PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 9, September 2009, Pages 2889–2898
S 0002-9939(09)09947-X
Article electronically published on May 4, 2009

ON THE SOLVABILITY OF SYSTEMS OF BILINEAR EQUATIONS IN FINITE FIELDS

LE ANH VINH

(Communicated by Ken Ono)

ABSTRACT. Given k sets $\mathcal{A}_i \subseteq \mathbb{F}_q^d$ and a non-degenerate bilinear form B in $\mathbb{F}_q^d$, we consider the system of $l \leq \binom{k}{2}$ bilinear equations

$$B(\boldsymbol{a}_i, \boldsymbol{a}_j) = \lambda_{ij}, \ \ \boldsymbol{a}_i \in \mathcal{A}_i, i = 1, \ldots, k.$$

We show that the system is solvable for any $\lambda_{ij} \in \mathbb{F}_q^*$, $1 \leq i, j \leq k$, given that the restricted sets $\mathcal{A}_i$ are sufficiently large.

1. INTRODUCTION

In [10], 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

$$ab + 1 = cd \tag{1.1}$$

can be solved with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$ and $d \in \mathcal{D}$. Gyarmati and Sárközy [3] generalized the results on the solvability of equation (1.1) to finite fields. They also studied 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 exponential sums, Hart and Iosevich [5] studied a similar problem for any bilinear equation over $\mathbb{F}_q^d$. They showed that for any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^d$, with

$$|\mathcal{A}||\mathcal{B}| > Cq^{d+1}$$

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

$$\boldsymbol{a} \cdot \boldsymbol{b} = \lambda, \ \ \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B},$$

is solvable for any $\lambda \in \mathbb{F}_q^*$. Although the proof is given only in the case of the dot product, it goes through without any essential changes if the dot product $\boldsymbol{a} \cdot \boldsymbol{b}$ is replaced by any non-degenerate bilinear form $B(\boldsymbol{a}, \boldsymbol{b})$. Using bounds of multiplicative character sums, Shparlinski [11] extended the class of sets which satisfy this property.

In this paper, we will use methods from graph theory to study the system of bilinear equations in finite fields. More precisely, we consider the following system:

$$B(\boldsymbol{a}_i, \boldsymbol{a}_j) = \lambda_{ij}, \ \ \boldsymbol{a}_i \in \mathcal{A}_i, i = 1, \ldots, k$$

Received by the editors December 1, 2008.
2000 *Mathematics Subject Classification.* Primary 11L40, 11T30; Secondary 11E39.
Key words and phrases. Bilinear equations, finite fields.

over $\mathbb{F}_q^d$, with variables from arbitrary sets $\mathcal{A}_i \subseteq \mathbb{F}_q^d$, $i = 1, \dots, k$. Our first result is the following.

Theorem 1.1. *Given k sets $\mathcal{A}_i \subseteq \mathbb{F}_q^d$, let $B(\cdot, \cdot)$ be a non-degenerate bilinear form in $\mathbb{F}_q^d$. Consider the system $\mathcal{L}$ of $l \leq \binom{k}{2}$ bilinear equations*

$$B(\boldsymbol{a}_i, \boldsymbol{a}_j) = \lambda_{ij}, \ \ \boldsymbol{a}_i \in \mathcal{A}_i, i = 1, \dots, k. \tag{1.2}$$

Suppose that each variable appears in at most $t \leq k-1$ equations and

$$|\mathcal{A}_i| \gg q^{\frac{d-1}{2}+t}.$$

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

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

solutions.

The study of systems of bilinear equations in vector spaces over finite fields in the context of Theorem 1.1 in the case $t = k - 1$ can be found in Chapter 2 of D. Hart's dissertation [4]. Theorem 1.1 is a quantitative improvement over the result given there.

Serious difficulties arise when the number of equations that each variable appears in is sufficiently large with respect to the ambient dimension. More precisely, Theorem 1.1 is only non-trivial in the range $d \geq 2t$. Even in the case of each variable appearing in at most two equations, Theorem 1.1 is not non-trivial for $d \geq 4$. The purpose of the following theorem is to fill in this gap. We show that the system of two bilinear equations and three variables in large restricted subsets of $\mathbb{F}_q^d$ is always solvable for $d \geq 2$.

Theorem 1.2. *Given three sets $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^d$, let $B(\cdot, \cdot)$ be a non-degenerate bilinear form in $\mathbb{F}_q^d$. Consider the system of two equations*

$$B(\boldsymbol{a}, \boldsymbol{b}) = \lambda_1, B(\boldsymbol{a}, \boldsymbol{c}) = \lambda_2, \ \ \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}, \boldsymbol{c} \in \mathcal{C}. \tag{1.3}$$

Suppose that

$$|\mathcal{A}||\mathcal{B}|, |\mathcal{A}||\mathcal{C}| \gg q^{d+1}.$$

Then for any $\lambda_1, \lambda_2 \in \mathbb{F}_q^*$, the above system has

$$(1 + o(1)) \frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}|}{q^2}$$

solutions.

