PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 4, April 2018, Pages 1377–1388
http://dx.doi.org/10.1090/proc/13915
Article electronically published on December 28, 2017

SUMS OF INVERSES IN THIN SETS OF FINITE FIELDS

IGOR E. SHPARLINSKI AND ANA ZUMALACÁRREGUI

(Communicated by Matthew A. Papanikolas)

Abstract. We obtain lower bounds for the cardinality of k-fold sum-sets of reciprocals of elements of suitable defined short intervals in high degree extensions of finite fields. Combining our results with bounds for multilinear character sums we obtain new results on incomplete multilinear Kloosterman sums in finite fields.

1. Introduction

1.1. **Background.** Let p be a prime number and let $\mathbb{F}_p$ be the finite field of p elements.

Bourgain and Garaev [4] have studied the additive properties of the multiple sum-sets of reciprocals from a short interval, that is, sum-sets of

$$\mathcal{I}_{u,h}^{-1} = \left\{x^{-1} \ : \ x \in \mathcal{I}_{u,h},\, x \neq 0\right\},$$

where $\mathcal{I}_{u,h}$ is the reduction modulo p of the set $\{u+1,\ldots,u+h\}$ of consecutive integers for some integers h and u with $p > h \geq 1$. In particular, by [4, Theorem 4] there is an absolute constant $c > 0$ such that if $h \leq p^{c/k^2}$, then for the k folded sum-set of $\mathcal{I}_{u,h}^{-1}$, that is, for

$$k\left(\mathcal{I}_{u,h}^{-1}\right) = \left\{x_1^{-1} + \cdots + x_k^{-1} \ : \ x_j \in \mathcal{I}_{u,h},\ x_j \neq 0, i = 1,\ldots,k\right\},$$

for any fixed k and $h \to \infty$, we have

$$\#k\left(\mathcal{I}_{u,h}^{-1}\right) \geq h^{k+o(1)}. \tag{1.1}$$

Observe that this estimate is almost optimal, since we trivially have $\#k\left(\mathcal{I}_{u,h}^{-1}\right) \leq h^k$.

Here we study an analogous problem in large extensions of finite fields. Namely, let $\mathbb{F}_q$ be the finite field of q elements, of characteristic p, and let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. We fix an algebraic element $\alpha \in \overline{\mathbb{F}}_q$ of degree n over $\mathbb{F}_q$, and denote by $\psi(x)$ its characteristic polynomial (that is, $\psi \in \mathbb{F}_q[T]$ is a monic irreducible polynomial of degree n and $\psi(\alpha) = 0$). Then we have that the finite extension $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q[\alpha]$, or equivalently $\mathbb{F}_{q^n} \cong \mathbb{F}_q[T]/\psi(T)$. In this setting the natural generalization of a *short interval* is the shifted set of *polynomials of small degree*.

Received by the editors December 6, 2016.
2010 *Mathematics Subject Classification.* Primary 11B30, 11T30.
Key words and phrases. Finite fields, polynomials, inversions, sum-sets.
This work was supported by ARC Grant DP140100118.

More precisely, for a given $m \le n$ let us consider the following vector space of dimension m:

$$\mathcal{V}_m = \left\{x \ : \ x = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1},\ a_0, \ldots, a_{m-1} \in \mathbb{F}_q\right\}.$$

Note that every element x in $\mathcal{V}_m$ can be identified with a polynomial $x(T)$ of degree at most $m-1$ in $\mathbb{F}_q[T]/\psi(T)$.

For a fixed element $\gamma \in \mathbb{F}_{q^n}$, we are interested in the additive properties of the inverses of elements in the affine vector space $\mathcal{J}_{\gamma,m} = \{\gamma\}+\mathcal{V}_m$. It is also convenient to define

$$\mathcal{J}^*_{\gamma,m} = \mathcal{J}_{\gamma,m} \setminus \{0\},$$

which we call an *interval* in $\mathbb{F}_{q^n}$. In particular $\mathcal{V}_m$ plays the role of the *initial interval*.

1.2. **Sums of reciprocals from a short interval.** We are interested in counting the number of solutions to

$$\frac{1}{x_1+\gamma} + \ldots + \frac{1}{x_k+\gamma} = \frac{1}{x_{k+1}+\gamma} + \ldots + \frac{1}{x_{2k}+\gamma},$$

with $x_1, \ldots, x_{2k} \in \mathcal{V}_m$ and fixed $\gamma \in \mathbb{F}_{q^n}$.

It is clear from the isomorphism $\mathbb{F}_{q^n} \cong \mathbb{F}_q[T]/\psi(T)$ that this problem is equivalent to counting the number $N_k(\gamma, m, \psi)$ of solutions to

$$\begin{aligned}\frac{1}{x_1(T)+\gamma(T)} + \ldots + \frac{1}{x_k(T)+\gamma(T)} \\ \equiv \frac{1}{x_{k+1}(T)+\gamma(T)} + \ldots + \frac{1}{x_{2k}(T)+\gamma(T)} \pmod{\psi(T)}\end{aligned}$$

where $x_1, \ldots, x_{2k} \in \mathbb{F}_q[T]$, with $\deg_T(x_i) \le m-1$ for $i = 1, \ldots, 2k$, and a fixed polynomial $\gamma(T) \in \mathbb{F}_q[T]$.

Theorem 1.1. *Uniformly over q, $\gamma \in \mathbb{F}_q[T]$ and fixed $k \ge 1$, if $m < n/(4k^2-2k)$, then*

$$N_k(\gamma, m, \psi) \le q^{(k+o(1))m}$$

as $m \to \infty$.

