Search Problems in Vector Spaces

Tamás Héger* Balázs Patkós† Marcella Takáts‡

January 30, 2014

Abstract

We consider the following q-analog of the basic combinatorial search problem: let q be a prime power and $\mathrm{GF}(q)$ the finite field of q elements. Let V denote an n-dimensional vector space over $\mathrm{GF}(q)$ and let $\mathbf{v}$ be an unknown 1-dimensional subspace of V. We will be interested in determining the minimum number of queries that is needed to find $\mathbf{v}$ provided all queries are subspaces of V and the answer to a query U is YES if $\mathbf{v} \leqslant U$ and NO if $\mathbf{v} \not\leqslant U$. This number will be denoted by $A(n,q)$ in the adaptive case (when for each queries answers are obtained immediately and later queries might depend on previous answers) and $M(n,q)$ in the non-adaptive case (when all queries must be made in advance).

In the case $n = 3$ we prove $2q - 1 = A(3,q) < M(3,q)$ if q is large enough. While for general values of n and q we establish the bounds

$$n \log q \leq A(n,q) \leq (1 + o(1))nq$$

and

$$(1 - o(1))nq \leq M(n,q) \leq 2nq,$$

provided q tends to infinity.

AMS subject classification: 68P10, 05B25.
Keywords: combinatorial search; q-analog; projective space; separating system.

*MTA–ELTE Geometric and Algebraic Combinatorics Research Group, H–1117 Budapest, Pázmány P. sétány 1/C, Hungary, HETAMAS@CS.ELTE.HU. Research supported by OTKA Grant No. K 81310 and partially supported by ERC Grant No. 227701 DISCRETECONT.

†Hungarian Academy of Sciences, Alfréd Rényi Institute of Mathematics, P.O.B. 127, Budapest H–1364, Hungary, PATKOS@RENYI.HU. Research supported by OTKA Grant PD-83586 and the János Bolyai Research Scholarship of the Hungarian Academy of Sciences

‡Department of Computer Science, Eötvös Loránd University, H–1117 Budapest, Pázmány P. sétány 1/C, Hungary, TAKATS@CS.ELTE.HU. Research supported by OTKA Grant No. K 81310.

1 Introduction

The starting point of combinatorial search theory is the following problem: given a set X of n elements out of which one x is marked, what is the minimum number s of queries of the form of subsets $A_1, A_2, \ldots, A_s$ of X such that after getting to know whether x belongs to A_i for all $1 \leq i \leq s$ we are able to determine x. Since decades, the number s is known to be equal to $\lceil \log n \rceil$ no matter if the ith query might depend on the answers to the previous ones (*adaptive search*) or we have to ask our queries at once (*non-adaptive search*). (Here and throughout the paper log denotes the logarithm of base 2.)

There are lots of variants of this problem. There can be multiple marked elements and our aim can be to determine at least one of them or all of them or a constant fraction of them. The number of marked elements can be known or unknown. There can be restrictions on the possible set Q of queries; only small subsets can be asked or other restrictions may apply. Also, there are models in between the adaptive and the non-adaptive version: we might be allowed to ask our queries in r *rounds*, that is our queries of the $i+1$st round may depend on the answers to all queries in the first i rounds and we would like to minimize the total number of queries. For these and further models we refer the reader to the monograph of Du and Hwang [8].

In this paper we address the q-analogue of the basic problem. Let q be a prime power and $\mathrm{GF}(q)$ the finite field of q elements. Let V denote an n-dimensional vector space over $\mathrm{GF}(q)$ and let $\mathbf{v}$ be a marked 1-dimensional subspace of V (throughout the paper 1-dimensional subspaces will be denoted by boldface lower case letters, vectors will be denoted by lower case letters with normal typesetting and upper case letters will denote subspaces of higher or unknown dimension). We will be interested in determining the minimum number of queries that is needed to find $\mathbf{v}$ provided all queries are subspaces of V and the answer to a query U is YES if $\mathbf{v} \leqslant U$ and NO if $\mathbf{v} \not\leqslant U$. This number will be denoted by $A(n,q)$ in the adaptive case and $M(n,q)$ in the non-adaptive case. Note that a set $\mathcal{U}$ of subspaces of V can be used as query set to determine the marked 1-space in a non-adaptive search if and only if for every pair $\mathbf{u}, \mathbf{v}$ of 1-subspaces of V there exists a subspace $U \in \mathcal{U}$ with $\mathbf{u} \leqslant U, \mathbf{v} \not\leqslant U$ or $\mathbf{u} \not\leqslant U, \mathbf{v} \leqslant U$. Such systems of subspaces are called *separating*.

