

Bilinear character sums over norm groups

By SU HU (Beijing) and YAN LI (Beijing)

Abstract. Let k be a finite field with q elements. Let k_n be the extension of k with degree n . Let N_n be the kernel of the norm map $N_{k_n/k} : k_n^\times \rightarrow k^\times$. In this paper we estimate the bilinear character sum

$$W_{\rho, \theta}(\psi, \mathcal{U}, \mathcal{V}) = \sum_{U \in \mathcal{U}} \sum_{V \in \mathcal{V}} \rho(U) \theta(V) \psi(UV),$$

where $\mathcal{U}$ and $\mathcal{V}$ are arbitrary subsets of N_n , $\rho(U)$ and $\theta(V)$ are arbitrary bounded complex functions supported on $\mathcal{U}$ and $\mathcal{V}$ and ψ is a nontrivial additive character of k_n . We apply this bound to two problems.

- (1) If $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ are subsets of N_n , we study the equation $S + T = UV$, where $S \in \mathcal{S}$, $T \in \mathcal{T}$, $U \in \mathcal{U}$, $V \in \mathcal{V}$.
- (2) We study the N_n analogy of the sum-product problem.

1. Introduction

Character sums over finite fields are very important and have many useful applications. Recently, GYARMATI and SÁRKÖZY [2] estimated certain character sums over finite fields and they used their results to show that if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are “large” subsets of a finite field $\mathbb{F}_q$, then the equations $a + b = cd$, resp., $ab + 1 = cd$ can be solved with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$ [3]. SHPARLINSKI [9] estimated bilinear character sums over elliptic curves and he also gave various applications in two papers [9], [10].

Mathematics Subject Classification: 11T23, 11T24.

Key words and phrases: finite field, equation, character sum, sum-product problem.

Let k be a finite field with q elements. Let k_n be the extension of k with degree n . Let N_n be the kernel of the norm map

$$N_{k_n/k} : k_n^\times \rightarrow k^\times.$$

In this paper, we estimate the bilinear character sum

$$W_{\rho,\theta}(\psi, \mathcal{U}, \mathcal{V}) = \sum_{U \in \mathcal{U}} \sum_{V \in \mathcal{V}} \rho(U) \theta(V) \psi(UV),$$

where $\mathcal{U}$ and $\mathcal{V}$ are arbitrary subsets of N_n , $\rho(U)$ and $\theta(V)$ are arbitrary bounded complex functions supported on $\mathcal{U}$ and $\mathcal{V}$, ψ is a nontrivial additive character of k_n . We apply this bound to the following two problems.

(1) If $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ are subsets of N_n , we study the equation $S+T=UV$, where $S \in \mathcal{S}, T \in \mathcal{T}, U \in \mathcal{U}, V \in \mathcal{V}$. This equation has been considered by SÁRKÖZY [4], GYARMATI–SÁRKÖZY [3] over finite fields and SHPARLINSKI [9] over elliptic curves.

(2) We study the N_n analogue of the sum-product problem which has been considered by GARAEV [6], KATZ–SEN [7], [8] over finite fields and SHPARLINSKI [10] over elliptic curves (also see the survey of TERENCE TAO [16]).

Our main tool is the following result obtained by DELIGNE [13] (also see Chapter 6 Section 3 of [14]).

Lemma 1.1 (DELIGNE [13]). *Let ψ be a nontrivial additive character over k_n , we have*

$$\left| \sum_{x \in N_n} \psi(x) \right| \leq nq^{(n-1)/2}.$$

2. Bilinear sums

Theorem 2.1. *Let ψ be a nontrivial additive character of k_n . Let $\mathcal{U}$ and $\mathcal{V}$ be arbitrary subsets of N_n such that*

$$|\rho(U)| \leq 1, \quad U \in \mathcal{U}, \quad \text{and} \quad |\theta(V)| \leq 1, \quad V \in \mathcal{V}.$$

We have

$$|W_{\rho,\theta}(\psi, \mathcal{U}, \mathcal{V})| \ll \sqrt{\#\mathcal{U}\#\mathcal{V}}q^{(n-1)/2} + \sqrt{\#\mathcal{U}\#\mathcal{V}}q^{(n-1)/4}.$$

Remark 2.2. If $\#\mathcal{V} \leq q^{(n+1)/2}$, we have

$$\sqrt{\#\mathcal{U}\#\mathcal{V}}q^{(n-1)/4} \leq \sqrt{\#\mathcal{U}\#\mathcal{V}q^n}$$

and our bound is stronger than the general proposed bound obtained by GYARMATI and SÁRKÖZY [2].