More concretely, this result gives an equivalent of the bound (1.1) for the set

$$k\left(\mathcal{J}^{-1}_{\gamma,m}\right) = \left\{x_1^{-1} + \cdots + x_k^{-1} \ : \ x_1, \ldots, x_k \in \mathcal{J}^*_{\gamma,m}\right\}.$$

Observe that the trivial bound in this case is

$$\#k\left(\mathcal{J}^{-1}_{\gamma,m}\right) \le \left(\#\mathcal{J}_{\gamma,m}\right)^k = q^{mk}.$$

Now, using the Cauchy inequality we immediately derive Theorem 1.1 (see a short standard proof in Section 3.2).

Corollary 1.2. *Uniformly over q, $\gamma \in \mathbb{F}_{q^n}$ and fixed $k \ge 1$, if $m < n/(4k^2-2k)$, then*

$$\#k\left(\mathcal{J}^{-1}_{\gamma,m}\right) \ge q^{(k+o(1))m}$$

as $m \to \infty$.

1.3. **Bounds of character sums.** As it has been noticed by Karatsuba [9], see also [8, 11], bounds on the number of solutions of equations with reciprocals can be translated into bounds for short multiple Kloosterman sums. In particular, we obtain an analogue of a similar result of Bourgain and Garaev [4, Theorem 12]. We note however that our estimate is weaker since the underlying tool, the bound on multilinear additive character sums in arbitrary finite fields, due to Bourgain and Glibichuk [7, Theorem 4] is weaker than its counterpart over prime fields given by Bourgain [3, Theorem 3] (but is somewhat more explicit, similarly to [3, Theorem 5]).

Besides, in the case of arbitrary finite fields $\mathbb{F}_{q^n}$ there are some necessary restrictions on the size of the intersections of the sets involved with proper subfields of $\mathbb{F}_{q^n}$. Within the above approach, these sets are related to the initial data in a rather complicated way so to avoid this difficulty we impose the primality condition on both q and n. These conditions can be relaxed, but they allow us to exhibit the ideas in the simplest form.

Theorem 1.3. *Let $\mathbb{F}_{p^n}$ be a finite field with a fixed prime p and a sufficiently large prime n. Assume that positive integers m and d satisfy*

$$m < n/4 \qquad \text{and} \qquad d \ge \frac{302900n}{(m^{1/2}n^{1/2} - 2m)}.$$

There exists $\delta > 0$ depending only on d, such that for any intervals $\mathcal{J}_1, \ldots, \mathcal{J}_d \subseteq \mathbb{F}_{p^n}$ of dimension m, an additive character χ in $\mathbb{F}_{p^n}$ and complex weights $\alpha_i(x_i)$ defined on $x_i \in \mathcal{J}_i$ with

$$|\alpha_i(x_i)| \le 1, \qquad x_i \in \mathcal{J}_i,$$

for $i = 1, \ldots, d$, we have

$$\left| \sum_{x_1 \in \mathcal{J}_1} \cdots \sum_{x_d \in \mathcal{J}_d} \alpha_1(x_1) \cdots \alpha_d(x_d)\, \chi\left((x_1 \cdots x_d)^{-1}\right) \right| \le p^{dm - \delta n}.$$

2. Preliminary results

2.1. **Some general results.** Since we have polynomials in variables T and also in Z, to avoid any confusion we always write $\deg_T$ to denote the degree in T (even when Z is not present).

The following result is necessary for the proof of Theorem 1.1 and can be found in [12, Corollary 3].

Lemma 2.1. *Let $2 \le s, \ell \le k$ be fixed integers. Let $f(Z)$ and $g(Z)$ be polynomials*

$$f(Z) = \sum_{i=1}^{s-1} a_i Z^i \quad \text{and} \quad g(Z) = \sum_{i=1}^{\ell-1} b_i Z^i,$$

with polynomial coefficients $a_i(T), b_i(T) \in \mathbb{F}_q[T]$, such that $a_{s-1}, b_{\ell-1} \ne 0$ and

$$\deg_T a_i, \deg_T b_i < (k-i)M, \qquad i = 1, \ldots, k-1,$$

for some integer $M \ge 1$. Then, the degree of the resultant $\operatorname{Res}(f, g)$ of f and g satisfies that

$$\deg_T \operatorname{Res}(f, g) \le (k^2 - 1)M.$$

The following result can be found in [12, Lemma 1] and it is useful in the proof of Theorem 1.1.

Lemma 2.2. *The number of divisors of a polynomial $f \in \mathbb{F}_q[T]$ of degree s is at most $q^{c_0 s/\log s}$ for some absolute constant c_0.*

The following result is a modification of [4, Lemma 5], but the proof is completely analogous and therefore it is omitted.

Lemma 2.3. *Let S be a finite subset of a field K, $c \in K$ and $c_1, \ldots, c_k \in K^*$. Let T_r denote the number of solutions of the equation*

$$c_1 x_1 + \cdots + c_r x_r = c, \quad x_1, \ldots, x_r \in S,$$

and J_{2s} the number of solutions of the equation

$$x_1 + \cdots + x_s = x_{s+1} + \cdots + x_{2s}, \quad x_1, \ldots, x_{2s} \in S.$$

If $r = 2k$ for some integer k, then $T_r \le J_{2k}$. If $r = 2k+1$ for some integer k, then $T_r^2 \le J_{2k-2} J_{2k}$.

