

F -DIOPHANTINE SETS OVER FINITE FIELDS

CHI HOI YIP AND SEMIN YOO

ABSTRACT. Let $k \geq 2$, q be an odd prime power, and $F \in \mathbb{F}_q[x_1, \dots, x_k]$ be a polynomial. An F -Diophantine set over a finite field \mathbb{F}_q is a set $A \subset \mathbb{F}_q^*$ such that $F(a_1, a_2, \dots, a_k)$ is a square in \mathbb{F}_q whenever a_1, a_2, \dots, a_k are distinct elements in A . In this paper, we provide a strategy to construct a large F -Diophantine set, provided that F has a nice property in terms of its monomial expansion. In particular, when $F = x_1 x_2 \dots x_k + 1$, our construction gives a k -Diophantine tuple over \mathbb{F}_q with size $\gg_k \log q$, significantly improving the $\Theta((\log q)^{1/(k-1)})$ lower bound in a recent paper by Hammonds-Kim-Miller-Nigam-Onghai-Saikia-Sharma.

1. INTRODUCTION

A set of m positive integers is a *Diophantine m -tuple* if the product of any two distinct elements in the set is one less than a perfect square. There are many interesting results in the study of Diophantine tuples and their variants. Perhaps most notable is the Diophantine quintuple conjecture, namely, there is no Diophantine quintuple, recently confirmed by He, Togbé, and Ziegler [11]. We refer to the Dujella's book [5] for a comprehensive discussion on the topic and their reference.

The definition of F -Diophantine sets were formally introduced by Bérczes, Dujella, Hajdu, Tengely [1] for a polynomial $F \in \mathbb{Z}[x, y]$. Given a polynomial $F \in \mathbb{Z}[x, y]$, they say that a subset A of integers is an *F -Diophantine set* if $F(x, y)$ is a perfect square for all $x, y \in A$ with $x \neq y$. F -Diophantine sets naturally appear in various contexts and are related to many interesting problems in number theory. In particular, an F -Diophantine set with $F(x, y) = xy + n$ and $n \neq 0$ corresponds to a Diophantine tuple with property $D(n)$ (see for example [4]). Similar to the study of classical Diophantine tuples, it is of special interest to construct large F -Diophantine sets or give bounds on the maximum size of F -Diophantine sets [1, 16].

In this paper, we study the natural analogue of F -Diophantine sets over finite fields. Throughout the paper, let q be an odd prime power, \mathbb{F}_q the finite field with q elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let $k \geq 2$ and $F \in \mathbb{F}_q[x_1, \dots, x_k]$ be a polynomial. We say $A \subset \mathbb{F}_q^*$ is an *F -Diophantine set over \mathbb{F}_q* if $F(a_1, a_2, \dots, a_k)$ is a square in \mathbb{F}_q whenever a_1, a_2, \dots, a_k are distinct elements in A . In the same spirit, we are interested in estimating the quantity $M(F; \mathbb{F}_q)$, the maximum size of F -Diophantine sets over \mathbb{F}_q ¹. Although such terminology appears to be new in general, for many special polynomials F , F -Diophantine sets over finite fields have been studied extensively in different contexts. The obvious choice $F(x, y) = xy + \lambda$ with $\lambda \in \mathbb{F}_q^*$ corresponds to generalized Diophantine tuples over \mathbb{F}_q [6, 9, 12, 14, 17, 18]. F -Diophantine sets over \mathbb{F}_q with

2020 *Mathematics Subject Classification.* 11D79, 11T06, 11T24.

Key words and phrases. Diophantine tuple, F -Diophantine set, finite field.

¹The definition of $M(F; \mathbb{F}_q)$ still makes sense when q is even, however in that case we trivially have $M(F; \mathbb{F}_q) = q - 1$ since each element in \mathbb{F}_q is a square.