Note that the q-analogue problem fits into the original subset settings. Indeed, let the set of k-dimensional subspaces of an n-dimensional vector space V over $\mathrm{GF}(q)$ be denoted by $\begin{bmatrix} V \\ k \end{bmatrix}$. Its cardinality $|\begin{bmatrix} V \\ k \end{bmatrix}|$ is

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}.$$

Then if we let the underlying set X be $\begin{bmatrix} V \\ 1 \end{bmatrix}$ and the set Q of allowed queries be

$$\left\{ F \subset \begin{bmatrix} V \\ 1 \end{bmatrix} : \exists U \leq V \text{ with } F = \left\{ \mathbf{u} \in \begin{bmatrix} V \\ 1 \end{bmatrix} : \mathbf{u} \leq U \right\} \right\},$$

then we obtain the same problem.

Let us note that it is easy to show that $A(n,2) = M(n,2) = n$ for all $n \geq 2$. The reader is welcome to think about the one line proof that we will describe in Section 3. Thus we will mainly focus on the case when $q \geq 3$.

The subspaces of an n-dimensional vector space over $\mathrm{GF}(q)$ are the elements of the Desarguesian projective geometry $\mathrm{PG}(n-1,q)$. In Section 2 we consider the case when n equals 3, that is the case of projective planes. After introducing some projective geometry terminology, we determine $A(3,q)$ for all prime powers q.

Theorem 1.1. *Consider a projective plane π_q of order q. Let $A(\pi_q)$ denote minimum number of queries in adaptive search that is needed to determine a point of π_q provided the queries can be either points or lines of π_q. With this notation we have $A(\pi_q) \leq 2q-1$; if q is a prime power, then $A(\mathrm{PG}(2,q)) = 2q-1$, that is the equality $A(3,q) = 2q-1$ holds.*

In Section 2, we also address the problem of determining $M(3,q)$. We obtain upper and lower bounds but not the exact value except if $q \geq 121$ is a square. The most important consequence of our results is the following theorem that states that the situation is completely different from that in the subset case where adaptive and non-adaptive search require the same number of queries.

Theorem 1.2. *For $q \geq 9$ the inequality $A(3,q) < M(3,q)$ holds.*

In Section 3, we address the general problem of giving upper and lower bounds on $A(n,q)$ and $M(n,q)$. Our main results are the following theorems.

Theorem 1.3. *For any prime power $q \geq 2$ and positive integer n the inequalities $\log \begin{bmatrix} n \\ 1 \end{bmatrix}_q \leq A(n,q) \leq (q-1)(n-1)+1$ hold.*

Theorem 1.4. *There exists an absolute constant $C > 0$ such that for any positive integer n and prime power q the inequalities $\frac{1}{C}qn \leq M(n,q) \leq 2qn$ hold. Moreover, if q tends to infinity, then $(1-o(1))qn \leq M(n,q)$ holds.*

We finish the Introduction by recalling the standard method to prove upper and lower bounds for adaptive search. In both cases we assume the existence of an Adversary. When showing a lower bound b for the number of queries needed to determine the marked elements, we have to come up with a strategy that ensures that no matter what sequence of $b-1$ queries the Adversary asks we are able to answer these queries such that there exist at least two elements that match the answers given. In this way we make sure that $b-1$ queries are insufficient. When proving an upper bound our and the Adversary's roles change and this time our task is to provide a strategy using at most b queries (depending on the answers of the Adversary) such that there exists exactly one element that matches the answers no matter what these answers are.

2 Projective planes, the case $n = 3$

In this section we prove Theorem 1.1 and Theorem 1.2. Before describing the proofs let us introduce some terminology. For an overview on projective geometries over finite fields we refer to [13]. Let π be a projective plane of order q with point set $\mathcal{P}$ and line set $\mathcal{L}$. We say that a point set B is a *blocking set* in π if $|B \cap \ell| \geq 1$ for any line $\ell \in \mathcal{L}$. A point P of a blocking set B is said to be *essential* if $B \setminus \{P\}$ is not a blocking set. A set $\mathcal{C}$ of lines *covers* π if $\cup_{\ell \in \mathcal{C}} \ell = \mathcal{P}$. A line ℓ of a cover $\mathcal{C}$ is *essential* if $\mathcal{C} \setminus \{\ell\}$ is not a cover. A line ℓ is said to be a *tangent* to a set $S \subseteq \mathcal{P}$ if $|\ell \cap S| = 1$ holds. Our main tool in proving Theorem 1.1 is the following result.

Theorem 2.1 (Blokhuis, Brouwer [6])**.** *Let S be a blocking set in $\mathrm{PG}(2, q)$. Then there are at least $2q + 1 - |S|$ distinct tangents to S through any essential point of S.*

This result is actually the same as a unique reducibility theorem of Szőnyi [15]; for more details, we refer to [11, 3]. To obtain Corollary 2.2 from Theorem 2.1 observe that its statement is the dual of Theorem 2.1.

