $\frac{1}{[\mathbb{Q}(e^{2\pi i/d}, n^{1/d}):\mathbb{Q}]}$. Among the family of such primes p, we can repeat the same argument as in the proof of Theorem 6.1 to show that if $(S_d(\mathbb{F}_p) - n) \setminus \{0\}$ admits a non-trivial multiplicative decomposition, then $p - (d+1)$ necessarily has a divisor which is "close to" $\sqrt{p}$. We remark that it is important to assume that n is a d-th power modulo p, so that we can take advantage of Corollary 1.10. Similar to the proof of Theorem 6.1, we can show that among the family of primes $p \equiv 1 \pmod{d}$, the property that $p - (d+1)$ has a divisor with the desired magnitude fails to hold for almost all p. This finishes the proof of the theorem. ∎

Remark 6.2 When n is a fixed negative integer, one can obtain a similar result to Theorem 1.11 following the idea of the above proof.

Remark 6.3 Theorem 1.11 essentially states if d is fixed, $p \equiv 1 \pmod{d}$ is a prime, and $\lambda \in S_d(\mathbb{F}_p)$, then it is very unlikely that we can decompose $(S_d(\mathbb{F}_p) - \lambda) \setminus \{0\}$ as the product of two subsets of $\mathbb{F}_p^*$ non-trivially. On the other hand, when $\lambda \notin S_d(\mathbb{F}_p)$, the above technique does not apply. Nevertheless, when $\lambda \notin S_d$ and we have two sets $A, B \subset \mathbb{F}_p^*$ such that $AB = (S_d - \lambda) \setminus \{0\} = S_d - \lambda$, Theorem 1.1 implies that

$$|S_d| \leq |A||B| \leq |S_d| + \min\{|A|, |B|\} - 1.$$

In particular, we get the following non-trivial fact: if $|A|$ is fixed, then $|B|$ is also uniquely fixed.

6.2 Applications to special multiplicative decompositions

In this subsection, we verify the ternary version of Conjecture 1.9 in a strong sense, which generalizes [31, Theorem 2].

Shkredov [33, Theorem 3] showed if G is a multiplicative subgroup of $\mathbb{F}_p$ with $1 \ll_\epsilon |G| \leq p^{6/7-\epsilon}$, then there is no $A \subset \mathbb{F}_p$ and $\xi \in \mathbb{F}_p^*$ such that $A/A = \xi G + 1$. In fact, due to the analytic nature of the proof, he pointed out that his proof can be slightly modified to show something stronger, namely $A/A \neq (\xi G + 1) \cup C$, as long as C is small(see also [33, Remark 15]). The following corollary of Theorem 1.1 is of a similar flavor.

***Corollary* 6.4** *Let p be a prime. If G is a proper multiplicative subgroup of $\mathbb{F}_p$ with $|G| \geq 8$, and $\lambda, \xi \in \mathbb{F}_p^*$, then there is no $A \subset \mathbb{F}_p^*$ such that $AA = (\xi G - \lambda) \setminus \{0\}$.*

Proof We assume, otherwise, that $AA = (\xi G - \lambda) \setminus \{0\}$ for some $A \subset \mathbb{F}_p^*$. Then we observe that $aa' = a'a$ for each $a, a' \in A$, it follows that

$$|G| - 1 \leq |AA| \leq \frac{|A|^2 + |A|}{2}.$$

Since $|G| \geq 8$, it follows that $|A| \geq 4$. Let $B = A/\xi$, and $\lambda' = \lambda/\xi$. Then we have $AB = (G - \lambda') \setminus \{0\}$ and thus Theorem 1.1 implies that $|A|^2 = |A||B| \leq |G| + |A| - 1$.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

Comparing the above two inequalities, we obtain that

$$|A|^2 - |A| \leq |G| - 1 \leq \frac{|A|^2 + |A|}{2},$$

which implies that $|A| \leq 3$, contradicting the assumption that $|A| \geq 4$. ∎

***Lemma* 6.5** *Let A, B, C be nonempty subsets of $\mathbb{F}_q$ and let $\lambda \in \mathbb{F}_q^*$. Then $|ABC + \lambda|^2 \leq |AB + \lambda||BC + \lambda||CA + \lambda|$.*

Proof It suffices to show $|ABC|^2 \leq |AB||BC||CA|$, which is a special case of [29, Theorem 5.1] due to Ruzsa. ∎

The following two theorems generalize Sárközy [31, Theorem 2] and confirm the ternary version of Conjecture 1.9 in a strong form.

