SOLVING LINEAR EQUATIONS IN A VECTOR SPACE OVER A FINITE FIELD II

MASATO MIMURA AND NORIHIDE TOKUSHIGE

ABSTRACT. Suppose that we are given a system of linear equations in k variables. We are interested in the maximum size of a subset in the n-dimensional vector space over the p-element field which contains no solution with k distinct elements. If the maximum size is less than $(cp)^n$ for some constant $0 < c < 1$, then we say that the system is moderate. We first show that any system consisting of just one equation is moderate provided the coefficients sum to zero. We then provide several moderate systems consisting of two or three equations. Our proofs are based on Tao's slice rank method [10] and its extension due to Sauermann [6].

1. INTRODUCTION

Let p be a fixed prime, and let $\mathbb{F}_p^n$ denote the n-dimensional vector space over the p-element field $\mathbb{F}_p$. We consider a subset $A \subset \mathbb{F}_p^n$ and a system of linear equations (S) in k variables where no solution in A has k distinct elements. According to Ruzsa [8] let $R_p(n, S)$ denote the maximum size of A satisfying the condition. We assume that n is sufficiently large compared with the fixed p and S, and we are interested in a system (S) satisfying $R_p(n, S) < (cp)^n$ for some constant $c = c(p, k)$ with $0 < c < 1$. Let us call such a system (S) *moderate*. In this paper we will give some moderate systems arising from the same polynomial.

Ellenberg and Gijswijt [4] proved that any system consisting of one equation in three variables is moderate provided the coefficients sum to zero. We extend this results to more than three variables.

Theorem 1. *Let $k \geq 3$ and let p be a prime. Let (S) be a system consisting of one equation*

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

where the coefficients $a_1, \ldots, a_k \in \mathbb{F}_p$ satisfy

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

If $n > n_0(p, k)$ then $R_p(n, S) < (Cp)^n$ for some constant $C = C(p, k)$ with $0 < C < 1$.

If the coefficients (considered in $\mathbb{Z}$ instead of $\mathbb{F}_p$) satisfy

$$0 < a_1 \leq a_2 \leq \cdots \leq a_{k-1} \leq -a_k < p,$$

then it is known from Behrend's construction that $R_p(n, S) \geq (c'p)^n$ where $c' := -1/a_k > 0$, see, e.g., Theorem 5.4 in [7].

By applying the result of Ellenberg–Gijswijt to equation

$$x_1 - 2x_2 + x_3 = 0,$$

we see that if $A \subset \mathbb{F}_p^n$ contains no 3-AP (an arithmetic progression of length three) then $|A| < (cp)^n$ for some $0 < c < 1$. Do we have a similar upper bound for 4-AP? This is a very interesting

Date: August 31, 2020.

open problem. For this case we consider the system of two equations

$$(\text{4-AP}) \begin{cases} x_1 - 2x_2 + x_3 = 0, \\ x_2 - 2x_3 + x_4 = 0, \end{cases}$$

and we ask if (4-AP) is moderate or not (see [5] for some related results). This 4-AP problem seems difficult, but we can find some other moderate systems, which are our main concern in this paper. In fact by changing the definition of 4-AP slightly we get a moderate system, which we call (T):

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

Let us present some more examples of moderate systems. For this we introduce a polynomial f in 5 variables:

$$f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 - 4x_5. \tag{1}$$

Let (S_0) denote the system consisting of one equation $f = 0$ only. Then, for fixed prime $p \geq 5$, we have $(c'p)^n < R_p(n, S_0) < (cp)^n$ for some $0 < c' < c < 1$. In particular, (S_0) is a moderate system, and this is a starting point. Then we define three systems (S_1) in 9 variables, (S_2) in 8 variables, and (S_3) in 11 variables as follows.

$$(S_1) \begin{cases} f(x_1, x_2, x_3, x_4, x_5) = 0, \\ f(x_1, x_2, x_3, x_4', x_5') = 0, \\ f(x_1, x_2, x_3, x_4'', x_5'') = 0, \end{cases} (S_2) \begin{cases} f(x_1, x_2, x_3, x_4, x_5) = 0, \\ f(x_1, x_2, x_3', x_4', x_5') = 0, \end{cases} (S_3) \begin{cases} f(x_1, x_2, x_3, x_4, x_5) = 0, \\ f(x_1, x_2, x_3', x_4', x_5') = 0, \\ f(x_1, x_2, x_3'', x_4'', x_5'') = 0. \end{cases}$$

We will show that both (S_1) and (S_2) are moderate. The authors were unable to determine whether system (S_3) is moderate or not.

Conjecture 1. *System (S_3) is moderate, that is, $R_p(n, S_3) < (cp)^n$ for some $0 < c < 1$.*

By changing the definition of (S_3) only slightly we get a moderate system (S_3^-):

$$(S_3^-) \begin{cases} f(x_1, x_2, x_3, x_4, x_5) = 0, \\ f(x_1, x_2, x_3', x_4', x_5') = 0, \\ f(x_1, x_2, x_3', x_4'', x_5'') = 0. \end{cases}$$

Note that x_3'' appears in S_3 but not in S_3^-. Note also that the fact that S_3^- is moderate implies that S_1 and S_2 are moderate as well.

To prove the results mentioned above we use Tao's slice rank method [10]. We apply the method, however, not in a straightforward way, but we apply a modified version developed by Sauermann. In [9] she considered the system of one equation in p variables

$$(T_p) \quad x_1 + x_2 + \cdots + x_p = 0,$$

and proved that

$$R_p(n, T_p) < C_p(2\sqrt{p})^n \tag{2}$$

for some constant C_p depending p only. Note that in this case the number of variables coincides with the number of elements of the base field. To prove (2) she showed that if $A \subset \mathbb{F}_p^n$ contains no solution to (T_p) without repeated elements then one can delete only a small part of A to make the remaining part applicable to the multicolored version of the Tao's slice rank bound. We employ the same process repeatedly and systematically.

In section 2 we prepare some tools for the proofs. As a warm-up we prove Theorem 1 in section 3. Next we show in section 4 that system (T) is moderate (Theorem 4). Then in sections 5 and 6 we prove our main results Theorems 5 and 6, respectively. These general results contain the fact that (S_1) and (S_2) are moderate as special cases. In the last section we show that system (S_3^-) is also moderate (Theorem 7).

2. Preliminaries

For a given system of linear equations (S) in k variables, we call a solution an *S-shape* if it consists of k distinct elements. So $R_p(n,S)$ is the largest size of $A \subset \mathbb{F}_p^n$ which contains no S-shape. We also call a solution which may have repeated elements an *S-semishape*. In this paper we always assume that p is a fixed prime, and we are interested in the situation $n \to \infty$.

2.1. **Multicolored version of Tao's slice rank method.** In the rest of the paper, by an equation we always mean a *balanced linear equation*, that is, an equation written in the form

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

where the coefficients satisfy

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

Let (S) be a system of equations in k variables. Let $\mathbf{x}_i = (x_{1,i}, x_{2,i}, \ldots, x_{k,i})$ be a solution to (S) for $1 \le i \le m$. We say that $M = \{\mathbf{x}_1, \ldots, \mathbf{x}_m\}$ is a *matching of S-semishape of size m* if the solutions in M are disjoint, that is,

$$\{x_{1,i_1}, x_{2,i_1}, \ldots, x_{k,i_1}\} \cap \{x_{1,i_2}, x_{2,i_2}, \ldots, x_{k,i_2}\} = \emptyset$$

for all $1 \le i < j \le m$. (We call M a matching of S-shape if each solution has no repeated elements.) Let $X_j = \{x_{j,1}, x_{j,2}, \ldots, x_{j,m}\}$ for $1 \le j \le k$, and let $\mathcal{X} = X_1 \times \cdots \times X_k$. We call $\mathcal{X} = \mathcal{X}(M)$ the *ground set* of M. We say that the matching M is *k-colored S-free* if the following holds:

$$(x_{1,i_1}, x_{2,i_2}, \ldots, x_{k,i_k}) \in \mathcal{X} \text{ is an } S\text{-semishape} \iff i_1 = i_2 = \cdots = i_k.$$

The following result is a consequence of Tao's slice rank method. (For one equation, see, e.g., [2, 6, 9].)

Theorem 2 ([7]). *Let p be a fixed prime. Let (S) be a system of L linear balanced equations in k variables which take values in $\mathbb{F}_p^n$, and let r be the number of variables which appear in only one of the equations. Suppose that there is a k-colored S-free matching of size m. If*

$$\tfrac{1}{2}r + \tfrac{1}{e}(k-r) > L \tag{3}$$

then

$$m < (cp)^n$$

for some constant $c = c(p,k,L)$ with $0 < c < 1$.