The solvability of the system of three bilinear equations and three variables in large restricted subsets of $\mathbb{F}_q^2$, however, is harder to determine. We will instead show that the system is solvable for a positive proportion of all triples $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_q^*$. More precisely, we have the following theorem.

Theorem 1.3. *Given three sets $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^2$, let $B(\cdot, \cdot)$ be a non-degenerate bilinear form in $\mathbb{F}_q^2$. Consider the system of equations*

$$B(\boldsymbol{a}, \boldsymbol{b}) = \lambda_1, B(\boldsymbol{a}, \boldsymbol{c}) = \lambda_2, B(\boldsymbol{b}, \boldsymbol{c}) = \lambda_3, \ \ \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}, \boldsymbol{c} \in \mathcal{C}.$$

Suppose that

$$|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \gg q^{3/2}.$$

Then the above system is solvable for $\Omega(\frac{\sqrt{|\mathcal{B}||\mathcal{C}|}}{q^2})q^3$ *triples* $(\lambda_1, \lambda_2, \lambda_3) \in (\mathbb{F}_q^*)^3$.

It is conceivable that we can chop off the term $\Omega(\frac{\sqrt{|\mathcal{B}||\mathcal{C}|}}{q^2})$ 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 this is indeed the case when the ambient space has dimension $d \geq 3$.

Theorem 1.4. *Given three sets* $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^d$, *let* $B(\cdot, \cdot)$ *be a non-degenerate bilinear form in* $\mathbb{F}_q^d$. *Consider the system of equations*

$$B(\boldsymbol{a}, \boldsymbol{b}) = \lambda_1, B(\boldsymbol{a}, \boldsymbol{c}) = \lambda_2, B(\boldsymbol{b}, \boldsymbol{c}) = \lambda_3, \ \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}, \boldsymbol{c} \in \mathcal{C}.$$

Suppose that

$$|\mathcal{A}||\mathcal{B}|, |\mathcal{A}||\mathcal{C}|, |\mathcal{B}||\mathcal{C}| \gg q^{d+2}.$$

Then the above system is solvable for $(1 - o(1))q^3$ *triples* $(\lambda_1, \lambda_2, \lambda_3) \in (\mathbb{F}_q^*)^3$.

Note that there is a series of papers dealing with similar results in the sovability of systems of quadratic forms; for example, see [2, 6, 8, 12, 13, 14, 15].

2. Bilinear equations in finite fields

Let $B(\cdot, \cdot)$ be a non-degenerate bilinear form in $\mathbb{F}_q^d$ and $\lambda \in \mathbb{F}_q^*$. For any $\boldsymbol{v} \in \mathbb{F}_q^d$ and a subset $V \subseteq \mathbb{F}_q^d$, denote by $N^\lambda(\boldsymbol{v})$ the set of all vectors $\boldsymbol{u} \in \mathbb{F}_q^d$ such that $B(\boldsymbol{v}, \boldsymbol{u}) = \lambda$, and let $N_V^\lambda(\boldsymbol{v}) = N^\lambda(\boldsymbol{v}) \cap V$. The following key estimate says that the cardinalities of $N_V^\lambda(\boldsymbol{v})$'s are close to $|V|/q$ when $|V|$ is large.

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

$$\sum_{\boldsymbol{v} \in \mathbb{F}_q^d} \left(|N_V^\lambda(\boldsymbol{v})| - \frac{|V|}{q} \right)^2 < q^{d-1}|V|.$$

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

$$\begin{aligned} |N_V^\lambda(\boldsymbol{v})| &= \sum_{\boldsymbol{u} \in \mathbb{F}_q^d, B(\boldsymbol{v}, \boldsymbol{u}) = \lambda} V(\boldsymbol{u}) \\ &= \sum_{u \in \mathbb{F}_q^d, s \in \mathbb{F}_q} \frac{1}{q} \chi(s(B(\boldsymbol{v}, \boldsymbol{u}) - \lambda)) V(\boldsymbol{u}) \\ &= \frac{|V|}{q} + \frac{1}{q} \sum_{u \in \mathbb{F}_q^d, s \in \mathbb{F}_q^*} \chi(s(B(\boldsymbol{v}, \boldsymbol{u}) - \lambda)) V(\boldsymbol{u}). \end{aligned}$$