***Theorem* 6.6** *There exists an absolute constant $M > 0$, such that whenever p is a prime, G is a proper multiplicative subgroup of $\mathbb{F}_p$ with $|G| > M$, and $\lambda \in \mathbb{F}_p^*$, there is no ternary multiplicative decomposition $ABC = (G - \lambda) \setminus \{0\}$ with $A, B, C \subset \mathbb{F}_p^*$ and $|A|, |B|, |C| \geq 2$.*

Proof Assume that there are sets $A, B, C \subset \mathbb{F}_p^*$ with $|A|, |B|, |C| \geq 2$, such that $ABC = (G - \lambda) \setminus \{0\}$ for some proper multiplicative subgroup G of $\mathbb{F}_p$ and some $\lambda \in \mathbb{F}_p^*$.

Then we can write $(G-\lambda) \setminus \{0\}$ in three different ways: $A(BC), B(CA), C(AB)$, so that we can apply the results in previous sections to each of them. Note that Lemma 3.6 implies that

$$|A|, |B|, |C| \geq |G|^{1/2+o(1)}.$$

On the other hand, Theorem 1.1 implies that

$$|AB||C|, |BC||A|, |CA||B| \ll |G|.$$

Therefore, from Lemma 6.5 and the fact $|ABC| \in \{|G|, |G| - 1\}$, we have

$$|G|^2|A||B||C| \ll |ABC|^2|A||B||C| \ll (|AB||C|)(|BC||A|)(|CA||B|) \ll |G|^3.$$

It follows that

$$|G|^{3/2+o(1)} \ll |A||B||C| \ll |G|,$$

that is, $|G| \ll 1$, where the implicit constant is absolute. This completes the proof of the theorem. ∎

***Theorem* 6.7** *Let $\epsilon > 0$. There is a constant $Q = Q(\epsilon)$, such that for each prime power $q > Q$ and a divisor d of $q - 1$ with $2 \leq d \leq q^{1/10-\epsilon}$, there is no ternary multiplicative decomposition $ABC = (S_d(\mathbb{F}_q) - \lambda) \setminus \{0\}$ with $A, B, C \subset \mathbb{F}_q^*$, $|A|, |B|, |C| \geq 2$, and $\lambda \in \mathbb{F}_q^*$.*

Proof The proof is similar to the proof of Theorem 6.6. While Lemma 3.6 does not hold in the new setting (see Remark 3.8), we can instead use Proposition 3.4. If $ABC =$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

$(S_d(\mathbb{F}_q) - \lambda) \setminus \{0\}$, then Proposition 3.4 implies that

$$|A|, |B|, |C| \gg \frac{\sqrt{q}}{d}, \quad |A||BC|, |BC||A|, |CA||B| \ll q.$$

A similar computation leads to $d \gg q^{1/10}$, which implies that $q \ll_\epsilon 1$ since we assume that $d \leq q^{1/10-\epsilon}$. ∎

Acknowledgments

The authors thank Andrej Dujella, Greg Martin, and József Solymosi for helpful discussions. The research of the second author was supported in part by an NSERC fellowship. The third author was supported by the KIAS Individual Grant (CG082701) at the Korea Institute for Advanced Study and the Institute for Basic Science (IBS-R029-C1).

References

[1] R. Becker and M. R. Murty. Diophantine m-tuples with the property $D(n)$. *Glas. Mat. Ser. III*, 54(74)(1):65–75, 2019.
[2] A. Bérczes, A. Dujella, L. Hajdu, and F. Luca. On the size of sets whose elements have perfect power n-shifted products. *Publ. Math. Debrecen*, 79(3-4):325–339, 2011.
[3] S. R. Blackburn, S. V. Konyagin, and I. E. Shparlinski. Counting additive decompositions of quadratic residues in finite fields. *Funct. Approx. Comment. Math.*, 52(2):223–227, 2015.
[4] Y. Bugeaud and A. Dujella. On a problem of Diophantus for higher powers. *Math. Proc. Cambridge Philos. Soc.*, 135(1):1–10, 2003.
[5] J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.*, pages 50–94. Springer, Berlin, 1993.
[6] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points. *J. Amer. Math. Soc.*, 10(1):1–35, 1997.
[7] A. B. Dixit, S. Kim, and M. R. Murty. Generalized Diophantine m-tuples. *Proc. Amer. Math. Soc.*, 150(4):1455–1465, 2022.
[8] A. Dujella. On the size of Diophantine m-tuples. *Math. Proc. Cambridge Philos. Soc.*, 132(1):23–33, 2002.
[9] A. Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.
[10] A. Dujella. *Diophantine m-tuples and Elliptic Curves*, volume 79 of *Developments in Mathematics*. Springer, Cham, 2024.
[11] A. Dujella and V. Petričević. Strong Diophantine triples. *Experiment. Math.*, 17(1):83–89, 2008.
[12] J.-H. Evertse. On the quantitative subspace theorem. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 377(Issledovaniya po Teorii Chisel. 10):217–240, 245, 2010.
[13] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
[14] K. Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2):367–433, 2008.
[15] P. X. Gallagher. A larger sieve. *Acta Arith.*, 18:77–81, 1971.
[16] A. M. Güloğlu and M. R. Murty. The Paley graph conjecture and Diophantine m-tuples. *J. Combin. Theory Ser. A*, 170:105155, 9, 2020.
[17] K. Gyarmati. On a problem of Diophantus. *Acta Arith.*, 97(1):53–65, 2001.
[18] L. Hajdu and A. Sárközy. On multiplicative decompositions of polynomial sequences, I. *Acta Arith.*, 184(2):139–150, 2018.
[19] L. Hajdu and A. Sárközy. On multiplicative decompositions of polynomial sequences, II. *Acta Arith.*, 186(2):191–200, 2018.
[20] L. Hajdu and A. Sárközy. On multiplicative decompositions of polynomial sequences, III. *Acta Arith.*, 193(2):193–216, 2020.