$F(x, y) = x - y$ (when $q \equiv 1 \pmod{4}$) corresponds to cliques in the Paley graph over \mathbb{F}_q . In the aforementioned two cases, when q is a non-square, we have the “trivial” bounds

$$(1 - o(1)) \log_4 q \leq M(F; \mathbb{F}_q) \leq \sqrt{q} + O(1);$$

see [12, 13, 19]. However, any bound beyond the above requires highly non-trivial efforts. We refer to [3, 12, 14, 13, 19, 20] for recent multiplicative constant improvement on the lower bounds and upper bounds from polynomial methods, finite geometry, number theory, and graph theory. Moreover, when $k = 2$, the authors [13] have studied lower bounds and upper bounds on $M(F; \mathbb{F}_q)$ for a generic polynomial $F \in \mathbb{F}_q[x, y]$. We focus on the case $k \geq 3$ in this paper.

Next we discuss lower bounds and upper bounds on $M(F; \mathbb{F}_q)$ for a generic polynomial $F \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$ with degree d . From [13, Section 3.3], one can deduce that $M(F; \mathbb{F}_q) = O_d(\sqrt{q})$ if F is generic. Note that this upper bound is sometimes sharp. Indeed, if q is a square and F is defined over $\mathbb{F}_{\sqrt{q}}$, then $A = \mathbb{F}_{\sqrt{q}}^*$ is an F -Diophantine set over \mathbb{F}_q since all elements in $\mathbb{F}_{\sqrt{q}}$ are squares in \mathbb{F}_q . Regarding the lower bound on $M(F; \mathbb{F}_q)$, it is helpful to use a probabilistic heuristic. Assuming that the set of squares in \mathbb{F}_q was a random subset of \mathbb{F}_q with density $1/2$, then we expect that there exists an F -Diophantine set over \mathbb{F}_q with size n provided that

$$\binom{q}{n} 2^{-\binom{n}{k}} \geq 1.$$

This suggests the heuristic lower bound that

$$M(F; \mathbb{F}_q) \geq \Theta((\log q)^{1/(k-1)}). \quad (1.1)$$

Here, for two functions f and g , $f = \Theta(g)$ means that both $f = O(g)$ and $g = O(f)$ are satisfied. Indeed, when $F(x_1, x_2, \dots, x_k) = x_1 x_2 \cdots x_k + 1$, Hammonds, Kim, Miller, Nigam, Onghai, Saikia, and Sharma [10, Theorem 1.3] confirmed inequality (1.1) (they only considered the case where q is an odd prime, but the same proof extends to all odd prime powers q). Unsurprisingly, in their terminology, such an F -Diophantine set over \mathbb{F}_q is a k -Diophantine tuple over \mathbb{F}_q .

Before stating our main result, we need to introduce a new definition. We define a partial order on non-constant monic monomials in $\mathbb{F}_q[x_1, x_2, \dots, x_k]$. Let $f = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ and $g = x_1^{\beta_1} x_2^{\beta_2} \cdots x_k^{\beta_k}$, where $\alpha_1, \beta_1, \dots, \alpha_k, \beta_k$ are nonnegative integers. We write $f \succeq g$ if $\alpha_i \geq \beta_i$ for each $1 \leq i \leq k$, and write $f \succ g$ if $f \succeq g$ and $f \neq g$. Let $F \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$ be a nonzero polynomial. We can write F in its monomial expansion as follows:

$$F = \sum_{i=1}^m a_i f_i + C,$$

where each $a_i \in \mathbb{F}_q^*$, f_i is a monomial of degree at least 1, and $C \in \mathbb{F}_q$. We say F is of type I if C is a non-zero square in \mathbb{F}_q . We say F is of type II if there is $1 \leq i \leq m$, such that a_i is a square in \mathbb{F}_q^* , and $f_i \succ f_j$ for all $1 \leq j \leq m$ with $j \neq i$.

