ACTA ARITHMETICA
Online First version

Product representations of polynomials over finite fields

by

Hyunwoo Lee, Chi Hoi Yip and Semin Yoo

Abstract. Erdős, Sárközy, and Sós studied the asymptotics of the maximum size of a subset of $\{1,\dots,N\}$ such that it does not contain k distinct elements whose product is a perfect square. More generally, Verstraëte proposed a conjecture regarding the asymptotic behavior of the same quantity with the set of perfect squares replaced by the value set of a polynomial in $\mathbb{Z}[x]$. In this paper, we study a finite field analogue of Verstraëte's conjecture.

1. Introduction. Throughout the paper, let q be a prime power. Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_q^*$ be its multiplicative group. For a positive integer n, we use $\mathbb{Z}_n$ to denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$.

In 1995, Erdős, Sárközy, and Sós [2] initiated the study of product representations of squares. More precisely, for each integer $k \geq 2$ and positive integer N, let $F_k(N)$ be the maximum size of a subset A of $\{1,\dots,N\}$ such that it does not contain k distinct elements in A whose product is a perfect square. They showed that the asymptotic behavior of $F_k(N)$ strongly depends on the parity of k. Moreover, they determined the asymptotics of $F_k(N)$ for k even and $k = 3$. There have been several refinements to the bounds on $F_k(N)$ for even $k \geq 4$; see, for example, the work of Győri [6], Naor–Verstraëte [8], Pach [9, 10], and Pach–Vizer [12].

Granville and Soundararajan [4] studied a variant of this problem: they provided an asymptotic formula for the maximum size of a subset A of $\{1,\dots,N\}$ such that A does not contain an odd number of distinct elements whose product is a perfect square. Recently, Tao [15] made important progress on $F_k(N)$ for $k \geq 5$ odd.

More generally, in 2006, Verstraëte [16] studied product representations of polynomials. For a polynomial $h \in \mathbb{Z}[X]$, and positive integers k, N, let $F_k(N;h)$ be the maximum size of a subset A of $\{1,\dots,N\}$ such that it does

2020 *Mathematics Subject Classification*: Primary 11B30; Secondary 11T06, 05D05.
Key words and phrases: product representation, polynomial, finite field.
Received 23 January 2026.
Published online 22 September 2026.

not contain k distinct elements in A whose product is in the value set of h, that is, there are no distinct $a_1, \dots, a_k \in A$ such that $a_1 \cdots a_k = h(x)$ for some $x \in \mathbb{Z}$. He formulated the following conjecture:

CONJECTURE 1.1 ([16, Conjecture 3]). Let $h \in \mathbb{Z}[X]$ and let k be a positive integer. Then, for some positive constant $\rho = \rho(k, h)$ depending only on k and h, either $F_k(N; h)/N \to \rho$ or $F_k(N; h)/\pi(N) \to \rho$ as $N \to \infty$.

Verstraëte [16] made some partial progress towards Conjecture 1.1. In particular, he confirmed the conjecture for a family of polynomials. Recently, Fleiner, Juhász, Kövér, Pach, and Sándor [3] studied product representations of perfect cubes, that is, they studied the asymptotics of $F_k(N; x^3)$. In particular, they disproved Conjecture 1.1 by showing that

$$F_6(N; x^3) = (1 + o(1))\frac{N \log\log N}{\log N}.$$

Very recently, Pach and Sándor [11] studied a related variant in which one requires that the product of every nonempty subset of the given set is not a perfect d-th power. More precisely, let $\rho_d(N)$ denote the maximum size of a subset $A \subseteq \{1, \dots, N\}$ such that no product of a nonempty collection of distinct elements of A is a perfect d-th power. They proved that, for every integer $d \geq 2$,

$$\rho_d(N) = \sum_{j=1}^{d-1} \pi(N/j) + O_d(\pi(\sqrt{N})),$$

and moreover, when d is a prime power, they obtained the exact formula

$$\rho_d(N) = \sum_{j=1}^{d-1} \pi(N/j)$$

for all sufficiently large N.

Motivated by the results discussed above, in this paper, we study finite field analogues of Conjecture 1.1. Before stating our main results, we first introduce the finite field analogue of $F_k(N; h)$ and provide some additional background.

DEFINITION 1.2. For a positive integer k, a prime power q, and a nonconstant polynomial $h \in \mathbb{F}_q[x]$, define

$$F_k(q; h) := \max\{|A| : A \subset \mathbb{F}_q^* \text{ and } A \text{ satisfies } (\star)\},$$

where $(\star)$ denotes that for all distinct $a_1, \dots, a_k \in A$ and all $x \in \mathbb{F}_q$, $a_1 \cdots a_k \neq h(x)$.

