Glasgow Math. J. **53** (2011) 427–435. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000425.

ON THE SOLVABILITY OF SYSTEMS OF SUM–PRODUCT EQUATIONS IN FINITE FIELDS

LE ANH VINH
Mathematics Department, Harvard University, Cambridge, MA 02138, USA
e-mail: vinh@math.harvard.edu

(Received 9 December 2008; accepted 25 August 2009)

Abstract. In an earlier paper, for 'large' (but otherwise unspecified) subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ of $\mathbb{F}_q$, Sárközy showed the solvability of the equations $a + b = cd$ with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$. This equation has been studied recently by many other authors. In this paper, we study the solvability of systems of equations of this type using additive character sums.

2010 *Mathematics Subject Classification.* 05C35, 05C38, 05C55.

1. Introduction. In **[8]**, Sárközy proved that if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are 'large' subsets of $\mathbb{Z}_p$, more precisely, $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \gg p^3$, then the equation

$$a + b = cd \tag{1.1}$$

can be solved with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$ and $d \in \mathcal{D}$. Gyarmati and Sárközy **[4]** generalized the results on the solvability of equation (1.1) to finite fields. They also study the solvability of other (higher degree) algebraic equations with solutions restricted to 'large' subsets of $\mathbb{F}_q$, where $\mathbb{F}_q$ denotes the finite field of q elements. Using bounds of multiplicative character sums, Shparlinski **[9]** extended the class of sets which satisfy this property. Furthermore, Garaev **[3]** considered equation (1.1) over some special sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ to obtain new results on the sum–product problem in finite fields. The author gave another proof of Garaev's results using graph theory methods in **[11]**.

In this paper, we will use additive character sums to study the systems of sum–product equations in finite fields. More precisely, we consider the following systems:

$$a_0 + a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda_1, \ \ a_0 + a_2 - \mathbb{b}_0 \cdot \mathbb{b}_2 = \lambda_2, \tag{1.2}$$

and

$$a_0 + a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda_1, \ \ a_0 + a_2 - \mathbb{b}_0 \cdot \mathbb{b}_2 = \lambda_2, \ \ a_1 + a_2 - \mathbb{b}_1 \cdot \mathbb{b}_2 = \lambda_3, \tag{1.3}$$

with $(a_i, b_i) \in \mathcal{A}_i$ and $\mathcal{A}_i \subseteq \mathbb{F}_q \times \mathbb{F}_q^d$, $i = 0, 1, 2$, $d \geq 1$. Our first result states that the system (1.2) of two sum–product equations in large restricted subsets of $\mathbb{F}_q$ is always solvable.

THEOREM 1.1. *Given three subsets $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2 \subseteq \mathbb{F}_q \times \mathbb{F}_q^d$. Suppose that*

$$|\mathcal{A}_0||\mathcal{A}_1|, |\mathcal{A}_0||\mathcal{A}_2| \gg q^{d+2},$$

then for any $\lambda_1, \lambda_2 \in \mathbb{F}_q$, *the system (1.2) has*

$$(1 + o(1))\frac{|\mathcal{A}_0||\mathcal{A}_1||\mathcal{A}_2|}{q^2}$$

solutions.

Theorem 1.1 can even be generalized to the system of k equations and $k+1$ variables without any costs.

THEOREM 1.2. *Given* $k+1$ *subsets* $\mathcal{A}_i \subset \mathbb{F}_q \times \mathbb{F}_q^d$, $i = 0, \ldots, k$. *Suppose that*

$$|\mathcal{A}_0||\mathcal{A}_i| \gg q^{d+2}$$

for all $i = 1, \ldots, k$, *and*

$$|\mathcal{A}_0|^2 \prod_{i \in I} |\mathcal{A}_i| \gg q^{(d+2)|I|}$$

for all $I \subset \{1, \ldots, k\}$, $|I| \geq 2$. *Consider the system* $\mathcal{L}$ *of* k *equations*

$$a_0 + a_i - \mathbb{b}_0 \cdot \mathbb{b}_i = \lambda_i, \quad (a_i, \mathbb{b}_i) \in \mathcal{A}_i, i = 1, \ldots, k.$$

Then, for any $\lambda_i \in \mathbb{F}_q$, *the above system has*

$$(1 + o(1))q^{-k} \prod_{i=0}^{k} |\mathcal{A}_i|$$

solutions.

