Glasgow Math. J. **50** (2008) 523–529. © 2008 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089508004382. Printed in the United Kingdom

ON THE SOLVABILITY OF BILINEAR EQUATIONS IN FINITE FIELDS

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au

(Received 25 September 2007; revised 29 February 2008; accepted 31 March 2008)

Abstract. We consider the equation

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

over a finite field $\mathbb{F}_q$ of q elements, with variables from arbitrary sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$. The question of solvability of such and more general equations has recently been considered by Hart and Iosevich, who, in particular, prove that if

$$\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} \geq Cq^3,$$

for some absolute constant $C > 0$, then above equation has a solution for any $\lambda \in \mathbb{F}_q^*$. Here we show that using bounds of multiplicative character sums allows us to extend the class of sets which satisfy this property.

2000 *Mathematics Subject Classification.* 11L40, 11T30.

1. Introduction.

1.1. Background.

Let $\mathbb{F}_q$ denote the final field of q elements.

Using exponential sums, Hart and Iosevich [**9**] have shown that for any $2n$ sets $\mathcal{A}_i, \mathcal{B}_i \subseteq \mathbb{F}_q$, $i = 1, \ldots, n$, with

$$\prod_{i=1}^{n} \#\mathcal{A}_i\#\mathcal{B}_i > Cq^{n+1}, \tag{1}$$

for some absolute constant $C > 0$, the equation

$$\sum_{i=1}^{n} a_i b_i = \lambda, \qquad a_i \in \mathcal{A}_i,\ b_i \in \mathcal{B}_i,\ i = 1, \ldots, n, \tag{2}$$

has a solution for any $\lambda \in \mathbb{F}_q^*$ (although the proof is given only in the case of $\mathcal{A}_1 = \mathcal{B}_1 = \cdots = \mathcal{A}_n = \mathcal{B}_n$, the method and results immediately extend to the general case, see [**9**, Remark 1.3]). These results have been put in a more general context in a recent work of Hart et al. [**10**].

In particular, for $n = 2$, one can easily derive from the proof of [**9**, Theorem 1.1] that the equation

$$ab + cd = \lambda, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}, \tag{3}$$

has

$$N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda) = \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q-1} + O\big((q\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D})^{1/2}\big) \tag{4}$$

solutions for any $\lambda \in \mathbb{F}_q^*$.

In particular, we see from (1) that for any $\lambda \in \mathbb{F}_q^*$, equation (3) has a solution for any four sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^*$ with

$$\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D} \ge Cq^3, \tag{5}$$

for some absolute constant $C > 0$.

Furthermore, for the number $T(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ of the solutions of the similar equation

$$a + b = cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}, \tag{6}$$

Sárközy has given an analogous bound

$$T(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) = \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q-1} + O\big((q\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D})^{1/2}\big) \tag{7}$$

in [**18**] and also the bound (1) in [**19**] (it is shown in [**18**, **19**] only for prime fields but the proofs and results extend to the general case at the cost of only typographical changes). Thus (6) has a solution under the condition (5) as well.

Hart and Iosevich [**9**] have also considered the set $\mathcal{E}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ of $\lambda \in \mathbb{F}_q$ for which (3) has no solution. Although only the case of $\mathcal{A} = \mathcal{B} = \mathcal{C} = \mathcal{D}$ has been worked out in [**9**], the same approach seems to give the bound

$$\#\mathcal{E}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) = O\left(\frac{q^3}{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}}\right)$$

(certainly if $\mathcal{D}$ is not of the smallest cardinality among $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ one can alter this bound in the obvious way). Thus only three sets out of four are relevant. This implies that instead of (3) one can consider the equation with only three variables

$$f + gh = \lambda, \qquad f \in \mathcal{F},\ g \in \mathcal{G},\ h \in \mathcal{H}, \tag{8}$$

for some sets $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_q$. If $\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H})$ is the set of $\lambda \in \mathbb{F}_q$ for which (8) has no solution then we have

$$\#\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H}) = O\left(\frac{q^3}{\#\mathcal{F}\#\mathcal{G}\#\mathcal{H}}\right). \tag{9}$$

