#A68 INTEGERS 11 (2011)

SUM-PRODUCT ESTIMATES APPLIED TO WARING'S PROBLEM OVER FINITE FIELDS

Todd Cochrane[1]
Department of Mathematics, Kansas State University, Manhattan, Kansas
cochrane@math.ksu.edu

James Cipra
Department of Mathematics, Kansas State University, Manhattan, Kansas
cipra@math.ksu.edu

Received: 5/13/11, Accepted: 10/31/11, Published: 11/2/11

Abstract

Let A be the set of nonzero k-th powers in $\mathbb{F}_q$ and $\gamma^*(k,q)$ denote the minimal n such that $nA = \mathbb{F}_q$. We use sum-product estimates for $|nA|$ and $|nA - nA|$, following the method of Glibichuk and Konyagin to estimate $\gamma^*(k,q)$. In particular, we obtain $\gamma^*(k,q) \le 633(2k)^{\log 4/\log|A|}$ for $|A| > 1$ provided that $\gamma^*(k,q)$ exists.

1. Introduction

Let $\mathbb{F}_q$ be a finite field in $q = p^f$ elements and k be a positive integer. The smallest s such that the equation

$$x_1^k + x_2^k + \cdots + x_s^k = a \tag{1}$$

is solvable for all $a \in \mathbb{F}_q$ (should such an s exist) is called Waring's number for $\mathbb{F}_q$, denoted $\gamma(k,q)$. Similarly, the smallest s such that

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k = a, \tag{2}$$

is solvable for all $a \in \mathbb{F}_q$ is denoted $\delta(k,p)$. If $d = (k, q-1)$ then clearly $\gamma(d,q) = \gamma(k,q)$ and so we may assume $k|(q-1)$. If A is the multiplicative subgroup of k-th powers in $\mathbb{F}_q^*$ then we write

$$\gamma(A,q) = \gamma(k,q), \qquad \delta(A,q) = \delta(k,q).$$

Also, we let $\gamma^*(A,q)$, $\delta^*(A,q)$ denote the minimal s such that every element of $\mathbb{F}_q$ is the sum ($\pm$ sum) of exactly s nonzero k-th powers, that is, (1), (2) resp. are

[1]Current address: Dept. of Mathematics, Georgia Institute of Technology, Atlanta, Georgia

solvable with all $x_i \neq 0$. It is well-known that $\gamma(A,q)$, $\delta(A,q)$, $\gamma^*(A,q)$, $\delta^*(A,q)$ exist if and only if A contains a set of f linearly independent points over $\mathbb{F}_p$; see Lemma 6.

For any subsets S, T of $\mathbb{F}_q$ and positive integer n, let

$$S+T=\{s+t : s\in S, t\in T\}, \quad S-T=\{s-t : s\in S, t\in T\},$$

$$nS = S+S+\cdots+S \ (n\text{-times}), \quad ST=\{st : s\in S, t\in T\}, \quad S^n = SS\cdots S \ (n\text{-times}).$$

Note that $(nS)T \subseteq n(ST)$. We let nST denote the latter, $n(ST)$. Also, for any $a \in \mathbb{F}_q$ we let $aS = \{as : s \in S\}$.

If A is a multiplicative subgroup of $\mathbb{F}_q^*$ then $\gamma^*(A,q)$ (if it exists) is the minimal s such that $sA = \mathbb{F}_q$, while $\gamma(A,q)$ is the minimal s such that $sA_0 = \mathbb{F}_q$, where $A_0 = A\cup\{0\}$. It is well-known that $\gamma(k,q) \leq k$ with equality if $k = q-1$ or $(q-1)/2$. This was first observed by Cauchy [5] for the case $q = p$. Our first result is the analogue for $\gamma^*(k,q)$. The proof makes use of Kneser's lower bound for $|A+B|$.

Theorem 1. *If A is the multiplicative subgroup of k-th powers in $\mathbb{F}_q^*$, $|A| > 2$ and $\gamma^*(A,q)$ exists, then $\gamma^*(A,q) \leq k+1$. When $|A| = 2$ (that is, q is an odd prime and $A = \{\pm 1\}$) then $\gamma^*(A,q) = 2k$.*

For $|A| > 2$ it was established by Tietäväinen [20], for odd q, and by Winterhof [22], [23, Lemma 1], for even q, that $\gamma(A,q) \leq [k/2]+1$. It is an open question whether the same improvement holds for $\gamma^*(A,q)$. For the case of prime fields Heilbronn [17] formulated two conjectures, which in the more general setting of $\mathbb{F}_q$ can be stated as follow:

1. If $|A| > 2$ then $\gamma(A,q) \ll \sqrt{k}$.
2. For any $\epsilon > 0$ there exists a constant $c(\epsilon)$ such that if $|A| > c(\epsilon)$ then $\gamma(A,q) \ll_\epsilon k^\epsilon$.

The second conjecture was proven by Konyagin [18] for prime fields. Cipra, Cochrane and Pinner [8] established the first conjecture for prime fields, and the explicit bound $\gamma(A,p) \leq 83\sqrt{k}$ was obtained in [9]. Cipra [6, Theorem 4] proved the first conjecture for the general finite field $\mathbb{F}_q$, obtaining

$$\gamma(A,q) \leq \begin{cases} 16\sqrt{k+1}, & \text{for } q = p^2. \\ 10\sqrt{k+1}, & \text{for } q = p^f,\ f \geq 3, \end{cases} \tag{3}$$

whenever $\gamma(A,q)$ is defined.

Next, let $A' = A \cap \mathbb{F}_p$, so that $|A'| = (|A|, p-1)$. Cipra [6], sharpening the work of Winterhof [22], established the bound

$$\gamma(k,q) \leq 8f \left\lceil \frac{(k+1)^{1/f}-1}{|A'|} \right\rceil, \tag{4}$$

whenever $\gamma(k,q)$ exists. He also established the bound

$$\gamma(k,q) \ll fk^{\frac{\log 4}{f \log |A'|}} \log\log(k), \tag{5}$$

which resolved the second Heilbronn conjecture provided $|A'|^f$ is sufficiently large.

For prime fields Glibichuk and Konyagin [15] used methods of additive combinatorics to obtain

$$\gamma^*(A,p) \leq 400\ k^{\frac{\log 4}{\log |A|}}, \tag{6}$$

for any multiplicative subgroup A with $|A| > 1$. Cochrane and Pinner [9, Corollary 7.1] obtained a similar bound for $q = p$, and Glibichuk [13] established the same type of bound for $q = p^2$. The main result of this paper is a generalization of (6) to arbitrary $\mathbb{F}_q$, thus resolving the second Heilbronn conjecture for any finite field.

Theorem 2. *If A is a multiplicative subgroup of $\mathbb{F}_q^*$ for which $\gamma^*(A,q)$ is defined and $|A| > 1$, then with $k = (q-1)/|A|$, we have*

$$\gamma^*(A,q) \leq 633(2k)^{\frac{\log 4}{\log |A|}}.$$

After submitting this work, the author's learned that Glibichuk [14, Corollary 1] recently proved a similar result, albeit with weaker constants. In particular, if $|A| = p^{\epsilon}$, then our result gives $\gamma^*(A,q) \ll 4^{1/\epsilon}$, whereas his result gives $\gamma^*(A,q) \ll 6^{1/\epsilon}$.