Let $M = \{\mathbf{x}_1, \ldots, \mathbf{x}_m\}$ be a matching of S-semishape of size m. For $I \subset [m] := \{1, 2, \ldots, m\}$ let

$$M' = \{\mathbf{x}_i : i \in I\}$$

and we say that *M' is the matching induced from M by I*. By renumbering the indices we may assume that $I = [s]$ if $|I| = s$, and we will always do so.

Let $\mathcal{X} = X_1 \times \cdots \times X_k$ be the ground set of M. We say that $(x_{a,l_a}, x_{b,l_b}) \in X_a \times X_b$ is *(a,b)-extendable* in $\mathcal{X}$ to mean that there exist complementing elements x_{j,l_j} $(j \in [k] \setminus \{a,b\})$ such that $(x_{1,l_1}, x_{2,l_2}, \ldots, x_{k,l_k}) \in \mathcal{X}$ is an S-semishape. This extendability is introduced by Sauermann in [9], which will play an important role in this paper. Let

$$B = \{(x_{a,l_a}, x_{b,l_b}) \in X_a \times X_b : (x_{a,l_a}, x_{b,l_b}) \text{ is } (a,b)\text{-extendable in } \mathcal{X}.\}$$

Then a *graph* $G = (V, E)$ *corresponding to* (M, B) is defined by $V = [m]$, and two vertices u and v in V are adjacent if $(x_{a,l_u}, x_{b,l_v}) \in B$ and $u \neq v$. Note that for all $u \in V$ we have $(x_{a,l_u}, x_{b,l_u}) \in B$ because M is a matching, but $\{u, u\} \notin E$ by definition. Thus we have

$$|E| \leq |B| - |V|. \tag{4}$$

2.2. **Independence number of a graph.** Let $G = (V, E)$ be a graph, and let α denote the independence number of G. Then, it is easy to see that

$$\alpha \geq \frac{|V|}{1 + \Delta},$$

where Δ denotes the maximum degree of the graph. It is also known that this inequality is still valid if we replace Δ with the average degree, see, e.g., [1] Probabilistic Lens: Turán's Theorem.

Theorem 3 (Caro [3], Wei [11])**.**

$$\alpha \geq \frac{|V|}{1 + (2|E|/|V|)}$$

3. A system consisting of one equation

In this section we prove Theorem 1 by induction on k, the number of variables. The base case $k = 3$ is exactly the result of Ellenberg and Gijswijt [4]. (This case also follows from Theorem 2 directly.)

Let $k \geq 3$. We assume that the statement of the theorem holds for all systems of k variables, and we prove the case $k + 1$ variables. Let (S_{k+1}) be a given system consisting of a balanced equation in $k + 1$ variables.

$$(S_{k+1}) \quad a_1x_1 + \cdots + a_{k-1}x_{k-1} + b_kx_k + b_{k+1}x_{k+1} = 0.$$

Define a system (S_k) in k variables by

$$(S_k) \quad a_1x_1 + \cdots + a_{k-1}x_{k-1} + a_kx_k = 0,$$

where $a_k = b_k + b_{k+1}$.

Suppose that $A \subset \mathbb{F}_p^n$ contains no S_{k+1}-shape. Our aim is to show that $|A| < (Cp)^n$ for some $0 < C < 1$. Fix a constant c with $1/3k < c < 1/2k$, and let $t := \lceil c|A| \rceil$. For simplicity we write S for S_k.

(CASE I) A does not contain t disjoint S-shapes.

In this case take disjoint S's as many as possible, say, t' of S, and delete all elements of them. Let A' be the resulting subset of A. Noting that $t' \leq t - 1 < c|A|$ we have

$$|A'| = |A| - t'k > (1 - ck)|A| > |A|/2.$$

On the other hand, A' contains no S-shape, and it follows from the induction hypothesis that $|A'| < (c'p)^n$ for some $0 < c' < 1$, and so $|A| < (c''p)^n$ for some $0 < c'' < 1$ provided $n > n_0(p, k + 1)$.

(CASE II) A contains t disjoint S-shapes.

Let $M_k = \{\mathbf{x}_i = (x_{1,i}, \ldots, x_{k,i}) : 1 \leq i \leq t\}$ be a matching of S-shape of size t, and let $\mathcal{X} = X_1 \times \cdots \times X_k$ be the ground set of M_k, that is, $X_j = \{x_{j,1}, \ldots, x_{j,t}\}$ for $1 \leq j \leq k$. Then for each i, $(\mathbf{x}_i, x_{k,i})$ is a semishape of S_{k+1}. So we can define a matching of S_{k+1}-semishape M of size t by

$$M = \{\mathbf{y}_i = (y_{1,i}, \ldots, y_{k+1,i}) : 1 \leq i \leq t\},$$

where $\mathbf{y}_i = (\mathbf{x}_i, x_{k,i})$. Let $\mathcal{Y} = Y_1 \times \cdots \times Y_{k+1} = \mathcal{X} \times X_k$ be the ground set of M. Note that k sets $Y_1, Y_2, \ldots, Y_k = Y_{k+1}$ are pairwise disjoint.

Claim 1. *If $(y_{1,i_1}, \dots, y_{k,i_k}, y_{k+1,i_{k+1}}) \in \mathcal{Y}$ is an S_{k+1}-semishape, then $i_k = i_{k+1}$.*

Proof. If not, then we get an S_{k+1}-shape, a contradiction. □

For $1 \le j < k$ let $B_{j,k} = \{(y,z) \in Y_j \times Y_k : (y,z) \text{ is } (j,k)\text{-extendable in } \mathcal{Y}\}$.

Claim 2. *Define a map $B_{1,k} \to \mathbb{F}_p^n$ by $(y,z) \mapsto (a_1 y + b_k z)$. Then this map is injective, and $|B_{1,k}| \le p^n$.*

Proof. Suppose the contrary, that is, there exist distinct $(1,k)$-extendable pairs (y_{1,i_1}, y_{k,i_k}) and (y_{1,i'_1}, y_{k,i'_k}) in $Y_1 \times Y_k$ such that

$$a_1 y_{1,i_1} + b_k y_{k,i_k} = a_1 y_{1,i'_1} + b_k y_{k,i'_k} \tag{5}$$

with $i_k \ne i'_k$. By the definition of extendability there are two corresponding S_{k+1}-semishapes

$$\begin{aligned} \mathbf{y} &:= (y_{1,i_1}, y_{2,i_2}, \dots, y_{k,i_k}, y_{k+1,i_{k+1}}),\\ \mathbf{y}' &:= (y_{1,i'_1}, y_{2,i'_2}, \dots, y_{k,i'_k}, y_{k+1,i'_{k+1}}), \end{aligned}$$

and, by the previous claim, $i_k = i_{k+1}$ and $i'_k = i'_{k+1}$. From $\mathbf{y}$ and $\mathbf{y}'$ we get another S_{k+1}-semishape

$$\mathbf{y}'' := (y_{1,i'_1}, y_{2,i_2}, \dots, y_{k,i'_k}, y_{k+1,i_{k+1}}),$$

where i' appears only in the first and the k-th entry. Indeed, by (5), we have

$$\begin{aligned} &a_1 y_{1,i'_1} + a_2 y_{2,i_2} + \cdots + b_k y_{k,i'_k} + b_{k+1} y_{k+1,i_{k+1}}\\ &= a_1 y_{1,i_1} + a_2 y_{2,i_2} + \cdots + b_k y_{k,i_k} + b_{k+1} y_{k+1,i_{k+1}} = 0. \end{aligned}$$

But in $\mathbf{y}''$ we have $i'_k \ne i_{k+1}$ because $i'_k \ne i_k$ and $i_k = i_{k+1}$. This contradicts the previous claim. □

In the same way we have $|B_{j,k}| \le p^n$ for $2 \le j < k$ as well.

Let $G = (V,E)$ be the graph corresponding to $(M, \bigcup_{j=1}^{k-1} B_{j,k})$, that is, $V = [|M|] = [t]$, and two vertices u and v in V are adjacent if $(y_{u,i_u}, y_{v,i_v}) \in B_{j,k}$ for some $1 \le j < k$ and $u \ne v$. By (4) we have

$$|E| \le (k-1)p^n - t.$$

Then it follows from Theorem 3 that there exists an independent set $I \subset V$ such that

$$s := |I| \ge \frac{|V|^2}{|V| + 2|E|} > \frac{t^2}{2kp^n}.$$

Let M' be the matching induced from M by I. By the construction M' is $(k+1)$-colored S-free. Thus by Theorem 2 we have $|M'| < (c'p)^n$ for some $0 < c' < 1$. Consequently we have

$$\frac{(c|A|)^2}{2kp^n} \le \frac{t^2}{2kp^n} < s = |M'| < (c'p)^n,$$

and, noting that $1/c < 3k$, we have

$$|A| < \sqrt{2k/c}\,(\sqrt{c'}\,p)^n < \sqrt{6}\,k(\sqrt{c'}\,p)^n < (Cp)^n$$

for some $C = C(p, k+1)$ with $0 < C < 1$ provided $n > n_0(p, k+1)$. □

4. T

Recall that T-shape is defined by the following equations.