[21] B. Hanson and G. Petridis. Refined estimates concerning sumsets contained in the roots of unity. *Proc. Lond. Math. Soc. (3)*, 122(3):353–358, 2021.
[22] B. He, A. Togbé, and V. Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, 371(9):6665–6709, 2019.
[23] A. A. Karatsuba. Distribution of values of Dirichlet characters on additive sequences. *Dokl. Akad. Nauk SSSR*, 319(3):543–545, 1991.
[24] S. Kim, C. H. Yip, and S. Yoo. Explicit constructions of Diophantine tuples over finite fields. *Ramanujan J.*, 65(1):163–172, 2024.
[25] E. Kummer. Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen. *Journal für die reine und angewandte Mathematik*, 44:93–146, 1852.
[26] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
[27] S. Macourt, I. D. Shkredov, and I. E. Shparlinski. Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields. *Canad. J. Math.*, 70(6):1319–1338, 2018.
[28] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.
[29] I. Z. Ruzsa. Cardinality questions about sumsets. In *Additive combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, pages 195–205. Amer. Math. Soc., Providence, RI, 2007.
[30] A. Sárközy. On additive decompositions of the set of quadratic residues modulo p. *Acta Arith.*, 155(1):41–51, 2012.
[31] A. Sárközy. On multiplicative decompositions of the set of the shifted quadratic residues modulo p. In *Number theory, analysis, and combinatorics*, De Gruyter Proc. Math., pages 295–307. De Gruyter, Berlin, 2014.
[32] T. Schoen and I. D. Shkredov. Character sums estimates and an application to a problem of Balog. *Indiana Univ. Math. J.*, 71(3):953–964, 2022.
[33] I. D. Shkredov. Any small multiplicative subgroup is not a sumset. *Finite Fields Appl.*, 63:101645, 15, 2020.
[34] I. E. Shparlinski. Additive decompositions of subgroups of finite fields. *SIAM J. Discrete Math.*, 27(4):1870–1879, 2013.
[35] S. A. Stepanov. On the number of points of a hyperelliptic curve over a finite prime field. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 33:1171–1181, 1969.
[36] I. M. Vinogradov. *Elements of number theory*. Dover Publications, Inc., New York, 1954. Translated by S. Kravetz.
[37] I. V. Vyugin and I. D. Shkredov. On additive shifts of multiplicative subgroups. *Mat. Sb.*, 203(6):81–100, 2012.
[38] C. H. Yip. Additive decompositions of large multiplicative subgroups in finite fields. *Acta Arith.*, 213(2):97–116, 2024.
[39] C. H. Yip. Improved upper bounds on Diophantine tuples with the property $D(n)$, 2024. Bull. Aust. Math. Soc., to appear. arXiv:2406.00840.
[40] C. H. Yip. Restricted sumsets in multiplicative subgroups, 2025. Canad. J. Math., to appear. https://doi.org/10.4153/S0008414X24000920.

Department of Mathematics and Computer Science, University of Basel, Basel, Switzerland
e-mail: seoyoung.kim@unibas.ch.

School of Mathematics, Georgia Institute of Technology, Atlanta, GA, United States
e-mail: cyip30@gatech.edu.

Discrete Mathematics Group, Institute for Basic Science, Daejeon, South Korea
e-mail: syoo19@ibs.re.kr.

