SOLVING LINEAR EQUATIONS IN A VECTOR SPACE OVER A FINITE FIELD

MASATO MIMURA AND NORIHIDE TOKUSHIGE

Abstract. We study the maximum possible size of a subset in a vector space over a finite field which contains no solution of a given linear equation (or a system of linear equations). This is a finite field version of Ruzsa's work [7].

1. Introduction

Ruzsa studied the maximum possible size of a subset of $[n] := \{1, 2, \ldots, n\}$ which contain no (non-trivial) solution to a given linear equation in [7]. In this paper the same problems are addressed in a vector space over a finite field instead of a set of integers. Let us introduce some basic definitions from [7].

Let p be a prime, and let $\mathbb{F}_p$ denote the p-element field. For a given equation we consider a solution in $\mathbb{F}_p^n$, the n-dimensional vector space over $\mathbb{F}_p$. More precisely, we deal with an equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0,$$

where $a_1, \ldots, a_k \in \mathbb{F}_p$, $x_1, \ldots, x_k \in \mathbb{F}_p^n$, and we always assume that the equation is *balanced*, that is, the coefficients satisfy

$$a_1 + a_2 + \cdots + a_k = 0.$$

The assumption makes sense because if $\sum a_i \neq 0$ then it is easy to construct a large subset of $\mathbb{F}_p^n$ which contains no solution to the equation, e.g., the set of vectors $(1, *, \ldots, *) \in \mathbb{F}_p^n$.

A solution $(x_1, x_2, \ldots, x_k)$ yields a partition of $[k] := \{1, 2, \ldots, k\}$ into disjoint non-empty subsets

$$[k] = T_1 \sqcup T_2 \sqcup \cdots \sqcup T_l$$

such that $x_i = x_j$ if and only if $i, j \in T_\nu$ for some $\nu \in [l]$. We say that the solution is *trivial* if

$$\sum_{i \in T_\nu} a_i = 0 \text{ for all } \nu \in [l]. \tag{1}$$

Note that we always have a trivial solution $(x, x, \ldots, x)$ with the partition $[k]$ itself. Also note that a solution with k distinct elements is necessarily a non-trivial solution. We define the *genus* of an equation by the largest l such that there is a partition of $[k]$ into l parts coming from a trivial solution, that is,

$$\text{genus} = \max\{l : [k] = T_1 \sqcup \cdots \sqcup T_l \text{ with } (1)\}$$

For example, consider the equation $x_1 + x_2 - x_3 - x_4 = 0$ in $\mathbb{F}_5^n$. In this case $a_1 = a_2 = 1$, $a_3 = a_4 = -1$, and a solution $(1, 2, 1, 2)$, which defines a partition $[4] = \{1, 3\} \sqcup \{2, 4\}$, is trivial. On the other hand, a solution $(1, 3, 2, 2)$ is non-trivial, because the corresponding partition is $[4] = \{1\} \sqcup \{2\} \sqcup \{3, 4\}$ but, say, $a_3 + a_4 \neq 0$. Indeed this equation is of genus 2.

For a fixed equation (or a system of equations) in k variables we are interested in a subset $A \subset \mathbb{F}_p^n$ which contains no non-trivial solution. We define

$$\begin{aligned} r_p(n) &:= \max\{|A| : A \text{ contains no non-trivial solution}\}, \\ R_p(n) &:= \max\{|A| : A \text{ contains no solution with } k \text{ distinct elements}\}. \end{aligned}$$

By definition $r_p(n) \leq R_p(n)$. We further define

$$\gamma_p := \lim_{n\to\infty} \frac{\log r_p(n)}{\log p^n}$$

if this limit exists. In other words $r_p(n)$ is roughly $p^{\gamma_p n}$ if n is sufficiently large. By translating Ruzsa's problem posed in [7] into the $\mathbb{F}_p^n$ setting we can ask whether

$$\gamma_p = \frac{1}{\text{genus}} \tag{2}$$

for every balanced equation. It is not difficult to show that $\gamma_p \leq 1/\text{genus}$, see Theorem 6. For the genus two equation $x_1 + x_2 - x_3 - x_4 = 0$ it is known that $\gamma_p = 1/2$ and we will discuss this topic (Sidon set) in detail in the next section. For comparison we briefly explain the original concept introduced by Ruzsa. He defines $\gamma_{\text{Ruzsa}}(N) := \lim_{n\to\infty} \log r(N)/\log N$, where $r(N)$ denotes the maximum possible size of $A \subset [N]$ which contains no non-trivial solution of the given equation. Then all known results suggest the possibility that the identity $\gamma_{\text{Ruzsa}} = 1/\text{genus}$ holds, where the genus in this case is defined in the same way as ours by replacing $\mathbb{F}_p^n$ with $[N]$.

A non-trivial solution to the equation $x_1 - 2x_2 + x_3 = 0$ is an arithmetic progression of length three with a non-zero difference. Thus we have $r_p(n) = R_p(n)$ for this equation, and Ellenberg and Gijswijt gave a good upper bound for $r_p(n)$ as follows.