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

In this section we show the following result.

Theorem 4. *Let $p \geq 3$ be a prime. If $n > n_0(p)$ then there exists a constant $C = C(p)$ with $0 < C < 1$ such that $R_p(n, T) < (Cp)^n$.*

For the proof we assume that $A \subset \mathbb{F}_p^n$ contains no T-shape and bound the size of A. If there is no element $x \in A$ such that x is the middle term of a 3-AP in A, and moreover x is the first or third term of another 3-AP in A, then we can bound the size of A easily (see Case III below). But there are two obstacles of T-semishapes for the non-existence of such x. One is the case when $x_2 = x_5$ in T-semishape, which we call P-shape. This configuration consists of 4 elements and defined by the following equations.

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

Actually P-shape is a 4-AP. The other is the case when $x_1 = x_5$ in T-semishape, which we call Q-shape. This is also 4-element configuration defined by the following equations.

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

Proof of Theorem 4. Suppose that $A \subset \mathbb{F}_p^n$ contains no T-shape. Let c be a fixed constant with $0 < c < \frac{1}{8}$ and let

$$t := \lceil c|A| \rceil . \tag{6}$$

(CASE I) A contains t disjoint P-shapes.

Let M_P be a matching of P-shape of size t:

$$M_P = \{(x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}) : 1 \leq i \leq t\}.$$

Let $\mathcal{X}_P = X_1 \times \cdots \times X_4$ be the ground set. Then we can define a matching of T-semishape of size t by

$$M = \{(x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}, x_{2,i}) : (x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}) \in M_P,\ 1 \leq i \leq t\}$$

on the ground set $\mathcal{X} := \mathcal{X}_P \times X_5$, where $X_5 := X_2$. Note that the four sets $X_1, X_2 = X_5, X_3, X_4$ are pairwise disjoint.

Claim 3. *If $(x_{1,i_1}, x_{2,i_2}, \ldots, x_{5,i_5}) \in \mathcal{X}$ is a T-semishape, then $i_2 = i_5$, that is, $x_{2,i_2} = x_{5,i_5}$.*

Proof. If not, then we get a T-shape, a contradiction. □

Let $B := \{(x, y) \in X_1 \times X_2 : (x, y) \text{ is } (1,2)\text{-extendable in } \mathcal{X}\}$.

Claim 4. *Define a map $B \to \mathbb{F}_p^n$ by $(x, y) \mapsto x - 2y$. Then this map is injective, and $|B| \leq p^n$.*

Proof. Suppose the contrary. Then there exist distinct pairs (x, y) and (x', y') in B such that $x - 2y = x' - 2y'$. In this case $y \neq y'$ and there are two corresponding T-semishapes (x, y, x_3, x_4, y) and (x', y', x_3', x_4', y'). Then we have another T-semishape (x', y', x_3, x_4, y). Indeed we have $x' - 2y' + x_3 = x - 2y + x_3 = 0$ and $x_4 - 2x_3 + y = 0$. But this contradicts Claim 3 because $y' \neq y$. □

In the same way we can show that $|B'| \le p^t$, where B' is the set of $(4,5)$-extendable pairs in $\mathcal{X}$.

Let $G = (V, E)$ be the graph corresponding to $(M, B \cup B')$. By (4) we have $|E| \le 2p^n - t$. By Theorem 3 there is an independent set $I \subset V$ with

$$|I| \ge \frac{|V|^2}{2|E| + |V|} > \frac{t^2}{2p^n}. \tag{7}$$

Let M' be the matching induced from M by I.

Claim 5. *M' is 5-colored T-free.*

Proof. Let $\mathcal{X}'$ be the ground set of M'. Suppose that $(x_{1,i_1}, x_{2,i_2}, \dots, x_{5,i_5}) \in \mathcal{X}'$ is an T-semishape. Then by construction it follows that $i_2 = i_5$, $i_1 = i_2$, and $i_4 = i_5$. So let $i := i_1 = i_2 = i_4 = i_5$. Moreover it follows from $x_{1,i} - 2x_{2,i} + x_{3,i_3} = 0$ that $i_3 = i$. □

By Theorem 2 we have $|I| = |M'| < (\mu p)^n$ for some $\mu < 1$. Then by (6) and (7) we get

$$|A| \le \tfrac{t}{c} \le \tfrac{\sqrt{2}}{c}(\sqrt{\mu} p)^n < (Cp)^n$$

for some $C < 1$ provided $n > n_0$.

(CASE II) A contains t disjoint Q-shapes.

One can show that $|A| < (Cp)^n$ for some $C < 1$ in almost the same way as in CASE I. So we just give a sketch of the proof. By extending a matching of Q-shape we get a matching of T-semishape on the ground set $\mathcal{X} = \mathcal{X}_Q \times X_1$. Then we can show the following.

- If $(x_{1,i_1}, x_{2,i_2}, \dots, x_{5,i_5}) \in \mathcal{X}$ is a T-semishape, then $i_1 = i_5$.
- The size of the set of $(1,2)$-extendable pairs in $\mathcal{X}$ is at most p^t.
- The size of the set of $(4,5)$-extendable pairs in $\mathcal{X}$ is at most p^t.

The remaining part is exactly the same as Case I.

(CASE III) A contains less than t disjoint P-shapes and less than t disjoint Q-shapes.

By deleting at most $4(t-1) + 4(t-1) < 8t$ elements from A we can destroy all P-shapes and Q-shapes. Let $A' \subset A$ be the resulting subset with $|A'| > |A| - 8t$. Let

$$A'_1 := \{x \in A' : x \text{ is the middle term of a 3-AP in } A'\},$$
$$A'_2 := \{x \in A' : x \text{ is the first or third term of a 3-AP in } A'\}.$$

Since A' contains no T-shape, no P-shape, no Q-shape, it follows that $A'_1 \cap A'_2 = \emptyset$. Let A'' be one of $A' \setminus A'_1$ and $A' \setminus A'_2$ such that $|A''| \ge \frac{1}{2}|A'|$. Since A'' contains no 3-AP it follows from Theorem 2 that $|A''| < (\lambda p)^n$ for some $\lambda < 1$. Thus we have

$$|A| - 8(c|A| + 1) < |A| - 8t < |A'| \le 2|A''| < 2(\lambda p)^n,$$

and $|A| < \frac{2}{1-8c}(\lambda p)^n + \frac{8}{1-8c} < (Cp)^n$ for some $C < 1$. □

5. Cycles sharing all but two vertices

Let f be the following $\mathbb{F}_p$-coefficient balanced polynomial in $k+2$ variables;

$$f(x_1, x_2, \dots, x_{k+2}) = \sum_{i=1}^{k+2} a_i x_i.$$

Let (S_{k+2}) be equation $f=0$, and let (lS_{k+2}) be the following system of l equations in $k+2l$ variables:

$$(8)\qquad (lS_{k+2})\quad \begin{cases} f(x_1,\dots,x_k,y_1,z_1)=0,\\ f(x_1,\dots,x_k,y_2,z_2)=0,\\ \cdots\\ f(x_1,\dots,x_k,y_l,z_l)=0.\end{cases}$$

Theorem 5. *Let p be a prime, and let $k\ge 1$ and $l\ge 2$. If $n>n_0(p,k,l)$ then there exists a constant $C=C(p,k,l)$ with $0<C<1$ such that $R_p(n,lS_{k+2})<(Cp)^n$.*

Proof. Suppose that $A\subset \mathbb{F}_p^n$ contains no lS_{k+2}-shape. Fix a constant $\frac{1}{3(k+2)}<c<\frac{1}{2(k+2)}$, and let $t:=\lceil c|A|\rceil$. For simplicity we write S for S_{k+2}.

(CASE I) A does not contain t disjoint S-shapes.

In this case take disjoint S's as many as possible, and delete all elements of them. Let A' be the resulting subset of A. Then we have

$$|A'|\ge |A|-(t-1)(k+2)>(1-c(k+2))|A|>|A|/2.$$

On the other hand, A' contains no S-shape, and it follows from Theorem 1 that $|A'|<(c'p)^n$ for some $c'<1$, and so $|A|<(c''p)^n$ for some $c''<1$ provided $n>n_0(p,k,l)$.

(CASE II) A contains t disjoint S-shapes.