Therefore

$$\begin{aligned} \sum_{\boldsymbol{v} \in \mathbb{F}_q^d} \left(|N_V^\lambda(\boldsymbol{v})| - \frac{|V|}{q} \right)^2 &= \frac{1}{q^2} \sum_{\boldsymbol{v} \in \mathbb{F}_q^d} \left(\sum_{\boldsymbol{u} \in \mathbb{F}_q^d, s \in \mathbb{F}_q^*} \chi(s(B(\boldsymbol{v}, \boldsymbol{u}) - \lambda)) V(\boldsymbol{u}) \right)^2 \\ = \frac{1}{q^2} \sum_{\boldsymbol{v}, \boldsymbol{u}, \boldsymbol{u}' \in \mathbb{F}_q^d, s, s' \in \mathbb{F}_q^*} &\chi((sB(\boldsymbol{v}, \boldsymbol{u}) - s'B(\boldsymbol{v}, \boldsymbol{u}'))\chi(\lambda(s' - s)) V(\boldsymbol{u}) V(\boldsymbol{u}') \\ (2.1) \quad = \frac{1}{q^2}(R_1 + R_2), \end{aligned}$$

where R_1 is taken over $s = s'$ and R_2 is taken over $s \neq s'$. We compute each term.

$$\begin{aligned} R_1 &= \sum_{\boldsymbol{v},\boldsymbol{u},\boldsymbol{u}' \in \mathbb{F}_q^d, s=s' \in \mathbb{F}_q^*} \chi((sB(\boldsymbol{v},\boldsymbol{u}) - s'B(\boldsymbol{v},\boldsymbol{u}'))\chi(\lambda(s'-s))V(\boldsymbol{u})V(\boldsymbol{u}') \\ &= \sum_{\boldsymbol{v},\boldsymbol{u},\boldsymbol{u}' \in \mathbb{F}_q^d, s=s' \in \mathbb{F}_q^*} \chi(sB(\boldsymbol{v},\boldsymbol{u}-\boldsymbol{u}'))V(\boldsymbol{u})V(\boldsymbol{u}') \\ &= (q-1)q^d|V|, \end{aligned} \tag{2.2}$$

where the last line follows from the orthogonality in $\boldsymbol{v}$. Now we compute R_2.

$$\begin{aligned} R_2 &= \sum_{\boldsymbol{v},\boldsymbol{u},\boldsymbol{u}' \in \mathbb{F}_q^d, s \in \mathbb{F}_q^*, a \neq 0,1} \chi(sB(\boldsymbol{v},\boldsymbol{u}-a\boldsymbol{u}'))\chi(\lambda(as-s))V(\boldsymbol{u})V(\boldsymbol{u}') \\ &= \sum_{\boldsymbol{v},\boldsymbol{u},\boldsymbol{u}' \in \mathbb{F}_q^d, s \in \mathbb{F}_q^*, a \neq 0,1, \boldsymbol{u}=a\boldsymbol{u}'} \chi(\lambda(as-s))V(\boldsymbol{u})V(a^{-1}\boldsymbol{u}) \\ &= -\sum_{\boldsymbol{v},\boldsymbol{u} \in \mathbb{F}_q^d, a \neq 0,1} V(\boldsymbol{u})V(a^{-1}\boldsymbol{u}) \\ &\geq -(q-2)q^d|V|, \end{aligned} \tag{2.3}$$

where the second line follows from the orthogonality in $\boldsymbol{v}$. The lemma follows immediately from (2.1), (2.2) and (2.3). □

The following result ([5, Theorem 2.1]) is an easy corollary of Lemma 2.1.

Theorem 2.2 ([5, Theorem 2.1])**.** *Let $B(\cdot,\cdot)$ be a non-degenerate bilinear form in $\mathbb{F}_q^d$ and $\lambda \in \mathbb{F}_q^*$. For any two subsets $V, U \subseteq \mathbb{F}_q^d$, denote by $N^\lambda(V,U)$ the set of pairs $(\boldsymbol{v},\boldsymbol{u}) \in V \times U$ such that $B(\boldsymbol{v},\boldsymbol{u}) = \lambda$. Then we have*

$$\left| N^\lambda(V,U) - \frac{|V||U|}{q} \right| < \sqrt{q^{d-1}|V||U|}.$$

Proof. By Lemma 2.1, we have

$$\sum_{\boldsymbol{u} \in U} \left(|N_V^\lambda(\boldsymbol{u})| - \frac{|V|}{q} \right)^2 \leq \sum_{\boldsymbol{u} \in \mathbb{F}_q^d} \left(|N_V^\lambda(\boldsymbol{u})| - \frac{|V|}{q} \right)^2 < q^{d-1}|V|.$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned} \left| N^\lambda(V,U) - \frac{|V||U|}{q} \right| &\leq \sum_{\boldsymbol{u} \in U} \left| |N_V^\lambda(\boldsymbol{u})| - \frac{|V|}{q} \right| \\ &\leq \sqrt{|U|} \sqrt{\sum_{\boldsymbol{u} \in U} \left(|N_V^\lambda(\boldsymbol{u}) - \frac{|V|}{q} \right)^2} \\ &\leq \sqrt{q^{d-1}|V||U|}. \end{aligned}$$