The system (1.3) of three sum–product equations in large restricted subsets of $\mathbb{F}_q$, however, is not always solvable. We will instead show that the system is solvable for a positive proportion of all triples $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^3$ in the smallest case, $d = 1$. More precisely, we have the following theorem.

THEOREM 1.3. *Given three subsets* $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2 \subseteq \mathbb{F}_q \times \mathbb{F}_q$. *Suppose that*

$$|\mathcal{A}_0|, |\mathcal{A}_1|, |\mathcal{A}_2| \gg q^{3/2},$$

then the system (1.3) is solvable for $\Omega\left(\frac{\sqrt{|\mathcal{A}_1||\mathcal{A}_2|}}{q^2}\right) q^3$ *triples* $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^3$.

It is conceivable that we can chop off the term $\Omega\left(\frac{\sqrt{|\mathcal{A}_1||\mathcal{A}_2|}}{q^2}\right)$ in the above theorem, or even better, the system is solvable for $(1 - o(1))q^3$ triples $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^3$. We show that it is indeed the case when the ambient space $\mathbb{F}_q \times \mathbb{F}_q^d$ has dimension $d + 1 \geq 3$.

THEOREM 1.4. *Given three subsets* $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2 \subseteq \mathbb{F}_q \times \mathbb{F}_q^d$. *Suppose that*

$$|\mathcal{A}_0||\mathcal{A}_1, |\mathcal{A}_1||\mathcal{A}_2|, |\mathcal{A}_0||\mathcal{A}_2| \gg q^{(d+2)/2},$$

then the system (1.3) is solvable for $(1 - o(1))q^3$ *triples* $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^3$. *Furthermore, if* $d \geq 3$ *and*

$$|\mathcal{A}_0||\mathcal{A}_1, |\mathcal{A}_1||\mathcal{A}_2|, |\mathcal{A}_0||\mathcal{A}_2| \gg q^{(d+3)/2},$$

then the system (1.3) is solvable for all triples $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^3$.

Interested readers can also find some interesting related problems in [**1**, **2**, **5**, **6**, **7**, **10**, **12**, **13**, **14**, **15**].

2. Sum–product equation – Revisited. For any $(a_0, \mathbb{b}_0) \in \mathbb{F}_q \times \mathbb{F}_q^d$ and a subset $V \in \mathbb{F}_q \times \mathbb{F}_q^d$, denote $N^\lambda(a_0, \mathbb{b}_0)$ be the set of all pairs $(a, \mathbb{b}) \in \mathbb{F}_q \times \mathbb{F}_q^d$ such that

$$a_0 + a - \mathbb{b}_0 \cdot \mathbb{b} = \lambda,$$

and let $N_V^\lambda(a_0, \mathbb{b}_0) = N^\lambda(a_0, \mathbb{b}_0) \cap V$. The following key estimate says that the cardinalities of $N_V^\lambda(a_0, \mathbb{b}_0)$'s are close to $|V|/q$ when $|V|$ is large.

LEMMA 2.1. *For every subset* V *of* $\mathbb{F}_q \times \mathbb{F}_q^d$ *then*

$$\sum_{(a_0,\mathbb{b}_0)\in\mathbb{F}_q\times\mathbb{F}_q^d} \left(|N_V^\lambda(a_0, \mathbb{b}_0)| - \frac{|V|}{q} \right)^2 < q^d |V|.$$