Let M be a matching of S-shape of size t:

$$M=\{(x_{1,i},x_{2,i},\dots,x_{k+2,i}):1\le i\le t\}.$$

Let $\mathcal{X}=X_1\times X_2\times\cdots\times X_{k+2}$ be the ground set of M. For simplicity we also write $Y:=X_{k+1}$, $Z:=X_{k+2}$, and $y_i:=x_{k+1,i}$, $z_i:=x_{k+2,i}$ for $1\le i\le t$. Then, $X_1,\dots,X_{k+2}$ are pairwise disjoint sets with the same size t. Let

$$B=\{(y,z)\in Y\times Z:(y,z)\text{ is }(k+1,k+2)\text{-extendable in }\mathcal{X}\}.$$

Claim 6. *Define a map $\phi:B\to\mathbb{F}_p^n$ by $\phi(y,z)=a_{k+1}y+a_{k+2}z$. Then $|\phi^{-1}(\alpha)|\le l-1$ for all $\alpha\in\mathbb{F}_p^n$, and $|B|\le (l-1)p^n$.*

Proof. Suppose the contrary. Then there exist $\alpha\in\mathbb{F}_p^n$ and $i_1,\dots,i_l\in[t]$ such that l pairs

$$(y_{i_1},z_{i'_1}),\dots,(y_{i_l},z_{i'_l})\in B$$

are distinct but take the same value α by ϕ. Since $(y_{i_1},z_{i'_1})$ is an extendable pair there is an S-semishape (actually an S-shape) $(x_{1,i''_1},x_{2,i''_2},\dots,x_{k,i''_k},y_{i_1},z_{i'_1})\in\mathcal{X}$ with

$$a_1x_{1,i''_1}+a_2x_{2,i''_2}+\cdots+a_kx_{k,i''_k}=-\alpha.$$

Thus we have

$$f(x_{1,i''_1},x_{2,i''_2},\dots,x_{k,i''_k},y_{i_u},z_{i'_u})=0$$

for all $1\le u\le l$. This means that A contains an lS_{k+2}-shape, a contradiction. □

Let $G=(V,E)$ be the graph corresponding to (M,B). Then by (4) we have $|E|\le|B|-|V|\le (l-1)p^n-t$. It follows from Theorem 3 that there is an independent set $I\subset V$ with

$$(9)\qquad s:=|I|\ge\frac{|V|^2}{2|E|+|V|}>\frac{t^2}{2(l-1)p^n}.$$

We may assume that $I=[s]$. Let M' be the matching induced from M by I:

$$M'=\{(x_{1,i},\dots,x_{k,i},y_i,z_i)\in M:1\le i\le s\}.$$

Let $\mathcal{X}' = X'_1 \times \cdots \times X'_k \times Y' \times Z'$ be the ground set of M'. By the construction we have the following.

Claim 7. *If $(x_{1,i_1}, \dots, x_{k,i_k}, y_i, z_{i'}) \in \mathcal{X}'$ is an S-semishape, then $i = i'$.*

For $1 \le j \le k$ let

$$B'_{j,k+2} = \{(x, z) \in X'_j \times Z' : (x, z) \text{ is } (j, k+2)\text{-extendable in } \mathcal{X}'\}.$$

Claim 8. *Let $B' = B'_{1,k+2}$. Define a map $B' \to \mathbb{F}_p^n$ by $(x, z) \mapsto a_1 x + a_{k+2} z$. Then the map is injective, and $|B'| \le p^n$.*

Proof. Suppose the contrary. Then there exist (x_{1,i_1}, z_v) and $(x_{1,i'_1}, z_{v'})$ in B' such that

$$a_1 x_{1,i_1} + a_{k+2} z_v = a_1 x_{1,i'_1} + a_{k+2} z_{v'} \tag{10}$$

with $i_1 \ne i'_1$ and $v \ne v'$. By the definition of extendability with the previous claim there are two S-semishapes in $\mathcal{X}'$:

$$(x_{1,i_1}, x_{2,i_2}, \dots, x_{k,i_k}, y_v, z_v),$$
$$(x_{1,i'_1}, x_{2,i'_2}, \dots, x_{k,i'_k}, y_{v'}, z_{v'}).$$

Then, using (10), we obtain another S-semishape

$$(x_{1,i'_1}, x_{2,i_2}, \dots, x_{k,i_k}, y_v, z_{v'}).$$

But this contradicts the previous claim because $v \ne v'$. □

In the same way we have $|B'_{j,k+2}| \le p^n$ for all $1 \le j \le k$. Let $G' = (V', E')$ be the graph corresponding to $(M', \bigcup_{j=1}^k B'_{j,k+2})$. By (4) we have $|E'| \le kp^n - s$. Then it follows from Theorem 3 that there is an independent set $I' \subset V'$ with

$$|I'| \ge \frac{|V'|^2}{2|E'| + |V'|} > \frac{s^2}{2kp^n} > \frac{t^4}{8kl^2p^{3n}},$$

where we used (9) in the last inequality. Let M'' be the matching induced from M' by I'. Then this is a $(k+2)$-colored S-free matching. Recall that in system (8) there are $k + 2l$ variables in total, and $2l$ of them appear only once. So the condition (3) in Theorem 2 holds trivially. Thus by Theorem 2 there is a constant $0 < d < 1$ such that $|M''| = |I'| < (dp)^n$. Thus we have

$$\frac{t^4}{8kl^2p^{3n}} < (dp)^n.$$

Then a simple computation using $t \ge c|A|$ and $1/c < 3(k+2)$ shows

$$|A| < \frac{1}{c}(8kl^2)^{\frac{1}{4}}(d^{\frac{1}{4}}p)^n < (24k(k+2)l^2)^{\frac{1}{4}}(d^{\frac{1}{4}}p)^n.$$

If $n > n_0(p, k, l)$ then the RHS is less than $(Cp)^n$ for some $C = C(p, k, l)$ with $0 < C < 1$. This completes the proof of Theorem 5. □

6. Two connecting circles

Let us define the following $\mathbb{F}_p$-coefficient balanced polynomial f in $k + l$ variables by

$$f(x_1, x_2, \dots, x_{k+l}) = \sum_{i=1}^{k+l} a_i x_i.$$

Let (T_{k+l}) be equation $f=0$, and let $(2T_{k,l})$ be the following system of two equations in $k+2l$ variables:

$$(2T_{k,l}) \quad \begin{cases} f(x_1,\dots,x_k,x_{k+1},\dots,x_{k+l})=0, \\ f(x_1,\dots,x_k,x_{k+l+1},\dots,x_{k+2l})=0. \end{cases} \tag{11}$$

We write a $2T_{k,l}$-semishape as a vector in $(\mathbb{F}_p^n)^{k+2l}$ in the form

$$(x_1,\dots,x_k,x_{k+1},\dots,x_{k+l},x_{k+l+1},\dots,x_{k+2l}).$$

Theorem 6. *Let p be a prime, and let $k\ge 1$, $l\ge 2$. If $n>n_0(p,k,l)$ then there exists a constant $C=C(p,k,l)$ with $0<C<1$ such that $R_p(n,2T_{k,l})<(Cp)^n$.*

We prove the theorem by induction on l. Lemma 1 will be the initial step, and Lemma 2 will be the induction step.

Lemma 1. *Theorem 6 holds for $l=2$.*

Proof. Let $l=2$. Suppose that $A\subset\mathbb{F}_p^n$ contains no $2T_{k,2}$-shape. Fix a constant $\frac{1}{3(k+2)}<c<\frac{1}{2(k+2)}$, and let $t:=\lceil c|A|\rceil$. For simplicity we write $T:=T_{k+2}$.

(CASE I) A does not contain t disjoint T-shapes.
This case is exactly same as (CASE I) in the proof of Theorem 5.

(CASE II) A contains t disjoint T-shapes.
Let M be a matching of T-semishape of size t, and let $\mathcal{X}=X_1\times X_2\times\cdots\times X_{k+2}$ be the ground set of M . Then, $X_1,\dots,X_{k+2}$ are pairwise disjoint sets with the same size t. Let

$$B=\{(x,y)\in X_{k+1}\times X_{k+2} : (x,y) \text{ is } (k+1,k+2)\text{-extendable in } \mathcal{X}\}.$$

Claim 9. *Define a map $B\to\mathbb{F}_p^n$ by $(x,y)\mapsto a_{k+1}x+a_{k+2}y$. Then the map is injective, and $|B|\le p^n$.*

Proof. Suppose the contrary. Then there exist distinct

$$(x_{k+1,i_{k+1}},x_{k+2,i_{k+2}}),(x_{k+1,i'_{k+1}},x_{k+2,i'_{k+2}})\in B$$

such that

$$a_{k+1}x_{k+1,i_{k+1}}+a_{k+2}x_{k+2,i_{k+2}}=a_{k+1}x_{k+1,i'_{k+1}}+a_{k+2}x_{k+2,i'_{k+2}} \tag{12}$$

with

$$i_{k+1}\ne i'_{k+1},\quad i_{k+2}\ne i'_{k+2}. \tag{13}$$

Then we have two $2T_{k,2}$-semishapes

$$(x_{1,i_1},\dots,x_{k,i_k},x_{k+1,i_{k+1}},x_{k+2,i_{k+2}},x_{k+1,i_{k+1}},x_{k+2,i_{k+2}}),$$
$$(x_{1,i'_1},\dots,x_{k,i'_k},x_{k+1,i'_{k+1}},x_{k+2,i'_{k+2}},x_{k+1,i'_{k+1}},x_{k+2,i'_{k+2}}).$$