We remark that for some special polynomials h, the quantity $F_k(q; h)$ has been well-studied. For example, if q is an odd prime power, α is a nonsquare in $\mathbb{F}_q$, and $h(x) = \alpha x^2 - 1$, then $F_k(q; h)$ is "essentially" the same as

the maximum size of a k-Diophantine tuple over $\mathbb{F}_q$ [17]. See for example [5, 14, 17] for further discussions. Recall that if q is an odd prime power, we say $A \subset \mathbb{F}_q^*$ is a *k-Diophantine tuple over* $\mathbb{F}_q$ if $a_1a_2\cdots a_k+1$ is a square in $\mathbb{F}_q$ for any distinct $a_1, \dots, a_k \in A$. If $A \subset \mathbb{F}_q^*$ is a *k-Diophantine tuple over* $\mathbb{F}_q$ with the additional property that $a_1 \cdots a_k \neq -1$ for any distinct $a_1, \dots, a_k \in A$, then A satisfies $(\star)$ in Definition 1.2. Conversely, if A satisfies $(\star)$ in Definition 1.2, then for any distinct $a_1, \dots, a_k \in A$, we have $a_1 \cdots a_k \notin h(\mathbb{F}_q)$, and thus $a_1 \cdots a_k + 1$ is a square in $\mathbb{F}_q^*$; thus A is necessarily a k-Diophantine tuple over $\mathbb{F}_q$.

In the spirit of Conjecture 1.1, our goal is to determine an asymptotic formula for $F_k(q; h)$, under the natural assumption that q is large compared to k and the degree of h. To state our main theorem, we define one more notion. Let k, n be positive integers with $k \geq 2$. For a subset $B \subset \mathbb{Z}_n$, its *k-fold sumset* is

$$kB := \{b_1 + \cdots + b_k : b_i \in B \text{ for } 1 \leq i \leq k\}.$$

For each $s \in \mathbb{Z}_n$, we define

$$m(k, n; s) := \max\{|B| : B \subset \mathbb{Z}_n,\ s \notin kB\},$$

that is, $m(k, n; s)$ is the maximum size of a subset B of $\mathbb{Z}_n$ such that the k-fold sumset kB avoids s. Observe that if λ is a unit in $\mathbb{Z}_n$, that is, $\gcd(\lambda, n) = 1$, then $m(k, n; s) = m(k, n; \lambda s)$. We now state our main theorem.

THEOREM 1.3. *Let $k \geq 2$ be an integer, q be a prime power, and $h \in \mathbb{F}_q[x]$ be a non-constant polynomial. Let ℓ be the largest positive integer such that $h = Cf^\ell$ for some $C \in \mathbb{F}_q^*$ and $f \in \mathbb{F}_q[x]$. Let $n = \gcd(\ell, q-1)$ and let H be the subgroup of $\mathbb{F}_q^*$ of index n. Let g be a generator of $\mathbb{F}_q^*$ and let s be the unique integer in $\{0, 1, \dots, n-1\}$ such that $C \in g^sH$. Then*

$$F_k(q; h) = \frac{m(k, n; s)}{n} \cdot q + O(\sqrt{q}),$$

where the implied constant of the error term depends only on k and the degree of h.

The proof of our main theorem is given in Section 2. In fact, our proof shows a stronger conclusion: if $m(k, n; s) > 0$, then extremal sets are essentially unions of $m(k, n; s)$ cosets of H. We refer to Remark 2.5 for a precise statement.

We make a few remarks on the theorem below.

REMARK 1.4. (1) The main term in Theorem 1.3 is independent of the chosen factorization of h and of the chosen generator g.

Indeed, suppose we have two factorizations $h = Cf^\ell = \widetilde{C}\widetilde{f}^\ell$, and two generators g and $\widetilde{g}$. Let $s, s' \in \{0, 1, \dots, n-1\}$ such that $C \in g^sH$ and $\widetilde{C} \in \widetilde{g}^{\widetilde{s}}H$. Then C and $\widetilde{C}$ are in the same coset of H, and thus $g^sH = \widetilde{g}^{\widetilde{s}}H$.

Assume $\widetilde{g} = g^u$, where $\gcd(u, q-1) = 1$. It follows that $g^s/\widetilde{g}^{\widetilde{s}} = g^{s-u\widetilde{s}} \in H$, that is, $s \equiv u\widetilde{s} \pmod{n}$. Since $\gcd(u, n) = 1$, we have $m(k, n; s) = m(k, n; s')$ by the observation before the theorem.

(2) When $m(k, n; s) > 0$, Theorem 1.3 yields

$$F_k(q; h) = \frac{m(k, n; s)}{n} \cdot q + O(\sqrt{q}),$$

so in this case $F_k(q; h)$ has a linear main term in q. In particular, this confirms a finite-field analogue of Verstraëte's conjecture (Conjecture 1.1).

The condition $m(k, n; s) > 0$ can be characterized by the following equivalence:

$$n \mid k \text{ and } s = 0 \iff m(k, n; s) = 0.$$

Suppose that $n \mid k$ and $s = 0$, B is nonempty, let $b \in B$. Then $kb \in kB$. Since $n \mid k$, $kb \equiv 0 \pmod{n}$, so $0 \in kB$, a contradiction. Thus $B = \varnothing$, so $m(k, n; 0) = 0$. Conversely, we prove the contrapositive. Assume that $n \nmid k$ or $s \neq 0$. We claim that $m(k, n; s) > 0$. If $s \neq 0$, take $B = \{0\}$. Then $kB = \{0\}$, so $s \notin kB$, and hence $m(k, n; s) \geq 1$. Now assume that $s = 0$ and $n \nmid k$. Take $B = \{1\}$. Then $kB = \{k\}$, and since $n \nmid k$ we have $k \not\equiv 0 \pmod{n}$, so $0 \notin kB$. Thus $m(k, n; 0) \geq 1$. Therefore, in either case, we have $m(k, n; s) > 0$.