Proof For any set X, let $X(\cdot)$ denote the characteristic function of X. Let χ be any non-trivial additive character of $\mathbb{F}_q$. We have

$$\begin{aligned}
|N_V^\lambda(a_0, \mathbb{b}_0)| &= \sum_{(a,\mathbb{b})\in\mathbb{F}_q\times\mathbb{F}_q^d, a_0+a-\mathbb{b}_0\cdot\mathbb{b}-\lambda=0} V(a, \mathbb{b}) \\
&= \sum_{(a,\mathbb{b})\in\mathbb{F}_q\times\mathbb{F}_q^d, s\in\mathbb{F}_q} \frac{1}{q}\chi(s(a_0 + a - \mathbb{b}_0 \cdot \mathbb{b} - \lambda))V(a, \mathbb{b}) \\
&= \frac{|V|}{q} + \frac{1}{q} \sum_{(a,\mathbb{b})\in\mathbb{F}_q\times\mathbb{F}_q^d, s\in\mathbb{F}_q^*} \chi(s(a_0 + a - \mathbb{b}_0 \cdot \mathbb{b} - \lambda))V(a, \mathbb{b}).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{(a_0,\mathbb{b}_0)\in\mathbb{F}_q\times\mathbb{F}_q^d} \left(|N_V^\lambda(a_0, \mathbb{b}_0)| - \frac{|V|}{q} \right)^2 \\
&= \frac{1}{q^2} \sum_{(a_0,\mathbb{b}_0)\in\mathbb{F}_q\times\mathbb{F}_q^d} \left(\sum_{(a,\mathbb{b})\in\mathbb{F}_q\times\mathbb{F}_q^d, s\in\mathbb{F}_q^*} \chi(s(a_0 + a - \mathbb{b}_0 \cdot \mathbb{b} - \lambda))V(a, \mathbb{b}) \right)^2 \\
&= \frac{1}{q^2} \sum_{\substack{s,s'\in\mathbb{F}_q^*, a_0,a,a'\in\mathbb{F}_q \\ \mathbb{b}_0,\mathbb{b},\mathbb{b}'\in\mathbb{F}_q^d}} \chi((s - s')(a_0 - \lambda))\chi(sa - s'a')\chi(\mathbb{b}_0 \cdot (s'\mathbb{b}' \\
&\quad - s\mathbb{b}))V(a, \mathbb{b})V(a', \mathbb{b}') \\
&= q^{d-1} \sum_{a,a'\in\mathbb{F}_q, \mathbb{b}\in\mathbb{F}_q^d, s=s'\in\mathbb{F}_q^*} \chi(s(a - a'))V(a, \mathbb{b})V(a', \mathbb{b}) \\
&= q^{d-1}(R_1 + R_2),
\end{aligned} \tag{2.1}$$

where R_1 is taken over $a = a'$ and R_2 is taken over $a \neq a'$ (the fourth line follows from the orthogonality in a_0 and $\mathbb{b}_0$ and we consider the third line as a sum over a_0 then $\mathbb{b}_0$

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

implies that all summands vanish unless $s = s'$ and $\mathbb{b} = \mathbb{b}'$). We have

$$R_1 = \sum_{a=a'\in\mathbb{F}_q, \mathbb{b}\in\mathbb{F}_q^d, s=s'\in\mathbb{F}_q^*} \chi(s(a-a'))V(a,\mathbb{b})V(a',\mathbb{b})$$
$$= (q-1)\sum_{a\in\mathbb{F}_q, \mathbb{b}\in\mathbb{F}_q^d} V(a,\mathbb{b})^2 = (q-1)|V|, \tag{2.2}$$

and

$$R_2 = \sum_{a\neq a'\in\mathbb{F}_q, \mathbb{b}\in\mathbb{F}_q^d, s=s'\in\mathbb{F}_q^*} \chi(s(a-a'))V(a,\mathbb{b})V(a',\mathbb{b})$$
$$= \sum_{a\in\mathbb{F}_q, \mathbb{b}\in\mathbb{F}_q^d, s\in\mathbb{F}_q^*, t\neq 0,1, a'=ta} \chi(sa(1-t))V(a,\mathbb{b})V(ta,\mathbb{b})$$
$$= -\sum_{a\in\mathbb{F}_q, b\in\mathbb{F}_q^d, t\neq 0,1} V(a,\mathbb{b})V(ta,\mathbb{b})$$
$$\geqslant -(q-2)|V|. \tag{2.3}$$

The lemma follows immediately from (2.1), (2.2) and (2.3). □

The following result (a generalization of Theorem 1 in [**4**]) is an easy corollary of Lemma 2.1.