Note that Lemma 2.3 is used to exclude degenerate cases when counting solutions to our equation.

The following result can be found in [7, Theorem 4] and it is a generalization of [4, Lemma 1] for finite fields.

We define $\omega = 156450$ (related to the constant that appears in the formulation of Theorem 1.3).

Lemma 2.4. *Let r be a sufficiently large prime power and let d be any integer with $3 \le d \le 0.9 \log_2 \log_2 r$. For $0 < \eta \le 1$ define $\tau = \min(1/\omega, \eta/120)$. Suppose that the sets $\mathcal{A}_1, \cdots, \mathcal{A}_d \subseteq \mathbb{F}_r^*$, with at least 3 elements are such that for every $i = 3, \ldots, d$, for any element $t \in \mathbb{F}_r^*$ and proper subfield $\mathbb{L} \subseteq \mathbb{F}_r^*$ we have $\#(\mathcal{A}_i \cap t\mathbb{L}) \le \#\mathcal{A}_i^{1-\eta}$. Assume further that for some $\varepsilon > 0$,*

$$\#\mathcal{A}_1 \cdot \#\mathcal{A}_2 \left(\#\mathcal{A}_3 \cdots \#\mathcal{A}_d\right)^{\tau} > r^{1+\varepsilon}.$$

Then, for any nontrivial additive character χ of $\mathbb{F}_r$ we have

$$\left| \sum_{a_1 \in \mathcal{A}_1} \cdots \sum_{a_d \in \mathcal{A}_d} \chi(a_1 \cdots a_d) \right| < 100\, \#\mathcal{A}_1 \cdots \#\mathcal{A}_d \cdot r^{-0.45\varepsilon/2^d}.$$

In order to effectively apply Lemma 2.4 one has to study carefully the elements of $k(\mathcal{J}_{\gamma,m}^{-1})$ in subfields. We restrict the study to the simplest case, where there is only one proper subfield.

Corollary 2.5. *Let $\mathcal{A}_1, \cdots, \mathcal{A}_d \subseteq \mathbb{F}_{p^n}^*$, with p and n prime, of cardinality $\#\mathcal{A}_i \ge p^{\sigma}$, $i = 1, \ldots, d$, for some real σ with*

$$\frac{\omega n}{2\omega + d - 2} < \sigma \le n.$$

Then, there exist $\delta > 0$ that depends only on d and σ such that for sufficiently large n, we have

$$\left| \sum_{a_1 \in \mathcal{A}_1} \cdots \sum_{a_d \in \mathcal{A}_d} \chi(a_1 \cdots a_d) \right| < 100\, \#\mathcal{A}_1 \cdots \#\mathcal{A}_d \cdot p^{-n\delta}.$$

Proof. The only proper subfield in $\mathbb{F}_{p^n}$ is $\mathbb{F}_p$, therefore it is clear that

$$\#(\mathcal{A}_i \cap t\mathbb{F}_p) \le p \le p^{\sigma(1-\eta)} \le \#\mathcal{A}_i^{1-\eta}$$

for any $0 < \eta < 1 - 1/\sigma$. Furthermore, from the hypothesis

$$\#\mathcal{A}_1 \cdot \#\mathcal{A}_2 \left(\#\mathcal{A}_3 \cdots \#\mathcal{A}_d\right)^{1/\omega} \geq p^{\sigma(2+(d-2)/\omega)} > p^{n(1+\varepsilon)},$$

for any

$$0 < \varepsilon < \frac{\sigma(2\omega + d - 2)}{\omega n} - 1.$$

The result now follows from Lemma 2.4 for $\delta = 0.45\varepsilon/2^d$. □

2.2. **Sums of inverses in function fields.** We now establish an analogue of [4, Lemma 6], which is the main ingredient in the proof of Theorem 1.1 and which we believe is of independent interest.

Let $\mathcal{P}_m$ be the set of polynomials $x \in \mathbb{F}_q[T]$ of degree $\deg_T x < m$. In particular $\#\mathcal{P}_m = q^m$.

For a fixed $\beta \in \overline{\mathbb{F}_q(T)}$, where $\overline{K}$ denotes the algebraic closure of the field K, and positive integers k and m we now define $N_k(\beta, m)$ as the number of solutions to the equation

$$\begin{aligned} \frac{1}{x_1(T) + \beta(T)} + \cdots + \frac{1}{x_k(T) + \beta(T)} \\ = \frac{1}{x_{k+1}(T) + \beta(T)} + \cdots + \frac{1}{x_{2k}(T) + \beta(T)}, \end{aligned} \tag{2.1}$$

with $x_i \in \mathcal{P}_m$ for $i = 1, \ldots, 2k$.

Lemma 2.6. *Let $k \geq 1$. Then uniformly over q and $\beta \in \overline{\mathbb{F}_q(T)}$ we have*

$$N_k(\beta, m) \leq q^{(k+o(1))m}$$

as $m \to \infty$.