For $\delta^*(A,q)$ we establish the stronger bound,

Theorem 3. *If A is a multiplicative subgroup of $\mathbb{F}_q^*$ for which $\delta^*(A,q)$ is defined and $|A| > 1$, then with $k = (q-1)/|A|$, we have*

$$\delta^*(A,q) \leq (40/3)k^{\frac{\log 4}{\log |A|}}.$$

As noted in Theorem 9, if q is even or $|A|$ is even then $\gamma^*(A,q) = \delta^*(A,q)$ and thus the stronger bound in Theorem 3 applies to $\gamma^*(A,q)$ as well. Further relations between $\delta(A,q)$ and $\gamma(A,q)$ are given in Theorem 9. The exponent on k in the theorem improves on (5) when $|A| > (|A|, p-1)^f$ and on (4) when $|A| > 4^f$. For small $|A|$ ($|A| = O(1)$ as $p \to \infty$) one can obtain a stronger result by employing the lattice method of Bovey. In this manner we prove,

Theorem 4. *For any positive integer t there is a constant $c_1(t)$ such that if A is a multiplicative subgroup of $\mathbb{F}_q^*$ with $|A| = t$, and such that $\gamma(A,q)$ is defined, then*

$$\gamma(A,q) \leq c_1(t)k^{1/\phi(t)}.$$

The constant $c_1(t)$, estimated in [4] for prime fields, depends on the size of the coefficients of the cyclotomic polynomial of order t.

Corollary 5. *For any positive integer l there is a constant $c(l)$ such that if A is a multiplicative subgroup of $\mathbb{F}_q^*$ of order t such that $\phi(t) \geq l$ and $\gamma(A,q)$ exists, then $\gamma(A,q) \leq c(l)k^{1/l}$.*

Proof. Suppose that $\phi(t) \geq l$. Put $c = \max_{t \leq 4^l} c_1(t)$, $c(l) = \max\{c, 2^{1/l}633\}$, with $c_1(t)$ as defined in Theorem 4. If $t > 4^l$ then, by Theorem 2, $\gamma(k,q) \leq 633 \cdot 2^{1/l} k^{1/l} \leq c(l)k^{1/l}$. If $t \leq 4^l$ then, by Theorem 4, $\gamma(k,q) \leq ck^{1/\phi(t)} \leq c(l)k^{1/l}$. □

2. Preliminary Lemmas

The first lemma gives equivalent conditions for the existence of $\gamma(k,q)$. It is well-known, and follows from the fact that the set of all sums of k-th powers is a multiplicatively closed set and therefore a subfield of $\mathbb{F}_q$; see Tornheim [21, Lemma 1], or Bhaskaran [1].

Lemma 6. *Let A be the set of nonzero k-th powers in $\mathbb{F}_q$. The following are equivalent.*

(i) $\gamma(k,q)$ *exists, that is, every element of $\mathbb{F}_q$ is a sum of k-th powers.*

(ii) *A is not contained in any proper subfield of $\mathbb{F}_q$; that is, A contains a set of f linearly independent points over $\mathbb{F}_p$.*

(iii) *$|A|$ does not divide $p^j - 1$ for any $j|f$, $j < f$, that is, $\frac{p^f-1}{p^j-1}$ does not divide k for any $j|f$, $j < f$.*

It is also not hard to show that $\gamma^*(A,q)$ exists if and only if $|A| > 1$ and $\gamma(A,q)$ exists.

An important tool needed throughout this paper is Rusza's triangle inequality (see, e.g., Nathanson [19, Lemma 7.4]),

$$|S+T| \geq |S|^{1/2}|T-T|^{1/2}, \tag{7}$$

for any $S, T \subseteq \mathbb{F}_q$, and its corollary

$$|nS| \geq |S|^{\frac{1}{2^{n-1}}}|S-S|^{1-\frac{1}{2^{n-1}}} \geq |S-S|^{1-\frac{1}{2^n}}, \tag{8}$$

for any positive integer n. The first inequality in (8) follows by induction on n, and the second from the trivial bound $|S-S| \leq |S|^2$.

The following is a key lemma for showing that a sum-product set fills up $\mathbb{F}_q$.

Lemma 7. *Let A, B be subsets of $\mathbb{F}_q$ and $m \geq 3$ be a positive integer.*

(a) *If $|B||A|^{1-\frac{2}{m}} > q\left(1 - \frac{|B|}{q}\right)^{2/m}$ then $mAB = \mathbb{F}_q$.*

(b) *If $|B||A| \geq 2q$ then $8AB = \mathbb{F}_q$.*

(c) *If $|B||A| > q$ and either A or B is symmetric ($A = -A$) or antisymmetric ($A \cap -A = \emptyset$) then $8AB = \mathbb{F}_q$.*

A slightly weaker form of part (a) was proven by Bourgain [2, Lemma 1] for $q = p$ and $m = 3$ and by Cochrane and Pinner [9, Lemma 2.1] for $q = p$ and general m. A similar proof works for $\mathbb{F}_q$ and is provided in Section 7. In the earlier versions of this statement, an extra hypothesis, $0 \notin A$, was included, and the factor $\left(1 - \frac{|B|}{q}\right)^{2/m}$ was excluded.

Part (b) is due to Glibichuk and Konyagin [15, Lemma 2.1] for prime fields and to Glibichuk and Rudnev [16] for general $\mathbb{F}_q$. Part (c) is due to Glibichuk [12] for prime fields and to Glibichuk and Rudnev [16] as well as Cipra [7] for general $\mathbb{F}_q$. In particular, if A is a multiplicative subgroup, then applying (c) with $B = A$ we see that $\gamma^*(A, q) \le 8$ provided that $|A| > \sqrt{q}$.

In the cases where $|A| = 3, 4$ or 6 one can actually evaluate $\gamma(A, q)$. This was done in [8] for the case of prime moduli.

Theorem 8. *Let A is a multiplicative subgroup of $\mathbb{F}_q$ of order 3,4 or 6 for which $\gamma(A, q)$ exists. Then $q = p$ or p^2. If $q = p^2$ then $\gamma(A, q) = p - 1$. If $q = p$ then*

$$\gamma(A,p) = \begin{cases} a + b - 1, & \text{if } |A| = 3, \\ c - 1, & \text{if } |A| = 4, \\ \left\lfloor \frac{2}{3}a + \frac{1}{3}b \right\rfloor, & \text{if } |A| = 6 \end{cases}$$

where, if $|A| = 3$ or 6, then a, b are the unique positive integers with $a > b$ and $a^2 + b^2 + ab = p$, while if $|A| = 4$ then c, d are the unique positive integers with $c > d$ and $c^2 + d^2 = p$.