PROOF. Writing

$$|W_{\rho,\theta}(\psi, \mathcal{U}, \mathcal{V})| \leq \sum_{U \in \mathcal{U}} \left| \sum_{V \in \mathcal{V}} \rho(U)\theta(V)\psi(UV) \right|$$

and applying the Cauchy's inequality, we obtain

$$\begin{aligned} |W_{\rho,\theta}(\psi, \mathcal{U}, \mathcal{V})|^2 &\leq \#\mathcal{U} \sum_{U \in \mathcal{U}} \left| \sum_{V \in \mathcal{V}} \theta(V)\psi(UV) \right|^2 \leq \#\mathcal{U} \sum_{U \in N_n} \left| \sum_{V \in \mathcal{V}} \theta(V)\psi(UV) \right|^2 \\ &= \#\mathcal{U} \sum_{V_1 \in \mathcal{V}} \sum_{V_2 \in \mathcal{V}} \theta(V_1)\bar{\theta}(V_2) \sum_{U \in N_n} \psi(UV_1 - UV_2). \end{aligned}$$

In the case $V_1 = V_2$, we estimate the sum over U as $\#N_n = O(q^{n-1})$. Otherwise $\tilde{\psi}(x) = \psi(x(V_1 - V_2))$ is also a nontrivial additive character over k_n . Using Lemma 1.1, we obtain

$$\left| \sum_{U \in N_n} \psi(UV_1 - UV_2) \right| = \left| \sum_{U \in N_n} \psi(U(V_1 - V_2)) \right| = \left| \sum_{U \in N_n} \tilde{\psi}(U) \right| \leq nq^{(n-1)/2}.$$

Therefore, we have the following estimate

$$|W_{\rho,\theta}(\psi, \mathcal{U}, \mathcal{V})|^2 \ll \#\mathcal{U}(\#\mathcal{V}q^{n-1} + (\#\mathcal{V})^2q^{(n-1)/2}). \quad \square$$

3. Sums and products

SÁRKÖZY [4] shows that for any subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ of $\mathbb{F}_q$, the number of solutions $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ of the equation

$$a + b = cd, a \in \mathcal{A}, \quad b \in \mathcal{B}, \quad c \in \mathcal{C}, \quad d \in \mathcal{D},$$

satisfies

$$\left| N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) - \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q} \right| \leq \sqrt{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}q}.$$

In particular,

$$N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) = (1 + O(q^{-\epsilon/2})) \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q},$$

where $\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} \geq q^{3+\epsilon}$ for some fixed ϵ and sufficiently large q .

Here we estimate the number of solutions $M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V})$ of the equation

$$S + T = UV, \quad S \in \mathcal{S}, \quad T \in \mathcal{T}, \quad U \in \mathcal{U}, \quad V \in \mathcal{V},$$

for any subsets $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ of N_n .

Theorem 3.1. *For every $\epsilon > 0$ and arbitrary subsets $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ of N_n with*

$$\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V} \geq q^{(7n-3)/2+(n-1)\epsilon},$$

we have

$$M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}) = (1 + O(q^{-(n-1)\epsilon/2})) \frac{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}{q^n}.$$

Remark 3.2. In fact, we show that when $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ are subsets of N_n , the equation

$$S + T = UV, \quad S \in \mathcal{S}, \quad T \in \mathcal{T}, \quad U \in \mathcal{U}, \quad V \in \mathcal{V},$$

has more solutions than the situation when $\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}$ are arbitrary subsets of $\mathbb{F}_{q^n}$. Since from the general proposed result of SÁRKÖZY [4], we have

$$M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}) = (1 + O(q^{-n\epsilon/2})) \frac{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}{q^n}.$$