Proof. To simplify the counting, we split the total number of solutions $N_k(\beta, m)$ separating the contribution $N_k^{=}(\beta, m)$ from the solutions satisfying $x_i = x_j$ for some $i \neq j$, and the contribution $N_k^{\neq}(\beta, m)$ from the solutions

$$\mathbf{x} = (x_1, \ldots, x_{2k}) \in \mathcal{P}_m^{2k}, \quad \text{with } x_i \neq x_j \text{ for } 1 \leq i \neq j \leq 2k.$$

We derive this bound by induction on k. It is clear that if $k = 1$ the assertion is trivial. Suppose that $k \geq 2$. It follows from Lemma 2.3 that the number $N_k^{=}(\beta, m)$ of solutions satisfying $x_i = x_j$ for some $i \neq j$ contributes to the total number of solutions $N_k(\beta, m)$ at most

$$N_k^{=}(\beta, m) = O\left(\sqrt{N_{k-1}(\beta, m) N_k(\beta, m)} + q^m N_{k-1}(\beta, m)\right)$$

(note that the first term is responsible for coincidences between the variables on the same side of the equation, while the second term comes from coincidences on the opposite sides).

Hence, by the induction hypothesis

$$\begin{aligned} N_k^{=}(\beta, m) &= O\left(q^{(k/2+o(1))m} \sqrt{N_k(\beta, m)} + q^{(k+o(1))m}\right) \\ &= O\left(q^{(k/2+o(1))m} \sqrt{N_k^{=}(\beta, m) + N_k^{\neq}(\beta, m)} + q^{(k+o(1))m}\right). \end{aligned}$$

Clearly it suffices to show that $N_k^{\neq}(\beta, m) \leq q^{(k+o(1))m}$.

We must now count the number of solutions in $\overline{\mathbb{F}_q(T)}$ to

$$\prod_{i\neq 1}(x_i+\beta)+\cdots+\prod_{i\neq k}(x_i+\beta)=\prod_{i\neq k+1}(x_i+\beta)+\cdots+\prod_{i\neq 2k}(x_i+\beta) \tag{2.2}$$

with $x_i \in \mathbb{F}_q[T]$, $x_i \neq x_j$ and $\deg_T(x_i) < m$, for $1 \leq i \neq j \leq 2k$.

Observe that if follows from (2.2) that β is algebraic over $\mathbb{F}_q(T)$ of degree d, with $1 \leq d \leq 2k-2$. Therefore, it can be written as $\beta = \xi/\mu$ with $\mu \in \mathbb{F}_q[T]$ a polynomial of degree at most $m(2k-2) = O(m)$ and ξ an algebraic integer of degree d over $\mathbb{F}_q[T]$.

From (2.2), the polynomial

$$\begin{aligned} q^{2k-1}\prod_{j\neq i}(x_j-x_i) &= \prod_{j\neq i}((\mu x_j+\xi)-(\mu x_i+\xi)) \\ &= (\mu x_i+\xi)\cdot H(x_1,\dots,x_{2k})+\prod_{j\neq i}(\mu x_j+\xi) \end{aligned}$$

(for some polynomial H in $2k$ variables) is divisible by $(\mu x_i+\xi)$ in a certain algebraic extension of the function field $\mathbb{F}_q(T)$ and is nonzero since $x_i \neq x_j$ for every $i \neq j$.

In particular the norm

$$\mathrm{Nm}(\mu x_i+\xi) \mid q^{(2k-1)d}\prod_{j\neq i}(x_j-x_i)^d \tag{2.3}$$

as a polynomial in $\mathbb{F}_q[T]$.

We now fix x_1. Recalling (2.3), we see that we can decompose the polynomial $\mathrm{Nm}(\mu x_1+\xi) = F_1G_1$ with $G_1 \mid \mu$ and $\gcd(F_1, q) = 1$, also

$$\deg_T F_1, \deg_T G_1 \leq d(2k-1)m = O(m).$$

For every divisor $f_1 = \prod_{j\geq 2} r_j$ of F_1, with $F_1 \mid f_1^d$, we can construct the arithmetic progressions $\mathcal{L}_{2,j}$

$$x_j \equiv x_1 \pmod{r_j}, \quad 2 \leq j \leq 2k. \tag{2.4}$$

Since the $\deg_T(x_j - x_1) < m$ the number of elements in $\mathcal{L}_{2,j}$ is at most $q^{m-\deg r_j}$ and therefore

$$\prod_{j\geq 2}\#\mathcal{L}_{2,j} < q^{m-\deg r_2}\cdots q^{m-\deg r_{2k}} = \frac{q^{m(2k-1)}}{q^{\deg f_1}}. \tag{2.5}$$

For any of the q^m possibilities for x_1 it follows from Lemma 2.2 that there are at most $q^{o(m)}$ choices for f_1 and thus, from (2.5),

$$N_k^{\neq}(\beta, m) \leq \frac{q^{2km+o(m)}}{q^{m_1}}, \tag{2.6}$$

where m_1 is the most popular degree amongst all the polynomials f_1.

On the next step for every $x_2 \in \mathcal{L}_{2,2}$ we can factor the norm $\mathrm{Nm}(\mu x_2+\xi)$ as

$$\mathrm{Nm}(\mu x_2+\xi) = F_2G_2$$

where the irreducible factors of G_2 either divide μ or $\mathrm{Nm}(\mu x_1+\xi)$, and F_2 is not only coprime with μ but also with $\mathrm{Nm}(\xi+\mu x_1)$ (and in particular with (x_2-x_1)). Once again, from (2.3) it follows that

$$F_2 \mid \prod_{j\geq 3}(x_j-x_2)^d.$$

Once again, every divisor f_2 of F_2 with $F_2 \mid f_2^d$ can be written as

$$f_2 = \prod_{j\geq 3} s_j,$$

with $s_j|(x_j - x_2)$. For every such divisor we can construct arithmetic progressions $\mathcal{L}_{3,j} \subseteq \mathcal{L}_{2,j}$, satisfying both (2.4) and

$$x_j \equiv x_2 \pmod{s_j}, \quad 3 \leq j \leq 2k,$$

where $\gcd(r_j, s_j) = 1$. In particular, this implies that

$$\#\mathcal{L}_{3,j} \leq q^{-\deg s_j} \#\mathcal{L}_{2,j}$$

and thus

$$\prod_{j\geq 3} \#\mathcal{L}_{2,j} \leq \frac{1}{q^{\deg f_2}} \prod_{j\geq 3} \#\mathcal{L}_{3,j}. \tag{2.7}$$