In particular, for $|A| = 3, 4$ or 6 we have

$$\begin{aligned} \sqrt{3k+1} - 1 \le & \gamma(A, q) \le 2\sqrt{k}, && \text{if } |A| = 3, \\ \sqrt{2k} - 1 \le & \gamma(A, q) \le 2\sqrt{k} - 1, && \text{if } |A| = 4, \\ \sqrt{2k} - \tfrac{1}{2} \le & \gamma(A, q) \le \tfrac{2}{3}\sqrt{6k}, && \text{if } |A| = 6. \end{aligned}$$

Proof. Since $|A| = 3, 4$ or 6, every element of A is of degree 1 or 2 over $\mathbb{F}_p$ and therefore $A \subset \mathbb{F}_{p^2}$. Thus, in order for $\gamma(k, q)$ to exist we must have $q = p$ or p^2. The case $q = p$ is just Theorem 2 of [8] and the case $q = 2^2$ is trivial, so we shall assume $q = p^2$ with p an odd prime and that A is not contained in $\mathbb{F}_p$.

Case i: $|A| = 3$. Say $A = \{1, T, T^2\}$ where $T \in \mathbb{F}_{p^2} - \mathbb{F}_p$ satisfies $T^2 + T + 1 = 0$. In particular, $p \equiv 2 \pmod 3$. We claim that $\gamma(A, q) = p - 1$ and consequently, since $3k = p^2 - 1$, $\gamma(k, q) = \sqrt{3k+1} - 1$. Let $w = x + yT$ denote a typical element of $\mathbb{F}_q$ where $0 \le x, y \le p - 1$ and let $\gamma(w)$ denote the minimal number of elements of A required to represent w. First note that $\gamma(0) = 3$ since $1 + T + T^2 = 0$ so we assume that $w \ne 0$. Suppose that $x \le y$. If $x + y < p$ then trivially $\gamma(w) < p$. If $x \le y < 2x$ then we write $w = (y - x)T + (p - x)T^2$ and get $\gamma(w) \le p + y - 2x < p$. If $y \ge 2x$ and $y > \frac{2}{3}p$ then we write $w = (x - y + p) \cdot 1 + (p - y)T^2$

and get $\gamma(w) \le (x - 2y + 2p) \le 2p - \frac{3}{2}y < p$. If $y \ge 2x$ and $y < \frac{2}{3}p$, then $x + y \le \frac{3}{2}y < p$. A similar argument holds for $x \ge y$. Finally, one can check that $\gamma(\frac{1}{3}(p+1) + \frac{2}{3}(p+1)T) = p - 1$.

Case ii: $|A| = 4$. Say $A = \{\pm 1, \pm T\}$, with $T^2 = -1$, $T \in \mathbb{F}_{p^2} - \mathbb{F}_p$. In particular, $p \equiv 3 \pmod 4$. Any element of $\mathbb{F}_q$ may be written $x + yT$ with $|x|, |y| \le \frac{p-1}{2}$, and so $\gamma(A, q) \le p - 1$. Also, it is plain that $\gamma(\frac{p-1}{2} + \frac{p-1}{2}T) = p - 1$. Thus, $\gamma(A, q) = p - 1$.

Case iii: $|A| = 6$. Say $A = \{\pm 1, \pm T, \pm T^2\}$ with $T^2 - T + 1 = 0$. As in case ii, any element of $\mathbb{F}_q$ may be written $x + yT$ with $|x|, |y| \le \frac{p-1}{2}$, and so $\gamma(A, q) \le p - 1$. Also, with just a little work one again sees that $\gamma(\frac{p-1}{2} + \frac{p-1}{2}T) = p - 1$. Thus, $\gamma(A, q) = p - 1$. □

The precise relationship between $\gamma(k, q)$ and $\delta(k, q)$ is an important unresolved problem. It is not known whether $\gamma(k, q) \le C\delta(k, q)$ for some constant C. Bovey [4, Lemma 2] established $\gamma(k, p) \le (\log_2 p + 1)\delta(k, p)$ for prime moduli, and improvements were given in [8]. Here we prove the analogue of [8, Theorem 4.1] for general finite fields.

Theorem 9. *Let A be the set of nonzero k-th powers in $\mathbb{F}_q$ with $k|(q-1)$, such that $\gamma(k, q)$ is defined. Then,*

(a) $\gamma(k, q) \le 3 \left\lceil \log_2 \left(\frac{3 \log q}{\log |A|} \right) \right\rceil \delta(k, q)$.

(b) $\gamma(k, q) \le 3 \lceil \log_2(4\delta(k, q)) \rceil \delta(k, q)$

(c) $\gamma(k, q) \le 2 \lceil \log_2(\log_2(q)) \rceil \delta(k, q)$.

(d) $\gamma(k, q) \le (p_{min} - 1)\delta(k, q)$, *where p_{min} is the minimal prime divisor of $|A|$.*

(e) *If q is even or $|A|$ is even then $\delta(k, q) = \gamma(k, q)$. If $|A|$ is odd and p is odd, then $\delta(k, q) = \gamma(\frac{k}{2}, q)$.*

Proof. a) Put $A_0 = A \cup \{0\}$, $\delta = \delta(k, q)$. Since $\delta A_0 - \delta A_0 = \mathbb{F}_q$ we obtain from (8), (observing that this inequality is strict for $|S| > 1$),

$$|j\delta A_0| > |\delta A_0 - \delta A_0|^{1-1/2^j} = q^{1-1/2^j}, \tag{9}$$

for any positive integer j. Hence if $j \ge \log_2 \left(\frac{3 \log q}{\log |A|} \right)$ we have $|j\delta A_0||A|^{\frac{1}{3}} \ge q$, and so by Lemma 7 (a) with $m = 3$, $3(j\delta A_0)A = \mathbb{F}_q$, that is, $3j\delta A_0 = \mathbb{F}_q$.

b) This follows from part (a) and the trivial bound $(2|A|+1)^\delta \ge q$, when $|A| \ge 11$. Indeed, in this case,

$$\frac{\log q}{\log |A|} \le \delta \frac{\log(2|A| + 1)}{\log |A|} < \frac{4}{3}\delta.$$

For $|A| < 11$, the result follow from part (d) of this theorem, since $p_{min} \le 7$ for such $|A|$.

c) We repeat the proof given by Cipra [6]. If $j \geq \log_2(\log_2(q))$ then $q^{1/2^j} \leq 2$ and so by (9), $|j\delta A| > q/2$. Thus, $2j\delta A = \mathbb{F}_q$. (Here we have used the fact that if S is a subset of a finite group G with $|S| > |G|/2$ then $S + S = G$.)

d) Let ℓ be the minimal prime divisor of $|A|$. Then A has a subgroup G of order ℓ and $\sum_{x \in G} x = 0$ so that -1 is a sum of $\ell - 1$ elements of A.

e) If q is even then $1 = -1$, and so trivially $\delta(k, q) = \gamma(k, q)$. If $|A|$ is even then -1 is a k-th power, and so again $\gamma(k, q) = \delta(k, q)$. If $|A|$ is odd then k must be even (for $p \neq 2$) and $A \cup (-A)$ is the set of $k/2$-th powers. □