Theorem 1 (Ellenberg-Gijswijt[2]). *Let p be a prime. For the equation $x_1 - 2x_2 + x_3 = 0$ there exists $\lambda < p$ such that*

$$r_p(n) \leq \lambda^n,$$

where λ is defined by

$$\lambda := \min_{0<t<1} t^{-\frac{p-1}{3}}(1 + t + \cdots + t^{p-1}).$$

In this case by writing $\lambda = p^c$ with $c < 1$ we get $\gamma_p \leq \log(p^c)^n/\log p^n = c$ while the equation $x_1 - 2x_2 + x_3 = 0$ is of genus 1. Thus $\gamma_p < 1/\text{genus}$ in this case. Indeed we prove in [6] that for any balanced equation with at least three variables it follows $R_p(n) \leq \mu^n$ for some constant $\mu < p$ depending only on p and the equation, see also [9] for a much more general result. This means that $\gamma_p < 1/\text{genus}$ for any balanced equation of genus one, and so (2) fails in our finite field setting. On the other hand for the equations of genus more than one, the authors were unable to find any counterexample to (2).

In the next section we explore Ruzsa's method in the finite field model. In many cases we get the corresponding results in a similar way. Subsection 2.1 deals with symmetric equations, and it follows from Theorem 2 and 4 that $r_p(n)/R_p(n) \to 0$ as $n \to \infty$ for some symmetric equations provided p sufficiently large. Subsection 2.2 deals with non-symmetric equations and Subsection 2.3 deals with Sidon sets. As for a Sidon set we get $r_p(2n) \geq p^n$ and $R_p(n) \leq p^{\frac{n}{2}} + \frac{3}{2} + O(p^{-\frac{n}{2}})$ for the equation $x_1 - x_2 + x_3 - x_4 = 0$ (Theorem 9 and 10). In Subsection 2.4 we show that $r_p(n) = (\Omega(p))^{\frac{n}{2}}$ for various balanced equation with four variables (Theorem 11).

In the last section we deal with a system of linear equations. Here we are interested in finding a large subset of $\mathbb{F}_p^n$ without some prescribed geometric shapes such as stars, W-shapes, double-parallelograms, and parallelepipeds. We will give some upper bounds for the maximum size of such a subset, that is, a subset containing no solutions to the corresponding system of equations with distinct variables. For example, the double-parallelograms is defined by a solution to the system of equations

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_3 - x_4 + x_5 - x_6 = 0 \end{cases}$$

with six distinct elements. Then we show that $R_p(n) < 2p^{\frac{n}{2}} + \frac{1}{2}$ (Theorem 14). This bound is almost tight up to constant factor if n is even, because $R_p(n) \geq p^{\frac{n}{2}}$ follows from Theorem 9. For the proofs in the last section we use combinatorial counting and probabilistic sampling argument. The latter approach goes back to Székely's proof [10] of the Szémeredi–Trotter theorem, and we refer to a paper [3] by Fox and Sauermann.

2. One equation

2.1. **Symmetric equations.** We say that an equation with even number of variables is *symmetric* if it is written in the following form:

$$a_1x_1 + a_2x_2 + \cdots + a_lx_l = a_1x_{l+1} + a_2x_{l+2} + \cdots + a_lx_{2l}.$$

The following result corresponds to Theorem 3.2 in [7].

Theorem 2. *Let $a_1, \dots, a_l$ be positive integers, and let p be a prime with $p \gg \max\{a_1, \dots, a_l, l\}$. For the equation*

$$a_1x_1 + \cdots + a_lx_l = a_1x_{l+1} + \cdots + a_lx_{2l}$$

with variables $x_1, \dots, x_{2l} \in \mathbb{F}_p^n$ we have

$$R_p(n) \leq \sqrt{\binom{2l}{2}}\, p^{\frac{n}{2}},$$
$$r_p(n) \leq O(p^{\frac{n}{l}}).$$

The proof of the above result is quite similar to the proof in [7]. For convenience we include the proof for an easier case with a slightly stronger bound as follows.

Theorem 3. *Let p be a prime, and let $a, b \in \mathbb{Z}$ with $a > b > 0$, $p > 2(a+b)$. For the equation $ax + by = au + bv$ with variables $x, y, u, v \in \mathbb{F}_p^n$ we have*

$$R_p(n) < \sqrt{5}\, p^{\frac{n}{2}}, \tag{3}$$

$$r_p(n) \leq p^{\frac{n}{2}}. \tag{4}$$

Proof. Let $A \subset \mathbb{F}_p^n$ attain $R_p(n)$, that is, A contains no solution with four distinct elements. Let $M := |A| = R_p(n)$. For $z \in \mathbb{F}_p^n$ let

$$t(z) := \#\{(x, y) \in A^2 : ax + by = z\}.$$

Then we have

$$\sum_{z \in \mathbb{F}_p^n} t(z) = M^2.$$

Let $N := p^n$. Then, using the power mean inequality[1], we have

$$M^4 = \left(\sum t(z)\right)^2 \leq N \sum t(z)^2, \tag{5}$$

where the sum is taken over $z \in \mathbb{F}_p^n$.

[1] $(\frac{1}{n}\sum t^r)^{\frac{1}{r}} \leq (\frac{1}{n}\sum t^s)^{\frac{1}{s}}$ for $r < s$.

On the other hand, we have

$$t(z)^2 = \#\{(x,y) \in A^2 : ax+by=z\} \times \#\{(u,v) \in A^2 : au+bv=z\},$$

which gives us that

$$\sum t(z)^2 = \#\{(x,y,u,v) \in A^4 : ax+by=au+bv\}.$$

The RHS counts the number of solutions where at least two variables have the same value because A contains no solution with four distinct elements. Let us bound this number from above. For trivial solutions, that is, $x=u$ and $y=v$, the number is at most M^2. For non-trivial solutions they should be one of the following four cases: $x=y$, $x=v$, $y=u$, or $u=v$. For the case $x=y$ we have M choices for x and y, and $M-1$ choices for u (then v is uniquely determined). Thus the number of non-trivial solutions with $x=y$ is at most $M(M-1)$, and the other three cases have the same estimation. Thus, in total, we have

$$\sum t(z)^2 \le M^2 + 4M(M-1) < 5M^2. \tag{6}$$

Consequently, by (5) and (6), we have (3).