Theorem 1.1. *Let $q \geq 257$ be an odd prime power and let $F \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$ be a nonzero polynomial of type I or type II. If F has degree d and the monomial expansion of F consists of m non-constant monomials, then*

$$M(F; \mathbb{F}_q) \geq \left\lfloor \frac{1}{d} (\log_4 q - 4 \log_4 \log_4 q)^{1/m} \right\rfloor.$$

Applying Theorem 1.1 to $F(x_1, x_2, \dots, x_k) = x_1 x_2 \dots x_k + 1$ (which is of both type I and type II), we get the following corollary immediately. In particular, it significantly improves the lower bound $\Theta((\log q)^{1/(k-1)})$ on the maximum size of k -Diophantine tuples over \mathbb{F}_q by Hammonds et. al [10].

Corollary 1.2. *Let $k \geq 2$ and let q be an odd prime power. There is an k -Diophantine tuple over \mathbb{F}_q with size at least $(\frac{1}{k} - o(1)) \log_4 q$, as $q \rightarrow \infty$.*

Interestingly, our approach provides a substantial improvement on the heuristic lower bound of $M(F; \mathbb{F}_q)$ given in inequality (1.1), whenever $k \geq 3$ and $F \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$ is a sparse polynomial. The constant factors in Theorem 1.1 and Corollary 1.2 are not optimal. Here we focus on improving the order of the magnitude of the lower bound and we do not attempt to optimize the constant factors. On the other hand, in the case $k = 2$, improving the constant factors in front of $\log q$ is of special interest; see [13] and references therein for more discussions.

2. CONSTRUCTIONS OF F -DIOPHANTINE SETS

Let q be an odd prime power. Let $F \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$ be a polynomial of type I or type II, with degree d . Write F in its monomial expansion as follows:

$$F = \sum_{i=1}^m a_i f_i + C,$$

where $a_i \in \mathbb{F}_q^*$ and f_i is a monomial of degree at least 1 for each $1 \leq i \leq m$, and $C \in \mathbb{F}_q$.

Let n be a positive integer to be determined such that $2 \leq n \leq q^{1/4}$. Consider the following collection of polynomials in $\mathbb{F}_q[x]$:

$$V := V(n) = \{F(x^{\theta_1}, x^{\theta_2}, \dots, x^{\theta_k}) : 1 \leq \theta_1, \theta_2, \dots, \theta_k \leq n\}.$$

Observe that

$$V \subset \left\{ \sum_{i=1}^m a_i x^{\alpha_i} + C : 1 \leq \alpha_1, \alpha_2, \dots, \alpha_m \leq dn \right\}. \quad (2.1)$$

Also, if F is of type I, then the constant term of each polynomial $g \in V$ is a non-zero square in \mathbb{F}_q ; if F is of type II, then the leading coefficient of each polynomial $g \in V$ is a non-zero square in \mathbb{F}_q . In both cases, it readily follows that the product of polynomials in any subset of V is not of the form ch^2 , where c is a non-square in \mathbb{F}_q , and h is a polynomial in $\mathbb{F}_q[x]$.

Let Y denote the collection of $y \in \mathbb{F}_q^*$ with order at least n , such that the set $\{g(y) : g \in V\}$ is contained in the set of squares in \mathbb{F}_q . Let $N = |Y|$ and let χ be the quadratic character in \mathbb{F}_q . We claim that

$$N \geq 2^{-|V|} \sum_{\substack{y \in \mathbb{F}_q^* \\ \text{ord } y \geq n}} \prod_{g \in V} \left(1 + \chi(g(y)) \right). \quad (2.2)$$

Indeed, if $y \notin Y$, then $g(y)$ is a non-square in \mathbb{F}_q for some $g \in V$, and thus such y does not contribute to the right-hand side of inequality (2.2). On the other hand, if $y \in Y$, then $\chi(g(y)) \in \{0, 1\}$ for each $g \in V$, and thus it contributes at most 1 to the right-hand side of inequality (2.2).