We now remark that the result of Sárközy [**18**] also implies (9). Indeed, we see that

$$T\left(-\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H}), \mathcal{F}, \mathcal{G}, \mathcal{H}\right) = 0,$$

and we derive from (7)

$$\frac{\#\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H})\#\mathcal{F}\#\mathcal{G}\#\mathcal{H}}{q-1} = O\big((q\#\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H})\#\mathcal{F}\#\mathcal{G}\#\mathcal{H})^{1/2}\big),$$

which leads to (9).

https://doi.org/10.1017/S0017089508004382 Published online by Cambridge University Press

We remark that in a recent work of Garaev [**5**] considering equation (6) (for some special sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$) has been the main tool in obtaining new results on the sum–product problem in finite fields (see also [**2**–**4**, **9**, **11**, **15**, **16**]). In fact, one can shorten the proof of [**5**, Theorem 1] by a direct appeal to (7).

1.2. Our results. Here we show that using multiplicative character sums one can extend the region of possible values for $\#\mathcal{A}, \#\mathcal{B}, \#\mathcal{C}, \#\mathcal{D}$ which guarantee the solvability of equations (3) and (6). We show that for any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that if

$$\#\mathcal{A} \ge q^{1/2+\varepsilon} \qquad \text{and} \qquad \#\mathcal{B} \ge q^{\varepsilon}, \tag{10}$$

as well as

$$\#\mathcal{C}\#\mathcal{D} \ge q^{2-\delta}, \tag{11}$$

then equations (3) and (6) have a solution for any $\lambda \in \mathbb{F}_q^*$ (provided that q is large enough).

More precisely, we obtain the following asymptotic formulas:

THEOREM 1. *For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that for any $\lambda \in \mathbb{F}_q^*$ and any set $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q$ which satisfy* (10) *and* (11)*, equations* (3) *and* (6) *have*

$$N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda) = \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q}(1 + O(q^{-\delta}))$$

and

$$T(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) = \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q}(1 + O(q^{-\delta}))$$

solutions, respectively.

The same argument which we have used to derive (9) from (7), combined with our bound on $T(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$, leads to the following estimates:

COROLLARY 2. *For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that for any set $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_q$ which satisfy*

$$\#\mathcal{F} \ge q^{\varepsilon} \qquad \text{and} \qquad \#\mathcal{G}\#\mathcal{H} \ge q^{2-\delta},$$

equation (8) *has a solution for all but*

$$\#\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H}) = O(q^{1/2+\varepsilon})$$

values of $\lambda \in \mathbb{F}_q$.

COROLLARY 3. *For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that for any set $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_q$ which satisfy*

$$\#\mathcal{F} \ge q^{1/2+\varepsilon} \qquad \text{and} \qquad \#\mathcal{G}\#\mathcal{H} \ge q^{2-\delta}$$

equation (8) *has a solution for all but*

$$\#\mathcal{E}(\mathcal{F}, \mathcal{G}, \mathcal{H}) = O(q^{\varepsilon})$$

values of $\lambda \in \mathbb{F}_q$.

https://doi.org/10.1017/S0017089508004382 Published online by Cambridge University Press

As far as we are aware, before the work of Sárközy [**19**] and the present work, multiplicative character sums have not been used in questions of this kind. The main purpose of this work is to show that multiplicative character sums may allow us to break through the $q^{1/2}$-threshold on the cardinalities of the sets involved, which usually occurs when one uses exponential sums.

2. Proof of Theorem 1.

2.1. Estimating $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda)$. Let us denote by $\mathcal{X}$ the set of all multiplicative characters of $\mathbb{F}_q^*$ and by $\mathcal{X}^*$ the set of all non-trivial characters. For the trivial character χ_0 we define $\chi_0(0) = 1$ and put $\chi(0) = 0$ for all other characters $\chi \in \mathcal{X}^*$.