Now we verify that the following element in $\mathcal{X}$ is a $2T_{k,2}$-shape:

$$(x_{1,i_1},\dots,x_{k,i_k},x_{k+1,i_{k+1}},x_{k+2,i_{k+2}},x_{k+1,i'_{k+1}},x_{k+2,i'_{k+2}}).$$

In fact, by (13), these $k+4$ elements are all distinct. It clearly satisfies the first equation in $(2T_{k,2})$ from (11), that is,

$$f(x_{1,i_1},\dots,x_{k,i_k},x_{k+1,i_{k+1}},x_{k+2,i_{k+2}})=0.$$

Using (12) we can also check the second equation:

$$\begin{aligned}
&f(x_{1,i_1},\dots,x_{k,i_k},x_{k+1,i'_{k+1}},x_{k+2,i'_{k+2}})\\
&=\sum_{j=1}^{k}a_jx_j+a_{k+1}x_{k+1,i'_{k+1}}+a_{k+2}x_{k+2,i'_{k+2}}\\
&=\sum_{j=1}^{k}a_jx_j+a_{k+1}x_{k+1,i_{k+1}}+a_{k+2}x_{k+2,i_{k+2}}\\
&=f(x_{1,i_1},\dots,x_{k,i_k},x_{k+1,i_{k+1}},x_{k+2,i_{k+2}})\\
&=0.
\end{aligned}$$

But this contradicts the assumption that A has no $2T_{k,2}$-shape. $\square$

Let $G=(V,E)$ be the graph corresponding to (M,B). Then $|E|\le|B|-|V|\le p^n-t$. It follows from Theorem 3 that there is an independent set $I\subset V$ with

$$s:=|I|\ge\frac{|V|^2}{2|E|+|V|}>\frac{t^2}{2p^n}. \tag{14}$$

Let M' be the matching induced from M by I, and let $\mathcal{X}'=X'_1\times\cdots\times X'_{k+2}$ be the ground set of M'. By this construction it follows that

Claim 10. *If $(x_{1,i_1},\dots,x_{k+2,i_{k+2}})\in\mathcal{X}'$ is a T-semishape, then $i_{k+1}=i_{k+2}\in I$.*

Let $B'_{1,k+1}=\{(x,y)\in X'_1\times X'_{k+1}:(x,y)\text{ is }(1,k+1)\text{-extendable in }\mathcal{X}'\}$.

Claim 11. *Define a map $B'_{1,k+1}\to\mathbb{F}_p^n$ by $(x,y)\mapsto a_1x+a_{k+1}y$. Then the map is injective, and $|B'_{1,k+1}|\le p^n$.*

Proof. Suppose the contrary. Then there exist distinct $(x_{1,i_1},x_{k+1,i_{k+1}}),(x_{1,i'_1},x_{k+1,i'_{k+1}})\in B'_{1,k+1}$ such that $a_1x_{1,i_1}+a_{k+1}x_{k+1,i_{k+1}}=a_1x_{1,i'_1}+a_{k+1}x_{k+1,i'_{k+1}}$ with $i_{k+1}\ne i'_{k+1}$. Then we have two T-semishapes

$$(x_{1,i_1},\dots,,x_{k+2,i_{k+2}}),\quad(x_{1,i'_1},\dots,,x_{k+2,i'_{k+2}}),$$

from which we get another T-semishape

$$(x_{1,i'_1},x_{2,i_2},x_{3,i_3},\dots,x_{k,i_k},x_{k+1,i'_{k+1}},x_{k+2,i_{k+1}}).$$

Indeed we have

$$\begin{aligned}
&f(x_{1,i'_1},x_{2,i_2},x_{3,i_3},\dots,x_{k,i_k},x_{k+1,i'_{k+1}},x_{k+2,i_{k+1}})\\
&=f(x_{1,i_1},x_{2,i_2},x_{3,i_3},\dots,x_{k,i_k},x_{k+1,i_{k+1}},x_{k+2,i_{k+1}})\\
&=0.
\end{aligned}$$

But This contradicts Claim 10 because $i_{k+1}\ne i'_{k+1}$. $\square$

In the same argument we have $|B'_{j,k+1}|\le p^n$ for all $1\le j\le k$. Let $G'=(V',E')$ be the graph corresponding to $(M',\bigcup_{j=1}^k B_{j,k+1})$. Then we have $|E'|\le kp^n-s$, and we can find an independent set $I'\subset V'$ with

$$|I'|\ge\frac{|V'|^2}{2|E'|+|V'|}>\frac{s^2}{2kp^n}>\frac{t^4}{8kp^{3n}},$$

where we used (14) in the last inequality. Let M'' be the matching induced from M' by I'. Then this is a $(k+2)$-colored T-free matching. Thus by Theorem 2 there is a constant $0 < d < 1$ such that $|M''| = |I'| < (dp)^n$, and

$$\frac{t^4}{8kp^{3n}} < (dp)^n.$$

This together with

$$\frac{|A|}{3(k+2)} < c|A| \leq t$$

we get $|A| < (Cp)^n$ for some $0 < C < 1$ provided $n > n_0(p, k)$. This completes the proof of Lemma 1. □

Lemma 2. *Let $k \geq 2$. If Theorem 6 holds for $2T_{k,l}$, then so does for $2T_{k-1,l+1}$.*

Proof. We assume that

> there exists a constant $D = D(p, k, l)$ with $0 < D < 1$ such that if $A \subset \mathbb{F}_p^n$ contains no $2T_{k,l}$-shape then $|A| < (Dp)^n$ (provided $n > n_0(p, k, l)$).

Under this assumption we will show that

> there exists a constant $C = C(p, k-1, l+1)$ with $0 < C < 1$ such that if $A \subset \mathbb{F}_p^n$ contains no $2T_{k-1,l+1}$-shape then $|A| < (Cp)^n$ (provided $n > n_0(p, k-1, l+1)$).

Suppose that $A \subset \mathbb{F}_p^n$ contains no $2T_{k-1,l+1}$-shape. Fix a constant $\frac{1}{3(k+2l)} < c < \frac{1}{2(k+2l)}$ and let $t = \lceil c|A| \rceil$. For simplicity we write $2T$ for $2T_{k,l}$. Note that $2T$-shape consists of $k + 2l$ elements while $2T_{k-1,l+1}$-shape consists of $k + 2l + 1$ elements.

(CASE I) A does not contain t disjoint $2T$-shapes.

In this case take disjoint $2T$'s as many as possible, and delete all elements of them. Let A' be the resulting subset of A. Then we have

$$|A'| \geq |A| - (t-1)(k+2l) > (1 - (k+2l)c)|A| > |A|/2.$$

On the other hand, A' contains no $2T$-shape, and it follows from the assumption that $|A'| \leq (Dp)^n$, and so $|A| < (c''p)^n$ for some $c'' < 1$ if $n > n_0(p, k, l)$.

(CASE II) A contains t disjoint $2T$-shapes.

Let M_{2T} be a matching of $2T$-shape of size t:

$$M_{2T} = \{(x_{1,i}, \ldots, x_{k+2l,i}) : 1 \leq i \leq t\},$$

where

$$\begin{cases} f(x_{1,i}, \ldots, x_{k,i}, x_{k+1,i}, \ldots, x_{k+l,i}) = 0, \\ f(x_{1,i}, \ldots, x_{k,i}, x_{k+l+1,i}, \ldots, x_{k+2l,i}) = 0 \end{cases}$$

for each i. Let $\mathcal{X} = X_1 \times \cdots \times X_{k+2l}$ be the ground set of M_{2T}. Next we define a matching M of $2T_{k-1,l+1}$-semishapes in M_{2T} of size t:

$$\begin{aligned} M = \{(y_{1,i}, \ldots, y_{k+2l+1,i}) : \; & y_{j,i} = x_{j,i} \text{ for } 1 \leq j \leq k+l, \\ & y_{k+l+1,i} = x_{k,i}, \\ & y_{k+l+j+1,i} = x_{k+l+j,i} \text{ for } 1 \leq j \leq l, \\ & (x_{1,i}, \ldots, x_{k+2l,i}) \in M_{2T}, \; 1 \leq i \leq t\}. \end{aligned}$$