3. Proof of Theorem 1

Let $k|(q-1)$, A be the set of nonzero k-th powers in $\mathbb{F}_q$ and $A_0 = A \cup \{0\}$. Before addressing Theorem 1, which is concerned with representing elements as sums of nonzero k-th powers, we start by reviewing the proof of Cauchy's theorem, $\gamma(k, q) \leq k$, which allows for some terms to be zero. For any positive integer n,

$$nA_0 = \{0\} \cup Ax_1 \cdots \cup Ax_l,$$

for some distinct cosets Ax_i of A, $1 \leq i \leq l$. If $nA_0 \neq \mathbb{F}_q$ then $(n+1)A_0$ contains nA_0 and, assuming that $\gamma(k, q)$ exists, must be strictly larger. Therefore, $|(n+1)A_0| \geq |nA_0| + |A|$. By induction we get a Cauchy-Davenport type inequality,

$$|nA_0| \geq \min\{q, 1 + n|A|\}, \tag{10}$$

for $n \geq 1$, and in view of the equality $k|A| = q-1$, deduce that $\gamma(k, q) \leq k$ whenever $\gamma(k, q)$ exists. To estimate $\gamma^*(k, q)$ we have to work a little harder since $(n+1)A$ doesn't contain nA in general, so it is not immediate that it has larger cardinality. However, we are able to recover the following analogue of (10), and Theorem 1 is an immediate consequence.

Lemma 10. *If A is a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$ and $|A| > 2$, then for any positive integer n, $|nA| \geq \min\{q, n|A|\}$.*

Proof. Let A be a multiplicative subgroup of $\mathbb{F}_q$ containing f linearly independent points over $\mathbb{F}_p$. We first show that if B is any subset of $\mathbb{F}_q$ such that $AB \subset B$ then either $A + B = \mathbb{F}_q$ or $|A + B| \geq |A| + |B| - 1$. This follows from Kneser's inequality (see [19, Theorem 4.1]): $|A + B| \geq |A| + |B| - |stab(A + B)|$, where $stab(A + B) = \{x \in \mathbb{F}_q : A + B + x = A + B\}$, an additive subgroup of $\mathbb{F}_q$, that is, an $\mathbb{F}_p$ subspace of $\mathbb{F}_q$. We need only establish that if $stab(A + B) \neq \{0\}$ then $A+B = \mathbb{F}_q$. Suppose x is a nonzero element of $stab(A+B)$. Then $A+B+x = A+B$. Since $AB \subset B$ and $AA = A$ we get $A+B+Ax \subset A+B$. Thus $Ax \subset stab(A+B)$, but

Ax contains f linearly independent points over $\mathbb{F}_p$. Thus $stab(A+B)$ is of dimension f over $\mathbb{F}_p$, and so $stab(A+B)=\mathbb{F}_q$. Plainly, we must also have $A+B=\mathbb{F}_q$ since for any point $c\in A+B$, $c+stab(A+B)\subset A+B$.

Now let n be any positive integer and $B=nA$. Then $AB\subset B$ and so either $(n+1)A=\mathbb{F}_q$ or $|(n+1)A|\geq |nA|+|A|-1$. The proof now follows by induction on n. Suppose $|nA|\geq n|A|$ for a given n and that $(n+1)A\neq \mathbb{F}_q$. Then $|(n+1)A|\geq (n+1)|A|-1$, but $(n+1)A$ is a union of cosets of A together (possibly) with 0. If $|A|>2$, this forces $(n+1)A$ to be a union of at least $(n+1)$ cosets of A together (possibly) with 0. Thus $|(n+1)A|\geq (n+1)|A|$. □

When $|A|=2$; that is, $q=p$ and $A=\{\pm 1\}$, then $|nA|=n+1$ for $n<p$. Thus $\gamma^*(A,q)=p-1=2k$.

4. Estimating $\delta^*(A,q)$ and Proof of Theorem 3

Following the method of Glibichuk and Konyagin [15], for any subsets X,Y of $\mathbb{F}_q$ let

$$\frac{X-X}{Y-Y}=\left\{\frac{x_1-x_2}{y_1-y_2}:x_1,x_2\in X,y_1,y_2\in Y,y_1\neq y_2\right\}.$$

The key lemma is a generalization of a lemma of Glibichuk and Konyagin [15, Lemma 3.2] to finite fields.

Lemma 11. *Let $q=p^f$, $X,Y\subseteq\mathbb{F}_q$ and $a_1,a_2,\ldots,a_f\in\mathbb{F}_q$ be a set of f linearly independent points over $\mathbb{F}_p$. If $\frac{X-X}{Y-Y}\neq\mathbb{F}_q$ then for some a_i we have*

$$|2XY-2XY+a_iY^2-a_iY^2|\geq |X||Y|.$$

Proof. Let $S=\frac{X-X}{Y-Y}$. Assume $S\neq\mathbb{F}_q$ and that $a_1,\ldots,a_f$ are linearly independent values in $\mathbb{F}_q$. We claim that for some a_i, $S+a_i\not\subseteq S$, for otherwise $S+k_1a_1+k_2a_2+\cdots+k_fa_f\subseteq S$ for all nonnegative integers $k_1,\ldots,k_f$, implying that $S=\mathbb{F}_q$. Say $\frac{x_1-x_2}{y_1-y_2}+a_i\notin S$, for some $x_1,x_2\in X$, $y_1,y_2\in Y$. Then the mapping from $X\times Y$ into $2XY-2XY+a_iY^2-a_iY^2$ given by

$$(x,y)\to(y_1-y_2)x+(x_1-x_2+a_iy_1-a_iy_2)y,$$

is one-to-one and the lemma follows. □

Applying the lemma to a multiplicative subgroup A of $\mathbb{F}_q^*$ containing a set $a_1,\ldots,a_f$ of linearly independent points, we immediately obtain,

Lemma 12. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$ and X be any subset of $\mathbb{F}_q$ such that $AX\subseteq X$ and $\frac{X-X}{A-A}\neq\mathbb{F}_q$. Then*

$$|2X-2X+A-A|\geq |X||A|.$$

We also need the following elementary result.