Expanding the product on the right-hand side of inequality (2.2) yields

$$\begin{aligned}
N &\geq 2^{-|V|} \sum_{\substack{y \in \mathbb{F}_q^* \\ \text{ord } y \geq n}} \sum_{W \subset V} \prod_{g \in W} \chi(g(y)) \\
&= 2^{-|V|} \sum_{W \subset V} \sum_{\substack{y \in \mathbb{F}_q^* \\ \text{ord } y \geq n}} \chi\left(\left(\prod_{g \in W} g\right)(y)\right) \\
&\geq -|Z| + 2^{-|V|} \sum_{W \subset V} \sum_{y \in \mathbb{F}_q} \chi\left(\left(\prod_{g \in W} g\right)(y)\right),
\end{aligned}$$

where $Z = \{0\} \cup \{y \in \mathbb{F}_q^* : \text{ord } y < n\}$. Since \mathbb{F}_q^* is a cyclic group, it is clear that $|Z| \leq n^2$.

We need to use Weil's bound for complete character sums (see for example [15, Theorem 5.41]), which we recall below.

Lemma 2.1. (Weil's bound) *Let χ be a multiplicative character of \mathbb{F}_q of order $k > 1$, and let $g \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an k -th power of a polynomial. Let s be the number of distinct roots of g in its splitting field over \mathbb{F}_q . Then for any $a \in \mathbb{F}_q$,*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(ag(x)) \right| \leq (s-1)\sqrt{q}.$$

We have mentioned that for each subset W of V , the product $\prod_{g \in W} g$ is not of the form ch^2 , where c is a non-square in \mathbb{F}_q , and h is a polynomial in $\mathbb{F}_q[x]$. Therefore, separating the contribution from $W = \emptyset$ and $W \neq \emptyset$, and applying Weil's bound, we further deduce that

$$\begin{aligned}
N &\geq -n^2 + 2^{-|V|} \sum_{W \subset V} \sum_{y \in \mathbb{F}_q} \chi\left(\left(\prod_{g \in W} g\right)(y)\right) \\
&\geq -n^2 + \frac{q}{2^{|V|}} - 2^{-|V|} \sum_{\substack{W \subset V \\ W \neq \emptyset}} \left(-1 + \sum_{g \in W} \deg(g)\right) \sqrt{q} \\
&= \frac{q}{2^{|V|}} - n^2 + \frac{\sqrt{q}(2^{|V|} - 1)}{2^{|V|}} - 2^{-|V|} \sqrt{q} \sum_{W \subset V} \sum_{g \in W} \deg(g). \tag{2.3}
\end{aligned}$$

Given inclusion (2.1), $\deg(g) \leq dn$ for each $g \in V$. Thus, a simple double-counting argument shows that

$$\sum_{W \subset V} \sum_{g \in W} \deg(g) = 2^{|V|-1} \sum_{g \in V} \deg(g) \leq 2^{|V|-1} |V| dn. \tag{2.4}$$

We conclude from the assumption $n \leq q^{1/4}$, inequality (2.3) and inequality (2.4) that

$$N \geq \frac{q}{2^{|V|}} - n^2 + \frac{\sqrt{q}(2^{|V|} - 1)}{2^{|V|}} - \frac{|V| dn \sqrt{q}}{2} \geq \frac{q}{2^{|V|}} - |V| dn \sqrt{q}.$$

Note that $|V| \leq (dn)^m$ from inclusion (2.1), thus

$$N \geq \frac{q}{2^{(dn)^m}} - (dn)^{m+1} \sqrt{q}. \tag{2.5}$$

Since $q \geq 257$, we have $\log_4 q > 4 \log_4 \log_4 q$. Set

$$n = \left\lfloor \frac{1}{d} (\log_4 q - 4 \log_4 \log_4 q)^{1/m} \right\rfloor.$$

Then we have $(dn)^m \leq \log_4 q - 4 \log_4 \log_4 q$ and thus

$$4^{(dn)^m} (dn)^{2m+2} \leq 4^{(dn)^m} (dn)^{4m} \leq \frac{q}{(\log_4 q)^4} \cdot (dn)^{4m} < q.$$