□

Remark 2.3. Theorem 2.2 has several applications in additive combinatorics (see [7]). We present here another application of this theorem to Waring's problem (mod p). Let p be a prime and k a positive integer. The smallest s such that the congruence

$$x_1^k + \cdots + x_s^k \equiv a \mod p \tag{2.4}$$

is solvable for all numbers a is called Waring's number (mod p), denoted $\gamma(k,p)$ (see [1] for a historical background and recent results on this problem). Let $\gamma^*(k,p)$ denote the smallest s such that the congruence (2.4) is solvable for all $a \neq 0$. It is clear that $\gamma(k,p) \leq \gamma^*(k,p)+1$. Take A to be the set of all k-powers in $\mathbb{F}_q$, and let $U \equiv V \equiv A^d$. From Theorem 2.2, the congruence (2.4) with $s=d$ is solvable for all $a \neq 0$ if $q^{\frac{d-1}{2d}} \geq k$. It follows that $\gamma^*(k,p) \leq d$ whenever $\gamma^*(k,p)$. This essentially matches with the classical bound of Weil in [16].

3. General systems of bilinear equations

Now we give a proof of Theorem 1.1. The proof is very similar to that of [9, Theorem 4.10]. Consider a random one-to-one mapping of the set of variables of $\mathcal{L}$ into the sets $\mathcal{A}_1, \ldots, \mathcal{A}_k$. Let $M(\mathcal{L})$ denote the event that all equations in $\mathcal{L}$ are satisfied under this mapping. We say that the mapping is an embedding of $\mathcal{L}$ in such a case. It suffices to prove that

$$\Pr(M(\mathcal{L})) = (1+o(1))q^{-l}. \tag{3.1}$$

We prove (3.1) by induction on l, the number of equations in $\mathcal{L}$. The base case $l=0$ is trivial. Suppose that the theorem holds for all systems of less than l equations. Let $B(\boldsymbol{a}_1, \boldsymbol{a}_2) = \lambda$, $\boldsymbol{a}_1 \in \mathcal{A}_1$, $\boldsymbol{a}_2 \in \mathcal{A}_2$, be an equation of $\mathcal{L}$. Let $\mathcal{L}_{\boldsymbol{a}_1}, \mathcal{L}_{\boldsymbol{a}_2}, \mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}$ be the subsystems obtained from $\mathcal{L}$ by removing all equations that contain $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$, respectively, and let $\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}$ be the subsystem obtained from $\mathcal{L}$ by removing the equation $B(\boldsymbol{a}_1, \boldsymbol{a}_2) = \lambda$. We have

$$\Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2})) = \Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}) | M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) \cdot \Pr(M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})). \tag{3.2}$$

Let l_1 be the number of equations in $\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}$. Since (3.1) holds for $\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}$ and $\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}$, we have

$$\Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2})) = (1+o(1))q^{1-l}$$

and

$$\Pr(M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) = (1+o(1))q^{-l_1}.$$

Therefore, we have

$$\Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}) | M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) = (1+o(1))q^{l_1+1-l}. \tag{3.3}$$

For an embedding f_1 of $\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}$ into $\mathcal{A}_1, \ldots, \mathcal{A}_k$, let $\phi(\boldsymbol{a}_1, f_1)$, $\phi(\boldsymbol{a}_2, f_1)$ and $\phi(\boldsymbol{a}_1\boldsymbol{a}_2, f_1)$ be the number of extensions of f_1 to an embedding of $\mathcal{L}_{\boldsymbol{a}_1}, \mathcal{L}_{\boldsymbol{a}_2}$ and $\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}$ into $\mathcal{A}_1, \ldots, \mathcal{A}_k$, respectively. Note that an extension $f_{\boldsymbol{a}_1}$ of f_1 to an embedding of $\mathcal{L}_{\boldsymbol{a}_1}$ and an extension $f_{\boldsymbol{a}_2}$ of f_1 to an embedding of $\mathcal{L}_{\boldsymbol{a}_2}$ give us a unique extension of f_1 to an embedding of $\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}$. Hence,

$$\phi(\boldsymbol{a}_1\boldsymbol{a}_2, f_1) = \phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1). \tag{3.4}$$

Averaging over all possible extensions of f_1 to a mapping from $\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}$ into $\mathcal{A}_1, \ldots, \mathcal{A}_k$, we have

$$\Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}) | f_1) = \frac{\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)}{|\mathcal{A}_1||\mathcal{A}_2|}.$$

Taking expectation over all embeddings f_1, the LHS becomes

$$\Pr(M(\mathcal{L}_{\boldsymbol{a}_1,\boldsymbol{a}_2}) | M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) = (1+o(1))q^{l_1+1-l}.$$

So we get

$$E_{f_1}(\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1) | M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) = (1+o(1))|\mathcal{A}_1||\mathcal{A}_2|q^{l_1+1-l}. \tag{3.5}$$