Corollary 2.2. *Let L be a set of covering lines in $\mathrm{PG}(2, q)$ and let ℓ be an essential line of L. Then the inequality $|\ell \setminus \cup_{\ell' \neq \ell, \ell' \in L} \ell'| \geq 2q + 1 - |L|$ holds.*

Now we recall and prove Theorem 1.1.

Theorem 1.1. *Consider a projective plane π_q of order q. Let $A(\pi_q)$ denote minimum number of queries in adaptive search that is needed to determine a point of π_q provided the queries can be either points or lines of π_q. With this notation we have $A(\pi_q) \leq 2q - 1$; if q is a prime power, then $A(\mathrm{PG}(2, q)) = 2q - 1$, that is the equality $A(3, q) = 2q - 1$ holds.*

Proof. To obtain the upper bound, let us consider the following simple algorithm. Let x be an arbitrary point of the plane and let $\ell_1, \ell_2, \ldots, \ell_{q+1}$ be the lines containing x. Let us ask $\ell_1, \ldots, \ell_q$ one after the other. Once the Adversary answers YES, then we have to find the unknown point on that particular line, this takes at most q further queries. Moreover, if the YES answer comes to a query ℓ_i with $i > 1$, then we only need at most $q - 1$ queries as we already know that x is not the unknown point. Thus if a YES answer comes to the ith query, $1 \leq i \leq q$, we are done using $1 + q$ or $i + q - 1 \leq 2q - 1$ queries according to whether $i = 1$ or $i > 1$. If all answers are NO, then we obtain that the unknown point is in $\ell_{q+1} \setminus \{x\}$ and thus we need at most $q + q - 1 = 2q - 1$ queries.

To obtain the lower bound let us assume first that the Adversary only asks lines as queries. Note that our only choice is about when to say YES for the first time. Indeed, if the queries are $\ell_1, \ell_2, \ldots, \ell_k$ and ℓ_k is the first query which we answer with YES, then the best we can do from then on is to say NO as many times as possible. As the only possibilities for the unknown point are the points in $\ell_k \setminus \cup_{i=1}^{k-1} \ell_i$, therefore the maximum number of queries we can reach is $k + |\ell_k \setminus \cup_{i=1}^{k-1} \ell_i| - 1$.

Our strategy is simple: let the kth query ℓ_k be the first one we answer with YES if there exists a line ℓ such that $\ell_1, \ell_2, \ldots, \ell_k, \ell$ form a covering set of lines. Observe that if an Adversary is able to identify the unknown point, then he must have received a YES answer from us. Indeed, if not, then by our strategy, there would be more than two points that are not contained in any of the lines and thus undistinguishable. Let the kth be the first query to which we answered YES. Then there exists a line ℓ such that $\ell_1, \ell_2, \ldots, \ell_k, \ell$ cover the projective plane. We claim that ℓ_k is essential. Indeed, if not then we should have answered YES earlier. Therefore, Corollary 2.2 applies with ℓ_k being an essential line of the covering set $\{\ell_1, \ell_2, \ldots, \ell_k, \ell\}$. Thus, by our observation in the previous paragraph, the minimum number of queries needed is

$$k + |\ell_k \setminus \cup_{i=1}^{k-1} \ell_i| - 1 \geq k + |\ell_k \setminus (\cup_{i=1}^{k-1} \ell_i \cup \ell)| - 1 \geq k + 2q + 1 - (k+1) - 1 = 2q - 1.$$

Let us now consider the general case where the Adversary is allowed to ask queries that are points. We will always try to replace a point query by a line. If the kth query is a point P_k and there is a line ℓ_k containing P_k such that all previously queried lines and the lines that replaced queried points cannot be extended by a single line to a cover, then we answer NO and provide the additional information to the Adversary that the unknown point does not lie in ℓ_k. Following this strategy when the Adversary asks a line and with one additional line we can obtain a cover, the reasoning of the previous paragraph goes through.

It remains to check the case when a point P_k is asked and for all lines $P_k \in \ell \notin L = \{\ell_1, \ell_2, \ldots, \ell_{k-1}\}$ there exists another line ℓ' such that $L \cup \{\ell, \ell'\}$ is a cover. In this case we may assume that $P_k \notin \ell'$ for the following reasons. Suppose not and P_k is the unique intersection point of ℓ and ℓ'. Then as neither $L \cup \{\ell\}$ nor $L \cup \{\ell'\}$ is a cover, there must exist points $Q_1 \in \ell \setminus (\cup_{\ell'' \in L} \ell'' \cup \{P_k\}), Q_2 \in \ell' \setminus (\cup_{\ell'' \in L} \ell'' \cup \{P_k\})$. Now for any line $\ell''' \neq \ell, \ell'$ that contains P_k the line ℓ^* that extends $L \cup \{\ell'''\}$ to a cover must contain Q_1 and Q_2 and thus $\ell^* = \langle Q_1, Q_2 \rangle$ and clearly $P_k \notin \langle Q_1, Q_2 \rangle$.