It follows from inequality (2.5) that

$$N \geq \frac{q}{2^{(dn)^m}} - (dn)^{m+1} \sqrt{q} > 0.$$

Note that $N > 0$ implies that $N \geq 1$, that is, there exists $y_0 \in \mathbb{F}_q^*$ with order at least n , such that the set $\{g(y_0) : g \in V\}$ is contained in the set of squares in \mathbb{F}_q . Let

$$A = \{y_0^1, y_0^2, \dots, y_0^n\};$$

then A is an F -Diophantine set over \mathbb{F}_q with $|A| = n$. This proves Theorem 1.1, as required.

Next, we give several remarks on our constructions.

Remark 2.2. Our constructions above in fact produce a *strong F -Diophantine set* A over \mathbb{F}_q in the sense that $F(a_1, a_2, \dots, a_k)$ is a square in \mathbb{F}_q whenever a_1, a_2, \dots, a_k are elements in A (not necessarily distinct), in the spirit of strong Diophantine tuples [8, 12]. In many cases, one can modify the definition of V in the above construction to obtain a slightly larger F -Diophantine set over \mathbb{F}_q .

Remark 2.3. In general, to construct a large F -Diophantine set over \mathbb{F}_q , we need to impose some assumptions on the polynomial F . Obviously, we have to assume that F is not of the form cG^2 , where c is a non-square in \mathbb{F}_q and $G \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$.

The assumption that F is of type I or type II made in the statement of Theorem 1.1 can be weakened. Indeed, as long as one can come up with a similar definition of V , and show that the product of polynomials in any subset of V is not of the form ch^2 (where c is a non-square in \mathbb{F}_q , and h is a polynomial in $\mathbb{F}_q[x]$), then one can modify the above proof to produce a large F -Diophantine set over \mathbb{F}_q .

As an illustration, consider a degree d homogeneous polynomial

$$F(x_1, x_2, \dots, x_k) = \sum_{i=1}^k c_i x_i^d \in \mathbb{F}_q[x_1, x_2, \dots, x_k]$$

with $k \geq 2$, where c_i is a non-zero square in \mathbb{F}_q for each $1 \leq i \leq k$. Note that such F is neither of type I nor type II. If we instead define

$$V := V(n) = \{F(x^{\theta_1}, x^{\theta_2}, \dots, x^{\theta_k}) : \theta_1, \theta_2, \dots, \theta_k \text{ are distinct elements in } \{1, 2, \dots, n\}\},$$

then the leading coefficient of each polynomial $g \in V$ is a non-zero square in \mathbb{F}_q . It follows that the product of polynomials in any subset of V is not of the form ch^2 , where c is a non-square in \mathbb{F}_q , and h is a polynomial in $\mathbb{F}_q[x]$. Thus, a similar argument as above shows that there is an F -Diophantine set A over \mathbb{F}_q with $|A| = n$, where

$$n \geq \left(\frac{1}{d} - o(1) \right) (\log_4 q)^{1/k}.$$

Note however in this case, if $\sum_{i=1}^k c_i$ is a non-square in \mathbb{F}_q , and d is even, then there is no strong F -Diophantine set over \mathbb{F}_q .

Remark 2.4. Recently, there have been a few papers devoted to the search for Diophantine tuples with additional properties. For example, looking for a Diophantine tuple with property $D(n)$ for multiple different n [2], or a rational Diophantine tuple with square elements [7]. In a similar flavor, it would be interesting to search for a large F -Diophantine set over a finite field with additional properties, and usually it is not hard to modify the above proof to achieve this purpose. For example, if we want to look for a large F -Diophantine set over \mathbb{F}_q with size n consisting of square elements, we can simply change the definition of V to

$$V := V(n) = \{F(x^{2\theta_1}, x^{2\theta_2}, \dots, x^{2\theta_k}) : 1 \leq \theta_1, \theta_2, \dots, \theta_k \leq n\}$$

and modify the above proof accordingly.