(3) When $m(k, n; s) = 0$, Theorem 1.3 implies that $F_k(q; h) = O(\sqrt{q})$. In fact, the $O(\sqrt{q})$ bound can sometimes be sharp by considering the following example.

Let $q = p^2$ with p odd, and consider the quadratic polynomial $h(x) = \alpha x^2 - 1 \in \mathbb{F}_q[x]$ for some nonsquare $\alpha \in \mathbb{F}_q^*$. Since $\ell = 1$, $n = \gcd(\ell, q-1) = 1$. Thus, $m(k, 1; 0) = 0$.

Let u be a generator of $\mathbb{F}_p^*$, so that $\mathbb{F}_p^* = \langle u \rangle$ has order $p-1$ and $-1 = u^{(p-1)/2}$. Set

$$t := \left\lfloor \frac{p-1}{2k} \right\rfloor + 1 \quad \text{and} \quad A := \{1, u, \ldots, u^{t-1}\} \subset \mathbb{F}_p^* \subset \mathbb{F}_{p^2}^*.$$

Then $|A| = t = \Theta(p) = \Theta(\sqrt{q})$. Moreover, for any k distinct elements $a_1, \ldots, a_k \in A$, denoting $a_j = u^{b_j}$ with $b_j \in \{0, 1, \ldots, t-1\}$, we have $a_1 \cdots a_k = u^{b_1 + \cdots + b_k}$. Since the exponents $b_1, \ldots, b_k$ are distinct and lie in $\{0, 1, \ldots, t-1\}$, for $k \geq 2$,

$$b_1 + \cdots + b_k \leq (t-1) + \cdots + (t-k) = k(t-1) - \frac{k(k-1)}{2} < \frac{p-1}{2}.$$

and so $b_1 + \cdots + b_k \not\equiv (p-1)/2 \pmod{p-1}$. Thus, we have $a_1 \cdots a_k \neq -1$.

Note that $\mathbb{F}_p^* \subset (\mathbb{F}_{p^2}^*)^2$. Indeed, $\mathbb{F}_p^* = \langle g^{p+1} \rangle$ for some generator g of $\mathbb{F}_{p^2}^*$ since the order of g^{p+1} is $p-1$. Since $p+1$ is even, the generator g^{p+1} of $\mathbb{F}_p^*$ is a square in $\mathbb{F}_{p^2}^*$. Moreover, since $\mathbb{F}_p$ is a subfield of $\mathbb{F}_{p^2}$, for any distinct $a_1, \ldots, a_k \in A$ we have $a_1 \cdots a_k + 1 \in \mathbb{F}_p \subset (\mathbb{F}_{p^2}^*)^2 \cup \{0\}$. Thus, for any $x \neq 0$,

we have $a_1 \cdots a_k + 1 \neq \alpha x^2$. Together with $a_1 \cdots a_k \neq -1$, which rules out the case $x = 0$, we conclude that $a_1 \cdots a_k \neq h(x)$ for all $x \in \mathbb{F}_{p^2}$. It follows that $F_k(q; h) = \Theta(\sqrt{q})$.

In general, it seems challenging to determine the asymptotic behavior of $F_k(q; h)$, and we believe that establishing the full analogue of Conjecture 1.1 over finite fields is completely out of reach. As an example, consider the same h as above, where q is an odd prime power but not necessarily a square. As discussed in the introduction, in this case, $F_k(q; h)$ is upper bounded by the maximum size of a k-Diophantine tuple over $\mathbb{F}_q$. However, the best-known general lower bound on the latter quantity is $\Omega(\log q)$, while the best-known upper bound is $O(\sqrt{q})$; see [17] and the references therein.

(4) The remarks above show that $F_k(q; h)$ could be of the order $\Theta(q)$ or $\Theta(\sqrt{q})$, but cannot be of the order $\Theta(q^\theta)$ for $1/2 < \theta < 1$. A natural question arises: is it possible to construct h and q such that $F_k(q; h)$ is $\Theta(q^\theta)$ for some $0 < \theta < 1/2$? We conjecture that the answer is positive if $\theta = 1/m$ for each positive integer $m \geq 3$, but we are not able to prove it. Nevertheless, below, we suggest a plausible construction.

Let $m \geq 3$ be a positive integer. Let $q = p^m$ with p a prime such that $p \equiv 1 \pmod{m}$. Note that $\mathbb{F}_p$ is the largest subfield of $\mathbb{F}_q$ contained in $(\mathbb{F}_q)^m$. To see that, if $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_q$ such that it is contained in $(\mathbb{F}_q)^m$, then we must have $r \mid m$ and $m \mid \frac{q-1}{p^r-1}$; however, since $p \equiv 1 \pmod{m}$, we have

$$\frac{q-1}{p^r-1} = \sum_{j=0}^{m/r-1} p^{jr} \equiv \frac{m}{r} \pmod{m},$$

that is, $r = 1$.