As before, if we denote by m_2 the most popular degree amongst all the polynomials f_2 it follows from (2.6) and (2.7)

$$N_k^{\neq}(\beta, m) \leq \frac{q^{2km+o(m)}}{q^{m_1} q^{m_2}}.$$

For every $x_3 \in \mathcal{L}_{3,3}$ once again we can factorize $\mathrm{Nm}(\mu x_3 + \xi) = F_3 G_3$ where the irreducible factors of G_3 either divide μ, $\mathrm{Nm}(\mu x_1 + \xi)$ or $\mathrm{Nm}(\mu x_2 + \xi)$ and F_3 is coprime to them. For each divisor f_3 of F_3, with $F_3 \mid f_3^d$, we can define arithmetic progressions $\mathcal{L}_{4,j} \subset \mathcal{L}_{3,j}$ for $4 \leq j \leq 2k$ as we did before so

$$\prod_{j\geq 4} \#\mathcal{L}_{3,j} \leq \frac{1}{q^{\deg f_3}} \prod_{j\geq 4} \#\mathcal{L}_{4,j}.$$

The process is now clear: we subsequently fix $x_1 \in \mathcal{P}_m$; then $x_2 \in \mathcal{L}_{2,2}$, then $x_3 \in \mathcal{L}_{3,3}$, and so on, and estimate the number of solutions as

$$N_k^{\neq}(\beta, m) \leq \frac{q^{2km+o(m)}}{q^{m_1+\cdots+m_{2k-1}}}. \tag{2.8}$$

On the other hand, since $G_1 \mid \mu^d$ and $\deg \mu^d = O(m)$, it is clear that $\deg G_1 = O(m)$. It follows from Lemma 2.2 that the number of possibilities for G_1 is, independently of x_1, at most $q^{o(m)}$.

Since $F_1 \mid f_1^d$ there are at most $q^{o(m)}$ possibilities for F_1 once f_1 is fixed. Thus, for any given f_1 there exist at most $q^{o(m)}$ possible values for x_1. Taking into account that the degree m_1 is chosen so the number of possible polynomials f_1 with degree different from m_1 is $O(mq^{m_1})$ (that is, it is the most popular degree amongst all the possible choices) we have that there are at most $q^{m_1+o(m)}$ possible values for x_1. For any fixed x_1, following the same arguments, we have that the number of possibilities for x_2 is at most $q^{m_2+o(m)}$. Thus, continuing this procedure

$$N_k^{\neq}(\beta, m) \leq q^{m_1+\cdots+m_{2k-1}+o(1)}.$$

Combining this bound with (2.8), the result follows. □

3. Proofs on main results

3.1. **Proof of Theorem 1.1.** Within the proof, we consider the elements in $\mathbb{F}_{q^n}$ as classes of polynomials $x(T)$ in $\mathbb{F}_q[T]/\psi(T)$, where $\psi(T)$ is an irreducible polynomial of degree n. Elements $x_i \in \mathcal{V}_m$ can be identified precisely with polynomials in $\mathcal{P}_m \subseteq \mathbb{F}_q[T]$.

Let us denote by $N_k(\gamma, m, \psi)$ the number of solutions to

$$\sum_{i=1}^{k} \frac{1}{x_i(T)+\gamma(T)} \equiv \sum_{j=k+1}^{2k} \frac{1}{x_j(T)+\gamma(T)} \pmod{\psi(T)}, \tag{3.1}$$

with $x_1, \dots, x_{2k} \in \mathbb{F}_q[x]$ with $\deg_T(x_i) < m$, and $N_k^{\neq}(\gamma, m, \psi)$ the number of solutions with $x_i \neq x_j$ for $1 \leq i \neq j \leq 2k$. As in the proof of Lemma 3.1 it suffices to show that $N_k^{\neq}(\gamma, m, \psi) \leq q^{(k+o(1))m}$.

For every solution $\mathbf{x} = (x_1, \dots, x_{2k})$ contributing to $N_k^{\neq}(\gamma, m, \psi)$ we construct the polynomial

$$\begin{aligned} P_{\mathbf{x}}(Z) &= \sum_{s=1}^{k} \prod_{j\neq s} (x_j(T)+Z) - \sum_{s=k+1}^{2k} \prod_{i\neq s}^{k} (x_i(T)+Z) \\ &= A_0(T) + A_1(T)Z + \cdots + A_{2k-2}(T)Z^{2k-2} \in \mathbb{F}_q[T][Z]. \end{aligned} \tag{3.2}$$

It follows from (3.1) that $P_{\mathbf{x}}(\gamma(T)) \equiv 0 \pmod{\psi(T)}$. Furthermore, since by hypothesis $x_1(T) \neq x_i(T)$ for $i = 2, \dots, 2k$, it is clear that

$$P_{\mathbf{x}}(-x_1(T)) = \prod_{i\neq 1} (x_i(T) - x_1(T)) \neq 0,$$

and the polynomial is nonconstant in $\mathbb{F}_q[T][Z]$. In fact, the polynomial is nonconstant modulo $\psi(T)$ either, since

$$\deg_T P_{\mathbf{x}}(-x_1) < (2k-1)m < n = \deg_T \psi$$

by hypothesis.