The proof for (4) is similar and easier. Let $A \subset \mathbb{F}_p^n$ attain $r_p(n)$. In this case we have that

$$M^4 \le N \sum t(z)^2 = NM^2,$$

which implies $M \le \sqrt{N}$, as needed. □

In Theorem 2 we have a main term $p^{\frac{n}{2}}$ in the upper bound for $R_p(n)$. The next result, which corresponds to Theorem 3.3 in [7], shows that the exponent $\frac{n}{2}$ cannot be improved in general.

Theorem 4. *Let $\epsilon > 0$ be a fixed real number. If a prime p is sufficiently large, then there is a symmetric equation with six variables such that*

$$R_p(n) > p^{(\frac{1}{2}-\epsilon)n}.$$

Proof. By choosing p sufficiently large we may assume that $p^\epsilon > 2$ and

$$2d^2 < p \le 4d^2$$

for some integer $d \ge 2$. We consider the following symmetric equation

$$x + d(y+z) = u + d(v+w)$$

in variables $x, y, z, u, v, w \in \mathbb{F}_p^n$. Let

$$A := \{(x_1, \dots, x_n) \in \mathbb{F}_p^n : 0 \le x_i \le d-1 \text{ for all } i \in [n]\}.$$

Then $|A| = d^n \ge (\sqrt{p}/2)^n > p^{(\frac{1}{2}-\epsilon)n}$. So it suffices to show that A contains no solution to the equation with 6 distinct elements. Suppose that $(x,y,z,u,v,w) \in A^6$ is a solution. Since $x_i, y_i, z_i \le d-1$ we have

$$x_i + d(y_i + z_i) \le (d-1) + d(2d-2) < 2d^2 < p.$$

Thus, for each i, we have

$$x_i + d(y_i+z_i) = u_i + d(v_i + w_i)$$

not only in $\mathbb{F}_p$ but also in $\mathbb{Z}$. By reading the equation in modulo d we have

$$x_i \equiv u_i \pmod{d}.$$

Since $x_i, u_i \in \{0, 1, \dots, d-1\}$ we can conclude $x_i = u_i$ for each i, that is, $x = u$. □

Similarly we can also prove the following.

Theorem 5. *Let a and b be mutually prime integers with $1 \le a < b$ and $b \ge 2$. Then for every prime p with $2b^2 < p \le 4b^2$ and the equation $ax + by = au + bv$, we have*

$$r_p(n) \ge (\sqrt{p}/2)^n .$$

Proof. Let $A := \{(x_1, \dots, x_n) \in \mathbb{F}_p^n : 0 \le x_i \le b-1 \text{ for all } i \in [n]\}$. Then $|A| = b^n \ge (\sqrt{p}/2)^n$. So it suffices to show that A contains no non-trivial solution. Suppose that $(x, y, u, v) \in A^4$ is a solution. Since $x_i, y_i \le b-1$ we have

$$ax_i + by_i \le (b-1)b + b^2 < 2b^2 < p.$$

Thus, for each i, we have

$$ax_i + by_i = au_i + bv_i$$

not only in $\mathbb{F}_p$ but also in $\mathbb{Z}$. By reading the equation in modulo b we have

$$ax_i \equiv au_i \pmod{b}.$$

Since a and b are mutually prime and $x_i, u_i \in \{0, 1, \dots, b-1\}$, we can conclude $x_i = u_i$ for each i, that is, $x = u$. Then we also have $y = v$, and (x, y, u, v) is a trivial solution. □

2.2. **Non-symmetric equations.** The following result follows from Theorem 2. The proof is identical to Theorem 3.6 in [7].

Theorem 6. *For any equation in $\mathbb{F}_p^n$ of genus m we have $r_p(n) = O(p^{\frac{n}{m}})$.*

The following result corresponds to Theorem 7.5 in [7].

Theorem 7. *Let $q \ge 5$ be a prime, and let $d = 3q$ and $n \gg q$. Let k be a non-negative integer, and let p be a prime with*

$$\tfrac{1}{3} d^{k+1} < p < \tfrac{2}{3} d^{k+1}.$$

Then for the equation

$$(d+1)x + y = (d-1)u + 3v \tag{7}$$

in variables $x, y, u, v \in \mathbb{F}_p^n$ we have

$$r_p(n) > \left(c_k \, p^{\frac{k}{k+1}}\right)^n ,$$

where $c_k > 0$ is a constant depending only on k.

Proof. We identify $\mathbb{F}_q$ with $Q := \{0, 1, \dots, q-1\} \subset \mathbb{Z}$. Choose $B \subset Q^n$ so that the equation $x + y + z = 3w$ has no non-trivial solution in B. We may assume that $|B| > (q/3)^n$ for $n \gg q$ by Theorem 5.4 in [5]. Let us define a set of vectors of non-negative integers:

$$A = \{a \in \mathbb{Z}^n : a = \sum_{i=0}^{k-1} d^i b^{(i)},\, b^{(i)} \in B\}.$$

Note that if $a = (a_1, \dots, a_n) \in A$ then each a_j is expanded in base d with coefficients in Q, and $|A| = |B|^k$.