Now, let f be a random one-to-one mapping of the set of variables of $\mathcal{L}$ into the sets $\mathcal{A}_1, \ldots, \mathcal{A}_k$. Let f_1 be a fixed embedding of $\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}$. Let $\mathcal{A}_2'$ and $\mathcal{A}_1'$ be the sets of all possible images of $\boldsymbol{a}_2$ and $\boldsymbol{a}_1$ over all possible extensions of f_1 to embeddings of $\mathcal{L}_{\boldsymbol{a}_1}$ and $\mathcal{L}_{\boldsymbol{a}_2}$ into $\mathcal{A}_1, \ldots, \mathcal{A}_k$, respectively. From Theorem 2.2, the number of possible pairs $(\boldsymbol{a}_1, \boldsymbol{a}_2)$ with $\boldsymbol{a}_1 \in \mathcal{A}_1'$ and $\boldsymbol{a}_2 \in \mathcal{A}_2'$ such that $B(\boldsymbol{a}_1, \boldsymbol{a}_2) = \lambda$ is bounded by

$$\frac{\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)}{q} \pm \sqrt{q^{d-1}\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)}. \tag{3.6}$$

Thus, we have

$$\Pr_{\ f}(M(\mathcal{L})|f_{|\{\boldsymbol{a}_3,\ldots,\boldsymbol{a}_k\}} = f_1) = \frac{\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)}{q|\mathcal{A}_1||\mathcal{A}_2|} + \delta,$$

where

$$|\delta| \le \frac{\sqrt{q^{d-1}\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)}}{|\mathcal{A}_1||\mathcal{A}_2|}.$$

Averaging over all possible embeddings f_1, we get

$$\begin{aligned}\Pr(M(\mathcal{L})|M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) &= \frac{E_{f_1}(\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1)|M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}))}{q|\mathcal{A}_1||\mathcal{A}_2|} + E_{f_1}(\delta)\\ &= (1+o(1))q^{l_1-l} + E_{f_1}(\delta),\end{aligned}$$

where the second line follows from (3.5) and (3.6). By Jensen's inequality, we have

$$|E_{f_1}(\delta)| \le q^{(d-1)/2}\frac{\sqrt{E(\phi(\boldsymbol{a}_1, f_1)\phi(\boldsymbol{a}_2, f_1))}}{|\mathcal{A}_1||\mathcal{A}_2|} = (1+o(1))\frac{q^{(d-1)/2}}{\sqrt{|\mathcal{A}_1||\mathcal{A}_2|}}q^{(l_1+1-l)/2}, \tag{3.7}$$

which is negligible to the first term as

$$\sqrt{|\mathcal{A}_1||\mathcal{A}_2|} \gg q^{\frac{d-1}{2}+t} \ge q^{(d-1)/2}q^{(l_1+1-l)/2}.$$

Thus, we have

$$\Pr(M(\mathcal{L})) = \Pr(M(\mathcal{L})|M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}}))\Pr(M(\mathcal{L}_{\{\boldsymbol{a}_1,\boldsymbol{a}_2\}})) = (1+o(1))q^{-l}. \tag{3.8}$$

This completes the proof of the theorem.

4. The system of two equations and three variables

We will prove Theorem 1.2 in this section. Our proof relies on Lemma 2.1 above. For any $\boldsymbol{v} \in \mathbb{F}_q^d$ and a subset $V \subseteq \mathbb{F}_q^d$, denote by $N^\lambda(\boldsymbol{v})$ the set of all vectors $\boldsymbol{u} \in \mathbb{F}_q^d$ such that $B(\boldsymbol{v}, \boldsymbol{u}) = \lambda$, and let $N_V^\lambda(\boldsymbol{v}) = N^\lambda(\boldsymbol{v}) \cap V$. The number of solutions of the system (1.3) is

$$\sum_{\boldsymbol{a}\in\mathcal{A}} |N_{\mathcal{B}}^{\lambda_1}(a)||N_{\mathcal{C}}^{\lambda_2}(a)|.$$

From Lemma 2.1, we have

$$\begin{aligned}\sum_{\boldsymbol{a}\in\mathcal{A}}\left(|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})| - \frac{|\mathcal{B}|}{q}\right)^2 &\le \sum_{\boldsymbol{a}\in\mathbb{F}_q^d}\left(|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})| - \frac{|\mathcal{B}|}{q}\right)^2 < q^{d-1}|\mathcal{B}|,\\ \sum_{\boldsymbol{a}\in\mathcal{A}}\left(|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})| - \frac{|\mathcal{C}|}{q}\right)^2 &\le \sum_{\boldsymbol{a}\in\mathbb{F}_q^d}\left(|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})| - \frac{|\mathcal{C}|}{q}\right)^2 < q^{d-1}|\mathcal{C}|.\end{aligned}$$

Thus, by the Cauchy-Schwarz inequality, we have

$$\left[\sum_{\boldsymbol{a}\in\mathcal{A}}\left(|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})|-\frac{|\mathcal{B}|}{q}\right)\left(|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{C}|}{q}\right)\right]^2$$
$$\leq \sum_{\boldsymbol{a}\in\mathcal{A}}\left(|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})|-\frac{|\mathcal{B}|}{q}\right)^2\sum_{\boldsymbol{a}\in\mathcal{A}}\left(|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{C}|}{q}\right)^2 < q^{2d-2}|\mathcal{B}||\mathcal{C}|.$$