Using the orthogonality property of characters, see [**17**, Equation (5.4)], we write for the number of solutions $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda)$ to equation (3)

$$\begin{aligned} N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda) &= \frac{1}{q-1} \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} \sum_{\chi \in \mathcal{X}} \chi(ab - \lambda) \overline{\chi}(cd) \\ &= \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q-1} + \frac{1}{q-1} \\ &\quad \times \sum_{\chi \in \mathcal{X}^*} \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab - \lambda) \sum_{c \in \mathcal{C}} \overline{\chi}(c) \sum_{d \in \mathcal{D}} \overline{\chi}(d). \end{aligned}$$

Let

$$W = \max_{\chi \in \mathcal{X}^*} \left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab - \lambda) \right|.$$

Then, using the Cauchy inequality (and again the orthogonality property of characters), we obtain

$$\begin{aligned} &\left| \sum_{\chi \in \mathcal{X}^*} \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab - \lambda) \sum_{c \in \mathcal{C}} \overline{\chi}(c) \sum_{d \in \mathcal{D}} \overline{\chi}(d) \right| \\ &\le W \sum_{\chi \in \mathcal{X}^*} \left| \sum_{c \in \mathcal{C}} \overline{\chi}(c) \right| \left| \sum_{d \in \mathcal{D}} \overline{\chi}(d) \right| \\ &< W \left(\sum_{\chi \in \mathcal{X}} \left| \sum_{c \in \mathcal{C}} \overline{\chi}(c) \right|^2 \right)^{1/2} \left(\sum_{\chi \in \mathcal{X}} \left| \sum_{d \in \mathcal{D}} \overline{\chi}(d) \right| \right)^{1/2} \\ &= W(q-1) \left(\#\mathcal{C}\#\mathcal{D}\right)^{1/2}. \end{aligned}$$

Therefore

$$\left| N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda) - \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{C}\#\mathcal{D}}{q-1} \right| < W \left(\#\mathcal{C}\#\mathcal{D}\right)^{1/2}. \tag{12}$$

We now recall a result of Karatsuba, see [**13**] or [**14**, Chapter VIII, Problem 9] (which in turn follows from the Weil bound and the Hölder inequality), asserting that

https://doi.org/10.1017/S0017089508004382 Published online by Cambridge University Press

for any integer $r \ge 1$, we have

$$W = O\big((\#\mathcal{A})^{1-1/2r}\#\mathcal{B}p^{1/4r} + (\#\mathcal{A})^{1-1/2r}(\#\mathcal{B})^{1/2}p^{1/2r}\big), \tag{13}$$

where the implied constant depends only on r. In particular, taking $r = \lceil \varepsilon^{-1} \rceil$, we see that for any $\varepsilon > 0$ there exists $\delta > 0$ such that under condition (10) we have

$$W \le \#\mathcal{A}\#\mathcal{B}q^{-2\delta} \tag{14}$$

provided that q is large enough. Substituting (14) in (12) and recalling (11), we obtain the desired estimate for $N(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}; \lambda)$.

2.2. Estimating $T(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$. We proceed exactly in the same way; however, instead of W, the bound on the number of solutions depends on

$$V = \max_{\chi \in \mathcal{X}^*} \left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b) \right|,$$

for which the same bound as in (14) holds as well.

3. Concluding remarks.

3.1. Links with the sum–product problem. We have already mentioned that equation (6) appears in the argument of Garaev [**5**] on the sum–product problem in finite fields. We present this argument in a slightly more general form. For two sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_q$ we consider their sum and product sets

$$\mathcal{U} = \{x + y \,:\, x \in \mathcal{X}, y \in \mathcal{Y}\} \qquad \text{and} \qquad \mathcal{V} = \{xy \,:\, x \in \mathcal{X}, y \in \mathcal{Y}\}.$$

The argument of [**5**] (presented there in the special case $\mathcal{X} = \mathcal{Y}$) is based on the observation that the equation

$$vx_1^{-1} + x_2 = u, \qquad x_1, x_2 \in \mathcal{X},\ u \in \mathcal{U},\ v \in \mathcal{V},$$

has at least $(\#\mathcal{X})^2\#\mathcal{Y}$ solutions of the form $(x_1, x_2, u, v) = (x_1, x_2, x_2 + y, x_1 y)$. Combining this observation with (7) (and assuming that $\#\mathcal{Y} \ge \#\mathcal{X}$) we obtain

$$\#\mathcal{U}\#\mathcal{V} \ge C_0 \min\left\{ p\max\{\#\mathcal{X}, \#\mathcal{Y}\}, \frac{(\#\mathcal{X})^2(\#\mathcal{Y})^2}{p} \right\},$$

for some absolute constant $C_0 > 0$, which for $\mathcal{X} = \mathcal{Y}$ coincides with the result of Garaev [**5**, Theorem 1]. It would be interesting to see whether our approach to estimating the number of solutions to (6) allows to obtain stronger estimates.