It also follows that ℓ^* is essential in the cover $L \cup \{\ell''', \ell^*\}$, thus if we answer NO to the query P_k and provide the additional information that the unknown point lies in ℓ^*, then the calculation for the restricted case gives us the desired lower bound. □ □

Let us now turn to the non-adaptive case. The following lemma states that it is enough to consider separating systems consisting of only lines.

Lemma 2.6. *For any separating system S of a projective plane π, there exists another one S' that contains only lines and $|S| = |S'|$ holds.*

Proof. It is enough to prove the statement for minimal separating systems. Let S be such a system such that it contains the minimum number of points. If this number is 0, then we are done. Suppose S contains a point P. By minimality of S, we know that $S \setminus \{P\}$ is not separating. Clearly, P only separates pairs of points one of which is P itself. There exists

exactly one point $Q \neq P$ such that $S \setminus \{P\}$ does not separate the pair (P, Q). Indeed, by the above there is at least one such point, furthermore if there was one more point Q', then Q and Q' would not even be separated by S. Let ℓ be any line containing P and not containing Q. Then $S' = S \setminus \{P\} \cup \ell$ is a separating system such that S' contains one point less than S. This contradicts the choice of S. □ □

Let us take a short graph theoretic detour. In a graph G a subset $H_1 \subset V(G)$ of vertices *resolves* another subset H_2 if the list of path-distances in G from the vertices in H_1 are unique in H_2, i.e. for any $h_2, h_2' \in H_2$ there exists an $h_1 \in H_1$ such that $d_G(h_1, h_2) \neq d_G(h_1, h_2')$ holds. A set R of vertices is a *resolving set* in G if it resolves $V(G)$.

For more information about resolving sets and related topics see [2].

If G is bipartite with classes A and B, then a subset A' of A (B' of B) is *semi-resolving* if it resolves B (A). Let G_π be the incidence graph of a projective plane π. Then by Lemma 2.6 the minimum size of a separating system in π equals the minimum size of a semi-resolving set in G_π. Héger and Takáts [12] showed that the minimum size of a resolving set in any projective plane of order $q \geq 23$ is $4q - 4$ and obtained the following lower bound on the size of any semi-resolving set in the incidence graph of $\mathrm{PG}(2, q)$. Note that $\tau_2(\pi)$ denotes the minimum size of a point set in π that meets every line of π in at least 2 points, that is $\tau_2(\pi)$ denotes the minimum size of a *double (2-fold) blocking set* in π.

Theorem 2.7 (Héger, Takáts [12])**.** *Let S be a semi-resolving set in $\mathrm{PG}(2, q)$, $q \geq 3$. Then $|S| \geq \min\{2q + q/4 - 3, \tau_2(\mathrm{PG}(2, q)) - 2\}$.*

Theorem 2.7 together with the following theorem implies Theorem 1.2.

Theorem 2.8 (Ball, Blokhuis [5])**.** *Let $q \geq 9$. Then $\tau_2(\mathrm{PG}(2, q)) \geq 2(q + \sqrt{q} + 1)$, and equality holds if and only if q is a square.*

On the other hand, Bailey [1] gave a semi-resolving set of size $\tau_2(\mathrm{PG}(2, q)) - 1$, and Héger and Takáts [12] constructed one of size $2(q + \sqrt{q})$ in $\mathrm{PG}(2, q)$, q a square prime power.

Corollary 2.9. *Let $q \geq 121$ be a square. Then $M(3, q) = 2q + 2\sqrt{q}$ holds.*

Recall that $A(3, q) = 2q - 1$ by Theorem 1.1. Thus Corollary 2.9 and Theorem 1.1 together prove Theorem 1.2, which we recall below.

Theorem 1.2. *For $q \geq 9$ the inequality $A(3, q) < M(3, q)$ holds.*

The exact value of $\tau_2(\mathrm{PG}(2, q))$ is not known in general. If $q > 3$ is a prime, then Ball proved $\tau_2(\mathrm{PG}(2, q)) \geq 2.5(q + 1)$ [4]. As for large square values of q we have $M(3, q)/q = 2 + 2/\sqrt{q}$, while for prime values of q we have $M(3, q)/q > 2.5$, we obtain the following.

Theorem 2.8. *The sequence $M(3, q)/q$ does not have a limit.*

In case of $q = p^{2d+1}$, p prime, $d \geq 1$, Blokhuis, Storme and Szőnyi [7] obtained the lower bound $\tau_2(\mathrm{PG}(2,q)) \geq 2(q+1) + c_p q^{2/3}$, where $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ otherwise. As for an upper bound if q is not a square, Bacsó, Héger and Szőnyi [3] showed $\tau_2(\mathrm{PG}(2,q)) \leq 2q + 2(q-1)/(r-1)$, where $q = r^d$, r an odd prime power, d odd. Thus for such parameters, Theorem 2.7 implies that if $r \geq 11$, then $M(3,q)$ is either $\tau_2(\mathrm{PG}(2,q)) - 1$ or $\tau_2(\mathrm{PG}(2,q)) - 2$.