This implies that

$$\left|\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})||N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{B}|}{q}\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{C}|}{q}\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})|+\frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}|}{q^2}\right| < q^{d-1}\sqrt{|\mathcal{B}||\mathcal{C}|}. \tag{4.1}$$

From Theorem 2.2, we have

$$\left|\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{A}||\mathcal{C}|}{q}\right| \leq \sqrt{q^{d-1}|\mathcal{A}||\mathcal{C}|}, \tag{4.2}$$

$$\left|\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})|-\frac{|\mathcal{A}||\mathcal{B}|}{q}\right| \leq \sqrt{q^{d-1}|\mathcal{A}||\mathcal{B}|}. \tag{4.3}$$

Putting (4.1), (4.2) and (4.3) together, it follows that

$$\left|\sum_{\boldsymbol{a}\in\mathcal{A}}|N_{\mathcal{B}}^{\lambda_1}(\boldsymbol{a})||N_{\mathcal{C}}^{\lambda_2}(\boldsymbol{a})|-\frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}|}{q^2}\right|$$
$$\leq \frac{|\mathcal{B}|}{q}\sqrt{q^{d-1}|\mathcal{A}||\mathcal{C}|}+\frac{|\mathcal{C}|}{q}\sqrt{q^{d-1}|\mathcal{A}||\mathcal{B}|}+q^{d-1}\sqrt{|\mathcal{B}||\mathcal{C}|},$$

completing the proof of the theorem.

5. The system of three equations and three variables

5.1. **The case $d=2$ (Proof of Theorem 1.3).** Let $\mathcal{A}^*=\mathcal{A}\cap\mathbb{F}_q^*\times\mathbb{F}_q^*$, $\mathcal{B}^*=\mathcal{B}\cap\mathbb{F}_q^*\times\mathbb{F}_q^*$ and $\mathcal{C}^*=\mathcal{C}\cap\mathbb{F}_q^*\times\mathbb{F}_q^*$. Then

$$|\mathcal{A}^*|,|\mathcal{B}^*|,|\mathcal{C}^*|\gg q^{3/2}.$$

For any $\lambda_1,\lambda_2\in\mathbb{F}_q^*$, it follows from Theorem 1.2 that

$$|\{(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})\in\mathcal{A}^*\times\mathcal{B}^*\times\mathcal{C}^*: B(\boldsymbol{a},\boldsymbol{b})=\lambda_1, B(\boldsymbol{a},\boldsymbol{c})=\lambda_2\}|=(1+o(1))\frac{|\mathcal{A}^*||\mathcal{B}^*||\mathcal{C}^*|}{q^2}.$$

By the pigeon-hole principle, there exists $\boldsymbol{a}_0\in\mathcal{A}^*$ such that

$$|\{(\boldsymbol{b},\boldsymbol{c})\in\mathcal{B}^*\times\mathcal{C}^*: B(\boldsymbol{a}_0,\boldsymbol{b})=\lambda_1, B(\boldsymbol{a}_0,\boldsymbol{c})=\lambda_2\}|=(1+o(1))\frac{|\mathcal{B}^*||\mathcal{C}^*|}{q^2}\gg q.$$

Let $\delta=\sqrt{|\mathcal{B}^*||\mathcal{C}^*|}/q^2\gg q^{-1/2}$. Let

$$\mathcal{B}_1=\{\boldsymbol{b}\in\mathcal{B}^*: B(\boldsymbol{a}_0,\boldsymbol{b})=\lambda_1\},\ \ \mathcal{C}_1=\{\boldsymbol{c}\in\mathcal{C}^*: B(\boldsymbol{a}_0,\boldsymbol{c})=\lambda_2\}.$$

Then $|\mathcal{B}_1||\mathcal{C}_1|\gg\delta^2q^2$. We assume that $|\mathcal{C}_1|\geq|\mathcal{B}_1|$. Then $|\mathcal{C}_1|\geq\delta q$. It suffices to show that there are at least δq values of λ such that

$$|\{(\boldsymbol{b},\boldsymbol{c})\in\mathcal{B}_1\times\mathcal{C}_1: B(\boldsymbol{b},\boldsymbol{c})=\lambda\}|>0.$$

For a fixed $\boldsymbol{b}_0 \in \mathcal{B}_1$, we want to solve the following system:

$$B(\boldsymbol{a}_0, \boldsymbol{c}) = \lambda_2, B(\boldsymbol{b}_0, \boldsymbol{c}) = \lambda, \boldsymbol{c} \in \mathcal{C}_1, \tag{5.1}$$

under the constraint $B(\boldsymbol{a}_0, \boldsymbol{b}_0) = \lambda_1$. Suppose that $B(\boldsymbol{x}, \boldsymbol{y}) = x_1y_1 + \kappa x_2y_2$ for some $\kappa \in \mathbb{F}_q^*$. Letting $\boldsymbol{a}_0 = (a_1, a_2)$, $\boldsymbol{b}_0 = (b_1, b_2)$ and $\boldsymbol{c} = (c_1, c_2)$, the system (5.1) becomes

$$\begin{aligned} a_1b_1 + \kappa a_2b_2 &= \lambda_1 \\ a_1c_1 + \kappa a_2c_2 &= \lambda_2 \\ b_1c_1 + \kappa b_2c_2 &= \lambda. \end{aligned}$$