Claim 1. *The equation (7) contains no non-trivial solution in $A \subset \mathbb{Z}^n$.*

Proof. Suppose, to the contrary, that $(x, y, u, v) \in A^4$ is a non-trivial solution to (7). Expand them as $x = \sum d^i x^{(i)}$, $x^{(i)} \in B$ etc. Let j be the minimum i for which $x^{(i)}, y^{(i)}, u^{(i)}, v^{(i)}$ are not all equal. Then we have

$$x^{(0)} = y^{(0)} = u^{(0)} = v^{(0)}, \; \cdots , \; x^{(j-1)} = y^{(j-1)} = u^{(j-1)} = v^{(j-1)}.$$

Since (x, y, u, v) is a solution we have

$$(d+1)d^j x^{(j)} + d^j y^{(j)} \equiv (d-1)d^j u^{(j)} + 3^j v^{(j)} \pmod{d^{j+1}},$$

and so

$$x^{(j)} + y^{(j)} + u^{(j)} \equiv 3v^{(j)} \pmod{d}. \tag{8}$$

But all these vectors are in B and each entry is $\leq q-1 < d/3$, so no carry over happens in both sides of (8). Thus we actually have that

$$x^{(j)} + y^{(j)} + u^{(j)} = 3v^{(j)}.$$

Since B contains no non-trivial solution to $x+y+z = 3v$ we must have $x^{(j)} = y^{(j)} = u^{(j)} = v^{(j)}$, which is a contradiction. □

We note that

$$\max_{a \in A} \max_j a_j \leq \sum_{i=0}^{k-1} d^i (\max Q) < \frac{d^k - 1}{d-1}\left(\frac{d}{3} - 1\right) < \frac{d^k}{3} < \frac{p}{d},$$

and $A \subset \{0, 1, \dots, \lfloor p/d \rfloor\}^n \subset \{0, 1, \dots, p-1\}^n$. Note also that

$$\max_{x,y \in A} \max_j \{(d+1)x_j + y_j\} \leq (d+2)\frac{d^k - 1}{d-1}\left(\frac{d}{3} - 1\right) < \frac{d^{k+1}}{3} < p,$$

and similarly $\max_{u,v \in A} \max_j \{(d-1)u_j + 3v_j\} < p$. Now we view A as a subset of $\mathbb{F}_p^n$. Even in this case the equation (7) has no non-trivial solution in $A \subset \mathbb{F}_p^n$. Using $|B| > (q/3)^n$ and $p < \frac{2}{3}d^{k+1}$ we have

$$|A| = |B|^k > (q/3)^{kn} = (d/9)^{kn} > \left(\tfrac{1}{9^k}\left(\tfrac{3}{2}p\right)^{\frac{k}{k+1}}\right)^n,$$

as needed. □

2.3. **Sidon sets.** We say that a subset $A \subset \mathbb{F}_p^n$ is a *Sidon set* if the equation $x + y = u + v$ has no non-trivial solution in A, and A is a *weak Sidon set* if the equation has no solution with four distinct elements in A. For $A \subset \mathbb{F}_p^n$ and $g \in \mathbb{F}_p^n$ let

$$\delta_A(g) := \{(x, y) \in A^2 : g = x - y\}.$$

We list some properties of a Sidon set, which can be easily verified.

Claim 2. *Let $A \subset \mathbb{F}_p^n$. Then the following three conditions are equivalent.*

- *A is a Sidon set.*
- *If $x, y, u, v \in A$ satisfy $x + y = u + v$ then $\{x, y\} = \{u, v\}$.*
- *If $g \in \mathbb{F}_p^n$ and $g \neq 0$ then $\delta_A(g) \leq 1$.*

Theorem 8. *If $A \subset \mathbb{F}_p^n$ is a Sidon set, then $|A| < p^{\frac{n}{2}} + \frac{1}{2}$, that is,*

$$r_p(n) < p^{\frac{n}{2}} + \tfrac{1}{2}$$

for the equation $x + y = u + v$.

Proof. We count $\sum \delta_A(g)$ in two ways. On one way we have

$$\sum_{g \in \mathbb{F}_p^n} \delta_A(g) = |A|^2.$$

On the other way we have

$$\sum_{g\in\mathbb{F}_p^n}\delta_A(g)=\delta_A(0)+\sum_{g\neq 0}\delta_A(g)\le |A|+(|\mathbb{F}_p^n|-1).$$

By solving $|A|^2\le |A|+p^n-1$ we get

$$|A|\le \tfrac{1}{2}\sqrt{4p^n-3}<p^{\frac{n}{2}}+\tfrac{1}{2}.$$

□

The above upper bound is well-known, in fact, if A is a Sidon set in a commutative group G then $|A|<\sqrt{|G|}+\frac{1}{2}$.

Huang, Tait, and Won studied a Sidon set in $\mathbb{F}_3^n$ in [4], and they proved that $r_3(2n)=3^n$, $3^n+1\le r_3(2n+1)\le \lceil 3^{n+\frac{1}{2}}\rceil$, $r_3(3)=5$, $r_3(5)=13$.

Claim 3 ([1])**.** *Let $A=\{(a,a^2):a\in\mathbb{F}_p\}\subset\mathbb{F}_p^2$. Then A is a Sidon set.*

Proof. Let $g,h\in\mathbb{F}_p$ with $(g,h)\neq(0,0)$ be given. We show that $\delta_A((g,h))\le 1$, that is, the number of pairs $((a,a^2),(b,b^2))\in A^2$ satisfying $(a,a^2)-(b,b^2)=(g,h)$ is at most one.