Consider the polynomial $h(x) = \alpha x^m - 1 \in \mathbb{F}_q[x]$ for some $\alpha \in \mathbb{F}_q \setminus (\mathbb{F}_q)^m$. Since $\ell = 1$, $n = \gcd(\ell, q-1) = 1$. Thus, $m(k, 1; 0) = 0$. By a similar argument to that in (3), we can pick $A \subset \mathbb{F}_p$ with $|A| \geq p/(2k)$ so that for any distinct $a_1, \ldots, a_k \in A$, we have $a_1 a_2 \cdots a_k \neq h(x)$ for any $x \in \mathbb{F}_q$. This shows that $F_k(q; h) = \Omega(q^{1/m})$. We suspect that in this setting, we actually have $F_k(q; h) = \Theta(q^{1/m})$.

Finally, in Section 3, we estimate $m(k, n; s)$ for each $s \in \mathbb{Z}_n$, where $k \geq 2$ and n are positive integers. In particular, when $\gcd(k, n) = 1$, we determine $m(k, n; s)$ for every $s \in \mathbb{Z}_n$.

2. Proof of Theorem 1.3. In this section, we prove Theorem 1.3. We first recall Weil's bound for multiplicative character sums; see, for example [7, Theorem 5.41].

LEMMA 2.1 (Weil's bound). *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $d > 1$, and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that*

is not a d-th power of a polynomial. Let n be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for any $a \in \mathbb{F}_q$,

$$\Big| \sum_{x \in \mathbb{F}_q} \chi(af(x)) \Big| \le (n-1)\sqrt{q}.$$

The following lemma is a generalization of [5, Theorem 10] proved by Gyarmati, where she established a similar result over prime fields. We include a short proof for the sake of completeness.

LEMMA 2.2. *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $1 < m < q$. Assume that for every integer $d > 1$ with $d \,|\, (q-1)$, the polynomial f is not a constant multiple of a d-th power in $\mathbb{F}_q[x]$. Let $A, B \subset \mathbb{F}_q^*$ and assume that*

$$|A|\,|B| > q\left(\frac{q-1}{q-m}\right)^2 (m-1)^2.$$

Then there exist $a \in A$, $b \in B$, and $x \in \mathbb{F}_q$ such that $ab = f(x)$.

Proof. Define

$$N := \#\{(a,b,x) \in A \times B \times \mathbb{F}_q : ab = f(x)\}.$$

Let χ_0 be the trivial character. We extend every (multiplicative) character χ on $\mathbb{F}_q^*$ to $\mathbb{F}_q$ by setting $\chi(0) = 0$. Note that, for $y \in \mathbb{F}_q^*$,

$$\mathbf{1}_{\{y=1\}} = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(y),$$

where $\widehat{\mathbb{F}_q^*}$ is the set of characters on $\mathbb{F}_q^*$. Then

$$N = \sum_{a \in A} \sum_{b \in B} \sum_{x \in \mathbb{F}_q} \mathbf{1}_{\{ab=f(x)\}} = \frac{1}{q-1} \sum_{a \in A} \sum_{b \in B} \sum_{x \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(a^{-1}b^{-1}f(x)).$$

Let r be the number of distinct $\mathbb{F}_q$-roots of $f(x)$. Then

$$(q-1)N - (q-r)|A|\,|B| = \sum_{a \in A} \sum_{b \in B} \sum_{x \in \mathbb{F}_q} \sum_{\chi \neq \chi_0} \chi(a^{-1}b^{-1}f(x)). \tag{2.1}$$

By the orthogonality relation,

$$\begin{aligned} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \Big| \sum_{a \in A} \chi(a^{-1}) \Big|^2 &= \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \sum_{a, \widetilde{a} \in A} \chi(a^{-1}) \overline{\chi(\widetilde{a}^{-1})} = \sum_{a, \widetilde{a} \in A} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(a^{-1}\widetilde{a}) \\ &= (q-1)|A|, \end{aligned}$$

and similarly for B. This, together with the Cauchy–Schwarz inequality and

Weil's bound, implies that

$$\begin{aligned}\Big|\sum_{a\in A}\sum_{b\in B}\sum_{x\in\mathbb{F}_q}\sum_{\chi\neq\chi_0}\chi(a^{-1}b^{-1}f(x))\Big| &\\ \le \sum_{\chi\neq\chi_0}\Big|\sum_{a\in A}\chi(a^{-1})\sum_{b\in B}\chi(b^{-1})\Big|\Big|\sum_{x\in\mathbb{F}_q}\chi(f(x))\Big| &\\ \le \sqrt{\sum_{\chi\neq\chi_0}\Big|\sum_{a\in A}\chi(a^{-1})\Big|^2}\sqrt{\sum_{\chi\neq\chi_0}\Big|\sum_{b\in B}\chi(b^{-1})\Big|^2}(m-1)\sqrt{q} &\\ \le (m-1)(q-1)\sqrt{q|A|\,|B|}.\end{aligned}$$

Thus (2.1) implies that

$$\big|(q-1)N-(q-r)|A|\,|B|\big| \le (m-1)(q-1)\sqrt{q|A|\,|B|}.$$

Since $q-r\ge q-m$, we have

$$(q-1)N \ge (q-m)|A|\,|B| - (m-1)(q-1)\sqrt{q|A|\,|B|}.$$

Since

$$|A|\,|B| > q\bigg(\frac{q-1}{q-m}\bigg)^2(m-1)^2,$$

we have $N>0$, as required. ∎

Using Lemma 2.2, we have the following corollary.