Further we let $Y_j = \{y_{j,1}, y_{j,2}, \dots, y_{j,t}\}$ for $j \in [k+2l+1]$, and let $\mathcal{Y} = Y_1 \times Y_2 \times \cdots \times Y_{k+2l+1}$ be the ground set of M. In other words we have

$$Y_j = \begin{cases} X_j & 1 \le j \le k+l, \\ X_k & j = k+l+1, \\ X_{j-1} & k+l+2 \le j \le k+2l+1, \end{cases}$$

and

$$\mathcal{Y} = (X_1 \times \cdots \times X_{k-1}) \times (X_k \times X_{k+1} \cdots X_{k+l}) \times (X_k \times X_{k+l+1} \cdots X_{k+2l}).$$

Note that $|Y_1| = \cdots = |Y_{k+2l+1}| = t$, $Y_{k+l+1} = Y_k$. Note also that the following $k+2l$ sets are pairwise disjoint:

$$Y_1, Y_2, \dots, Y_{k-1}, Y_k = Y_{k+l+1}, Y_{k+1}, \dots, Y_{k+l}, Y_{k+l+2}, \dots, Y_{k+2l+1}$$

Claim 12. *If $(y_{1,i_1}, y_{2,i_2}, \dots, y_{k+2l+1,i_{k+2l+1}}) \in \mathcal{Y}$ is a $2T_{k-1,l+1}$-semishape, then $i_k = i_{k+l+1}$, and $y_{k,i_k} = y_{k+l+1,i_{k+l+1}}$.*

Proof. If not, we get a $2T_{k-1,l+1}$-shape, a contradiction. □

Let $B_{k,k+1} = \{(y,z) \in Y_k \times Y_{k+1} : (y,z)$ is $(k,k+1)$-extendable in $\mathcal{Y}\}$. This means that if $(x_{k,i_k}, x_{k+1,i_{k+1}}) \in B_{k,k+1}$, then there exist

$$x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k+2,i_{k+2}}, \dots, x_{k+2l,i_{k+2l}}$$

such that

$$(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i_k}, \dots, x_{k+l,i_{k+l}}, x_{k,i_k}, x_{k+l+1,i_{k+l+1}}, \dots, x_{k+2l,i_{k+2l}}) \in \mathcal{Y}$$

is a $2T_{k-1,l+1}$-semishape.

Claim 13. *Define a map $B_{k,k+1} \to \mathbb{F}_p^n$ by $(x,y) \mapsto a_k x + a_{k+1} y$. Then the map is injective, and $|B_{k,k+1}| \le p^n$.*

Proof. Suppose the contrary. Then there exist distinct $(x_{k,i_k}, x_{k+1,i_{k+1}}), (x_{k,i'_k}, x_{k+1,i'_{k+1}}) \in B_{k,k+1}$ such that

$$a_k x_{k,i_k} + a_{k+1} x_{k+1,i_{k+1}} = a_k x_{k,i'_k} + a_{k+1} x_{k+1,i'_{k+1}} \tag{15}$$

with $i_k \ne i'_k$. Then we get the following two $2T_{k-1,l+1}$-semishapes:

$$(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i_k}, \dots, x_{k+l,i_{k+l}}, x_{k,i_k}, x_{k+l+1,i_{k+l+1}}, \dots, x_{k+2l,i_{k+2l}}), \tag{16}$$

$$(x_{1,i'_1}, \dots, x_{k-1,i'_{k-1}}, x_{k,i'_k}, \dots, x_{k+l,i'_{k+l}}, x_{k,i'_k}, x_{k+l+1,i'_{k+l+1}}, \dots, x_{k+2l,i'_{k+2l}}), \tag{17}$$

from which we can construct a $2T_{k-1,l+1}$-shape as follows. We take k-th and $(k+1)$-th entries from (17), the other entries from (16) to get

$$(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i'_k}, x_{k+1,i'_{k+1}}, x_{k+2,i_{k+2}}, \dots, x_{k+l,i_{k+l}}, x_{k,i_k}, x_{k+l+1,i_{k+l+1}}, \dots, x_{k+2l,i_{k+2l}}). \tag{18}$$

Note that these $k+2l+1$ elements are all distinct because $i_k \ne i'_k$. Let us verify that (18) is a $T_{k-1,l+1}$-shape. For the first equation of ($2T_{k-1,l+1}$) from (11), we use (15) and

$$\begin{aligned} &f(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i'_k}, x_{k+1,i'_{k+1}}, \dots, x_{k+l,i_{k+l}}) \\ &= f(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i_k}, x_{k+1,i_{k+1}}, \dots, x_{k+l,i_{k+l}}) \\ &= 0. \end{aligned}$$

For the second equation, we use (16) to get

$$f(x_{1,i_1}, \dots, x_{k-1,i_{k-1}}, x_{k,i_k}, x_{k+l+1,i_{k+l+1}}, \dots, x_{k+2l+1,i_{k+2l+1}}) = 0.$$

But this contradicts the assumption that A has no $2T_{k-1,l+1}$-shape. $\square$

By the same argument we have $|B_{k,j}| \le p^n$ for all $j = k+1, \dots, k+l$. For $j = k+l+2, \dots, k+2l+1$ letting $B_{k+l+1,j} = \{(y,z) \in Y_{k+l+1} \times Y_j : (y,z) \text{ is } (k+l+1,j)\text{-extendable}\}$, we also get $|B_{k+l+1,j}| \le p^n$ similarly.

Let $G = (V, E)$ be the graph corresponding to

$$\left(M, (\textstyle\bigcup_{j=k+1}^{k+l} B_{k,j}) \cup (\bigcup_{j=k+l+2}^{k+2l+1} B_{k+l+1,j})\right).$$

Since $|E| \le 2lp^n - t$ there is an independent set $I \subset V$ such that

$$s := |I| \ge \frac{|V|^2}{2|E| + |V|} > \frac{t^2}{2lp^n}. \tag{19}$$

Let M' be the matching induced from M by I, and let $\mathcal{Y}' = Y'_1 \times \cdots \times Y'_{k+2l+1}$ be the ground set of M'. By the construction we have the following.

Claim 14. *If $(y_{1,i_1}, \dots, y_{k+2l+1,i_{k+2l+1}}) \in \mathcal{Y}'$ is a $2T_{k-1,l+1}$-semishape, then $i_k = i_{k+1} = \cdots = i_{k+2l+1} \in I$.*

Let $B'_{1,k} := \{(y_{1,i_1}, y_{k,i_k}) \in Y'_1 \times Y'_k : (y_{1,i_1}, y_{k,i_k}) \text{ is } (1,k)\text{-extendable in } \mathcal{Y}'\}$.

Claim 15. *Define a map $B'_{1,k} \to \mathbb{F}_p^n$ by $(y_{1,i_1}, y_{k,i_k}) \mapsto a_1 y_{1,i_1} + a_k y_{k,i_k}$. Then the map is injective, and $|B'_{1,k}| \le p^n$.*

Proof. Suppose the contrary. Then there exist distinct $(y_{1,i_1}, y_{k,i_k}), (y_{1,i'_1}, y_{k,i'_k}) \in B'_{1,k}$ such that

$$a_1 y_{1,i_1} + a_k y_{k,i_k} = a_1 y_{1,i'_1} + a_k y_{k,i'_k} \tag{20}$$

with $i_k \ne i'_k$. Then we get two $2T_{k-1,l+1}$-semishapes:

$$(y_{1,i_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}}, y_{k,i_k}, y_{k+1,i_k}, \dots, y_{k+2l+1,i_k}),$$
$$(y_{1,i'_1}, y_{2,i'_2}, \dots, y_{k-1,i'_{k-1}}, y_{k,i'_k}, y_{k+1,i'_k}, \dots, y_{k+2l+1,i'_k}),$$

from which we obtain another $2T_{k-1,l+1}$-semishape:

$$\begin{aligned}&(y_{1,i'_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}},\\ &\ y_{k,i'_k}, y_{k+1,i_k}, \dots, y_{k+l,i_k},\\ &\ y_{k+l+1,i'_k}, y_{k+l+2,i_k}, \dots, y_{k+2l+1,i_k}).\end{aligned}$$

Note that i'_* appears only on the first, k-th, and $(k+l+1)$-th entries. Let us check that this is actually a solution to $(2T_{k-1,l+1})$. For the first equation it follows from (20) that

$$\begin{aligned}&f(y_{1,i'_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}}, y_{k,i'_k}, y_{k+1,i_k}, \dots, y_{k+l,i_k})\\ &= f(y_{1,i_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}}, y_{k,i_k}, y_{k+1,i_k}, \dots, y_{k+l,i_k})\\ &= 0.\end{aligned}$$

For the second equation we note that $y_{k,i'_k} = y_{k+l+1,i'_k}$ by Claim 12, and we get

$$\begin{aligned}&f(y_{1,i'_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}}, y_{k+l+1,i'_k}, y_{k+l+2,i_k}, \dots, y_{k+2l+1,i_k})\\ &= f(y_{1,i'_1}, y_{2,i_2}, \dots, y_{k-1,i_{k-1}}, y_{k,i'_k}, y_{k+1,i_k}, \dots, y_{k+l,i_k})\\ &= 0.\end{aligned}$$