If $g=0$ then $a-b=g=0$, that is, $a=b$, and $0=a^2-b^2=h$, a contradiction. So we may assume that $g\neq 0$. Substituting $a=b+g$ into $h=a^2-b^2$ we have $h=(b+g)^2-b^2=2bg+g^2$, and $2bg=h-g^2$. Thus $b=(2g)^{-1}(h-g^2)$ is uniquely determined, and so is $a=b+g$. □

The following result is shown in [4] for the case $p=3$, and the same proof works for the general p.

Theorem 9. *For the equation $x+y=u+v$ we have*

$$r_p(2n)\ge p^n.$$

Proof. Let $A=\{(a,a^2):a\in\mathbb{F}_{p^n}\}\subset\mathbb{F}_{p^n}^2$. Then, by Claim 3, A is a Sidon set with $|A|=p^n$. Since $\mathbb{F}_{p^n}^2$ and $\mathbb{F}_p^{2n}$ are isomorphic as vector spaces over $\mathbb{F}_p$ we can view $A\subset\mathbb{F}_p^{2n}$. □

For subsets $A,B\subset\mathbb{F}_p^n$ let $A+B$ denote the *sumset* $\{a+b:a\in A,\ b\in B\}$. The following claim is corresponding to Theorem 4.7 in [7]. Ruzsa's counting argument works for $\mathbb{F}_p^n$ as well provided $p\ge 5$, and we omit the proof.

Claim 4 ([7])**.** *Let $p\ge 5$, and let $A,B\subset\mathbb{F}_p^n$ with $|A|=m$, $|B|=N$. If A is a weak Sidon set then*

$$|A+B|\ge\frac{m^2N}{3m+N-1}.$$

Theorem 10. *Let $p\ge 5$, and let $A\subset\mathbb{F}_p^n$ be a weak Sidon set. Then*

$$|A|\le\tfrac{1}{2}(\sqrt{4p^n+5}+3)=p^{\frac{n}{2}}+\tfrac{3}{2}+O(p^{-\frac{n}{2}}).$$

In other words for the equation $x+y=u+v$ it follows

$$R_p(n)\le p^{\frac{n}{2}}+\tfrac{3}{2}+O(p^{-\frac{n}{2}}).$$

Proof. Let $B=\mathbb{F}_p^n$. We estimate $|A+B|$ in two ways. For a lower bound we apply Claim 4 with $N=p^n$. For a trivial upper bound we use $N\ge |A+B|$. Then the result follows from solving $N\ge\frac{m^2N}{3m+N-1}$. □

2.4. **An equation with four variables.** Let a, b, c, d be positive integers with $a + b = c + d$. In this subsection we consider the equation

$$aX + bY = cU + dV, \tag{9}$$

where X, Y, U, V run over $\mathbb{F}_p^n$. Without loss of generality we may assume that $a \leq b$ and $d \leq c$. Moreover, by symmetry, we may assume that $d \leq a \leq b \leq c$. We have dealt with the symmetric case $(a, b) = (d, c)$ in Theorem 5, so here we focus on the case

$$d < a \leq b < c. \tag{10}$$

Theorem 11. *Let a, b, c, d satisfy (10). Then there exist positive constants γ, p_0 and n_0 such that if p is a prime with $p \geq p_0$ and $n \geq n_0$ then for the equation (9) it follows*

$$r_p(n) \geq (\gamma\sqrt{p})^n.$$

This result corresponds to Theorem 7.3 in [7]. We closely follow Ruzsa's proof. For the case when *abcd* is not a square, he uses a version of Behrend's construction, while we use the following result due to Salem and Spencer [8].

Claim 5. *Let a, b, c, b', c', m be positive integers with $a = b + c = b' + c'$ and $a < m$. Then for all $n > n_0(a, m)$ there exists $A \subset \mathbb{Z}_m^n$ satisfying the following conditions.*

- *$|A| \geq (\alpha m)^n$ for some constant α independent of m and n.*
- *If $x, y, z \in A$ satisfy one of $ax_i = by_i + cz_i$ and $ax_i = b'y_i + c'z_i$ for every $1 \leq i \leq n$ (here we write $x = (x_1, \dots, x_n)$ etc.), then $x = y = z$.*

Proof. Let $d := \lfloor \frac{m}{a} \rfloor$. For simplicity we assume that $(d+1)|n$ and let $k = \frac{n}{d+1}$. Let A be the set of vectors having exactly k entries of value j for each $j = 0, 1, \dots, d$, that is,

$$A = \{(x_1, \dots, x_n) : \#\{i : x_i = j\} = k \text{ for all } 0 \leq j \leq d\}.$$

Then $|A|$ is given by the multinomial coefficient (with k repeated $d + 1$ times), and

$$|A| = \binom{n}{k, k, \dots, k} > \frac{(d+1)^n}{n^{\frac{d+1}{2}}} > \left(\frac{m}{2a}\right)^n$$

if $n \gg d$. This verifies the first item of the conditions.

To verify the second item assume that $x, y, z \in A$ satisfies one of the two equations for each j. Let $I = \{i : x_i = d\}$. Then by the equations we have $y_i = z_i = d$ for all $i \in I$. In other words we have $x = y = z$ on I. Next let $I' = \{i : x_i = d - 1\}$. Then the same reasoning yields that $x = y = z$ on I'. Continuing this we eventually get $x = y = z$. □

Proof of Theorem 11. First we consider the case $n = 1$. Let $S := a + b$, and let $q > S$ be a prime with

$$\sqrt{p/2S^2} < q < \sqrt{p/S^2}. \tag{11}$$

Define

$$B := \{1 + x + Sqx' : 0 \leq x, x' < q,\ x' \equiv x^2 \pmod{q}\}.$$

We focus on a solution of (9) in B, that is, a solution $(X, Y, U, V) \in B^4$, where

$$X = 1 + x + Sqx',\ Y = 1 + y + Sqy',\ U = 1 + u + Squ',\ V = 1 + v + Sqv'. \tag{12}$$

Then $aX + bY = cU + dV < p$ follows from $p > S^2q^2$. It is shown in [7] that if B contains a non-trivial solution to (9) then *abcd* is a quadratic residue modulo q.