A Algorithm and Computations

We continue our discussion from the introduction on the following constant

$$\gamma_k = \limsup_{n\to\infty} \frac{M_k(n)}{\log n}.$$

It is implicit in [7] that $\gamma_k \le 3\phi(k)$. We also write $\nu_k = \frac{2k}{k-2}\eta_k\phi(k)$.

Our main result, Theorem 1.2, implies that $\gamma_k \le \nu_k$. In particular, in view of Remark 5.1, it follows that $\gamma_k \le 6$ for all $k \ge 2$ and $\gamma_k \le 2+o(1)$ when $k \to \infty$. In Figure A.1, we pictorially compare our new bound ν_k with the bound $3\phi(k)$ when $2 \le k \le 1000$.

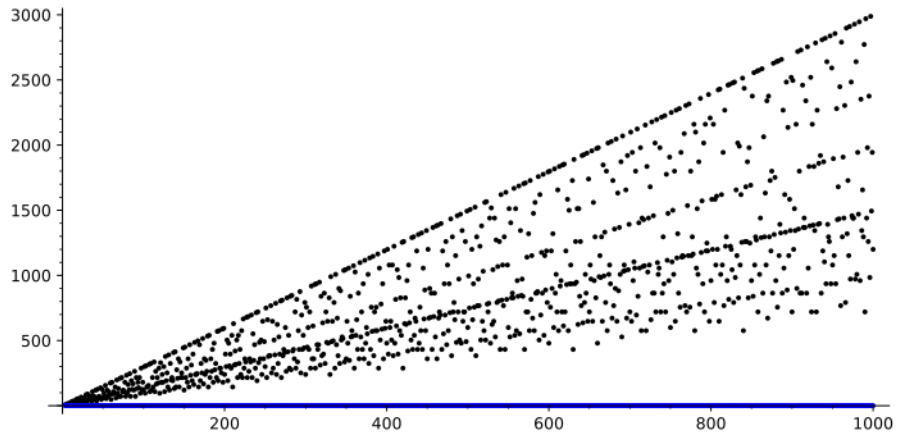

Figure A.1: Comparison between the new bound ν_k and the bound $3\phi(k)$ in [7] when $2 \le k \le 1000$. The black dots denote $3\phi(k)$, and the blue dots denote ν_k.

Recall that for $k \ge 2$, we defined the constant $\eta_k = \min_{\mathcal{I}} |\mathcal{I}|/T_{\mathcal{I}}^2$, where the minimum is taken over all nonempty subsets $\mathcal{I}$ of $\{1 \le i \le k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\}$, and $T_{\mathcal{I}} = \sum_{i\in\mathcal{I}} \sqrt{\gcd(i-1,k)}$.

To compute η_k, we use the following simple greedy algorithm with running time $O(k \log k)$. The observation is as follows. If $|\mathcal{I}|$ is fixed, our goal is to minimize $|\mathcal{I}|/T_{\mathcal{I}}^2$. Thus, we should choose those residue classes $i \pmod k$ with $\gcd(i-1,k)$ as large as possible to maximize $T_{\mathcal{I}}$. Then, we can sort these gcds in decreasing order, and when $|\mathcal{I}|$ is fixed, we pick those residue classes corresponding to the largest $|\mathcal{I}|$ gcds. The following is a precise description of the algorithm:

***Algorithm* A.1** *Let $k \ge 2$. We follow the notations defined in Subsection 5.2.*

Step 1. *Let $\mathcal{A} = \{1 \le i \le k : \gcd(i,k) = 1, \gcd(i-1,k) > 1\}$. We list the elements of $\mathcal{A}$ by $\{a_1, a_2, \dots\}$ such that $\gcd(a_j - 1, k)$ is decreasing by using a sorting algorithm.*

Step 2. *Set $I_r = \{a_1, \dots, a_r\}$, $T_{I_r} = \sum_{i\in I_r} \sqrt{\gcd(i-1,k)}$, and $\xi_{I_r} = |I_r|/T_{I_r}^2$.*

Step 3. *Return $\eta_k = \min_r \xi_{I_r}$ and terminate the algorithm.*

Note that the running time of the above algorithm is $O(k \log k)$: sorting takes $O(k \log k)$ time, while other steps take linear time.