COROLLARY 2.3. *Let $f(x)\in\mathbb{F}_q[x]$ be a polynomial of degree $1\le m<q$. Assume that $f(x)\in\mathbb{F}_q[x]$ is not a constant multiple of a d-th power of a polynomial in $\mathbb{F}_q[x]$ for any divisor d of $q-1$ with $d\ge 2$. Let $A_1,\dots,A_k$ be subsets of $\mathbb{F}_q^*$ (not necessarily distinct). If $|A_i|\ge 8C_m\sqrt{q}+2k+2$ for each $1\le i\le k$, where*

$$C_m := (m-1)\frac{q-1}{q-m},$$

then there exist distinct elements $a_1,\dots,a_k$ such that $a_i\in A_i$ for $1\le i\le k$, and

$$a_1\cdots a_k = f(x_0)$$

for some $x_0\in\mathbb{F}_q$.

Proof. If $m=1$, then f is a bijection on $\mathbb{F}_q$, thus $f(\mathbb{F}_q)=\mathbb{F}_q$. We choose $a_1\in A_1$ arbitrarily, and for $2\le j\le k$ choose $a_j\in A_j\setminus\{a_1,\dots,a_{j-1}\}$, which is possible since at step j we exclude at most $j-1\le k-1$ elements. Set $y:=a_1\cdots a_k\in\mathbb{F}_q^*$. Since $f(\mathbb{F}_q)=\mathbb{F}_q$, there exists $x_0\in\mathbb{F}_q$ such that $f(x_0)=y$, as required.

Next, assume that $m\ge 2$. We consider two cases.

CASE 1: $k=2$. Choose disjoint subsets $X'\subset A_1$ and $Y'\subset A_2$ with

$$|X'|\ge\lfloor|A_1|/2\rfloor \quad\text{and}\quad |Y'|\ge\lceil|A_2|/2\rceil.$$

Then $X' \cap Y' = \varnothing$, and

$$|X'|\,|Y'| \geq \left\lfloor \frac{|A_1|}{2} \right\rfloor \cdot \left\lceil \frac{|A_2|}{2} \right\rceil \geq \frac{|A_1|-1}{2} \cdot \frac{|A_2|}{2} \geq \frac{(8C_m\sqrt{q}+2k+1)(8C_m\sqrt{q}+2k+2)}{4}.$$

In particular, since $k \geq 2$, the right-hand side is at least $16C_m^2 q$, and so

$$|X'|\,|Y'| > 16C_m^2 q \geq q\left(\frac{q-1}{q-m}\right)^2 (m-1)^2.$$

By applying Lemma 2.2 to f and (X', Y'), we have $a_1 \in X'$, $a_2 \in Y'$, and $x_0 \in \mathbb{F}_q$ such that $a_1 a_2 = f(x_0)$. In particular, $a_1 \neq a_2$ since $X' \cap Y' = \varnothing$.

Case 2: $k \geq 3$. We choose $a_1 \in A_1$ arbitrarily, and for $2 \leq j \leq k-2$ choose $a_j \in A_j \setminus \{a_1, \ldots, a_{j-1}\}$, which is possible since at step j we exclude at most $j-1 \leq k-3$ elements. Let $c := (a_1 \cdots a_{k-2})^{-1} \in \mathbb{F}_q^*$ and define

$$X := A_{k-1} \setminus \{a_1, \ldots, a_{k-2}\}, \quad Y := A_k \setminus \{a_1, \ldots, a_{k-2}\}.$$

Then

$$|X| \geq |A_{k-1}| - (k-2) \geq 8C_m\sqrt{q} + k + 2,$$
$$|Y| \geq |A_k| - (k-2) \geq 8C_m\sqrt{q} + k + 2.$$

Choose disjoint subsets $X_0 \subset X$ and $Y_0 \subset Y$ such that

$$|X_0| \geq \lfloor |X|/2 \rfloor \quad \text{and} \quad |Y_0| \geq \lceil |Y|/2 \rceil.$$

In particular, $|X_0| \geq (|X|-1)/2 > 4C_m\sqrt{q}$ and $|Y_0| \geq |Y|/2 > 4C_m\sqrt{q}$ and thus

$$|X_0|\,|Y_0| > 16C_m^2 q \geq q\left(\frac{q-1}{q-m}\right)^2 (m-1)^2.$$

Moreover, since $c \in \mathbb{F}_q^*$, the polynomial cf is not a constant multiple of a d-th power for any $d \,|\, (q-1)$ with $d > 1$. Thus, by applying Lemma 2.2 to cf and (X_0, Y_0), there exist $a_{k-1} \in X_0$, $a_k \in Y_0$, and $x_0 \in \mathbb{F}_q$ such that $a_{k-1}a_k = cf(x_0)$. Therefore, $a_1 \cdots a_k = f(x_0)$ with $a_1, \ldots, a_k$ distinct, as required. ∎

Now we are ready to present the proof of Theorem 1.3.

Proof of Theorem 1.3. We first prove an upper bound for $F_k(q; h)$. Let $A \subset \mathbb{F}_q^*$ be such that $a_1 \cdots a_k \neq Cf(x)^\ell$ for any distinct $a_1, \ldots, a_k \in A$ and for any $x \in \mathbb{F}_q$. Then we decompose

$$A = \bigcup_{i=0}^{n-1} A_i,$$

where $A_i = A \cap g^i H$ for $0 \leq i \leq n-1$.