PROOF. Let Ψ be the set of all additive characters of k_n and Ψ^* be the set of nontrivial characters. Using the orthogonality property of the additive characters, we obtain

$$M(\mathcal{S}, \mathcal{T}, \mathcal{U}, \mathcal{V}) = \frac{1}{q^n} \sum_{S \in \mathcal{S}} \sum_{T \in \mathcal{T}} \sum_{U \in \mathcal{U}} \sum_{V \in \mathcal{V}} \sum_{\psi \in \Psi} \psi(S + T - UV) = \frac{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}{q^n} + \Delta,$$

where

$$\begin{aligned} |\Delta| &\leq \frac{1}{q^n} \left| \sum_{S \in \mathcal{S}} \sum_{T \in \mathcal{T}} \sum_{U \in \mathcal{U}} \sum_{V \in \mathcal{V}} \sum_{\psi \in \Psi^*} \psi(S + T - UV) \right| \\ &\leq \frac{1}{q^n} \sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right| \left| \sum_{T \in \mathcal{T}} \psi(T) \right| \left| \sum_{U \in \mathcal{U}} \sum_{V \in \mathcal{V}} \psi(UV) \right|. \end{aligned}$$

Using Theorem 2.1 and the Cauchy's inequality, we obtain

$$\begin{aligned} |\Delta| &\ll \frac{1}{q^n} \left(\sqrt{\#\mathcal{U}\#\mathcal{V}q^{n-1}} + \sqrt{\#\mathcal{U}\#Vq^{(n-1)/4}} \right) \sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right| \left| \sum_{T \in \mathcal{T}} \psi(T) \right| \\ &\leq \frac{1}{q^n} \left(\sqrt{\#\mathcal{U}\#\mathcal{V}q^{n-1}} + \sqrt{\#\mathcal{U}\#Vq^{(n-1)/4}} \right) \\ &\quad \times \sqrt{\sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right|^2} \sqrt{\sum_{\psi \in \Psi^*} \left| \sum_{T \in \mathcal{T}} \psi(T) \right|^2}. \end{aligned}$$

Now we conclude that

$$\sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right|^2 \leq \sum_{\psi \in \Psi} \left| \sum_{S \in \mathcal{S}} \psi(S) \right|^2 = q^n \#S.$$

Using the same argument for the sum over $T \in \mathcal{T}$, we obtain the bound

$$\begin{aligned} |\Delta| &\ll \left(\sqrt{\#\mathcal{U}\#\mathcal{V}q^{n-1}} + \sqrt{\#\mathcal{U}\#Vq^{(n-1)/4}} \right) \sqrt{\#\mathcal{S}\#\mathcal{T}} \\ &= \sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}q^{n-1}} + \sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#Vq^{(n-1)/4}}. \end{aligned}$$

It is obvious that for $\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V} \geq q^{(7n-3)/2+(n-1)\epsilon} \geq q^{(3n-1)+(n-1)\epsilon}$, we have

$$\frac{\sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}q^{n-1}}}{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}q^{-n}} = \frac{q^{(3n-1)/2}}{\sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}}} \leq q^{-(n-1)\epsilon/2}.$$

Clearly, we can assume that $\#\mathcal{U} \geq \#\mathcal{V}$. Then

$$\#\mathcal{S}\#\mathcal{T} \geq \frac{q^{(7n-3)/2+(n-1)\epsilon}}{\#\mathcal{U}\#\mathcal{V}} \geq \frac{q^{(7n-3)/2+(n-1)\epsilon}}{(\#\mathcal{U})^2}.$$

Therefore,

$$\frac{\sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}q^{(n-1)/4}}}{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}\#\mathcal{V}q^{-n}} = \frac{q^{(5n-1)/4}}{\sqrt{\#\mathcal{S}\#\mathcal{T}\#\mathcal{U}}} \leq \frac{\sqrt{\#\mathcal{U}}}{q^{(n-1)/2+(n-1)\epsilon/2}} \ll q^{-(n-1)\epsilon/2},$$

which concludes the proof. $\square$

4. Sum-product problem

We study the N_n analogy of the sum-product problem by modifying the method of GARAEV [6]. This method has also been used by SHPARLINSKI [11] to investigate the elliptic curve analogy of the sum-product problem.