THEOREM 2.1. *For any two subsets $V, U \subseteq \mathbb{F}_q \times \mathbb{F}_q^d$, let $N^\lambda(U, V)$ be the set of pairs $(a_0, \mathbb{b}_0) \in V$, $(a_1, \mathbb{b}_1) \in U$ such that $a_0 + a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda$. Then, we have*

$$\left| N^\lambda(V, U) - \frac{|V||U|}{q} \right| < \sqrt{q^d|V||U|}.$$

Proof By Lemma 2.1, we have

$$\sum_{(a_1,\mathbb{b}_1)\in U} \left(|N_V^\lambda(a_1,\mathbb{b}_1)| - \frac{|V|}{q} \right)^2 \leqslant \sum_{(a_1,\mathbb{b}_1)\in\mathbb{F}_q\mathbb{F}_q^d} \left(|N_V^\lambda(a_1,\mathbb{b}_1)| - \frac{|V|}{q} \right)^2 < q^d|V|.$$

By the Cauchy–Schwartz inequality,

$$\left| N^\lambda(V, U) - \frac{|V||U|}{q} \right| \leqslant \sum_{(a_1,\mathbb{b}_1)\in U} \left| |N_V^\lambda(a_1,\mathbb{b}_1)| - \frac{|V|}{q} \right|$$
$$\leqslant \sqrt{|U|}\sqrt{\sum_{(a_1,\mathbb{b}_1)\in U} \left(|N_V^\lambda(a_1,\mathbb{b}_1) - \frac{|V|}{q} \right)^2}$$
$$\leqslant \sqrt{q^d|V||U|}.$$

□

3. The system of k equations, $k+1$ variables. We will prove Theorem 1.2 in this section (Theorem 1.1 is just a special case of this result). The proof proceeds by

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

induction. The base step $k = 1$ is Theorem 2.1 above. Assuming that the theorem holds for all systems of l equations and $l + 1$ variables with $l < k$, from Lemma 2.1, we have

$$\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\left(|N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0)| - \frac{|\mathcal{A}_i|}{q}\right)^2 \leqslant \sum_{(a_0,\mathbb{b}_0)\in\mathbb{F}_q\times\mathbb{F}_q^d}\left(|N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0)| - \frac{|\mathcal{A}_i|}{q}\right)^2 \leqslant q^d|\mathcal{A}_i|. \tag{3.1}$$

For any $k \geqslant 2$, by the Cauchy–Schwartz inequality, we have

$$\prod_{i=1}^{k}\left(\sum_{j=1}^{n} a_{i,j}^2\right) \geqslant \left(\sum_{j=1}^{n}\prod_{i=1}^{k-1} a_{i,j}^2\right)\left(\sum_{j=1}^{n} a_{k,j}^2\right) \geqslant \left(\sum_{j=1}^{n}\prod_{i=1}^{k} a_{i,j}\right)^2. \tag{3.2}$$

It follows from (3.1) and (3.2) that

$$\left(\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{i=1}^{k}\left(N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0\right) - \frac{|\mathcal{A}_i|}{q})\right)^2$$
$$\leqslant \sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{i=1}^{k}\left(N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0) - \frac{|\mathcal{A}_i|}{q}\right)^2 \leqslant q^{dk}\prod_{i=1}^{k}|\mathcal{A}_i|,$$

which can be written as

$$\left|\sum_{I\subset\{1,\ldots,k\}}\left((-1)^{k-|I|}\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{j\notin I}\frac{|\mathcal{A}_j|}{q}\prod_{i\in I}N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0)\right)\right| \leqslant \sqrt{q^{kd}\prod_{i=1}^{k}|\mathcal{A}_i|}. \tag{3.3}$$

For any $I \subset \{1, \ldots, k\}$ with $0 < |I| < k$, by the induction hypothesis, we have

$$\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{i\in I}N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0) = (1 + o(1))q^{-|I|}|\mathcal{A}_0|\prod_{i\in I}|\mathcal{A}_i|. \tag{3.4}$$