3 General bounds

In this section we recall and prove Theorem 1.3 and Theorem 1.4.

Theorem 1.3. *For any prime power $q \geq 2$ and positive integer n the inequalities $\log \begin{bmatrix} n \\ 1 \end{bmatrix}_q \leq A(n,q) \leq (q-1)(n-1)+1$ hold.*

Proof. Let us begin with the lower bound as it follows from the trivial lower bound that any separating system of subsets of X should contain at least $\lceil \log |X| \rceil$ sets. Therefore any separating system of subspaces of V should contain at least $\lceil \log |\begin{bmatrix} V \\ 1 \end{bmatrix}| \rceil \geq (n-1)\log q$ subspaces. Note that if $q = 2$, then the formula gives $\lceil \log 2^n - 1 \rceil = n$ as lower bound.

We will describe two algorithms to show the upper bound $A(n,q) \leq (q-1)(n-1)+1$. The first algorithm is a very simple inductive one and generalizes the algorithm that we had in the projective plane case. First of all, note that if $n = 2$, then the bound to prove is q and just by asking q out of the $q+1$ possible 1-subspaces we can determine the unknown 1-subspace $\mathbf{u}$. Let us assume that for all $k < n$ we obtained an algorithm in the k dimensional space that uses only $(k-1)$-subspaces as queries.

Consider any $(n-2)$-subspace U of V. There are exactly $q+1$ $(n-1)$-subspaces $U_1, \ldots, U_{q+1}$ of V that contain U. Let us ask q of them. After getting the answers to these queries, we will know whether $\mathbf{u} \leqslant U$ or $\mathbf{u} \subset U_i \setminus U$ holds for some $1 \leq i \leq q+1$ and in the latter case we even know the value of i. If $\mathbf{u} \leqslant U$, then by induction we can finish our algorithm in $(n-3)(q-1)+1$ queries that gives a total of $(n-2)(q-1)+2$ queries. If $\mathbf{u} \subset U_i \setminus U$, then by our assumption that an algorithm for the $(n-1)$ dimensional case uses only $(n-2)$-spaces, we can assume that the first query is U and thus we need only $(n-2)(q-1)$ more queries giving a total of $(n-1)(q-1)+1$ queries. Note that we can also satisfy the assumption that we only use $(n-1)$-subspaces, since, instead of querying an $(n-2)$-subspace A of U_i, we can ask an $(n-1)$-subspace $A' \leqslant V$ such that $A' \cap U_i = A$.

Note that even this easy algorithm does not utilize the whole power of adaptiveness as when decreasing the dimension by one, we can ask the q queries at once. Thus the above algorithm uses at most $n-1$ rounds. In what follows, we introduce a two-round algorithm that uses the same number of queries to determine the unknown 1-subspace $\mathbf{u}$.

Before describing the two-round algorithm note that to determine a 1-subspace $\mathbf{u}$ it is enough to identify one non-zero vector $u \in \mathbf{u}$ as then $\mathbf{u} = \{\lambda u : \lambda \in \mathrm{GF}(q)\}$. In the next reasoning we will think of a vector $v \in V$ as an n-tuple of elements of $\mathrm{GF}(q)$. For

$i = 1, 2, \ldots, n$ let us define the following $(n-1)$-subspaces of V: $A_i = \{v = (v_1, v_2, \ldots, v_n) \in V : v_i = 0\}$. Let $e_1, e_2, \ldots, e_n$ denote the standard basis of V and for $1 \leq i < j \leq n$ let us write $E_{i,j} = \langle e_i, e_j \rangle$. All $E_{i,j}$'s have dimension 2, therefore each of them contains $q+1$ 1-subspaces. Two of those are $\{v = (v_1, v_2, \ldots, v_n) \in E_{i,j} : v_i = 0\}$ and $\{v = (v_1, v_2, \ldots, v_n) \in E_{i,j} : v_j = 0\}$. For every pair i, j let $\mathbf{l}_{i,j,1}, \mathbf{l}_{i,j,2}, \ldots, \mathbf{l}_{i,j,q-1}$ be an arbitrary enumeration of the $q-1$ other 1-subspaces of $E_{i,j}$. Finally, for any $1 \leq i < j \leq n$ and $1 \leq k \leq q-1$ let us write $L_{i,j,k} = \{v = (v_1, v_2, \ldots, v_n) \in V : (0, \ldots, 0, v_i, 0, \ldots, 0, v_j, 0, \ldots, 0) \in \mathbf{l}_{i,j,k}\}$. Clearly, all $L_{i,j,k}$'s are $(n-1)$-subspaces of V.