Lemma 13. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ and X, Y be subsets of $\mathbb{F}_q$ such that $AX \subseteq X$, $AY \subseteq Y$. If $|X-X||Y-Y| \leq q|A|$ then $\frac{X-X}{Y-Y} \neq \mathbb{F}_q$.*

Proof. If $c = (x_1 - x_2)/(y_1 - y_2)$ for some $x_1, x_2 \in X$, $y_1 \neq y_2 \in Y$, then $c = (ax_1 - ax_2)/(ay_1 - ay_2)$ for any $a \in A$. Thus

$$\left|\frac{X-X}{Y-Y}\right| \leq \frac{|X-X|(|Y-Y|-1)}{|A|}.$$

Since the right-hand side is less than q by assumption, the result follow. □

For $l \in \mathbb{N}$, let $n_1 = 1$ and $n_l = \frac{5}{24}4^l - \frac{1}{3}$, for $l \geq 2$, so that $n_2 = 3$, $n_3 = 13$, $n_4 = 53$, $n_5 = 213$ and

$$n_{l+1} = 4n_l + 1, \quad \text{for } l \geq 2. \tag{11}$$

Put $A_1 = A$ and, for $l \geq 2$, $A_l = (n_l A - n_l A)$ so that, for $l \geq 2$,

$$2A_{l-1} - 2A_{l-1} + A - A = A_l. \tag{12}$$

Lemma 14. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$. Then for $l \geq 1$,*

(a) *If* $|A_{l-1} - A_{l-1}||A - A| < q|A|$ *then* $|A_l| \geq |A|^l$.

(b) *In all cases,* $|A_l| \geq \min\{|A|^l, q/|A|\}$.

One can compare the above result with Lemma 5.2 of [15] where it is shown for $\mathbb{F}_p$ that $|A_l| \geq \frac{3}{8}\min\{|A|^l, \frac{p-1}{2}\}$.

Proof. The proof of (a) is by induction on l, the statement being trivial for $l = 1$. For $l > 1$, put $X = A_{l-1}$, $Y = A$. If $|A_{l-1} - A_{l-1}||A - A| < q|A|$ then by Lemma 13, $\frac{X-X}{Y-Y} \neq \mathbb{F}_q$. Also, by (12) we have $2X - 2X + A - A = A_l$. Thus by Lemma 12, $|A_l| \geq |A_{l-1}||A|$ and so by the induction assumption, $|A_l| \geq |A|^l$. If $|A_{l-1} - A_{l-1}||A - A| \geq q|A|$ then since $|A - A| \leq |A|^2$ we have $|A_{l-1} - A_{l-1}| \geq q/|A|$. Since $|A_l| = |n_l A - n_l A| \geq |2n_{l-1}A - 2n_{l-1}A| = |A_{l-1} - A_{l-1}|$, we obtain $|A_l| \geq |A_{l-1} - A_{l-1}| \geq q|A|/|A - A| \geq q/|A|$. □

Lemma 15. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$. Set $l = \lfloor \log(q-1)/\log|A| \rfloor$. Then $\delta^*(A, q) \leq 16n_l$.*

Proof. For such l we have $l + 1 > \log(q-1)/\log|A|$ and so $|A|^{l+1} \geq q$. Thus, by Lemma 14 (b), $|A_l||A| \geq \min\{|A|^{l+1}, q\} = q$. Since $(|A|, q) = 1$ we must in fact have $|A_l||A| > q$. Since A is symmetric $(-1 \in A)$ or antisymmetric $(-1 \notin A)$, it follows from Lemma 7 (c) that $8A_l A = \mathbb{F}_q$, that is, $8n_l A - 8n_l A = \mathbb{F}_q$. □

Proof of Theorem 3. With l as in Lemma 15 we have using $k|A| = (q-1)$,

$$l = \left\lfloor \frac{\log(q-1)}{\log|A|} \right\rfloor \le 1 + \frac{\log k}{\log|A|}.$$

Thus by Lemma 15, $\delta^*(A,q) \le 16n_l \le 16\frac{5}{24}4^l \le \frac{40}{3}4^{\log k/\log|A|}$, thereby finishing the proof. $\square$

5. Estimating $\gamma^*(A,q)$ and Proof of Theorem 2

Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points. We start by obtaining growth estimates for $|nA|$. If $|A| = 1$ then $q = p$ and $|nA| = 1$ for any n. If $|A| = 2$ then $q = p$, $A = \pm 1$ and $|nA| = \min\{p, n+1\}$. Next we note that

$$|4A| \ge \begin{cases} |A|^{3/2} & \text{if} \quad |A-A|^2 < q|A|, \\ q^{1/2}|A|^{3/8}, & \text{otherwise.} \end{cases} \tag{13}$$

Indeed, by (7) and Lemma 14 (a) we have

$$|4A| \ge |A|^{1/2}|3A-3A|^{1/2} = |A|^{1/2}|A_2|^{1/2} \ge |A|^{3/2}, \qquad \text{if} \qquad |A-A|^2 < q|A|.$$

Otherwise, $|A-A| \ge (q|A|)^{1/2}$. In particular, $|A|^2 > (q|A|)^{1/2}$, and so $|A| \ge q^{1/3}$. Thus, by (8), $|4A| \ge |A-A|^{15/16} \ge (q|A|)^{15/32} \ge q^{15/32}|A|^{3/32}|A|^{12/32} \ge q^{1/2}|A|^{3/8}$.

For $l \in \mathbb{N}$ set

$$m_l = \frac{5}{18}4^l - \frac{l}{3} + \frac{2}{9},$$

so that $m_1 = 1$, $m_2 = 4$, $m_3 = 17$, $m_4 = 70$, $m_5 = 283$ and $m_l = m_{l-1} + n_l$ for $l \ge 2$, with n_l as defined in the previous section.

Lemma 16. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$. Then for $l \ge 1$ we have*

$$|m_lA| \ge \begin{cases} |A|^{l-1+\frac{1}{2^{l-1}}}, & \text{if } l = 1, \text{ or } l \ge 2 \text{ and} \quad |A_{l-1} - A_{l-1}||A-A| < q|A|, \\ \max\left\{ \left(\frac{|A|}{|A-A|}\right)^{3/4} q^{3/4}, |A|^{1/4}q^{1/2} \right\}, & \text{otherwise.} \end{cases} \tag{14}$$

Proof. The result is trivial when $l = 1$. Assume that the theorem holds for $l-1$ with $l \ge 2$. Suppose that $|A_{l-1} - A_{l-1}||A-A| < q|A|$. In particular, if $l \ge 3$ then $|A_{l-2} - A_{l-2}||A-A| < q|A|$. Then using $m_l = n_l + m_{l-1}$, inequality (7), the induction assumption and Lemma 14, we have

$$|m_lA| \ge |m_{l-1}A|^{1/2}|n_lA - n_lA|^{1/2} \ge |A|^{\left(l-2+\frac{1}{2^{l-2}}\right)\frac{1}{2}}|A|^{l/2} = |A|^{l-1+\frac{1}{2^{l-1}}}.$$

Suppose next that

$$|A_{l-1} - A_{l-1}||A - A| \geq q|A|. \tag{15}$$

Then, since $m_l > n_l > 4n_{l-1}$, we have by inequality (8) that

$$|m_l A| \geq |2(2n_{l-1}A)| \geq |2n_{l-1}A - 2n_{l-1}A|^{3/4} = |A_{l-1} - A_{l-1}|^{3/4} \geq \left(\frac{q|A|}{|A-A|}\right)^{3/4}.$$