3.2. Possible improvements. Certainly for every concrete value of ε one can use the bound (13), instead of its simplified form (14), and optimise the choice of r.

Clearly (5) is not implied by (10) and (11). On the other hand, we show that our approach also gives an alternative proof of the corresponding results of [**9**] and [**18**] for

https://doi.org/10.1017/S0017089508004382 Published online by Cambridge University Press

equations (3) and (6), respectively. In turn, using the well-known bound

$$W \le (q\#\mathcal{A}\#\mathcal{B})^{1/2},$$

(see [**21**, Exercise 8.c]) we easily derive (4) from (12). The bound (7) follows similarly from the inequality

$$V \le (q\#\mathcal{A}\#\mathcal{B})^{1/2}.$$

Certainly, if more information about the arithmetic structure of the sets $\mathcal{A}$ and $\mathcal{B}$ is known then better bounds can be available, see for example, estimates which are given by Friedlander and Iwaniec [**12**] and by Karatsuba [**13**]. Moreover, in the case where $q = p$ is prime and $\mathcal{A} = \mathcal{B} = \mathcal{C} = \mathcal{D} = \{1, \ldots, H\}$, a slight modification of the proof of [**1**, Theorem 12] shows that (3) has $H^4/p + O\left(H^2 p^{o(1)}\right)$ solutions for every $\lambda \in \mathbb{F}_p^*$. This is non-trivial starting with $H \ge p^{1/2+\varepsilon}$ for any $\varepsilon > 0$ and sufficiently large p. Several more results of the similar flavour are given by Garaev and Garcia [**6**].

3.3. Further problems. Unfortunately, our approach does not seem to extend to the general equation (2). More precisely, combining bounds of exponential and multiplicative character sums, some results can be obtained, but they are weaker than those of [**9**, **10**]. So, it would certainly be interesting to find a way of using bounds of multiplicative character sums to obtain an alternative proof of the result of [**9**] on the solvability of equation (2) under condition (1). Such a proof is likely to lead to the solvability of this equation under several more conditions as well.

Following, Hart, Iosevich and Solymosi [**11**] we now consider the equation

$$(a_1 - b_1) \cdots (a_n - b_n) = \lambda, \qquad a_i \in \mathcal{A}_i,\ b_i \in \mathcal{B}_i,\ i = 1, \ldots, n, \tag{15}$$

where $\mathcal{A}_i, \mathcal{B}_i \subseteq \mathbb{F}_q$, $i = 1, \ldots, n$ and use $Q_n(\mathcal{A}_1, \mathcal{B}_1, \ldots, \mathcal{A}_n, \mathcal{B}_n; \lambda)$ to denote its number of solutions. In the case $\mathcal{A}_1 = \mathcal{B}_1 = \cdots = \mathcal{A}_n = \mathcal{B}_n = \mathcal{A}$, it is shown in [**11**], using bounds of *Kloosterman sums*, that (15) has a solution for any $\lambda \in \mathbb{F}_q$, provided that $\#\mathcal{A} \ge q^{1/2+1/(2n)}$. Clearly, using multiplicative character sums one can also obtain new results for equation (15) (for example, in the case when the sets $\mathcal{B}_1, \ldots, \mathcal{B}_n$ are 'thin').

Gyarmati and Sárközy [**7**, **8**] have considered several more generalisations of equations (3) and (6). For some of these generalisations one may wish to study for which classes of polynomials $F(U, V) \in \mathbb{F}_q[U, V]$ the method of Karatsuba [**13**] can be used to obtain analogues of bound (13) for the sums

$$\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(F(a, b)), \qquad \chi \in \mathcal{X}^*.$$

There is little doubt that in principle the whole approach works in this case too; however, it may require to study the root multiplicities of the rational functions $F(U, u_1) \cdots F(U, u_r) F(U, v_1)^{-1} \cdots F(U, v_r)^{-1}$ with $u_1, v_1, \ldots, u_r, v_r \in \mathbb{F}_q$.