Note that $H = \langle g^n \rangle = \langle g^\ell \rangle = (\mathbb{F}_q^*)^\ell$ and $|H| = (q-1)/n$. Therefore, for each $a \in A_i \subset g^i H$, we may write $a = g^i x^\ell$ for some $x \in \mathbb{F}_q^*$, and choosing one such x for each $a \in A_i$ gives a set $B_i \subset \mathbb{F}_q^*$ with $|B_i| = |A_i|$ and $A_i = \{g^i x^\ell : x \in B_i\}$. Let $M := M(k,m)$ be a constant such that Corollary 2.3 applies whenever $|A_i| \geq M\sqrt{q}$ for all i (for example, one may take $M = 8C_m + 2k + 2$). Define

$$B = \{0 \leq i \leq n-1 \colon |A_i| \geq M\sqrt{q}\} \subset \mathbb{Z}_n.$$

Next, we prove the following key claim.

Claim 2.4. *$s \notin kB$.*

Proof. Suppose that $s \in kB$. Then there exist indices $i_1, \ldots, i_k \in B$ (not necessarily distinct) such that

$$i_1 + \cdots + i_k \equiv s \pmod{n}.$$

Let $i_1 + \cdots + i_k = tn + s$ for some $t \in \mathbb{Z}$. Note that there exists an integer t' such that

$$(g^{t'})^\ell = \frac{g^{tn+s}}{C}. \tag{2.2}$$

Indeed, since $C \in g^s H$, we may write $C = g^s h_0$ for some $h_0 \in H$. Then

$$\frac{g^{tn+s}}{C} = \frac{g^{tn}}{h_0} \in H.$$

Since the index of H is n, every element of H is an ℓ-th power in $\mathbb{F}_q^*$. Thus, there exists $u \in \mathbb{F}_q^*$ with $u^\ell = g^{tn+s}/C$, and write $u = g^{t'}$. This gives the required t'.

Since ℓ is chosen maximal in the representation $h = Cf^\ell$, the polynomial f is not a constant multiple of a d-th power in $\mathbb{F}_q[x]$ for any integer $d \,|\, (q-1)$ with $d > 1$. Also, since $|B_i| = |A_i| \geq M\sqrt{q}$ for each i, by Corollary 2.3 applied to the polynomial $f(x)/g^{t'}$ and sets $B_{i_1}, \ldots, B_{i_k}$, there exist distinct $x_1, \ldots, x_k$, where $x_j \in B_{i_j}$ for $1 \leq j \leq k$, such that

$$x_1 \cdots x_k = \frac{f(x_0)}{g^{t'}}$$

for some $x_0 \in \mathbb{F}_q$. Thus, by (2.2),

$$g^{i_1} x_1^\ell g^{i_2} x_2^\ell \cdots g^{i_k} x_k^\ell = g^{tn+s}(x_1 \cdots x_k)^\ell = C(f(x_0))^\ell.$$

Note that $g^{i_j} x_j^\ell \in A_{i_j} \subset A$ for each $1 \leq j \leq k$. Moreover, these k elements are distinct. Indeed, let $1 \leq j_1, j_2 \leq k$ with $j_1 \neq j_2$. If $i_{j_1} \neq i_{j_2}$, then $g^{i_{j_1}} x_{j_1}^\ell$ and $g^{i_{j_2}} x_{j_2}^\ell$ are in different cosets of H so they are different; if $i_{j_1} = i_{j_2}$, then since $x_{j_1} \neq x_{j_2}$ by the construction of $B_{i_{j_1}}$, we know $g^{i_{j_1}} x_{j_1}^\ell \neq g^{i_{j_2}} x_{j_2}^\ell$. This contradicts the defining property of A. Thus, $s \notin kB$. ∎

Thus, by the definition of $m(k,n;s)$, we obtain $|B| \le m(k,n;s)$. We conclude that

$$|A| = \sum_{i\in B}|A_i| + \sum_{i\notin B}|A_i| \le |B|\cdot\frac{q-1}{n} + O(\sqrt{q}) \le \frac{m(k,n;s)}{n}\cdot q + O(\sqrt{q}),$$

as required.

Now, we obtain a lower bound of $F_k(q;h)$. Let $B_0 \subset \mathbb{Z}_n$ with $|B_0| = m(k,n;s)$ and $s \notin kB_0$. Define

$$A_0 := \bigcup_{i\in B_0} g^i H \subset \mathbb{F}_q^*.$$

Then

$$|A_0| = |B_0|\,|H| = m(k,n;s)\cdot\frac{q-1}{n}.$$

To finish our proof, we show that for any distinct $a_1,\dots,a_k \in A_0$ and any $x \in \mathbb{F}_q$, we have $a_1\cdots a_k \ne h(x)$. For each $1 \le j \le k$, choose $i_j \in B_0$ such that $a_j \in g^{i_j}H$. Then $a_1\cdots a_k \in g^{i_1+\cdots+i_k}H$, so there exists $t \in kB_0$ such that $a_1\cdots a_k \in g^tH$. Note that $h(x) \in g^sH$ for all $x \in \mathbb{F}_q$. Since $s \notin kB_0$, we have $t \ne s$ in $\mathbb{Z}_n$, and therefore $g^tH \ne g^sH$. This implies $a_1\cdots a_k \ne h(x)$ for all $x \in \mathbb{F}_q$. ∎