To prove the second inequality, $|m_l A| \geq |A|^{1/4} q^{1/2}$, under the assumption of (15), more work is required. A stronger result was established (13) for $l = 2$, so we assume $l \geq 3$. First observe that by Lemma 12, with $X = A - A$, if $|2A - 2A||A - A| < q|A|$, (so that by Lemma 13, $(X - X)/(A - A) \neq \mathbb{F}_q$), then

$$|5A - 5A| = |2(A - A)A - 2(A - A)A + A - A| \geq |A - A||A|,$$

and so by (15),

$$|5A - 5A||2n_{l-1}A - 2n_{l-1}A| = |5A - 5A||A_{l-1} - A_{l-1}| \geq |A - A||A||A_{l-1} - A_{l-1}| \geq q|A|^2.$$

Since $2n_{l-1} > 5$ for $l \geq 3$, it follows that

$$|2n_{l-1}A - 2n_{l-1}A| > |5A - 5A|^{1/2}|2n_{l-1}A - 2n_{l-1}A|^{1/2} \geq q^{1/2}|A|. \tag{16}$$

Also, since for any set B, $|B - B| \leq |B|^2$, using (15),

$$|2n_{l-1}A|^2|A|^2 \geq |2n_{l-1}A - 2n_{l-1}A||A - A| = |A_{l-1} - A_{l-1}||A - A| \geq q|A|,$$

and so

$$|2n_{l-1}A|^2|A| \geq q. \tag{17}$$

Thus since $m_l > n_l > 4n_{l-1}$ we obtain from (7), (16) and (17),

$$\begin{aligned} |m_l A| &\geq |4n_{l-1}A| \geq |2n_{l-1}A|^{1/2}|2n_{l-1}A - 2n_{l-1}A|^{1/2} \geq |2n_{l-1}A|^{1/2} q^{1/4}|A|^{1/2} \\ &= (|2n_{l-1}A|^{1/2}|A|^{1/4}) q^{1/4}|A|^{1/4} \geq q^{1/4} q^{1/4}|A|^{1/4} = q^{1/2}|A|^{1/4}. \end{aligned}$$

There remains the case $|2A - 2A||A - A| \geq q|A|$. In this case $|2A - 2A| \geq q^{1/2}|A|^{1/2}$ and $|2A|^2|A| \geq q$. The latter implies $|2A| \geq (q/|A|)^{1/2}$. Thus, by (7),

$$|4A| \geq |2A|^{1/2}|2A - 2A|^{1/2} \geq q^{1/4}|A|^{-1/4} q^{1/4}|A|^{1/4} = q^{1/2},$$

and

$$|m_l A| \geq |6A| \geq |4A|^{1/2}|2A - 2A|^{1/2} \geq q^{1/4} q^{1/4}|A|^{1/4} = q^{1/2}|A|^{1/4},$$

which finishes the proof. □

Lemma 17. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$. Then for $l \geq 1$ we have*

$$|m_l A| \geq \min\left\{|A|^{l-1+\frac{1}{2^{l-1}}}, \sqrt{2q}\right\}. \tag{18}$$

Proof. If $l = 1$ or $|A| = 1$ the statement is trivial. For $|A| = 2$,

$$|m_l A| \geq \min\{m_l + 1, q\} = \min\{\frac{5}{18}4^l - \frac{l}{3} + \frac{11}{9}, q\} \geq \min\{2^l, \sqrt{2q}\}.$$

For $|A| \geq 4$ the result follows from Lemma 16, since $q^{1/2}|A|^{1/4} \geq \sqrt{2q}$ in this case. For $|A| = 3$ and $l = 2$ the result follows from (13) in a similar manner. Suppose that $|A| = 3$ and $l \geq 3$. Then $A = \{1, \alpha, \alpha^2\} = \{1, \alpha, -1-\alpha\}$, where α is a primitive cube root of 1, and $A - A = \{0, \pm(1-\alpha), \pm(2+\alpha), \pm(2\alpha+1)\}$, whence $|A - A| = 7$. Then, by Lemma 16, $|m_l A| \geq q^{3/4}|A|^{3/4}|A - A|^{-3/4} \geq (3/7)^{3/4}q^{3/4} \geq \sqrt{2q}$, provided that $q \geq 4(7/3)^3 = 50.8..$, and so the result follows from Lemma 16 when $q \geq 51$. We are left with testing the prime powers less than 50. If q is a prime then we can use the Cauchy-Davenport inequality to get $|m_k A| \geq |17A| \geq \min\{q, 35\} \geq \sqrt{2q}$. The prime powers remaining with $3|q - 1$ are 4,16,25,49. We can't have $q = 16$ or 49 since $3|(2^2 - 1)$ and $3|(7 - 1)$, implying that A does not contain a set of f linearly independent points. For $q = 4$, $A = \mathbb{F}_4^*$, $2A = \mathbb{F}_4$ and trivially $|2A| \geq \sqrt{2q}$. For $q = 25$ one can check that $|3A| = 10 \geq \sqrt{50}$. □

Applying Lemma 7 (b) with $A = B = m_l A$ we immediately obtain,

Lemma 18. *Let A be a multiplicative subgroup of $\mathbb{F}_q^*$ containing f linearly independent points over $\mathbb{F}_p$. If $|A| \geq (2q)^{\frac{1}{2}\left(l-1+\frac{1}{2^{l-1}}\right)^{-1}}$, then $8m_l^2 A = \mathbb{F}_q$.*

In particular,

$$\begin{aligned} 8A &= \mathbb{F}_q \quad \text{for } |A| > q^{1/2}, \\ 128A &= \mathbb{F}_q \quad \text{for } |A| > 1.26\ q^{1/3}, \\ 2312A &= \mathbb{F}_q \quad \text{for } |A| > 1.17\ q^{2/9}, \\ 39200A &= \mathbb{F}_q \quad \text{for } |A| > 1.12\ q^{4/25}, \\ 640712A &= \mathbb{F}_q \quad \text{for } |A| > 1.09\ q^{8/65}. \end{aligned}$$

In comparison, for $\mathbb{F}_p$ Cochrane and Pinner [9] obtained

$$\begin{aligned} 8A &= \mathbb{F}_p \quad \text{for } |A| > p^{1/2}, \\ 32A &= \mathbb{F}_p \quad \text{for } |A| > 3.91\ p^{1/3}, \\ 392A &= \mathbb{F}_p \quad \text{for } |A| > 2.78\ p^{1/4}, \\ 2888A &= \mathbb{F}_p \quad \text{for } |A| > 3.19\ p^{1/5}, \\ 12800A &= \mathbb{F}_p \quad \text{for } |A| > 2.28\ p^{1/6}, \\ 56448A &= \mathbb{F}_p \quad \text{for } |A| > 2.43\ p^{1/7}, \\ 228488A &= \mathbb{F}_p \quad \text{for } |A| > 1.91\ p^{1/8}. \end{aligned}$$

We cannot do quite as well for $\mathbb{F}_q$ because we do not have a lower bound on $|2A|$. For $\mathbb{F}_p$ it was shown in [9, Theorem 5.2] that $|2A| \geq \min\{\frac{1}{4}|A|^{3/2}, \frac{p}{2}\}$. We do not know if such a bound holds in $\mathbb{F}_q$.