We also remark that equation (3) (after a sign change and renaming some variables) transforms into the determinant equation

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}.$$

This suggests also to consider higher-dimensional determinant equations

$$\det(a_{ij})_{i,j=1}^n = \lambda, \qquad a_{ij} \in \mathcal{A}_{ij},\ i, j = 1, \ldots, n,$$

https://doi.org/10.1017/S0017089508004382 Published online by Cambridge University Press

for n^2 sets $\mathcal{A}_{ij} \subseteq \mathbb{F}_q$, $i, j = 1, \ldots, n$. For structural sets, such as intervals, this and similar questions have been studied in [**1**], however its methods do not seem to apply to the case of arbitrary sets.

An analogue of bound (13) has been given in [**20**] for character sum over points of an elliptic curve over $\mathbb{F}_q$, which has also been applied to study an elliptic curve analogue of equation (6). One can also consider some mixed cases involving points on an elliptic curve and field elements.

ACKNOWLEDGEMENT. The author is grateful to Andras Sárközy for several useful comments. This work was supported in part by ARC grant DP0556431.

REFERENCES

1. O. Ahmadi and I. E. Shparlinski, Distribution of matrices with restricted entries over finite fields, *Indag. Math.* **18** (2007), 327–337.

2. 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. Lond. Math. Soc.* **73** (2006), 380–398.

3. J. Bourgain, N. Katz and T. Tao, A sum product estimate in finite fields and applications, *Geom. Funct. Anal.* **14** (2004), 27–57.

4. M. Z. Garaev, An explicit sum–product estimate in $\mathbb{F}_p$, *Intern. Math. Res. Notices* **2007** (2007), 1–11 (article ID rnm035).

5. M. Z. Garaev, The sum–product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **136** (2008), 2735–2739.

6. M. Z. Garaev and V. Garcia, The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications, *J. Number Theory*, 2007.

7. K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, I (Character sums), *Acta Math. Hungar.* **118** (2008), 129–148.

8. K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets, II (Algebraic equations), *Acta Math. Hungar* **119** (2008), 259–280.

9. D. Hart and A. Iosevich, Sums and products in finite fields: An integral geometric viewpoint, *Contemp. Mathem.* (in press).

10. D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum–product theory in finite fields, and the Erdos–Falconer distance conjecture, Preprint, 2007 (available from http://arxiv.org/abs/0707.3473).

11. D. Hart, A. Iosevich and J. Solymosi, Sums and products in finite fields via Kloosterman Sums, *Intern. Math. Res. Notices* **2007** (2007), 1–14 (article ID rnm007).

12. J. Friedlander and H. Iwaniec, Estimates for character sums, *Proc. Amer. Math. Soc.* **119** (1993), 363–372.

13. A. A. Karatsuba, The distribution of values of Dirichlet characters on additive sequences, *Doklady Acad. Sci. USSR* **319** (1991), 543–545 (in Russian).

14. A. A. Karatsuba, *Basic analytic number theory* (Springer-Verlag, Berlin, 1993).

15. N. H. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *J. Anal. Combin.* **3** (2008).

16. N. H. Katz and C.-Y. Shen, A slight improvement to Garaev's sum product estimate, *Proc. Amer. Math. Soc.* **136** (2008), 2499–2504.

17. R. Lidl and H. Niederreiter, *Finite fields* (Cambridge University Press, Cambridge, UK, 1997).

18. A. Sárközy, On sums and products of residues modulo p, *Acta Arith.* **118** (2005), 403–409.

19. A. Sárközy, On products and shifted products of residues modulo p, *Integers* (in press).

20. I. E. Shparlinski, Bilinear character sums over elliptic curves, *Finite Fields Their Appl.* **14** (2008), 132–141.

21. I. M. Vinogradov, *Elements of number theory* (Dover Publications, NY, 1954).