Remark 2.5. Our proof shows that if $A \subset \mathbb{F}_q^*$ satisfies $(\star)$ for h in Definition 1.2 and satisfies

$$|A| \ge \frac{m(k,n;s)}{n}\cdot q - O(\sqrt{q}),$$

then the set A consists of $m(k,n;s)$ cosets of H, up to $O(\sqrt{q})$ exceptional elements. More precisely, there exists a set $B_0 \subset \mathbb{Z}_n$ with $|B_0| = m(k,n;s)$ and $s \notin kB_0$ such that

$$\Big|A \mathbin{\triangle} \bigcup_{i\in B_0} g^iH\Big| = O(\sqrt{q}).$$

In other words, if $m(k,n;s) > 0$, then extremal sets are essentially unions of $m(k,n;s)$ cosets of H.

Remark 2.6. We finally remark that the natural k-set analogues of Lemma 2.2 and Corollary 2.3 do not hold. More precisely, if one replaces the hypotheses by $\prod_{i\in[k]}|A_i| \ge \Omega(qm^k)$ and $|A_i| \ge \Omega(q^{1/k})$, respectively, then the resulting statements fail in general. Here, the implicit constants only depend on $m = \deg f$ and k. Assume for contradiction that these analogues hold. Then, by following the proof of Theorem 1.3, one can deduce that

$$F_k(q;h) = \frac{m(k,n;s)}{n}\cdot q + O(q^{1/k}).$$

However, Remark 1.4(3) guarantees that there exists a polynomial h and infinitely many prime powers q for which $m(k,n;s)=0$, while $F_k(q;h)=\Theta(\sqrt{q})$ for each fixed $k\geq 2$. Hence, taking k strictly larger than two yields a contradiction.

3. An estimate for $m(k,n;s)$. In this section, we estimate $m(k,n;s)$ for each $s\in\mathbb{Z}_n$, where $k\geq 2$ and n are positive integers. We obtain an upper bound from Bajnok's work [1] and a lower bound by a proper explicit construction.

PROPOSITION 3.1. *Let $k\geq 2$ and n be positive integers. Then, for each $s\in\mathbb{Z}_n$, we have*

$$\max_{d\mid n}\left(\left\lfloor\frac{d-1-\gcd(d,k)}{k}\right\rfloor+1\right)\frac{n}{d}\leq m(k,n;s)\leq\max_{d\mid n}\left(\left\lfloor\frac{d-2}{k}\right\rfloor+1\right)\frac{n}{d}.$$

Proof. The upper bound is immediate from [1, Theorem 6]. Let $\chi(\mathbb{Z}_n,k)$ be the minimum value of m, if exists, for which the k-fold sumset of every m-subset of $\mathbb{Z}_n$ equals $\mathbb{Z}_n$ itself. Then, every subset $B\subset\mathbb{Z}_n$ with $|B|\geq\chi(\mathbb{Z}_n,k)$ satisfies $kB=\mathbb{Z}_n$, so $m(k,n;s)\leq\chi(\mathbb{Z}_n,k)-1$. The formula for $\chi(\mathbb{Z}_n,k)-1$ can be found in [1, Theorem 6], which coincides with the upper bound.

We now consider a lower bound of $m(k,n;s)$. Fix a divisor $d\,|\,n$ and let $K:=d\mathbb{Z}_n\leq\mathbb{Z}_n$ be the subgroup of index d. Let $\pi:\mathbb{Z}_n\to\mathbb{Z}_n/K\cong\mathbb{Z}_d$ be the canonical projection. Set $r:=\gcd(d,k)$ and define

$$t:=\left\lfloor\frac{d-1-r}{k}\right\rfloor+1.$$

Choose a subset $T\subset\mathbb{Z}_d$ of size t,

$$T=\{a,a+1,\ldots,a+t-1\}\subset\mathbb{Z}_d,$$

for some $a\in\mathbb{Z}_d$. Let $B:=\pi^{-1}(T)\subset\mathbb{Z}_n$. Then $|B|=|T|\,|K|=tn/d$.

We claim that $s\notin kB$ for a suitable choice of a. Indeed, since π is a homomorphism, we have $\pi(kB)=kT$. In addition, since T is an interval of length t, we have

$$kT=\{ka,ka+1,\ldots,ka+k(t-1)\},$$

so $|kT|=k(t-1)+1\leq d-r$ by the definition of t. Let

$$F:=\pi(s)-\{0,1,\ldots,k(t-1)\}\subset\mathbb{Z}_d.$$

Then $\pi(s)\notin kT$ is equivalent to $ka\notin F$.