This contradicts Claim 14 because $i_k \ne i'_k$. $\square$

In the same way we have $|B'_{j,k}| \le p^n$ for all $j = 1, 2, \ldots, k-1$. Let $G' = (V', E')$ be the graph corresponding to $(M', \bigcup_{j=1}^{k-1} B'_{j,k})$. Since $|E'| \le (k-1)p^n - s$ there is an independent set $J \subset V'$ such that

$$|J| \ge \frac{|V'|^2}{2|E'| + |V'|} > \frac{s^2}{2(k-1)p^n} > \frac{t^4}{8kl^2p^{3n}}, \tag{21}$$

where we used (19) in the last inequality. Let M'' be the matching induced from M' by J. Then this is a $(k+2l+1)$-colored $2T_{k-1,l+1}$-free matching. Thus by Theorem 2 there exists a constant $0 < d < 1$ such that $|M''| = |J| < (dp)^n$. This together with (21) implies $t < \sqrt[4]{8kl^2}\,(\sqrt[4]{d}\,p)^n$, and

$$|A| \le \frac{t}{c} < 3(k+2l)\sqrt[4]{8kl^2}\,(\sqrt[4]{d}\,p)^n.$$

If $n > n_0(p,k,l)$ then the RHS is less than $(Cp)^n$ for some $C = C(p,k,l)$ with $0 < C < 1$. □

Proof of Theorem 6. Let k, l be given. By Lemma 1 the statement holds for $(2T_{k+l-2,2})$. Then by Lemma 2 the statement holds for $(2T_{k+l-3,3})$. Now we apply Lemma 2 repeatedly as follows:

$$2T_{k+l-2,2} \to 2T_{k+l-3,3} \to 2T_{k+l-4,4} \to \cdots \to 2T_{k+1,l-1} \to 2T_{k,l},$$

and we get the statement for $(2K_{k,l})$ in the end. □

7. Three equations with ten variables

In this section we show that system S_3^- from section 1 is moderate. To make the description for the proof easier we rename the systems and variables. Let f be the following $\mathbb{F}_p$-coefficient polynomial in 5 variables:

$$f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 - 4x_5.$$

Let (T) be the system consisting of $f = 0$. We redefine systems $(3S_5)$ in section 5 and (S_3^-) in section 1 as (T_{333}) and (T_{abb}), respectively:

$$(T_{333}) \begin{cases} f(x_1, x_2, x_3, x_4, x_5) = 0, \\ f(x_1, x_2, x_3, x_6, x_7) = 0, \\ f(x_1, x_2, x_3, x_8, x_9) = 0, \end{cases}$$

$$(T_{abb}) \begin{cases} f(x_1, x_2, x_a, x_4, x_5) = 0, \\ f(x_1, x_2, x_b, x_6, x_7) = 0, \\ f(x_1, x_2, x_b, x_8, x_9) = 0. \end{cases}$$

Recall that T_{333} is the system in 9 variables, and T_{abb} in 10 variables.

Theorem 7. *If $n > n_0(p)$ then there exists a constant $C = C(p)$ with $0 < C < 1$ such that $R_p(n, T_{abb}) < (Cp)^n$.*

Proof. Suppose that $A \subset \mathbb{F}_p^n$ contains no T_{abb}-shape. Fix a constant $0 < c < 1$, and let $t = c|A|$.

(CASE I) A does not contains t disjoint T_{333}-shapes.
We have already settled this case in Theorem 5.

(CASE II) A contains t disjoint T_{333}-shapes. Let

$$M_{T_{333}} = \{(x_{1,i}, \ldots, x_{9,i}) : 1 \le i \le t\}$$

be a matching of T_{333}-shape of size t, that is,

$$\begin{cases} f(x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}, x_{5,i}) = 0, \\ f(x_{1,i}, x_{2,i}, x_{3,i}, x_{6,i}, x_{7,i}) = 0, \\ f(x_{1,i}, x_{2,i}, x_{3,i}, x_{8,i}, x_{9,i}) = 0. \end{cases}$$

Let $\mathcal{X} = X_1 \times \cdots \times X_9$ be the ground set of M, that is, $X_j = \{x_{j,1}, x_{j,2}, \ldots, x_{j,t}\}$ for $1 \le j \le 9$. Next we define a matching M of T_{abb}-semishape of size t as follows.

$$\begin{aligned} M = \{(y_{1,i}, y_{2,i}, y_{a,i}, y_{b,i}, y_{4,i}, y_{5,i}, y_{6,i}, y_{7,i}, y_{8,i}, y_{9,i}) :& \\ y_{j,i} = x_{j,i} \text{ for } j \in \{1, 2, 4, 5, 6, 7, 8, 9\},& \\ y_{a,i} = y_{b,i} = x_{3,i},& \\ (x_{1,i}, \ldots, x_{9,i}) \in M_{T_{333}}, \ 1 \le i \le t\}.& \end{aligned}$$

Then the ground set $\mathcal{Y}$ of M is as follows.

$$\begin{aligned} \mathcal{Y} &= Y_1 \times Y_2 \times Y_a \times Y_b \times Y_4 \times Y_5 \times Y_6 \times Y_7 \times Y_8 \times Y_9, \text{ where} \\ Y_j &= \{y_{j,1}, y_{j,2}, \ldots, y_{j,t}\} \text{ for } j \in \{1, 2, a, b, 4, 5, 6, 7, 8, 9\}. \end{aligned}$$

We can also write $\mathcal{Y} = X_1 \times X_2 \times X_3 \times X_3 \times X_4 \times X_5 \times X_6 \times X_7 \times X_8 \times X_9$. Note that $|Y_j| = t$, $Y_a = Y_b$, and the following 9 sets $Y_1, Y_2, Y_a = Y_b, Y_4, Y_5, Y_6, Y_7, Y_8, Y_9$ are pairwise disjoint.

Claim 16. *If $(y_{1,i_1}, y_{2,i_2}, y_{a,i_a}, y_{b,i_b}, y_{4,i_4}, y_{5,i_5}, y_{6,i_6}, y_{7,i_7}, y_{8,i_8}, y_{9,i_9}) \in \mathcal{Y}$ is a T_{abb}-semishape, then $i_a = i_b$ and $y_{a,i_a} = y_{b,i_b}$.*

Proof. If not, we have a T_{abb}-shape, a contradiction. □

Let $B_{a,4} = \{(x_{3,i_3}, x_{4,i_4}) \in Y_a \times Y_4 : (x_{3,i_3}, x_{4,i_4}) \text{ is } (a,4)\text{-extendable in } \mathcal{Y}\}$. This means that if $(x_{3,i_3}, x_{4,i_4}) \in B_{a,4}$ then there exist $x_{1,i_1}, x_{2,i_2}, x_{5,i_5}, \ldots, x_{9,i_9}$ such that

$$(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5} x_{6,i_6}, x_{7,i_7}, x_{8,i_8}, x_{9,i_9}) \in \mathcal{Y}$$

is a T_{abb}-semishape.

Claim 17. *Define a map $B_{a,4} \to \mathbb{F}_p^n$ by $(x_{3,i_3}, x_{4,i_4}) \mapsto x_{3,i_3} + x_{4,i_4}$. Then this map is injective, and $|B_{a,4}| \le p^n$.*

Proof. Suppose the contrary. Then there exist distinct $(x_{3,i_3}, x_{4,i_4}), (x_{3,i'_3}, x_{4,i'_4}) \in B_{3,4}$ such that

$$x_{3,i_3} + x_{4,i_4} = x_{3,i'_3} + x_{4,i'_4}. \tag{22}$$

Then we have two T_{abb}-semishapes:

$$(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5}, x_{6,i_6}, x_{7,i_7}, x_{8,i_8}, x_{9,i_9}) \in \mathcal{Y}, \tag{23}$$

$$(x_{1,i'_1}, x_{2,i'_2}, x_{3,i'_3}, x_{3,i'_3}, x_{4,i'_4}, x_{5,i'_5}, x_{6,i'_6}, x_{7,i'_7}, x_{8,i'_8}, x_{9,i'_9}) \in \mathcal{Y}. \tag{24}$$

Using them we get another T_{abb}-semishape (actually T_{abb}-shape), that is,

$$(x_{1,i_1}, x_{2,i_2}, x_{3,i'_3}, x_{3,i_3}, x_{4,i'_4}, x_{5,i_5}, x_{6,i_6}, x_{7,i_7}, x_{8,i_8}, x_{9,i_9}) \in \mathcal{Y},$$

where the entries in Y_a and Y_4 come from (24), otherwise from (23). Let us check that this is actually a solution to (T_{abb}). Clearly it satisfies the second and the third equations. For the first equation, it follows from (22) that

$$f(x_{1,i'_1}, x_{2,i_2}, x_{3,i'_3}, x_{4,i_4}, x_{5,i_5}) = f(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5}) = 0.$$

But this contradicts Claim 16 because $i_3 \ne i'_3$. □

In the same way we have $|B_{a,5}| \le p^n$. The next claim is similar but more delicate.