Putting (3.3) and (3.4) together, we have

$$\left|\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{i=1}^{k}N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0) - (1 + o(1))q^{-k}\prod_{i=0}^{k}|\mathcal{A}_i|\right| \leqslant \sqrt{q^{k}\prod_{i=1}^{k}|\mathcal{A}_i|}.$$

Since $|\mathcal{A}_0|^2\prod_{i=1}^{k}|\mathcal{A}_i| \gg q^{(d+2)k}$, the left-hand side is dominated by $(1 + o(1))q^{-k}\prod_{i=0}^{k}|\mathcal{A}_i|$. This implies that

$$\sum_{(a_0,\mathbb{b}_0)\in\mathcal{A}_0}\prod_{i=1}^{k}N^{\lambda_i}_{\mathcal{A}_i}(a_0,\mathbb{b}_0) = (1 + o(1))q^{-k}\prod_{i=0}^{k}|\mathcal{A}_i|,$$

completing the proof of the theorem.

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

4. The system of three equations, three variables.

4.1. The case $d = 1$ (proof of Theorem 1.3). Let $\mathcal{A}_i^* = \mathcal{A}_i \cap \mathbb{F}_q^* \times \mathbb{F}_q^*$, $i = 0, 1, 2$, then

$$|\mathcal{A}_i^*| \gg q^{3/2},$$

for $i \in \{0, 1, 2\}$. For any $\lambda_1, \lambda_2 \in \mathbb{F}_q^*$, it follows from Theorem 1.1 that

$$|\{(a_i, b_i) \in \mathcal{A}_i^*, i = 0, 1, 2 : a_0 + a_1 - b_0 b_1 = \lambda_1, a_0 + a_2 - b_0 b_2 = \lambda_2\}| = (1 + o(1)) \frac{|\mathcal{A}_0^*||\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2}.$$

By the pigeon-hole principle, there exists $(a_0, b_0) \in \mathcal{A}_0^*$ such that

$$|\{(a_i, b_i) \in \mathcal{A}_i^*, i = 1, 2 : a_0 + a_1 - b_0 b_1 = \lambda_1, a_0 + a_2 - b_0 b_2 = \lambda_2\}| = (1 + o(1)) \frac{|\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2} \gg q.$$

Let $\delta = \sqrt{|\mathcal{A}_1^*||\mathcal{A}_2^*|/q^2} \gg q^{-1/2}$. Let $\mathcal{A}_i' = \{(a_i, b_i) \in \mathcal{A}_i^* : a_0 + a_i - b_0 b_i = \lambda_i\}$, $i = 1, 2$, then $|\mathcal{A}_1'||\mathcal{A}_2'| \gg \delta^2 q^2$. We assume that $|\mathcal{A}_2'| \geqslant |\mathcal{A}_1'|$, then $|\mathcal{A}_2'| \geqslant \delta q$. It suffices to show that there are at least $c\delta q$ values of λ such that the equation

$$a_1 + a_2 - b_1 b_2 = \lambda, \quad (a_i, b_i) \in \mathcal{A}_i', i = 1, 2 \tag{4.1}$$

is solvable. For a fix $(a_1, b_1) \in \mathcal{A}_1'$, we want to solve the following system:

$$a_0 + a - b_0 b = \lambda_2,$$
$$a_1 + a - b_1 b = \lambda,$$

under the constraint $a_0 + a_1 - b_0 b_1 = \lambda_1$. It follows that $(b_1 - b_0)b = \lambda_2 - \lambda + a_1 - a_0$. Thus, the system has at most one solution unless $b_1 - b_0 = \lambda_2 - \lambda + a_1 - a_0 = 0$. Suppose that $b_1 = b_0$ and $\lambda = \lambda_2 + a_1 - a_0$, then from the constraint $a_0 + a_1 - b_0 b_1 = \lambda_1$, we have $a_1 = b_0^2 + \lambda_1 - a_0$ and $\lambda = \lambda_2 + \lambda_1 + b_0^2 - 2a_0$. We consider two cases. Since $|\mathcal{A}_2'| \leq q$, $|\mathcal{A}_1'| \geq \delta^2 q \gg 1$. Thus, we can choose $(a_1, b_1) \in \mathcal{A}_1'$ such that $(a_1, b_1) \neq (b_0^2 + \lambda_1 - a_0, b_0)$. Equation (4.1) now has at most one solution for each λ. So, there exists at least $|\mathcal{A}_2'| \geq \delta q$ values of λ such that equation (4.1) is solvable. This complete the proof of the theorem.