Observe that since for every $1 \leq i \leq 2k$ we have $\deg_T x_i < m$, the coefficients of $P_{\mathbf{x}}$ satisfy

$$\deg_T A_j < (2k-1-j)m, \quad \text{for } j = 0, \dots, 2k-2.$$

For any $\mathbf{x}, \mathbf{y}$ two solutions the corresponding polynomials $P_{\mathbf{x}}, P_{\mathbf{y}}$ satisfy: $P_{\mathbf{x}}(\gamma) \equiv P_{\mathbf{y}}(\gamma) \equiv 0 \pmod{\psi(T)}$ and hence its resultant

$$\operatorname{Res}(P_{\mathbf{x}}, P_{\mathbf{y}}) \equiv 0 \pmod{\psi(T)}.$$

Furthermore, it follows from Lemma 2.1 that

$$\deg_T \operatorname{Res}(P_{\mathbf{x}}, P_{\mathbf{y}}) \leq 4k(k-1)m < n = \deg_T(\psi)$$

so in fact $\operatorname{Res}(P_{\mathbf{x}}, P_{\mathbf{y}}) = 0$ as a polynomial with coefficients in $\mathbb{F}_q[T]$. In particular, this implies that any two polynomials $P_{\mathbf{x}}, P_{\mathbf{y}}$ have a common root in $\overline{\mathbb{F}}_q(T)$.

We fix a solution $\mathbf{c} = (c_1, \dots, c_{2k})$ and consider the set $\{\beta_1, \dots, \beta_s\}$ of all $s \leq 2k-2$ roots of $P_{\mathbf{c}}(Z)$ in $\overline{\mathbb{F}}_q(T)$, Then, for every solution $\mathbf{x}$ the polynomial $P_{\mathbf{x}}$ has a common root with $P_{\mathbf{c}}$. Hence, the number of solutions to (3.1) can be bounded by

$$(2k-2) \max_{1\leq i\leq s} \#\{P \in \mathbb{F}_q[T][Z] : \text{ of the form (3.2) and } P(\beta_i) = 0\}.$$

For any fixed root $\beta \in \{\beta_1, \dots, \beta_s\}$ of $P_{\mathbf{c}}$ the number of polynomials of the form (3.2) with $P(\beta) = 0$ is precisely the number $N_k(\beta, m)$ of solutions to (2.1) which, from Lemma 2.6, is at most $q^{(k+o(1))m}$.

3.2. **Proof of Corollary 1.2.** Let $T(\lambda)$ be the number of solutions to the equation

$$x_1^{-1} + \dots + x_k^{-1} = \lambda, \qquad x_1, \dots, x_k \in \mathcal{J}_{\gamma,m}^*.$$

Obviously

$$\sum_{\lambda \in k\left(\mathcal{J}_{\gamma,m}^{-1}\right)} T(\lambda) = \left(\#\left(\mathcal{J}_{\gamma,m}^*\right)\right)^k \geq \left(q^m - 1\right)^k$$

and

$$\sum_{\lambda \in k\left(\mathcal{J}_{\gamma,m}^{-1}\right)} T(\lambda)^2 = N_k(\gamma, m, \psi).$$

Then, by the Cauchy inequality, we have

$$\begin{aligned}\left(q^m - 1\right)^{2k} &\leq \left(\#\left(\mathcal{J}_{\gamma,m}^*\right)\right)^{2k} \\ &\leq \#k(\mathcal{J}_{\gamma,m}^{-1}) \sum_{\lambda \in k\left(\mathcal{J}_{\gamma,m}^{-1}\right)} T(\lambda)^2 = \#k(\mathcal{J}_{\gamma,m}^{-1}) N_k(\gamma, m, \psi).\end{aligned}$$

Using Theorem 1.1, we conclude the proof.

3.3. **Proof of Theorem 1.3.** For a nontrivial additive character χ, let

$$S = \sum_{x_1 \in \mathcal{J}_1} \cdots \sum_{x_d \in \mathcal{J}_d} \alpha_1(x_1) \cdots \alpha_d(x_d)\, \chi\left(\left(x_1 \cdots x_d\right)^{-1}\right).$$

It follows from the simple observation that for any complex number $|z|^2 = z \cdot \overline{z}$, for any sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_{p^n}$ and the weights $\{\alpha(v)\}_{v \in \mathcal{V}}$ with $|\alpha(v)| \leq 1$, we have

$$\sum_{u \in \mathcal{U}} \left| \sum_{v \in \mathcal{V}} \alpha(v) \chi(uv) \right|^{2k} \leq \sum_{v_1, \dots, v_{2k} \in \mathcal{V}} \left| \sum_{u \in \mathcal{U}} \chi\left(u \sum_{i=1}^{2k} (-1)^i v_i\right) \right|, \tag{3.3}$$

for every integer k.

Let us denote $J = \#\mathcal{J}_i = p^m$, to simplify the notation.