In the first round, our algorithm asks all subspaces A_i, $i = 1, 2, \ldots, n$ as queries. Let Z and NZ denote the set of coordinates for which the answer was YES and NO, respectively. (Note that if $q = 2$, then we are done as with the answers to the queries of the first round we will be able to tell the one and only non-zero vector u of $\mathbf{u}$. This gives an algorithm of n queries that matches the trivial lower bound mentioned earlier.) Let T be any tree with vertex set NZ. Then in a second round of queries our algorithm asks the subspaces $L_{i,j,k}$ with $(i, j) \in E(T)$ and $1 \leq k \leq q-2$. We claim that after obtaining the answers to these queries, we are able to identify a vector $0 \neq u = (u_1, u_2, \ldots, u_n) \in \mathbf{u}$. Clearly, we have $u_i = 0$ if and only $i \in Z$. As for any $i \in NZ$, we have $u_i \neq 0$, we obtain that for any pair $i, j \in NZ$ we have $(0, \ldots, 0, u_i, 0, \ldots, 0, u_j, \ldots, 0) \in \mathbf{l}_{i,j,k}$ for some $1 \leq k \leq q-1$. Thus by our queries of the second round, we will be able to tell to which such 1-subspace of $E_{i,j}$ the vector $(0, , , 0, u_i, 0, \ldots, 0, u_j, \ldots, 0)$ belongs.

Let us pick an arbitrary coordinate $x \in NZ$. We may assume that $u_x = 1$ as if not, then we can consider $u_x^{-1}u$ instead of u. Now for any $j \in NZ$ with $(x, j) \in E(T)$ we can find out u_j as there is exactly one vector in $\mathbf{l}_{x,j,k}$ with x-coordinate 1. As T is connected and contains all coordinates from NZ, we can determine all u_i's with $i \in NZ$ one by one. □ □

One may obtain a bound in the non-adaptive case using a very similar strategy to that in the 2-round proof of Theorem 1.3. As this time we have to ask all queries at a time, we have to make sure that no matter what NZ turns out to be we ask queries according to the edges of a connected graph on NZ. To this end we do not have any other choice than to query for all pairs $1 \leq i < j \leq n$. That is, we ask the separating system of the following subspaces:

$$\{A_i : i = 1, 2, \ldots, n\} \cup \{L_{i,j,k} : 1 \leq i < j \leq n, 1 \leq k \leq q-2\}.$$

A proof identical to that in the adaptive case shows that this set of subspaces form a separating system. This shows the bound $M(n, q) \leq n + \binom{n}{2}(q-2)$. Thus we obtain that if n is fixed, then $M(n, q)$ grows linearly in q. Our aim is not only to prove a similar statement for n, but to show that $M(n, q)$ grows linearly in nq. It is easy to see that the number of pairs of 1-subspaces separated by a subspace U is maximized when $\dim(U) = n-1$. Thus a natural idea is to consider a set of randomly picked $(n-1)$-subspaces as candidate for a separating system of small size. This would yield the upper bound $M(n, q) = O(nq \log q)$. Another idea is to generalize what we used in the case of projective planes. If $n = 3$, then

the set of lines incident to at least one of 3 non-collinear points forms a separating system of size $3q-3$. Results of Section 2 show that this is not optimal, but is still of the right order of magnitude. Combining these two ideas, we obtain a proof of Theorem 1.4.

Theorem 1.4 (upper bound)**.** *$M(n,q) \leq 2qn$.*

Proof. Let V be an n-dimensional vector space over $\mathrm{GF}(q)$ and let $X_1, X_2, \ldots, X_l$ be independent identically distributed random variables taking their values uniformly among all $(n-2)$-dimensional subspaces of V. For every X_i, there are exactly $q+1$ $(n-1)$-subspaces containing X_i, let us denote them by $X_{i,1}, X_{i,2}, \ldots, X_{i,q+1}$. For any pair $\mathbf{u}, \mathbf{v}$ of 1-subspaces of V, let $S_{\mathbf{u},\mathbf{v}}$ denote the indicator random variable of the event that $\mathbf{u}$ and $\mathbf{v}$ are not separated by $X_{1,1}, \ldots, X_{1,q}, X_{2,1}, \ldots, X_{2,q}, \ldots, X_{l,1}, \ldots, X_{l,q}$.