Claim 18. *Define a map* $B_{a,6} \to \mathbb{F}_p^n$ *by* $(x_{3,i_3}, x_{6,i_6}) \mapsto x_{3,i_3} + x_{6,i_6}$. *Then this is injective, and* $|B_{a,6}| \le p^n$.

Proof. Suppose the contrary. Then there exist distinct $(x_{3,i_3}, x_{6,i_6}), (x_{3,i'_3}, x_{6,i'_6}) \in B_{a,6}$ such that

$$x_{3,i_3} + x_{6,i_6} = x_{3,i'_3} + x_{6,i'_6}$$

with $i_3 \ne i'_3$. Then we have two T_{abb}-semishapes:

$$(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5}, x_{6,i_6}, x_{7,i_7}, x_{8,i_8}, x_{9,i_9}) \in \mathcal{Y},$$
$$(x_{1,i'_1}, x_{2,i'_2}, x_{3,i'_3}, x_{3,i'_3}, x_{4,i'_4}, x_{5,i'_5}, x_{6,i'_6}, x_{7,i'_7}, x_{8,i'_8}, x_{9,i'_9}) \in \mathcal{Y}.$$

We also have

$$f(x_{1,i_1}, x_{2,i_2}, x_{3,i'_3}, x_{6,i'_6}, x_{7,i_7}) = f(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{6,i_6}, x_{7,i_7}) = 0.$$

Now we consider the following element in $\mathcal{Y}$:

$$(x_{1,i_1}, x_{2,i_2}, x_{3,i'_3}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5}, x_{6,i'_6}, x_{7,i_7}, x_{8,i_8}, x_{9,i_9}) \in \mathcal{Y}.$$

This is not a solution to (T_{abb}) as it is in the order above, and here is the tricky point. By sorting these 10 values in the following order, we obtain a T_{abb}-shape, that is,

$$\begin{cases} f(x_{1,i_1}, x_{2,i_2}, x_{3,i'_3}, x_{6,i'_6}, x_{7,i_7}) = 0, \\ f(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{4,i_4}, x_{5,i_5}) = 0, \\ f(x_{1,i_1}, x_{2,i_2}, x_{3,i_3}, x_{8,i_8}, x_{9,i_9}) = 0. \end{cases}$$

But this contradicts the assumption that A contains no T_{abb}-shape. □

In the same way we have $|B_{a,j}| \le p^n$ for $j = 7, 8, 9$.

Let $G = (V, E)$ be the graph corresponding to $(M, \bigcup_{j=4}^{9} B_{a,j})$. Then $|E| \le 6p^n - t$ and there exists an independent set $I \subset V$ such that

$$s := |I| \ge \frac{|V|^2}{2|E| + |V|} > \frac{t^2}{12p^n}. \tag{25}$$

Let M' be the matching induced from M by I:

$$M' := \{(y_{1,i}, y_{2,i}, y_{a,i}, y_{b,i}, y_{4,i}, y_{5,i}, y_{6,i}, y_{7,i}, y_{8,i}, y_{9,i}) \in M : i \in I\},$$

and let $\mathcal{Y}' = Y'_1 \times \cdots \times Y'_9$ be the ground set of M'. By the construction we have the following.

Claim 19. *If* $(y_{1,i_1}, \ldots, y_{9,i_9}) \in \mathcal{Y}'$ *is a* T_{abb}*-semishape, then* $i_a = i_b = i_4 = \cdots = i_9 \in I$.

Let $B'_{1,a} := \{(y_{1,i_1}, y_{a,i_a}) \in Y'_1 \times Y'_a : (y_{1,i_1}, y_{a,i_a})$ is $(1, a)$-extendable in $\mathcal{Y}'\}$.

Claim 20. *Define a map* $B'_{1,a} \to \mathbb{F}_p^n$ *by* $(y_{1,i_1}, y_{a,i_a}) \mapsto y_{1,i_1} + y_{a,i_a}$. *Then this is injective, and* $|B'_{1,a}| \le p^n$.

Proof. Suppose the contrary. Then there exist distinct $(y_{1,i_1}, y_{a,i}), (y_{1,i'_1}, y_{a,i'}) \in B'_{1,a}$ such that

$$y_{1,i_1} + y_{a,i} = y_{1,i'_1} + y_{a,i'}, \tag{26}$$

and $i \ne i'$. Then we have two T_{abb}-semishapes

$$(y_{1,i_1}, y_{2,i_2}, y_{a,i}, y_{b,i}, y_{4,i}, y_{5,i}, y_{6,i}, y_{7,i}, y_{8,i}, y_{9,i}) \in \mathcal{Y},$$
$$(y_{1,i'_1}, y_{2,i'_2}, y_{a,i'}, y_{b,i'}, y_{4,i'}, y_{5,i'}, y_{6,i'}, y_{7,i'}, y_{8,i'}, y_{9,i'}) \in \mathcal{Y}.$$

Using them we get another T_{abb}-semishape as follows.

$$(y_{1,i'_1}, y_{2,i_2}, y_{a,i'}, y_{b,i'}, y_{4,i}, y_{5,i}, y_{6,i}, y_{7,i}, y_{8,i}, y_{9,i}) \in \mathcal{Y}.$$

Let us verify that it is indeed a solution to (T_{abb}). The first equality follows from (26). For the second equality, we use Claim 16 and (26) to get

$$y_{1,i'} + y_{b,i'} = y_{1,i'} + y_{a,i'} = y_{1,i} + y_{a,i} = y_{1,i'} + y_{b,i},$$

and

$$f(y_{1,i_1'}, y_{2,i_2}, y_{b,i'}, y_{5,i}, y_{6,i}) = f(y_{1,i_1}, y_{2,i_2}, y_{a,i}, y_{5,i}, y_{6,i}) = 0.$$

The third equality can be verified similarly. But this contradicts Claim 19 because $i \neq i'$. □

Similarly we have $|B'_{2,a}| \le p^n$.

Let $G' = (V', E')$ be the graph corresponding to $(M', B'_{1,a} \cup B'_{2,a})$. Since $|E'| \le 2p^n - s$ we can find an independent set $J \subset V'$ such that

$$|J| \ge \frac{|V'|^2}{2|E'| + |V'|} > \frac{s^2}{4p^n} > \frac{t^4}{4 \cdot 12^2 p^{3n}} = \frac{t^4}{2^4 6^2 p^{3n}}, \tag{27}$$

where we used (25) for the last inequality. Let M'' be the matching induced from M' by J:

$$M'' := \{(y_{1,i}, \dots, y_{9,i}) \in M' : i \in J\}.$$

Then this is a 10-colored strongly T_{abb}-free matching. Thus we have $|M''| = |J| < (dp)^n$ for some $0 < d < 1$ by Theorem 2. Consequently it follows that

$$|A| = \frac{t}{c} < \frac{2\sqrt{6}}{c} (\sqrt[4]{d}\, p)^n.$$

The RHS is less than $(Cp)^n$ for some $C = C(p)$ with $0 < C < 1$ if $n > n_0(p)$. □

Acknowledgements

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] N. Alon, J. H. Spencer. The Probabilistic Method. 4th ed., Wiley, 2016.

[2] J. Blasiak, T. Church, H. Cohn, J. Grochow, E. Naslund, W. Sawin, C. Umans. On cap sets and the group-theoretic approach to matrix multiplication. Discrete Anal. 2017, Paper No. 3, 27pp.

[3] Y. Caro. New Results on the Independence Number. Technical Report, Tel-Aviv University, 1979.

[4] 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.

[5] Y. Lin, J. Wolf. On subsets of $\mathbb{F}_q^n$ containing no k-term progressions. European J. Combin. 31 (2010), no. 5, 1398–1403.

[6] L. M. Lovász, L. Sauermann. A lower bound for the k-multicolored sum-free problem in $\mathbb{Z}_m^n$. Proc. Lond. Math. Soc. 119 (2019) 55–103.

[7] M. Mimura, N. Tokushige. Avoiding a shape, and the slice rank method for a system of equations. to appear in JCTA.

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

[9] L. Sauermann. On the size of subsets of $\mathbb{F}_p^n$ without p distinct elements summing to zero. arXiv:1904.09560v2 (2019).

[10] T. Tao. A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound. `terrytao.wordpress.com/2016/05/18/a` (2016)

[11] V. K. Wei. A Lower Bound on the Stability Number of a Simple Graph. Technical memorandum, TM 81-11217-9, Bell laboratories, 1981