Now, the set of possible values of ka as a varies is exactly $k\mathbb{Z}_d=r\mathbb{Z}_d$. Since $r\mathbb{Z}_d=\{0,r,2r,\ldots,d-r\}$, any interval that contains all of $r\mathbb{Z}_d$ must have length at least $d-r+1$. Thus, F cannot contain all elements of $r\mathbb{Z}_d$ since $|F|=k(t-1)+1\leq d-r$. So, we may choose $y\in r\mathbb{Z}_d\setminus F$. Since

$y \in r\mathbb{Z}_d = k\mathbb{Z}_d$, there exists $a \in \mathbb{Z}_d$ such that $ka = y$. For this choice of a, we have $ka \notin F$, hence $\pi(s) \notin kT$, and therefore $s \notin kB$. ∎

When $\gcd(k, n) = 1$, we obtain the following corollary immediately.

COROLLARY 3.2. *Let $k \geq 2$ and n be positive integers. If $\gcd(k, n) = 1$, then for each $s \in \mathbb{Z}_n$, we have*

$$m(k, n; s) = \max_{d|n} \left(\left\lfloor \frac{d-2}{k} \right\rfloor + 1 \right) \frac{n}{d}. \tag{3.1}$$

When $s = 0$, this quantity $m(k, n; s)$ asks for the maximum size of a *k-zero-free subset* of $\mathbb{Z}_n$. It was first studied by Sargsyan [13]. He was not able to determine the exact values of $m(k, n; 0)$ in general, although several lower and upper bounds are given in [13, Section 3]. Instead, he determined an exact formula for $m(k, n; 0)$ when $\gcd(k, n) = 1$. In this case, his result can also yield the same formula for $m(k, n; s)$, described in Corollary 3.2.

Indeed, for $t \in \mathbb{Z}_n$ we have $k(B + t) = kB + kt$. Since $\gcd(k, n) = 1$, multiplication by k is a bijection on $\mathbb{Z}_n$, so for any s we can choose $t \equiv -k^{-1}s \pmod{n}$. Note that $0 \notin k(B + t)$ is equivalent to $-kt = s \notin kB$. Since $|B| = |B + t|$, $m(k, n; s) = m(k, n; 0)$ for all $s \in \mathbb{Z}_n$. When $s = 0$, [13, Corollary in Section 3] gives an exact formula of $m(k, n; 0)$, which coincides with equation (3.1).

Acknowledgements. The authors thank Péter Pál Pach for helpful discussions. They also thank the anonymous referees for their valuable comments and suggestions. C. H. Yip thanks the Institute for Basic Science for hospitality during his visit, when part of this project was discussed.

Funding. H. Lee was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) No. RS-2023-00210430, and the Institute for Basic Science (IBS-R029-C4). C. H. Yip was supported in part by an NSERC fellowship. S. Yoo was supported by the Institute for Basic Science (IBS-R029-C1).

References

[1] B. Bajnok, *The h-critical number of finite Abelian groups*, Unif. Distrib. Theory 10 (2015), 93–115.

[2] P. Erdős, A. Sárközy, and V. T. Sós, *On product representations of powers. I*, Eur. J. Combin. 16 (1995), 567–588.

[3] Z. G. Fleiner, M. H. Juhász, B. Kövér, P. P. Pach, and C. Sándor, *Product representation of perfect cubes*, Eur. J. Combin. 134 (2026), art. 104342, 25 pp.

[4] A. Granville and K. Soundararajan, *The spectrum of multiplicative functions*, Ann. of Math. (2) 153 (2001), 407–470.

[5] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (2001), 53–65.

[6] E. Győri, *C_6-free bipartite graphs and product representation of squares*, Discrete Math. 165/166 (1997), 371–375.
[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge Univ. Press, Cambridge, 1997.
[8] A. Naor and J. Verstraëte, *Parity check matrices and product representations of squares*, Combinatorica 28 (2008), 163–185.
[9] P. P. Pach, *Generalized multiplicative Sidon sets*, J. Number Theory 157 (2015), 507–529.
[10] P. P. Pach, *An improved upper bound for the size of the multiplicative 3-Sidon sets*, Int. J. Number Theory 15 (2019), 1721–1729.
[11] P. P. Pach and C. Sándor, *Product representations of perfect powers*, arXiv: 2601.07000v1 (2026).
[12] P. P. Pach and M. Vizer, *Improved lower bounds for multiplicative square-free sequences*, Electron. J. Combin. 30 (2023), art. 4.31, 10 pp.
[13] V. G. Sargsyan, *On the maximum size of a k-zero-free set in an abelian group*, J. Appl. Industr. Math. 7 (2013), 574–587.
[14] I. E. Shparlinski, *On the number of Diophantine m-tuples in finite fields*, Finite Fields Appl. 90 (2023), art. 102241, 7 pp.
[15] T. Tao, *On product representations of squares*, Acta Math. Hungar. 175 (2025), 142–157.
[16] J. Verstraëte, *Product representations of polynomials*, Eur. J. Combin. 27 (2006), 1350–1361.
[17] C. H. Yip and S. Yoo, *F-Diophantine sets over finite fields*, Int. J. Number Theory 21 (2025), 1043–1050.

Hyunwoo Lee
Department of Mathematical Sciences, KAIST
and
Extremal Combinatorics and Probability Group
Institute for Basic Science
Daejeon, South Korea
E-mail: hyunwoo.lee@kaist.ac.kr

Chi Hoi Yip
Department of Mathematics
Hong Kong University of Science and Technology
Clear Water Bay, Hong Kong
E-mail: machyip@ust.hk

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