If *abcd* is not a square, then we can choose q with (11) so that *abcd* is a quadratic nonresidue modulo q (see [7] for details, note also that his N and p correspond to our p and q, respectively).

In this case B contains no non-trivial solution to (9), and $|B| = q \geq \sqrt{p/2S^2}$ by (11). Thus we have $r_p(1) \geq \sqrt{p/2S^2}$, and for the general n case we get $r_p(n) \geq (r_p(1))^n \geq (\gamma\sqrt{p})^n$.

If $abcd = t^2$ for some positive integer t, then let

$$\epsilon := \frac{1}{2S^2 + 2t}$$

and define $B' \subset B$ by

$$B' := \{1 + x + Sqx' : 0 \leq x < \epsilon q,\ 0 \leq x' < q,\ x' \equiv x^2 \pmod q\}.$$

Then in the same way as in [7] we see that any non-trivial (resp. trivial) solution to (9) in B' gives rise to a non-trivial (resp. trivial) solution to the following system of balanced equations with variables x, y, u, v:

$$cSu = (ac+t)x + (bc-t)y, \quad dSv = (ad-t)x + (bd+t)y,$$

or

$$cSu = (ac-t)x + (bc+t)y, \quad dSv = (ad+t)x + (bd-t)y.$$

Now to consider the general n case let

$$B'^{(n)} = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_i \in B' \text{ for } 1 \leq i \leq n\}.$$

Then $|B'^{(n)}| = (\lfloor \epsilon q \rfloor + 1)^n \geq (\epsilon q)^n$. If $x, y, u, v \in B'^{(n)}$ satisfy (9) then

$$cSu_i = (ac+t)x_i + (bc-t)y_i, \quad dSv_i = (ad-t)x_i + (bd+t)y_i, \tag{13}$$

or

$$cSu_i = (ac-t)x_i + (bc+t)y_i, \quad dSv_i = (ad+t)x_i + (bd-t)y_i \tag{14}$$

holds for each $1 \leq i \leq n$, where write $x = (x_1, \ldots, x_n), \ldots, v = (v_1, \ldots, v_n)$.

By (10) we have $ac > bd$, and so $ac > t > bd$ because $abcd = t^2$. Again by (10) we have $bc \geq ac > t$. Thus, in the first equations in (13) and (14), no coefficient vanishes. Therefore by Claim 5 we can find $C^{(n)} \subset ([0, \epsilon q] \cap \mathbb{Z})^n$ such that

(C1) $|C^{(n)}| \geq (\alpha\epsilon q)^n$ for some constant α independent of ϵq and m, and
(C2) if $x, y, u \in C^{(n)}$ satisfy one of

$$cSu_i = (ac+t)x_i + (bc-t)y_i \text{ and } cSu_i = (ac-t)x_i + (bc+t)y_i$$

for every $1 \leq i \leq n$, then $x = y = u$.

For $x = (x_1, \ldots, x_n) \in C^{(n)}$ let $x' = (x'_1, \ldots, x'_n)$ be such that $x'_i \equiv x_i^2 \pmod q$ with $0 \leq x'_i < q$ for $1 \leq i \leq n$, and define

$$D^{(n)} := \{1 + x + Sqx' : x \in C^{(n)}\} \subset B'^{(n)}.$$

Then it follows from (C1) and (11) that $|D^{(n)}| = |C^{(n)}| \geq (\alpha\epsilon q)^n > \left(\alpha\epsilon\sqrt{\frac{p}{2S^2}}\right)^n$. We claim that $D^{(n)}$ contains no non-trivial solution to (9). Let (X, Y, U, V) be a solution to (9) in $D^{(n)}$. This defines (x, y, u, v) from (12). Then, for each $1 \leq i \leq n$, (x_i, y_i, u_i, v_i) satisfies one of (13) and (14). Thus by (C2) we have $x = y = u$, and by (13) or (14) we have $x = y = u = v$. This, in turn, implies that $X = Y = U = V$, that is, (X, Y, U, V) is a trivial solution. □

3. System of equations

For a given system of linear equations (S) in k variables, we call a solution (S)-*shape* if it consists of k distinct elements. Then let $R_p(n)$ denote the largest size of $A \subset \mathbb{F}_p^n$ which contains no (S)-shape. By k-AP we mean an arithmetic progression of length k with non-zero difference, that is, a sequence of the form $x, x+d, x+2d, \dots, x+(k-1)d$ with $d \neq 0$.

The proofs in this section use probabilistic sampling argument (cf. [3, 10]), and combinatorial counting similar to the one used in the proof for Theorem 3. The first two proofs (for k-star and W) are suggested by Sauermann, and the last two proofs (for $2P$ and Q) were rewritten according to the referees' suggestion which improves the exponent of the upper bounds.

3.1. k-star.