This implies that $\kappa(a_2b_1 - a_1b_2)c_2 = \lambda_2b_1 - \lambda a_1$. Thus the system has at most one solution if $a_2b_1 - a_1b_2 \neq 0$. If $a_2b_1 = a_1b_2$, the system is solvable only if $\lambda = \lambda_2b_1/a_1$. Besides, from the first equation, $(\kappa a_2^2 + a_1^2)b_2 = \lambda_1a_2$ and $(\kappa a_2^2 + a_1^2)b_1 = \lambda_1a_1$. It follows that the system (5.1) has at most one solution if

$$\boldsymbol{b}_0 = (b_1, b_2) \neq \left(\frac{\lambda_1 a_1}{\kappa a_2^2 + a_1^2}, \frac{\lambda_1 a_2}{\kappa a_2^2 + a_1^2} \right). \tag{5.2}$$

Since $|\mathcal{C}^*| \leq q$, $|\mathcal{B}_1| \geq \delta^2 q \gg 1$. Thus, we can choose $\boldsymbol{b}_0 \in \mathcal{B}_1$ satisfying (5.2). The system (5.1) has at most one solution for each λ. So there exist at least $|\mathcal{C}_1| \geq \delta q$ values of λ such that the system (5.1) is solvable. This completes the proof of the theorem.

5.2. **The case $d \geq 3$ (Proof of Theorem 1.4).** Let $\mathcal{A}^* = \mathcal{A}\backslash(0, \dots, 0)$, $\mathcal{B}^* = \mathcal{B}\backslash(0, \dots, 0)$ and $\mathcal{C}^* = \mathcal{C}\backslash(0, \dots, 0)$. For any $\lambda_1, \lambda_2 \in \mathbb{F}_q^*$, it follows from Theorem 1.2 that

$$|\{(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) \in \mathcal{A}^* \times \mathcal{B}^* \times \mathcal{C}^* : B(\boldsymbol{a}, \boldsymbol{b}) = \lambda_1, B(\boldsymbol{a}, \boldsymbol{c}) = \lambda_2\}| = (1 + o(1)) \frac{|\mathcal{A}^*||\mathcal{B}^*||\mathcal{C}^*|}{q^2}.$$

By the pigeon-hole principle, there exists $\boldsymbol{a}_0 \in \mathcal{A}^*$ such that

$$|\{(\boldsymbol{b}, \boldsymbol{c}) \in \mathcal{B}^* \times \mathcal{C}^* : B(\boldsymbol{a}_0, \boldsymbol{b}) = \lambda_1, B(\boldsymbol{a}_0, \boldsymbol{c}) = \lambda_2\}| = (1 + o(1)) \frac{|\mathcal{B}^*||\mathcal{C}^*|}{q^2} \gg q^d.$$

For any $\boldsymbol{a} \in \mathbb{F}_q^d\backslash(0, \dots, 0)$, set $\Pi_\lambda(\boldsymbol{a}) = \{\boldsymbol{v} \in \mathbb{F}_q^d : B(\boldsymbol{a}, \boldsymbol{v}) = \lambda\}$. Let

$$\mathcal{B}_1 = \Pi_{\lambda_1}(\boldsymbol{a}_0) \cap \mathcal{B}^*, \ \ \mathcal{C}_1 = \Pi_{\lambda_2}(\boldsymbol{a}_0) \cap \mathcal{C}^*.$$

Then $|\mathcal{B}_1||\mathcal{C}_1| \gg q^d$. Theorem 1.4 follows immediately from the following lemma.

Lemma 5.1. *For any $\boldsymbol{a} \in \mathbb{F}_q^d\backslash(0, \dots, 0)$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q^*$, suppose that $\mathcal{E} \subseteq \Pi_{\lambda_1}(\boldsymbol{a})$, $\mathcal{F} \subseteq \Pi_{\lambda_2}(\boldsymbol{a})$. If $d \geq 3$ and $|\mathcal{E}||\mathcal{F}| \gg q^d$, then*

$$|\Pi(\mathcal{E}, \mathcal{F}) := \{B(\boldsymbol{e}, \boldsymbol{f}) : \boldsymbol{e} \in \mathcal{E}, \boldsymbol{f} \in \mathcal{F}\}| \geq (1 - o(1))q.$$

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

$$v_\lambda(\mathcal{E}, \mathcal{F}) = \{(\boldsymbol{e}, \boldsymbol{f}) \in \mathcal{E} \times \mathcal{F} : B(\boldsymbol{e}, \boldsymbol{f}) = \lambda\}.$$