Theorem 4.1. *Let $\mathcal{R}$ and $\mathcal{S}$ be arbitrary subsets of N_n . Then for the subsets*

$$\mathcal{U} = \{S + T : S \in \mathcal{S}, T \in \mathcal{R}\} \quad \text{and} \quad \mathcal{V} = \{ST : S \in \mathcal{S}, T \in \mathcal{R}\},$$

we have

$$\#\mathcal{U}\#\mathcal{V} \gg \min\{q^n \#\mathcal{R}, (\#\mathcal{R}\#\mathcal{S})^2 q^{1-n}, (\#\mathcal{R})^2 \#\mathcal{S} q^{(1-n)/2}\}.$$

Remark 4.2. If $\#\mathcal{S} \leq q^{(n+1)/2}$, we have

$$(\#\mathcal{R}\#\mathcal{S})^2 q^{-n} \leq (\#\mathcal{R})^2 \#\mathcal{S} q^{(1-n)/2}$$

and our bound is stronger than the general proposed bound obtained by GARAIEV [6].

PROOF. We denote J the number of solutions (S_1, S_2, V, U) to the equation

$$VS_1^{-1} + S_2 = U, \quad S_1, S_2 \in \mathcal{S}, V \in \mathcal{V}, U \in \mathcal{U}.$$

Since obviously the vectors

$$(S_1, S_2, RS_1, R + S_2), \quad R \in \mathcal{R}, S_1, S_2 \in \mathcal{S},$$

are all pairwise distinct solution of the above equation, we obtain

$$J \geq \#\mathcal{R}(\#\mathcal{S})^2.$$

To obtain an upper bound on J , we use Ψ to denote the set of all additive characters of k_n and write Ψ^* the set of nontrivial characters. Using the orthogonality property of the additive characters, we obtain

$$\begin{aligned} J &= \sum_{S_1 \in \mathcal{S}} \sum_{S_2 \in \mathcal{S}} \sum_{V \in \mathcal{V}} \sum_{U \in \mathcal{U}} \frac{1}{q^n} \sum_{\psi \in \Psi} \psi(VS_1^{-1} + S_2 - U) \\ &= \frac{1}{q^n} \sum_{\psi \in \Psi} \sum_{S_1 \in \mathcal{S}} \sum_{V \in \mathcal{V}} \psi(VS_1^{-1}) \sum_{S_2 \in \mathcal{S}} \psi(S_2) \sum_{U \in \mathcal{U}} \psi(-U). \end{aligned}$$

For ψ being nontrivial, Theorem 2.1 implies that

$$\left| \sum_{S_1 \in \mathcal{S}} \sum_{V \in \mathcal{V}} \psi(VS_1^{-1}) \right| \ll (\#\mathcal{V})^{1/2} (\#\mathcal{S})^{1/2} q^{(n-1)/2} + (\#\mathcal{V})^{1/2} \#\mathcal{S} q^{(n-1)/4}.$$

Therefore,

$$J - \frac{(\#\mathcal{S})^2 \#\mathcal{U} \#\mathcal{V}}{q^n} \ll ((\#\mathcal{V})^{1/2} (\#\mathcal{S})^{1/2} q^{(n-1)/2} + (\#\mathcal{V})^{1/2} \#\mathcal{S} q^{(n-1)/4}) \frac{1}{q^n} \sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right| \left| \sum_{U \in \mathcal{U}} \psi(U) \right|.$$

Extending the summation over Ψ^* to the full set Ψ and using the Cauchy's inequality, we obtain

$$\sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right| \left| \sum_{U \in \mathcal{U}} \psi(U) \right| \leq \sqrt{\sum_{\psi \in \Psi} \left| \sum_{S \in \mathcal{S}} \psi(S) \right|^2} \sqrt{\sum_{\psi \in \Psi} \left| \sum_{U \in \mathcal{U}} \psi(U) \right|^2}.$$

From the orthogonality property of the additive characters, we have

$$\sum_{\psi \in \Psi} \left| \sum_{S \in \mathcal{S}} \psi(S) \right|^2 \leq q^n \#\mathcal{S}.$$

Similarly,

$$\sum_{\psi \in \Psi} \left| \sum_{U \in \mathcal{U}} \psi(U) \right|^2 \leq q^n \#\mathcal{U}.$$

Thus

$$\sum_{\psi \in \Psi^*} \left| \sum_{S \in \mathcal{S}} \psi(S) \right| \left| \sum_{U \in \mathcal{U}} \psi(U) \right| \ll q^n \sqrt{\#\mathcal{S} \#\mathcal{U}}.$$