Next, we also consider the minimum value m_k of the upper bounds $\{\nu_i : 2 \le i \le k\}$ for each $k \ge 2$. Table A.1 shows the values of m_k for $2 \le k \le 1{,}000{,}000$ when they are changed.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

k	m_k	k	m_k	k	m_k
2	2.00000	720	0.09693	30240	0.03647
4	1.37258	840	0.09266	50400	0.03343
6	0.80385	1260	0.08465	55440	0.02997
8	0.72776	1440	0.08445	83160	0.02877
12	0.44134	1680	0.07624	110880	0.02574
24	0.31910	2520	0.06465	166320	0.02343
36	0.29027	5040	0.05317	221760	0.02280
48	0.25836	7560	0.05171	277200	0.02138
60	0.21636	10080	0.04592	332640	0.02008
120	0.16570	15120	0.04252	498960	0.01985
180	0.15191	20160	0.04111	554400	0.01827
240	0.13876	25200	0.03887	665280	0.01774
360	0.11708	27720	0.03665	720720	0.01654

Table A.1: The minimum m_k of the upper bounds $\{\nu_i : 1 \leq i \leq k\}$ for $2 \leq k \leq$ 1,000,000.

We also report our computations on ν_k for $2 \leq k \leq 201$ in the following table.

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press

k	ν_k	k	ν_k	k	ν_k	k	ν_k
2	2.0000	52	0.4818	102	0.3827	152	0.3928
3	4.0000	53	2.0392	103	2.0198	153	0.5366
4	1.3726	54	0.3596	104	0.3757	154	0.3772
5	2.6667	55	0.7678	105	0.3626	155	0.9081
6	0.8038	56	0.3486	106	0.8114	156	0.2471
7	2.4000	57	0.8290	107	2.0190	157	2.0129
8	0.7278	58	0.7742	108	0.2355	158	0.8353
9	1.1077	59	2.0351	109	2.0187	159	0.9532
10	0.7295	60	0.2164	110	0.3768	160	0.2385
11	2.2222	61	2.0339	111	0.9094	161	0.8485
12	0.4413	62	0.7783	112	0.2864	162	0.3140
13	2.1818	63	0.4746	113	2.0180	163	2.0124
14	0.7185	64	0.4124	114	0.3874	164	0.5392
15	0.7222	65	0.7860	115	0.8621	165	0.3857
16	0.5383	66	0.3643	116	0.5220	166	0.8382
17	2.1333	67	2.0308	117	0.5160	167	2.0121
18	0.4522	68	0.4950	118	0.8179	168	0.1737
19	2.1176	69	0.8515	119	0.8087	169	1.2965
20	0.4450	70	0.3548	120	0.1657	170	0.4049
21	0.7355	71	2.0290	121	1.2615	171	0.5453
22	0.7251	72	0.2171	122	0.8200	172	0.5416
23	2.0952	73	2.0282	123	0.9220	173	2.0117
24	0.3191	74	0.7892	124	0.5254	174	0.4053
25	1.1180	75	0.5005	125	0.8820	175	0.5104
26	0.7313	76	0.5006	126	0.2335	176	0.3077
27	0.7508	77	0.7644	127	2.0160	177	0.9660
28	0.4552	78	0.3713	128	0.3877	178	0.8422
29	2.0741	79	2.0260	129	0.9278	179	2.0113
30	0.3351	80	0.2730	130	0.3869	180	0.1519
31	2.0690	81	0.6359	131	2.0155	181	2.0112
32	0.4555	82	0.7956	132	0.2413	182	0.3854
33	0.7709	83	2.0247	133	0.8226	183	0.9700
34	0.7438	84	0.2263	134	0.8256	184	0.4014
35	0.7311	85	0.8195	135	0.3709	185	0.9365
36	0.2903	86	0.7985	136	0.3878	186	0.4080
37	2.0571	87	0.8796	137	2.0148	187	0.8001
38	0.7497	88	0.3682	138	0.3955	188	0.5459
39	0.7873	89	2.0230	139	2.0146	189	0.3843
40	0.3353	90	0.2239	140	0.2400	190	0.4129
41	2.0513	91	0.7794	141	0.9387	191	2.0106
42	0.3465	92	0.5103	142	0.8291	192	0.2075
43	2.0488	93	0.8877	143	0.7812	193	2.0105
44	0.4739	94	0.8040	144	0.1809	194	0.8471
45	0.4581	95	0.8346	145	0.8976	195	0.3948
46	0.7604	96	0.2261	146	0.8307	196	0.3652
47	2.0444	97	2.0211	147	0.5506	197	2.0103
48	0.2584	98	0.5376	148	0.5342	198	0.2493
49	1.1716	99	0.5038	149	2.0136	199	2.0102
50	0.4974	100	0.3344	150	0.2468	200	0.2517
51	0.8163	101	2.0202	151	2.0134	201	0.9811

Table A.2: The upper bound ν_k of γ_k when $2 \le k \le 201$

https://doi.org/10.4153/S0008414X25000136 Published online by Cambridge University Press