Claim 3.9. *Let $\mathbf{u}$ and $\mathbf{v}$ be different 1-subspaces of V. Then the number of $(n-2)$-subspaces U of V such that the family $\{U_1, U_2, \ldots, U_{q+1}\}$ of all $(n-1)$-subspaces of V containing U does not separate $\mathbf{u}$ and $\mathbf{v}$ is $(q-1)\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - (q-2)\begin{bmatrix} n-2 \\ n-4 \end{bmatrix}$.*

Proof of Claim. Clearly, if $\mathbf{u}, \mathbf{v} \in U$, then $U_1, U_2, \ldots, U_{q+1}$ do not separate $\mathbf{u}$ and $\mathbf{v}$, while if exactly one of them lies in U, then $U_1, U_2, \ldots, U_{q+1}$ do separate them. If $\mathbf{u}, \mathbf{v} \notin U$, then $\mathbf{u}$ and $\mathbf{v}$ are not separated by $U_1, U_2, \ldots, U_{q+1}$ if and only if $\dim(U, \langle \mathbf{u}, \mathbf{v} \rangle) = n-1$, that is if U meets $\langle \mathbf{u}, \mathbf{v} \rangle$ in a 1-subspace different from both $\mathbf{u}$ and $\mathbf{v}$. As there are $q-1$ such 1-subspaces, the number of such U's is $(q-1)\left(\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - \begin{bmatrix} n-2 \\ n-4 \end{bmatrix}\right)$. Thus the number of $(n-2)$-subspaces satisfying the condition of the claim is $\begin{bmatrix} n-2 \\ n-4 \end{bmatrix} + (q-1)\left(\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - \begin{bmatrix} n-2 \\ n-4 \end{bmatrix}\right)$ as claimed. ■

By the above claim we obtain the expected value of $S_{\mathbf{u},\mathbf{v}}$ satisfies

$$\mathbb{E}(S_{\mathbf{u},\mathbf{v}}) = \left(\frac{(q-1)\begin{bmatrix} n-1 \\ 2 \end{bmatrix} - (q-2)\begin{bmatrix} n-2 \\ 2 \end{bmatrix}}{\begin{bmatrix} n \\ 2 \end{bmatrix}} \right)^l \leq \left(\frac{(q-1)(q^{n-2}-1)}{q^n - 1} \right)^l \leq \frac{1}{q^l}.$$

And thus if we set $l = 2n$, then we have

$$\mathbb{E}(\sum_{\mathbf{u},\mathbf{v}} S_{\mathbf{u},\mathbf{v}}) \leq \binom{\begin{bmatrix} n \\ 1 \end{bmatrix}}{2} \frac{1}{q^l} \leq 1/2.$$

Therefore, there exists a collection of $2n$ $(n-2)$-dimensional subspaces such that the set of $(n-1)$-dimensional subspaces containing any of them is a separating family. Clearly, to separate pairs of 1-subspaces, it is enough to query q of the $q+1$ $(n-1)$-subspaces containing a fixed $(n-2)$-subspace, and thus we have $M(n,q) \leq 2nq$. □ □

To obtain the lower bound in Theorem 1.4 we will use the following theorem of Katona [14] about separating systems of sub*sets* of an underlying set.

Theorem 3.10 (Katona [14]). *Let X be an M-element set and $\mathcal{A} \subseteq 2^X$ be a separating system of subsets of X such that for all $A \in \mathcal{A}$ we have $|A| \leq m$ for some integer $m < M/2$. Then the following inequality holds*

$$|\mathcal{A}| \geq \frac{\log M}{\log e\frac{M}{m}} \frac{M}{m}.$$

Theorem 1.4 (lower bound). *There exists an absolute constant $C > 0$ such that for any positive integer n and prime power q the inequality $\frac{1}{C}qn \leq M(n,q)$ holds. Moreover, if q tends to infinity, then $(1-o(1))qn \leq M(n,q)$ holds.*

Proof. Theorem 3.10 can be applied to obtain the desired bound. Indeed, as mentioned in the Introduction, if X is the set of all 1-subspaces of V and the set Q of all allowed queries is

$$\left\{ F \subset \begin{bmatrix} V \\ 1 \end{bmatrix} : \exists U \leq V \text{ with } F = \left\{ \mathbf{u} \in \begin{bmatrix} V \\ 1 \end{bmatrix} : \mathbf{u} \leq U \right\} \right\},$$

then we can write $M = \begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{q^n-1}{q-1}$ and $m = \begin{bmatrix} n-1 \\ 1 \end{bmatrix} = \frac{q^{n-1}-1}{q-1}$ since the largest "meaningful" query sets are those corresponding to $(n-1)$-subspaces of V. Substituting these values to the formula of Theorem 3.10 we obtain

$$M(n,q) \geq \frac{\log M}{\log e\frac{M}{m}} \frac{M}{m} = \frac{\log \frac{q^n-1}{q-1}}{\log e\frac{q^n-1}{q^{n-1}-1}} \frac{q^n-1}{q^{n-1}-1} \geq (n-1)q \frac{\log q}{2+\log \frac{q^n-1}{q^{n-1}-1}}.$$