Proof of Theorem 2. An integer l satisfies the hypothesis of Lemma 18 provided that

$$l + \frac{1}{2^{l-1}} \geq \frac{\log 2q}{2\log|A|} + 1. \tag{19}$$

We claim that the value

$$l = \left\lceil \frac{\log(2(q-1))}{2\log|A|} + 1 \right\rceil,$$

suffices. To see this, first observe that for this choice of l, $l < \log_2(4(q-1))$, that is, $q - 1 > 2^{l-2}$, and so using the inequality

$$\log(2q) - \log(2(q-1)) = \log(q/(q-1)) < \frac{q}{q-1} - 1 = \frac{1}{q-1},$$

we have

$$\frac{\log(2q)}{2\log|A|} - \frac{\log(2(q-1))}{2\log|A|} < \frac{1}{2(q-1)\log|A|} < \frac{1}{2^{l-1}\log|A|} < \frac{1}{2^{l-1}}.$$

Thus (19) is satisfied, and so by Lemma 18, $\gamma^*(A,q) \leq 8m_l^2$. Since $m_l \leq \frac{5}{18}4^l$, we have

$$\begin{aligned}\gamma^*(A,q) &\leq 8(5/18)^2 4^{2\left\lceil \frac{\log 2(q-1)}{2\log|A|}+1\right\rceil} < 158.03 \cdot 4^{\frac{\log 2(q-1)}{\log|A|}} = 158.03(2(q-1))^{\log 4/\log|A|} \\ &= 158.03(2|A|k)^{\frac{\log 4}{\log|A|}} \leq 633(2k)^{\frac{\log 4}{\log|A|}},\end{aligned}$$

completing the proof of Theorem 2. □

We cannot do quite as well for $\mathbb{F}_q$ as for $\mathbb{F}_p$ because we do not have a good lower bound on $|2A|$. For $\mathbb{F}_p$ we were able to use the bound [9, Theorem 5.2], $|2A| \geq \min\{\frac{1}{4}|A|^{3/2}, \frac{p}{2}\}$. We do not know if such a bound holds in $\mathbb{F}_q$.

6. Proof of Theorem 4

For small $|A|$ we use the method of Bovey [4] to bound $\delta(A,q)$ and $\gamma(A,q)$. We start by generalizing [4, Lemma 3]. For any n-tuple $u = (u_1,\ldots,u_n) \in \mathbb{R}^n$ let $\|u\|_1 = \sum_{i=1}^n |u_i|$.

Lemma 19. *Let $\mathbb{F}_q$ be any finite field and $u_1, u_2, \ldots, u_n \in \mathbb{F}_q$. Let $T : \mathbb{Z}^n \to \mathbb{F}_q$ be the linear function $T(x_1,\ldots,x_n) = \sum_{i=1}^n x_i u_i$. Suppose that $v_1,\ldots,v_n \in \mathbb{Z}^n$ are linearly independent vectors over $\mathbb{R}$ with $T(v_i) = 0$, $1 \leq i \leq n$. Then for any value a in the range of T there exists a vector $u \in \mathbb{Z}^n$ with $T(u) = a$ and $\|u\|_1 \leq \frac{1}{2}\sum_{i=1}^n \|v_i\|_1$.*

Proof. Let $w \in \mathbb{Z}^n$ with $T(w) = a$. Write $w = \sum_{i=1}^n y_i v_i$ for some $y_i \in \mathbb{R}$, $1 \le i \le n$. Say $y_i = x_i + \epsilon_i$ for some $x_i \in \mathbb{Z}$ and $\epsilon_i \in \mathbb{R}$ with $|\epsilon_i| \le 1/2$, $1 \le i \le n$. Put $u = \sum_{i=1}^n \epsilon_i v_i = w - \sum_{i=1}^n x_i v_i$. Then $u \in \mathbb{Z}^n$, $T(u) = a$ and $\|u\|_1 \le \frac{1}{2}\sum_{i=1}^n \|v_i\|_1$. □

Proof of Theorem 4. By Theorem 9 (d), $\gamma(k,q) \le (t-1)\delta(k,q)$, where $t = |A|$, and so it suffices to prove the statement of Theorem 4 for $\delta(k,q)$. Put $r = \phi(t)$. Let R be a primitive t-th root of unity in $\mathbb{F}_q$, $\Phi_t(x)$ be the t-th cyclotomic polynomial over $\mathbb{Q}$ of degree r and ω be a primitive t-th root of unity over $\mathbb{Q}$. In particular, $\Phi_t(R) = 0$ and the set of nonzero k-th powers in $\mathbb{F}_q$ is just $\{1, R, R^2, \ldots, R^{t-1}\}$. Let $f : \mathbb{Z}^r \to \mathbb{Z}[\omega]$ be given by

$$f(x_1, x_2, \ldots, x_r) = x_1 + x_2\omega + \cdots + x_r\omega^{r-1}.$$

Then f is a one-to-one $\mathbb{Z}$-module homomorphism.

Let $T : \mathbb{Z}^r \to \mathbb{F}_q$ be the linear map $T(x_1, \ldots, x_r) = \sum_{i=1}^r x_i R^{i-1}$ and $\mathcal{L}$ be the lattice of points satisfying $T(x_1, \ldots, x_r) = 0$. Since the set of k-th powers $1, R, \ldots, R^{r-1}$ spans all of $\mathbb{F}_q$ we have $Vol(\mathcal{L}) = q$. Thus by Minkowski's fundamental theorem there is a nonzero vector $v_1 = (a_1, a_2, \ldots, a_r)$ in $\mathcal{L}$ with $|a_i| \le q^{1/r}$, $1 \le i \le r$. For $2 \le i \le r$ set $v_i = f^{-1}(\omega^{i-1} f(v_1))$. Then $v_1, \ldots, v_r$ form a set of linearly independent points in $\mathcal{L}$ and so, by Lemma 19, for any $a \in \mathbb{F}_q$ there is an r-tuple of integers $u = (u_1, \ldots, u_r)$ such that

$$u_1 + u_2 R + u_3 R^2 + \cdots + u_r R^{r-1} = a,$$

and $\sum_{i=1}^r |u_i| \le \frac{1}{2}\sum_{i=1}^r \|v_i\|_1$. Thus $\delta(k,q) \le \frac{1}{2}\sum_{i=1}^r \|v_i\|_1$. Now plainly $\|v_i\|_1 \ll_t q^{1/r}$, (indeed, as shown in [4], $\|v_i\|_1 \le r(A(t)+1)^r p^{n/r}$, where $A(t)$ is the maximal absolute value of the coefficients of $\Phi_t(x)$). Thus $\delta(k,q) \ll_t q^{1/r}$. □