From the above inequalities, we have

$$J - \frac{(\#\mathcal{S})^2 \#\mathcal{V} \#\mathcal{U}}{q^n} \ll (\#\mathcal{V} \#\mathcal{U})^{1/2} (\#\mathcal{S} q^{(n-1)/2} + (\#\mathcal{S})^{3/2} q^{(n-1)/4}).$$

Thus,

$$\frac{(\#\mathcal{S})^2 \#\mathcal{V} \#\mathcal{U}}{q^n} + (\#\mathcal{V} \#\mathcal{U})^{1/2} (\#\mathcal{S} q^{(n-1)/2} + (\#\mathcal{S})^{3/2} q^{(n-1)/4}) \gg \#\mathcal{R} (\#\mathcal{S})^2.$$

Hence

$$\#\mathcal{U} \#\mathcal{V} \gg \min\{q^n \#\mathcal{R}, (\#\mathcal{R} \#\mathcal{S})^2 q^{1-n}, (\#\mathcal{R})^2 \#\mathcal{S} q^{(1-n)/2}\}. \quad \square$$

ACKNOWLEDGEMENTS. The authors are grateful to the two anonymous referees for their valuable comments.

References

- [1] K. GYARMATI, On a problem of Diophantus, *Acta. Arith.* **97** (2001), 53–65.
- [2] K. GYARMATI and A. SÁRKÖZY, Equations in finite fields with restricted solution sets, I (character sums), *Acta. Math Hungar.* **118** (2008), 129–148.
- [3] K. GYARMATI and A. SÁRKÖZY, Equations in finite fields with restricted solution sets, II (algebraic equations), *Acta. Math Hungar.* **119** (2008), 259–280.
- [4] A. SÁRKÖZY, On sums and product of residues modulo p , *Acta. Arith.* **118** (2005), 403–409.
- [5] M. Z. GARAЕV, Double exponential sums related to Diffie–Hellman distributions, *Int. Math. Res. Not.* **17** (2005), 1005–1014.
- [6] M. Z. GARAЕV, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **8** (2008), 2735–2739.
- [7] N. H. KATZ and C.-Y. SHEN, Garaev’s inequality in finite fields not of prime order, *J. Anal. Combin.* **3** (2008), Article#3.
- [8] N. H. KATZ and C.-Y. SHEN, A slight improvement to Garaev’s sum product estimate, *Proc. Amer. Math. Soc.* **136** (2008), 499–2504.
- [9] I. E. SHPARLINSKI, Bilinear character sums over elliptic curves, *Finite Fields Appl.* **14** (2008), 132–141.
- [10] I. E. SHPARLINSKI, On the elliptic curve analogue of the sum-product problem, *Finite Fields Appl.* **15** (2008), 721–726.
- [11] I. E. SHPARLINSKI, On the solvability of bilinear equations in finite fields, *Glasgow Math. J.* **50** (2008), 523–529.
- [12] W. D. BANKS, J. B. FRIEDLANDER, M. Z. GARAЕV and I. E. SHPARLINSKI, Double character sums over elliptic curves and finite fields, *Pure Appl. Math. Q.* **2** (2006), 179–197.
- [13] P. DELIGNE, Cohomologie étale, Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 $\frac{1}{2}$, Lecture Notes in Math. 569, *Springer-Verlag, New York*, 1977.
- [14] WEN-CHING WININE LI, Number theory with applications, *World Scientific Publishing*, 1996.
- [15] WEN-CHING WININE LI, Character sums over norm groups, *Finite Fields Appl.* **12** (2006), 1–15.
- [16] T. TAO, The sum-product phenomenon in arbitrary rings, arxiv:0806.2497V4.

SU HU
 DEPARTMENT OF MATHEMATICAL SCIENCES
 TSINGHUA UNIVERSITY
 BEIJING 100084
 CHINA

E-mail: hus04@mails.tsinghua.edu.cn

YAN LI
 DEPARTMENT OF MATHEMATICAL SCIENCES
 TSINGHUA UNIVERSITY
 BEIJING 100084
 CHINA

E-mail: liyan_00@mails.tsinghua.edu.cn

(Received December 15, 2009; revised April 19, 2010)