ACKNOWLEDGEMENTS

The second author was supported by the Institute for Basic Science (IBS-R029-C1). The authors thank Seoyoung Kim for helpful discussions. The authors are also grateful to anonymous referees for their valuable comments and corrections.

REFERENCES

- [1] A. Bérczes, A. Dujella, L. Hajdu, and S. Tengely. Finiteness results for F -Diophantine sets. *Monatsh. Math.*, 180(3):469–484, 2016.
- [2] K. Chakraborty, S. Gupta, and A. Hoque. Diophantine triples with the property $D(n)$ for distinct n 's. *Mediterr. J. Math.*, 20(1):Paper No. 31, 13, 2023.
- [3] S. D. Cohen. Clique numbers of Paley graphs. *Quaestiones Math.*, 11(2):225–231, 1988.
- [4] A. Dujella. On the size of Diophantine m -tuples. *Math. Proc. Cambridge Philos. Soc.*, 132(1):23–33, 2002.
- [5] A. Dujella. *Diophantine m -tuples and Elliptic Curves*, volume 79 of *Developments in Mathematics*. Springer, Cham, 2024.
- [6] A. Dujella and M. Kazalicki. Diophantine m -tuples in finite fields and modular forms. *Res. Number Theory*, 7(1):Paper No. 3, 24, 2021.
- [7] A. Dujella, M. Kazalicki, and V. Petričević. $D(n)$ -quintuples with square elements. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 115(4):Paper No. 172, 10, 2021.
- [8] A. Dujella and V. Petričević. Strong Diophantine triples. *Experiment. Math.*, 17(1):83–89, 2008.
- [9] K. Gyarmati. On a problem of Diophantus. *Acta Arith.*, 97(1):53–65, 2001.
- [10] T. Hammonds, S. Kim, S. J. Miller, A. Nigam, K. Onghai, D. Saikia, and L. M. Sharma. k -Diophantine m -tuples in finite fields. *Int. J. Number Theory*, 19(4):891–912, 2023.
- [11] B. He, A. Togbé, and V. Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, 371(9):6665–6709, 2019.
- [12] S. Kim, C. H. Yip, and S. Yoo. Diophantine tuples and multiplicative structure of shifted multiplicative subgroups. arXiv:2309.09124, 2023.
- [13] S. Kim, C. H. Yip, and S. Yoo. Paley-like quasi-random graphs arising from polynomials. arXiv:2405.09319, 2024.
- [14] S. Kim, C. H. Yip, and S. Yoo. Explicit constructions of Diophantine tuples over finite fields. *Ramanujan J.*, 65(1):163–172, 2024.
- [15] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [16] M. Sadek and N. El-Sissi. On large F -Diophantine sets. *Monatsh. Math.*, 186(4):703–710, 2018.
- [17] I. E. Shparlinski. On the number of Diophantine m -tuples in finite fields. *Finite Fields Appl.*, 90:Paper No. 102241, 7, 2023.

- [18] C. H. Yip. Multiplicatively reducible subsets of shifted perfect k -th powers and bipartite Diophantine tuples. *Acta Arith.*, to appear. arXiv:2312.14450.
- [19] C. H. Yip. On the clique number of Paley graphs of prime power order. *Finite Fields Appl.*, 77:Paper No. 101930, 2022.
- [20] C. H. Yip. Exact values and improved bounds on the clique number of cyclotomic graphs, 2023. arXiv:2304.13213.

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GA 30332, UNITED STATES

Email address: cyip30@gatech.edu

DISCRETE MATHEMATICS GROUP, INSTITUTE FOR BASIC SCIENCE, 55 EXPO-RO YUSEONG-GU, DAEJEON 34126, SOUTH KOREA

Email address: syool19@ibs.re.kr