The bound (3.3), together with the Hölder inequality, applied d times, exactly as in the proof of [4, Theorem 12], gives

$$|S|^{(2k)^d} \leq J^{d(2k)^d - 2kd} \sum_{\substack{x_{i,1} \in \mathcal{J}_1 \\ i=1,\cdots,2k}} \cdots \sum_{\substack{x_{i,d,} \in \mathcal{J}_d \\ i=1,\cdots,2k}} \prod_{j=1}^{d} \chi\left(\sum_{i=1}^{2k} (-1)^i x_{i,j}^{-1}\right).$$

We can fix $x_{2i-1,j}$ for every $i = 1, \dots, k$ and $j = 1, \dots, d$ in such a way that for some elements $c_1, \dots, c_d$ we have

$$\begin{aligned}|S|^{(2k)^d} &\leq J^{d(2k)^d - kd} \left| \sum_{\substack{x_{i,1} \in \mathcal{J}_1 \\ i=1,\cdots,k}} \cdots \sum_{\substack{x_{i,d} \in \mathcal{J}_d \\ i=1,\cdots,k}} \chi\left(\prod_{j=1}^{d} \left(\sum_{i=1}^{k} x_{i,j}^{-1} - c_j\right)\right) \right| \\ &\leq J^{d(2k)^d - kd} \left| \sum_{\lambda_1 \in \mathbb{F}_{p^n}} \cdots \sum_{\lambda_d \in \mathbb{F}_{p^n}} T_1(\lambda_1) \cdots T_d(\lambda_d)\, \chi(\lambda_1 \cdots \lambda_d) \right|, \end{aligned} \tag{3.4}$$

where $T_j(\lambda)$ denotes the number of solutions to

$$y_1^{-1} + \cdots + y_k^{-1} - c_j = \lambda, \qquad y_1, \ldots, y_k \in \mathcal{J}_j.$$

For any k, to be chosen later, satisfying

$$m < \frac{n}{4k^2 - 2k} \tag{3.5}$$

we have from Theorem 1.1 that the number of solutions to the congruence

$$y_1^{-1} + \cdots + y_k^{-1} = y_{k+1}^{-1} + \cdots + y_{2k}^{-1}, \qquad y_1, \ldots, y_{2k} \in \mathcal{J}_j,$$

is bounded by $J^{k+o(1)}$. Therefore, in particular, for every $j = 1, \ldots, d$, for the L^2-norm of T_j we have

$$\|T_j\|_2^2 = \sum_{\lambda \in \mathbb{F}_{p^n}} T_j(\lambda)^2 \le J^{k+o(1)}. \tag{3.6}$$

Now, let us estimate the sum in (3.4), that is,

$$W = \sum_{\lambda_1 \in \mathbb{F}_{p^n}} \cdots \sum_{\lambda_{d-1} \in \mathbb{F}_{p^n}} T_1(\lambda_1) \cdots T_d(\lambda_d)\, \chi(\lambda_1 \cdots \lambda_{d-1}).$$

Let

$$\mathcal{A}_j = \{\lambda \in \mathbb{F}_{p^n} \ : \ \lambda = y_1^{-1} + \cdots + y_k^{-1} - c_j, \text{ for } y_1, \ldots, y_k \in \mathcal{J}_j\}$$

be the set on which $T_j(\lambda)$ is supported, $j = 1, \ldots, d$. By the Cauchy inequality

$$|W|^2 \le \|T_1\|_2^2 \cdots \|T_{d-1}\|_2^2 \left| \sum_{u,v \in \mathcal{A}_d} \sum_{\lambda_1 \in \mathcal{A}_1} \cdots \sum_{\lambda_{d-1} \in \mathcal{A}_{d-1}} T_d(u) T_d(v) \chi(\lambda_1 \cdots \lambda_{d-1}(u - v)) \right|.$$

Hence, using the bounds in (3.6), we have

$$|W|^2 \le J^{(d-1)k+o(1)} \sum_{u,v \in \mathcal{A}_d} T_d(u) T_d(v) \left| \sum_{\lambda_1 \in \mathcal{A}_1} \cdots \sum_{\lambda_{d-1} \in \mathcal{A}_{d-1}} \chi\left(\lambda_1 \cdots \lambda_{d-1}(u - v)\right) \right|. \tag{3.7}$$

Let us note that, to estimate the contribution from the inner sum in (3.7) we use Corollary 2.5 with $d - 1$ and $\sigma = m(k + o(1))$. Clearly, from Corollary 1.2, which applies due to the condition (3.5), we have $\#\mathcal{A}_j = J^{k+o(1)}$, $j = 1, \ldots, d$. Also, let us further assume that k satisfies

$$m > \frac{\omega n}{k(2\omega + d - 3)}. \tag{3.8}$$

Therefore, it follows from Corollary 2.5 that the contribution to (3.7) from diagonal terms with $u = v$ is precisely

$$\|T_d\|_2^2 \, \#\mathcal{A}_1 \cdots \#\mathcal{A}_{d-1} \le J^{dk+o(1)}. \tag{3.9}$$

It follows from Corollary 2.5 that for some $\delta_0 > 0$, depending only on d, for every $t \in \mathbb{F}_{p^n}^*$ we have

$$\left| \sum_{\lambda_1 \in \mathcal{A}_1} \cdots \sum_{\lambda_{d-1} \in \mathcal{A}_{d-1}} \chi(\lambda_1 \cdots \lambda_{d-1} t) \right| \le J^{(d-1)k} p^{-\delta_0 n}. \tag{3.10}$$

The bound (3.10), together with the trivial observation

$$\sum_{u \in \mathcal{A}_d} T_d(u) = J^k,$$

implies that the contribution to (3.7) from nondiagonal terms with $u \neq v$ is at most $J^{(d+1)k} p^{-\delta_0 n}$.