We consider the following system of equations with $2k+1$ variables:

$$(k\text{-star}) \begin{cases} x_1 + x_2 - 2z = 0, \\ x_3 + x_4 - 2z = 0, \\ \quad \cdots \\ x_{2k-1} + x_{2k} - 2z = 0. \end{cases}$$

We call a solution $(x_1, x_2, \dots, x_{2k}, z)$ to the above equations a *(k-star)-shape*, or simply k-star, if $x_1, \dots, x_{2k}, z$ are all distinct. This configuration consists of k 3-APs gluing at the middle term z. Recall the definition of λ from Theorem 1. Since λ depends on p we also write $\lambda = \lambda_p$.

Theorem 12. *For the system of equations* (k*-star*) *we have*

$$R_p(n) < c\sqrt{k}\,\lambda_p^n,$$

where $c = \frac{3}{2}\sqrt{3} < 2.6$.

Proof. Suppose that $A \subset \mathbb{F}_p^n$ contains no k-star. Then each element of A can be a middle term of at most $k-1$ 3-APs. Thus the number of 3-APs in A is at most $(k-1)|A|$.

Let $B \subset A$ be a random subset obtained by choosing each element in A with probability $q = 1/\sqrt{3k}$ uniformly at random. Let $X = |B|$, and let Y be the number of 3-APs in B. Then we have $\mathbb{E}[X] = q|A|$ and $\mathbb{E}[Y] \leq q^3(k-1)|A| = q|A|\frac{k-1}{3k} < \frac{1}{3}q|A|$. Thus $\mathbb{E}[X-Y] > \frac{2}{3}q|A|$.

This means that there exists some actual subset $B' \subset A$ which can be made 3-AP-free by deleting one element from each 3-AP in B', and the resulting subset $B'' \subset B$ after deletion still has size more than $\frac{2}{3}q|A|$. On the other hand since B'' contains no 3-AP we have $|B''| \leq \lambda^n$ by Theorem 1. Thus we have $\frac{2}{3}q|A| < \lambda^n$ and $|A| < \frac{3}{2q}\lambda^n = c\sqrt{k}\,\lambda^n$. □

3.2. W.

We consider the following system of equations:

$$(W) \begin{cases} x_1 - x_2 - x_3 + x_4 = 0, \\ x_2 - x_3 - x_4 + x_5 = 0. \end{cases}$$

Recall that we call a solution $(x_1, x_2, \dots, x_5)$ to (W) a *W-shape* if $x_1, x_2, \dots, x_5$ are all distinct.

Theorem 13. *For the system of equations* (W) *we have*

$$R_p(n) < 2(\lambda_p^{\frac{2}{3}} p^{\frac{1}{3}})^n.$$

Proof. Suppose, to the contrary, that $A \subset \mathbb{F}_p^n$ contains no W-shape but $|A| \geq 2(\lambda^{\frac{2}{3}} p^{\frac{1}{3}})^n$.

A 5-AP is a W-shape, so there is no 5-AP in A.

Suppose that (x, y, z) and (x', y', z') are disjoint two 3-APs with the same difference. Then (x, x', y, y', z) is a W-shape. Thus A contains at most two 3-APs with the same difference, and if there are two of them, then they consist of a 4-AP.

If (x, y, z) is a 3-AP with difference d, then (z, y, x) is a 3-AP with difference $-d$, and these two 3-APs determine the same 3-element set. Thus the number of non-zero differences for feasible 3-APs in $\mathbb{F}_p^n$ is at most $\frac{p^n-1}{2} < \frac{1}{2}p^n$. Consequently,

$$\#(\text{3-APs in } A) < \tfrac{1}{2}p^n \cdot 2 = p^n.$$

Now we choose each element in A with probability $q := (\frac{\lambda}{p})^{\frac{n}{3}}$ uniformly at random. This yields a random subset $B \subset A$. Let $X = |B|$. Then we have

$$\mathbb{E}[X] = q|A| \geq \left(\tfrac{\lambda}{p}\right)^{\frac{n}{3}} \cdot 2(\lambda^{\frac{2}{3}} p^{\frac{1}{3}})^n = 2\lambda^n.$$

Let $Y = \#(\text{3-APs in } B)$. Then we have

$$\mathbb{E}[Y] < p^n \cdot q^3 = \lambda^n.$$

Thus $\mathbb{E}[X - Y] > \lambda^n$, which means that A contains a 3-AP-free subset of size larger than λ^n. This contradicts Theorem 1. □

3.3. $2P$. We consider the following system of equations:

$$(2P) \begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_3 - x_4 + x_5 - x_6 = 0. \end{cases}$$

We call a solution $(x_1, x_2, \ldots, x_6)$ to $(2P)$ a *$2P$-shape* (double-parallelograms) if $x_1, x_2, \ldots, x_6$ are all distinct.

Theorem 14. *Let $p > 5$. For the system of equations $(2P)$ we have*

$$R_p(n) < 2\,p^{\frac{n}{2}} + \tfrac{1}{2}.$$

Proof. Let $t(z) := \#\{(x, y) \in A^2 : x - y = z\}$. On one hand we have

$$\sum_{z \in \mathbb{F}_p^n \setminus \{0\}} t(z) = \#\{(x, y) \in A^2 : x - y \neq 0\} = |A|(|A| - 1).$$

On the other hand we have $t(z) \leq 4$ for $z \neq 0$. Indeed if $t(z) \geq 5$ then we can find 6 distinct elements $x_1, \ldots, x_6 \in A$ such that $z = x_1 - x_2 = x_4 - x_3 = x_5 - x_4$, that is, A contains $2P$-shape. Thus we have

$$\sum_{z \in \mathbb{F}_p^n \setminus \{0\}} t(z) \leq 4(p^n - 1).$$

By solving $|A|(|A| - 1) \leq 4(p^n - 1)$ we get $|A| \leq \frac{1}{2}\left(\sqrt{16p^n - 15} + 1\right) < 2p^{\frac{n}{2}} + \frac{1}{2}$. □