7. Proof of Lemma 7(a)

Let $m \ge 3$ be a positive integer, $A, B \subseteq \mathbb{F}_q$, $A' = A - \{0\}$, $a \in \mathbb{F}_q$ and N denote the number of $2m$-tuples $(x_1, \ldots, x_m, y_1, \ldots y_m)$ with $x_1, x_2 \in A'$, $x_3, \ldots, x_m \in A$, $y_i \in B$, $1 \le i \le m$, and $x_1 y_1 + \cdots + x_m y_m = a$. Let ψ denote the additive character on $\mathbb{F}_q$, $\psi(z) = e^{2\pi i Tr(z)/p}$. Then

$$\begin{aligned} qN &= |A'|^2|A|^{m-2}|B|^m + \sum_{\lambda \ne 0} \sum_{x_1, x_2 \in A'} \sum_{x_3, .., x_m \in A} \sum_{y_i \in B} \psi(\lambda(x_1 y_1 + \cdots + x_m y_m - a)) \\ &= |A'|^2|A|^{m-2}|B|^m + Error, \end{aligned} \tag{20}$$

with

$$Error = \sum_{\lambda \ne 0} \psi(-\lambda a) \left(\sum_{x \in A} \sum_{y \in B} \psi(\lambda x y) \right)^{m-2} \left(\sum_{x \in A'} \sum_{y \in B} \psi(\lambda x y) \right)^2 .$$

Now, by the Cauchy-Schwarz inequality,

$$\left|\sum_{x\in A}\sum_{y\in B}\psi(\lambda xy)\right| \le \sum_{y\in B}\left|\sum_{x\in A}\psi(\lambda xy)\right| \le |B|^{1/2}\left(\sum_{y\in B}\left|\sum_{x\in A}\psi(\lambda xy)\right|^2\right)^{1/2}$$
$$\le |B|^{1/2}\left(\sum_{y\in\mathbb{F}_q}\left|\sum_{x\in A}\psi(\lambda xy)\right|^2\right)^{1/2} = |B|^{1/2}(q|A|)^{1/2}.$$

Also,

$$\sum_{\lambda\in\mathbb{F}_q}\left|\sum_{x\in A'}\sum_{y\in B}\psi(\lambda(xy))\right|^2 = \sum_{x_1,x_2\in A'}\sum_{y_1,y_2\in B}\sum_{\lambda\in\mathbb{F}_q}\psi(\lambda(x_1y_1-x_2y_2))$$
$$= q|\{(x_1,x_2,y_1,y_2) : x_1,x_2\in A', y_1,y_2\in B, x_1y_1 = x_2y_2\}| \le q|A'|^2|B|,$$

the latter following since $0\notin A'$, so $x_1y_1 = x_2y_2$ can be written $y_1 = x_1^{-1}x_2y_2$. Thus,

$$|Error| \le |A|^{\frac{m-2}{2}}|B|^{\frac{m-2}{2}}q^{\frac{m-2}{2}}\sum_{\lambda\neq 0}\left|\sum_{x\in A'}\sum_{y\in B}\psi(\lambda(xy))\right|^2$$
$$= |A|^{\frac{m-2}{2}}|B|^{\frac{m-2}{2}}q^{\frac{m-2}{2}}\left(\sum_{\lambda\in\mathbb{F}_q}\left|\sum_{x\in A'}\sum_{y\in B}\psi(\lambda(xy))\right|^2 - |A'|^2|B|^2\right)$$
$$\le |A|^{\frac{m-2}{2}}|B|^{\frac{m-2}{2}}q^{\frac{m-2}{2}}\left(q|A'|^2|B| - |A'|^2|B|^2\right)$$
$$= |A|^{\frac{m}{2}-1}|A'|^2|B|^{\frac{m}{2}}q^{\frac{m}{2}}\left(1-\tfrac{|B|}{q}\right),$$

and we see that the main term in (20) exceeds the error term provided that

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

References

[1] M. Bhaskaran, Sums of m-th powers in algebraic and abelian number fields, Arch. Math. (Basel) 17 (1966), 497-504; Correction, ibid. 22 (1972), 370-371.

[2] J. Bourgain,Mordell's exponential sum estimate revistited, J. Amer. Math. Soc. 18, no. 2 (2005), 477-499.

[3] J. Bourgain, A.A. Glibichuk and S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. London Math. Soc. (2) 73 (2006), 380-398.

[4] J. D. Bovey, A new upper bound for Waring's problem (mod p), Acta Arith. 32 (1977), 157-162.

[5] A. Cauchy, Recherches sur les nombres, J. Ecole Polytechnique 9 (1813), 99-116.

[6] J.A. Cipra, Waring's number in a finite field, Integers 9 (2009), 435-440.

[7] J.A. Cipra, Waring's Number over Finite Fields, Ph.D. Thesis, Kansas State University, 2009.

[8] J. A. Cipra, T. Cochrane and C. Pinner, Heilbronn's conjecture on Waring's number (mod p), J. Number Theory 125 (2007), no. 2, 289-297.

[9] T. Cochrane and C. Pinner, Sum-product estimates applied to Waring's problem mod p, Integers 8 (2008), 1-18.

[10] M. M. Dodson, On Waring's problem in GF[p], Acta Arith. 19 (1971), 147-173.

[11] M. M. Dodson and A. Tietäväinen, A note on Waring's problem in GF[p], Acta Arith. 30 (1976), 159-167.

[12] A.A. Glibichuk, Combinatorial properties of sets of residues modulo a prime and the Erdös-Graham problem, Mat. Zametki 79, no. 3, (2006), 384-395. Translated in Math. Notes 79, no. 3, (2006), 356-365.

[13] A.A. Glibichuk, Additive properties of products of subsets in the field $\mathbb{F}_{p^2}$, (Russian) Vestnik Moskov. Univ. Ser. I Mat. Mekh. 2009, , no. 1, 3-8, 71; translation in Moscow Univ. Math. Bull. 64 (2009), no. 1, 1-6.

[14] A.A. Glibichuk, Sums of powers of subsets of an arbitrary finite field, Izvestiya Math 75 (2011), no. 2, 253-285.

[15] A.A. Glibichuk and S.V. Konyagin, Additive properties of product sets in fields of prime order, Additive combinatorics, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007, 279-286.

[16] A.A. Glibichuk and M. Rudnev, On additive properties of product sets in an arbitrary finite field, (English summary) J. Anal. Math. 108 (2009), 159170.

[17] H. Heilbronn, Lecture Notes on Additive Number Theory mod p, California Institute of Technology (1964).

[18] S. V. Konyagin, On estimates of Gaussian sums and Waring's problem for a prime modulus, Trudy Mat. Inst. Steklov 198 (1992), 111-124; translation in Proc. Steklov Inst. Math. 1994, 105-107.

[19] M.B. Nathanson, Additive Number Theory, Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics 165, Springer, New York, 1996.

[20] A. Tietäväinen, Proof of a conjecture of S. Chowla, J. Number Theory 7 (1975), 353-356.

[21] L. Tornheim, Sums of n-th powers in fields of prime characteristic, Duke Math J. (1938), 359-362.

[22] A. Winterhof, On Waring's problem in finite fields, Acta Arith. 87 (1998), 171-177.

[23] A. Winterhof, A note on Waring's problem in finite fields, Acta Arith. 96 (2001), 365-368.