4.2. The case $d \geq 2$ (proof of Theorem 1.4). Let $\mathcal{A}_i^* = \mathcal{A}_i \backslash (0; 0, \ldots, 0)$. For any $\lambda_1, \lambda_2 \in \mathbb{F}_q$, it follows from Theorem 1.1 that

$$|\{(a_i, \mathbb{b}_i) \in \mathcal{A}_i^*, i = 0, 1, 2 : a_0 a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda_1, a_0 a_2 - \mathbb{b}_0 \cdot \mathbb{b}_2 = \lambda_2\}| = (1 + o(1)) \frac{|\mathcal{A}_0^*||\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2}.$$

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

By the pigeon-hole principle, there exists $(a_0, \mathbb{b}_0) \in \mathcal{A}_0^*$ such that

$$|\{((a_1, \mathbb{b}_1), (a_2, \mathbb{b}_2)) \in \mathcal{A}_1^* \times \mathcal{A}_2^* : a_0 a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda_1, a_0 a_2 - \mathbb{b}_0 \cdot \mathbb{b}_2 = \lambda_2\}| \\ = (1 + o(1)) \frac{|\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2}.$$

For any $(a, \mathbb{b}) \in \mathbb{F}_q \times \mathbb{F}_q^d \backslash (0; 0, \dots, 0)$, set $\Pi_\lambda(a, \mathbb{b}) = \{(u, \mathbb{v}) \in \mathbb{F}_q \times \mathbb{F}_q^d : au - \mathbb{b} \cdot \mathbb{v} = \lambda\}$. Let $\mathcal{A}_1' = \Pi_{\lambda_1}(a_0, \mathbb{b}_0) \cap \mathcal{A}_1^*$ and $\mathcal{A}_2' = \Pi_{\lambda_2}(a_0, \mathbb{b}_0) \cap \mathcal{A}_2^*$, then

$$|\mathcal{A}_1'||\mathcal{A}_2'| = (1 + o(1)) \frac{|\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2} \gg q^{d+1}.$$

The first part of Theorem 1.4 follows immediately from the following lemma:

LEMMA 4.1. *For any $(a, \mathbb{b}) \in \mathbb{F}_q \times \mathbb{F}_q^d \backslash (0; 0, \dots, 0)$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$, suppose that $\mathcal{E} \subseteq \Pi_{\lambda_1}(a, \mathbb{b})$, $\mathcal{F} \subseteq \Pi_{\lambda_2}(a, \mathbb{b})$. If $d \geqslant 2$ and $|\mathcal{E}||\mathcal{F}| \gg q^{d+1}$, then*

$$|\Pi(\mathcal{E}, \mathcal{F}) := \{e_0 f_0 - \mathbb{e}_1 \cdot \mathbb{f}_1 : (e_0, \mathbb{e}_1) \in \mathcal{E}, (f_0, \mathbb{f}_1) \in \mathcal{F}\}| \geqslant (1 - o(1))q.$$

Proof The proof is similar to that of Theorem 2.8 in [7]. Define the incidence function

$$\upsilon_\lambda(\mathcal{E}, \mathcal{F}) = \{((e_0, \mathbb{e}_1), (f_0, \mathbb{f}_1)) \in \mathcal{E} \times \mathcal{F} : e_0 f_0 - \mathbb{e}_1 \cdot \mathbb{f}_1 = \lambda\}.$$