3.4. Q. We consider the following system of equations:

$$(Q) \begin{cases} x_1 + x_3 = x_2 + x_4, \\ y_1 + y_3 = y_2 + y_4, \\ x_1 + y_2 = x_2 + y_1, \\ x_1 + y_4 = x_4 + y_1. \end{cases}$$

We call a solution $(x_1, \ldots, x_4, y_1, \ldots, y_4)$ to (Q) a *Q-shape* (cube or parallelepiped) if the 8 elements are all distinct. We also call a solution $(x_1, \ldots, x_4)$ to the first equality of (Q) a *P-shape* if the four elements are all distinct. For a P-shape (x_1, x_2, x_3, x_4) we define its *type* by $\{x_2 - x_1, x_4 - x_1\} \in (\mathbb{F}_p^n \setminus \{0\})^2$. Four P-shapes of types $\{\pm s, \pm t\}$ are congruent to each other, and let $[s,t]$ denote the corresponding equivalence class. The number of equivalence classes of types in $\mathbb{F}_p^n$ is

$$\binom{\frac{p^n-1}{2}}{2} < \tfrac{1}{8}p^{2n}. \tag{15}$$

Theorem 15. *Let $p>3$. For the system of equations (Q) we have*

$$R_p(n) < \tfrac{3}{2}p^{\frac{3}{4}n}.$$

Proof. Let $A \subset \mathbb{F}_p^n$ with $|A| \geq \frac{3}{2}p^{\frac{3}{4}n}$. We need to show that A contains a Q-shape. To this end we will show that the number of P-shapes in A is at least p^{2n}. Suppose that this is true, and recall from (15) that the number of types of P-shapes is $< \frac{1}{8}p^{2n}$. Then at least 8 of the p^{2n} different P-shapes in A must have the same type. Thus we can find two disjoint P-shapes which produce a Q-shape. (Indeed one can find a Q-shape in any 5 different P-shapes.)

Now we estimate the number of P-shapes in A. We have

$$\sum_{z\in\mathbb{F}_p^n} t(z) = |A|^2 \geq (\tfrac{3}{2})^2 p^{\frac{3}{2}n},$$

where $t(z) := \#\{(x,y)\in A^2 : x-y=z\}$. Then, using the power mean inequality,

$$\#\{(x_1,x_2,x_3,x_4)\in A^4 : x_1-x_2=x_4-x_3\} = \sum_{z\in\mathbb{F}_p^n} t(z)^2 \geq \frac{1}{p^n}\left(\sum_z t(z)\right)^2 \geq (\tfrac{3}{2})^4 p^{2n}.$$

In the above we count not only the number of P-shapes but also the number of (x_1,x_2,x_3,x_4) satisfying $x_1-x_2=x_4-x_3$ and $\#\{x_1,x_2,x_3,x_4\}<4$. The latter is at most $4p^{2n}$ because it counts the number of the following (not exclusive) four cases (i) $x_1=x_2$ and $x_3=x_4$, (ii) $x_1=x_4$ and $x_2=x_3$, (iii) $x_1=x_3$ and $2x_1=x_2+x_4$, and (iv) $x_2=x_4$ and $2x_2=x_1+x_3$. Thus the number of P-shapes in A is at least $((3/2)^4-4)p^{2n}>p^{2n}$, as needed. □

Acknowledgments

The authors thank the referees for their very careful reading and many helpful suggestions including the improvement of the exponents of the bounds in Theorem 14 (from 5/8 to 1/2) and Theorem 15 (from 7/8 to 3/4). Masato Mimura is supported in part by JSPS KAKENHI Grant Number JP17H04822, and Norihide Tokushige is supported by JSPS KAKENHI Grant Number JP18K03399.

References

[1] J. Cilleruelo. Combinatorial problems in finite fields and Sidon sets. Combinatorica, 32(5):497–511, 2012.

[2] J. S. Ellenberg, D. Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Ann. of Math. (2) 185 (2017), no. 1, 339–343.

[3] J. Fox, L. Sauermann. Erdős–Ginzburg–Ziv constants by avoiding three-term arithmetic progressions. Electron. J. Combin. 25 (2018), no. 2, Paper 2.14, 9 pp.

[4] Y. Huang, M. Tait, R. Won. Sidon sets and 2-caps in $\mathbb{F}_3^n$. Involve 12 (6) 995–1003.

[5] M. Mimura, N. Tokushige. Avoiding a shape, and the slice rank method for a system of equations. arXiv:1909.10509

[6] M. Mimura, N. Tokushige. Solving linear equations in a vector space over a finite field II. preprint.

[7] I. Ruzsa. Solving a linear equation in a set of integers I. Acta Arithmetica, LXV.3, 259–282, 1993.

[8] R. Salem, D. C. Spencer. On sets of integers which contain no three terms in arithmetical progression. Proc. Nat. Acad. Sci. USA 28 (1942), 561–563.

[9] L. Sauermann. Finding solutions with distinct variables to systems of linear equations over $\mathbb{F}_p$. arXiv:2105.06863

[10] L. A. Székely. Crossing numbers and hard Erdős problems in discrete geometry. Combin. Probab. Comput. 6 (1997), 353–358.

Masato Mimura, Mathematical Institute, Tohoku University, Japan
Email address: m.masato.mimura.m@tohoku.ac.jp

Norihide Tokushige, College of Education, University of the Ryukyus, Japan
Email address: hide@u-ryukyu.ac.jp