Combining this bound with (3.9) we see from (3.7) that for any choice of k satisfying (3.5) and (3.8) we have

$$|W|^2 \leq \left(J^{-k} + p^{-\delta_0 n}\right) J^{2kd+o(1)},$$

together with (3.4) implies that

$$|S| \leq J^{d+o(1)} \left(J^{-k} + p^{-\delta_0 n}\right)^{1/2(2k)^d} \leq p^{dm-\delta n}$$

for some positive δ. To complete the proof it suffices to choose any integer k satisfying the conditions (3.5) and (3.8). In fact it is more convenient to work with a slightly more stringent condition than (3.8) and we choose k to satisfy

$$\frac{\omega \cdot n}{(d + 2\omega - 3)m} < \frac{\omega n}{dm} < k < \frac{1}{2} \left(\frac{n}{m}\right)^{1/2}.$$

In particular, the existence of such a $k \in \mathbb{N}$ in the previous range can be guaranteed if

$$\frac{1}{2} \left(\frac{n}{m}\right)^{1/2} - \frac{\omega n}{dm} \geq 1,$$

or equivalently

$$d \geq \frac{2\omega n}{(m^{1/2} n^{1/2} - 2m)},$$

which coincides with the hypothesis for d, m and n.

4. Comments

We note that it is not difficult to get an explicit (but rather cluttered) expression for the saving δ in Theorem 1.3.

Although we have presented extensions to finite fields of only two selected results of Bourgain and Garaev [4], one can easily check that our approach allows us to get extensions of several other bounds from [4]. However, these methods do not apply to yet another natural generalization of [4] when the role of short intervals is played by arbitrary low-dimensional affine vector subspaces over $\mathbb{F}_{q^n}$ (considered as a vector space over $\mathbb{F}_q$) rather than by very special affine spaces $\mathcal{J}_{\gamma,m}$. We recall that for additive character sums with polynomials such results are known; see [10]. However character sums with rational functions, even in the simplest case of multilinear sums with reciprocals, are not covered by this technique and seem to require new ideas. We also remark that some of the motivation to question come from the problem of constructing efficient affine dispersers and extractors over finite fields; see [1, 2] for more details and further references.

References

[1] Eli Ben-Sasson and Ariel Gabizon, *Extractors for polynomial sources over fields of constant order and small characteristic*, Theory Comput. **9** (2013), 665–683, DOI 10.4086/toc.2013.v009a021. MR3090730

[2] Eli Ben-Sasson and Swastik Kopparty, *Affine dispersers from subspace polynomials*, SIAM J. Comput. **41** (2012), no. 4, 880–914, DOI 10.1137/110826254. MR2974756

[3] Jean Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. **18** (2009), no. 5, 1477–1502, DOI 10.1007/s00039-008-0691-6. MR2481734

[4] J. Bourgain and M. Z. Garaev, *Sumsets of reciprocals in prime fields and multilinear Kloosterman sums* (Russian, with Russian summary), Izv. Ross. Akad. Nauk Ser. Mat. **78** (2014), no. 4, 19–72; English transl., Izv. Math. **78** (2014), no. 4, 656–707. MR3288401

[5] Jean Bourgain, Moubariz Z. Garaev, Sergei V. Konyagin, and Igor E. Shparlinski, *On the hidden shifted power problem*, SIAM J. Comput. **41** (2012), no. 6, 1524–1557, DOI 10.1137/110850414. MR3023803

[6] Jean Bourgain, Moubariz Z. Garaev, Sergei V. Konyagin, and Igor E. Shparlinski, *Multiplicative congruences with variables from short intervals*, J. Anal. Math. **124** (2014), 117–147, DOI 10.1007/s11854-014-0029-2. MR3286051

[7] J. Bourgain and A. Glibichuk, *Exponential sum estimates over a subgroup in an arbitrary finite field*, J. Anal. Math. **115** (2011), 51–70, DOI 10.1007/s11854-011-0023-x. MR2855033

[8] D. R. Heath-Brown, *The least square-free number in an arithmetic progression*, J. Reine Angew. Math. **332** (1982), 204–220, DOI 10.1515/crll.1982.332.204. MR656864

[9] A. A. Karatsuba, *Analogues of Kloosterman sums* (Russian, with Russian summary), Izv. Ross. Akad. Nauk Ser. Mat. **59** (1995), no. 5, 93–102, DOI 10.1070/IM1995v059n05ABEH000044; English transl., Izv. Math. **59** (1995), no. 5, 971–981. MR1360637

[10] A. Ostafe, *Polynomial values in affine subspaces over finite fields*, J. D'Analyse Math., (to appear).

[11] L. B. Pierce, *The 3-part of class numbers of quadratic fields*, J. London Math. Soc. (2) **71** (2005), no. 3, 579–598, DOI 10.1112/S002461070500637X. MR2132372

[12] Igor E. Shparlinski, *Products with variables from low-dimensional affine spaces and shifted power identity testing in finite fields*, J. Symbolic Comput. **64** (2014), 35–41, DOI 10.1016/j.jsc.2013.12.005. MR3170320

Department of Pure Mathematics, University of New South Wales, 2052 NSW, Australia

E-mail address: igor.shparlinski@unsw.edu.au

Department of Pure Mathematics, University of New South Wales, 2052 NSW, Australia

E-mail address: ana.zumalacarregui@gmail.com