The Fourier transform of a complex-valued function f on $\mathbb{F}_q^d$ with respect to a non-trivial additive character χ on $\mathbb{F}_q$ is given by

$$\hat{f}(k) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot k) f(x), \tag{4.2}$$

and the Fourier inversion formula takes the form

$$f(x) = \sum_{k \in \mathbb{F}_q^d} \chi(x \cdot k) \hat{f}(k). \tag{4.3}$$

The Cauchy–Schwartz inequality applied to the sum in the variable $(a_0, \mathbb{b}_0)$ yields

$$\begin{aligned}
\sum_{\lambda \in \mathbb{F}_q} \upsilon_\lambda(\mathcal{E}, \mathcal{F})^2 &\leqslant |\mathcal{E}| \sum_{\lambda \in \mathbb{F}_q} \sum_{\substack{a_0 + a_1 - \mathbb{b}_0 \cdot \mathbb{b}_1 = \lambda \\ a_0 + a_1' - \mathbb{b}_0 \cdot \mathbb{b}_1' = \lambda}} \mathcal{E}(a_0, \mathbb{b}_0) \mathcal{F}(a_1, \mathbb{b}_1) \mathcal{F}(a_1', \mathbb{b}_1') \\
&= |\mathcal{E}| \sum_{(a_1 - a_1') - \mathbb{b}_0 \cdot (\mathbb{b}_1 - \mathbb{b}_1') = 0} \mathcal{E}(a_0, \mathbb{b}_0) \mathcal{F}(a_1, \mathbb{b}_1) \mathcal{F}(a_1', \mathbb{b}_1') \\
&= |\mathcal{E}| q^{-1} \sum_{\substack{s, a_0, a_1, a_1' \in \mathbb{F}_q \\ \mathbb{b}_0, \mathbb{b}_1, \mathbb{b}_1' \in \mathbb{F}_q^d}} \chi(s(a_1 - a_1' - \mathbb{b}_0 \cdot (\mathbb{b}_1 - \mathbb{b}_1')) \mathcal{E}(a_0, \mathbb{b}_0) \mathcal{F}(a_1, \mathbb{b}_1) \mathcal{F}(a_1', \mathbb{b}_1') \\
&= q^{-1} |\mathcal{E}|^2 |\mathcal{F}|^2 + q^{-1} |\mathcal{E}| q^{2d+2} \sum_{s \neq 0, a_0 \in \mathbb{F}_q, b_0 \in \mathbb{F}_q^d} \mathcal{E}(a_0, \mathbb{b}_0) |\hat{\mathcal{F}}(s(1, \mathbb{b}_0))|^2,
\end{aligned}$$

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

where the last line follows from (4.2). By changing variables $a_0 \to a_1$, $s \to a_0$ and $s\mathbb{b}_0 \to \mathbb{b}_0$, we have

$$\begin{aligned}\sum_{\lambda\in\mathbb{F}_q} \nu_\lambda(\mathcal{E},\mathcal{F})^2 &\leqslant q^{-1}|\mathcal{E}|^2|\mathcal{F}|^2 + q^{2d+1}|\mathcal{E}| \sum_{a_0\neq 0, a_1\in\mathbb{F}_q, \mathbb{b}_0\in\mathbb{F}_q^d} \mathcal{E}(a_1, a_0^{-1}\mathbb{b}_0)|\hat{\mathcal{F}}(a_0,\mathbb{b}_0)|^2 \\ &\leqslant q^{-1}|\mathcal{E}|^2|\mathcal{F}|^2 + q^{2d+1}|\mathcal{E}| \sum_{a_0\neq 0, \mathbb{b}_0\in\mathbb{F}_q^d} |\hat{\mathcal{F}}(a_0,\mathbb{b}_0)|^2 \\ &\leqslant q^{-1}|\mathcal{E}|^2|\mathcal{F}|^2 + q^{2d+1}|\mathcal{E}|q^{-(d+1)} \sum_{(a_0^*,\mathbb{b}_0^*)\in\mathbb{F}_q\times\mathbb{F}_q^d} |\mathcal{F}(a_0^*,\mathbb{b}_0^*)|^2 \\ &= q^{-1}|\mathcal{E}|^2|\mathcal{F}|^2 + q^d|\mathcal{E}||\mathcal{F}|,\end{aligned}$$