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

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

and the Fourier inversion formula takes the form

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

Using exponential sums, Hart, Iosevich, Koh, and Rudnev ([7, Theorem 2.1]) showed that

$$\sum_{\lambda \in \mathbb{F}_q} v_\lambda^2(\mathcal{E}, \mathcal{F}) \leq |\mathcal{E}|^2 |\mathcal{F}|^2 q^{-1} + |\mathcal{E}| q^{2d-1} \sum_{\boldsymbol{f} \in \mathbb{F}_q^d \backslash (0,\ldots 0)} |\mathcal{F} \cap l_{\boldsymbol{f}}| |\hat{\mathcal{F}}(\boldsymbol{f})|^2$$
$$+ (q-1) q^{-1} |\mathcal{E}| |\mathcal{F}| \mathcal{F}((0,\ldots,0)),$$

where

$$l_{\boldsymbol{f}} = \{t\boldsymbol{f} : t \in \mathbb{F}_q^*\}.$$

Since $\mathcal{F} \subseteq \Pi_{\lambda_2}(\boldsymbol{a})$, $(0,\ldots,0) \notin \mathcal{F}$ and $|\mathcal{F} \cap l_{\boldsymbol{f}}| \leq 1$ for any $\boldsymbol{f} \in \mathbb{F}_q^d \backslash (0,\ldots 0)$. Therefore,

$$\begin{aligned} \sum_{\lambda \in \mathbb{F}_q} v_\lambda(\mathcal{E}, \mathcal{F})^2 &\leq |\mathcal{E}|^2 |\mathcal{F}|^2 q^{-1} + |\mathcal{E}| q^{2d-1} \sum_{\boldsymbol{f} \in \mathbb{F}_q^d \backslash (0,\ldots,0)} |\hat{\mathcal{F}}(\boldsymbol{f})|^2 \\ &\leq |\mathcal{E}|^2 |\mathcal{F}|^2 q^{-1} + |\mathcal{E}| q^{2d-1} q^{-d} \sum_{\boldsymbol{f}' \in \mathbb{F}_q^d} \mathcal{F}(\boldsymbol{f}')^2 \\ &= |\mathcal{E}|^2 |\mathcal{F}|^2 q^{-1} + |\mathcal{E}| |\mathcal{F}| q^{d-1}. \end{aligned}$$

By the Cauchy-Schwarz inequality, we have

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

This implies that

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

It 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. □

References

1. J. A. Cipra, T. Cochrane and C. Pinner, *Heilbronn's conjecture on Waring's number (mod p)*, J. Number Theory **125**(2) (2007), 289–297. MR2332590 (2008d:11116)
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*, preprint 2008, arXiv:0804.4894.
3. K. Gyarmati and A. Sárközy, *Equations in finite fields with restricted solution sets, II (algebraic equations)*, Acta Math. Hungar. **119** (2008), 259-280. MR2407038
4. D. Hart, *Explorations of Geometric Combinatorics in Vector Spaces over Finite Fields*, Ph.D. Thesis, Missouri University.
5. D. Hart and A. Iosevich, *Sums and products in finite fields: An integral geometric viewpoint*, Contemp. Math. **464**, Amer. Math. Soc., Providence, RI, 2008, pp. 129–135. MR2440133
6. D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Anal. Math. **34**(1) (2008), 29–38. MR2379694 (2008m:05296)
7. D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture*, to appear in Trans. Amer. Math. Soc., arXiv:0707.3473.
8. D. Hart, A. Iosevich, D. Koh, S. Senger, and I. Uriarte-Tuero, *Distance graphs in vector spaces over finite fields, coloring, pseudo-randomness and arithmetic progressions*, preprint, 2008, arXiv:0804.3036.

9. M. Krivelevich and B. Sudakov, *Pseudo-random graphs*, in More Sets, Graphs and Numbers, Bolyai Soc. Math. Studies 15, Springer, Berlin, 2006, 199-262. MR2223394 (2007a:05130)
10. A. Sárközy, *On products and shifted products of residues modulo p,* Integers **8**(2) (2008), A9. MR2438294
11. I. E. Shparlinski, *On the solvability of bilinear equations in finite fields*, Glasg. Math. J. **50** (2008), 523–529. MR2451747
12. L. A. Vinh, *On a Furstenberg-Katznelson-Weiss type theorem over finite fields*, to appear in Ann. Comb., arXiv:0807.2849
13. L. A. Vinh, *On kaleidoscopic pseudo-randomness of finite Euclidean graphs*, preprint, 2008, arXiv:0807.2689.
14. L. A. Vinh, *On k-simplexes in $(2k-1)$-dimensional vector spaces over finite fields*, to appear in Proc. 21st FPSAC, 2009.
15. L. A. Vinh, *Triangles in vector spaces over finite fields*, to appear in Online J. Anal. Comb. (2009).
16. A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR0029393 (10:592e)

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138
E-mail address: vinh@math.harvard.edu