□ □

4 Remarks

We may formulate the dual searching problem: a hyperplane H_0 of $\mathrm{PG}(n-1,q)$ is marked, and we can ask whether a subplane H is contained in H_0; how many queries do we need to identify H_0? Let us consider now the non-adaptive case in $\mathrm{PG}(n,q)$. Suppose that we only ask points as queries. Thus we are to find a point set S such that its intersection with any hyperplane is unique. Clearly, if the intersection of S and any hyperplane contains n points in general position, we are done. Note that, however, this condition implies that any hyperplane is generated by its intersection with S, which is clearly stronger than our original goal. Such a point set may be called a *hyperplane generating set*. Let us denote the size of the smallest hyperplane generating set by $\sigma(\mathrm{PG}(n,q))$, and denote the size of the smallest n-fold blocking set with respect to hyperplanes by $\tau_n^{n-1}(\mathrm{PG}(n,q))$. In case of $n=3$, that is projective planes, a hyperplane (line) generating set is just a double blocking set, thus $\sigma(\mathrm{PG}(2,q)) = \tau_2^1(\mathrm{PG}(2,q)) = \tau_2(\mathrm{PG}(2,q))$; furthermore, as seen in the remark after Theorem 2.8, $M(3,q)$ is usually a bit smaller than $\tau_2(\mathrm{PG}(2,q))$.

In higher dimensions an n-fold blocking set with respect to hyperplanes is not necessarily a hyperplane generating set. Trivially, $\tau_n^{n-1}(\mathrm{PG}(n,q)) \le \sigma(\mathrm{PG}(n,q))$ and $M(n+1,q) \le \sigma(\mathrm{PG}(n,q))$, but it is not clear how far these parameters are from each other if $n \ge 3$.

As any line intersects every hyperplane in at least one point, the union of n pairwise nonintersecting lines is an n-fold blocking set with respect to hyperplanes. We may also try to find a hyperplane generating set as the union of some lines. Let us say that a set of lines is in *higgledy-piggledy position* if their union is a hyperplane generating set.

Thus if we could find a set of $h(n,q)$ lines in higgledy-piggledy position in $\mathrm{PG}(n,q)$, then $M(n+1,q) \le h(n,q)q$ would follow. For $n = 2$, any three non-concurrent lines suffice; for $n = 3$, one may take three lines of the same regulus of a hyperbolic quadric and a fourth line disjoint from the quadric; for $n = 4$, five lines turn out not to be enough [10]. For $n \ge 4$, we could not construct a small set of lines in higgledy-piggledy position so far. The arising finite geometrical questions seem quite interesting [9].

5 Acknowledgments

We thank the anonymous referees for their helpful suggestions. Tamás Héger and Marcella Takáts were supported by Hungarian National Scientific Fund (OTKA) Grant No. K 81310. Tamás Héger was also supported partially by ERC Grant No. 227701 DISCRETECONT. Balázs Patkós was supported by OTKA Grant PD-83586 and the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

[1] R. F. Bailey, Resolving sets for incidence graphs, Session talk at the 23rd British Combinatorial Conference, Exeter, 5th July 2011. Slides available online at `http://www.math.uregina.ca/~bailey/talks/bcc23.pdf` (last accessed June 21, 2013)

[2] R. F. Bailey, P. J. Cameron, Base size, metric dimension and other invariants of groups and graphs, Bull. London Math. Soc. **43** 209–242 (2011)

[3] G. Bacsó, T. Héger, T. Szőnyi, The 2-blocking number and the upper chromatic number of $\mathrm{PG}(2,q)$, to appear in J. Comb. Des.

[4] S. Ball, Multiple blocking sets and arcs in finite planes, J. London Math. Soc. (2) **54** no. 3, 581–593 (1996)

[5] S. Ball, A. Blokhuis, On the size of a double blocking set in $\mathrm{PG}(2,q)$, Finite Fields Appl., **2** 125–137 (1996)

[6] A. Blokhuis, A. E. Brouwer, Blocking sets in Desarguesian projective planes, Bull. London Math. Soc. **18** no. 2, 132–134 (1986)

[7] A. Blokhuis, L. Storme, T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, J. London Math. Soc. (2) **60** no. 2, 321–332 (1999)

[8] D.-Z. Du, F.K. Hwang, **Combinatorial Group Testing and its Applications**, 2nd ed. (English) Series on Applied Mathematics (Singapore). 12. Singapore: World Scientific. xii, 323 p. (2000).

[9] Sz. L. Fancsali, P. Sziklai, Lines in higgledy-piggledy position. *Submitted.*

[10] Sz. L. Fancsali, P. Sziklai, T. Szőnyi, Personal communication (2013).

[11] N. V. Harrach, Unique reducibility of multiple blocking sets, J. Geometry **103** 445–456 (2012)

[12] T. Héger, M. Takáts, Resolving Sets and Semi-Resolving Sets in Finite Projective Planes, Electronic J. of Combinatorics, **19** no. 4, P30 (2012)

[13] J. W. P. Hirschfeld, **Projective geometries over finite fields**, Clarendon Press, Oxford, 1979, 2nd edition, 1998.

[14] G. Katona, On separating systems of a finite set, J. Combin. Theory **1** 174–194 (1966)

[15] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes. Finite Fields and Appl. **3** 187–202 (1997)