where the second line follows from the fact that for each $a_0^{-1}\mathbb{b}_0$, there exists at most one $a_1 \in \mathbb{F}_q$ such that $(a_1, a_0^{-1}\mathbb{b}_0) \in \mathcal{E} \subseteq \Pi_{\lambda_1}(a,\mathbb{b})$. By the Cauchy–Schwartz inequality again, we have

$$|\mathcal{E}|^2|\mathcal{F}|^2 = \left(\sum_\lambda \nu_\lambda(\mathcal{E},\mathcal{F})\right)^2 \leqslant |\Pi(\mathcal{E},\mathcal{F})| \sum_\lambda \nu_\lambda(\mathcal{E},\mathcal{F})^2.$$

This implies that

$$|\Pi(\mathcal{E},\mathcal{F})| \geqslant \frac{q}{1+\frac{q^d}{|\mathcal{E}||\mathcal{F}|}}.$$

This follows that if $|\mathcal{E}||\mathcal{F}| \gg q^d$, then $|\Pi(\mathcal{E},\mathcal{F})| = q(1-o(1))$, completing the proof of the lemma. □

If $d \geq 3$ and

$$|\mathcal{A}_0||\mathcal{A}_1, |\mathcal{A}_1||\mathcal{A}_2|, |\mathcal{A}_0||\mathcal{A}_2| \gg q^{(d+3)/2},$$

then

$$|\mathcal{A}_1'||\mathcal{A}_2'| = (1+o(1))\frac{|\mathcal{A}_1^*||\mathcal{A}_2^*|}{q^2} \gg q^{d+1}.$$

From Theorem 2.2, for any $\lambda_3 \in \mathbb{F}_q$, there are $(a_1,\mathbb{b}_1) \in \mathcal{A}_1'$ and $(a_2,\mathbb{b}_2) \in \mathcal{A}_2'$ such that $a_1a_2 - \mathbb{b}_1\cdot\mathbb{b}_2 = \lambda_3$. Therefore, the system (1.3) is solvable for all triples $(\lambda_1,\lambda_2,\lambda_3) \in \mathbb{F}_q^3$. This complete the proof of the theorem.

REFERENCES

1. J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich and D. Koh, Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates, *Math. Zeitschr.* (to appear).

2. D. Covert, D. Hart, A. Iosevich and I. Uriarte-Tuero, An analog of the Furstenberg-Katznelson–Weiss theorem on triangles in sets of positive density in finite field geometries, *Discr. Math.* (to appear).

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

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

https://doi.org/10.1017/S0017089511000425 Published online by Cambridge University Press

5. D. Hart and A. Iosevich, Ubiquity of simplices in subsets of vector spaces over finite fields, *Anal. Math.* **34** (2007), 29–38.

6. D. Hart and A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, *Contemp. Math.* **464** (2008).

7. D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum–product theory in finite fields, and the Erdös-Falconer distance conjecture, *Trans. AMS* **363** (2011) 3255–3275.

8. A. Sárközy, On products and shifted products of residues modulo p, *Integers: Electron. J. Combin. Numb. Theory* **8**(2) (2008), A9, 1–8.

9. I. E. Shparlinski, On the solvability of bilinear equations in finite fields, *Glassgow Math. J.* **50** (2008), 523–529.

10. L. A. Vinh, On the solvability of bilinear equations in finite fields, *Proc. Amer. Math. Soc.* **137** (2009), 2889–2898.

11. L. A. Vinh, Szemerédi–Trotter type theorem and sum–product estimate in finite fields, *Eur. J. Combin.*, accepted.

12. L. A. Vinh, On a Furstenberg-Katznelson-Weiss type theorem over finite fields, *Ann. Combin.* (to appear).

13. L. A. Vinh, Triangles in vector spaces over finite fields, *Online J. Anal. Combin.* (to appear).

14. L. A. Vinh, On kaleidoscopic pseudorandomness of finite Euclidean graphs, *Discuss. Math. Graph Theory* (to appear).

15. L. A. Vinh, On some problems of Sárközy and Gyarmati, *Integers: Electron. J. Combin. Numb. Theory* (to appear).