COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **14** (2) (1994) 149–157

ON THE NUMBER OF NOWHERE ZERO POINTS IN LINEAR MAPPINGS

R. D. BAKER, J. BONIN, F. LAZEBNIK, and E. SHUSTIN

Received January 2, 1991
Revised May 6, 1993

Let A be a nonsingular n by n matrix over the finite field GF_q, $k=\lfloor \frac{n}{2} \rfloor$, $q=p^a, a\geq 1$, where p is prime. Let $P(A,q)$ denote the number of vectors x in $(GF_q)^n$ such that both x and Ax have no zero component. We prove that for $n\geq 2$, and $q>2\binom{2n}{3}$, $P(A,q)\geq[(q-1)(q-3)]^k(q-2)^{n-2k}$ and describe all matrices A for which the equality holds. We also prove that the result conjectured in [1], namely that $P(A,q)\geq 1$, is true for all $q\geq n+2\geq 3$ or $q\geq n+1\geq 4$.

1. Introduction

Let GF_q be the finite field containing $q=p^a$ elements, where p is prime, $a\geq 1$, and let $GL_n(q)$ denote the set of all nonsingular n by n matrices whose entries are elements of GF_q. Let $(GF_q)^n$ denote the n-dimensional vector space over GF_q in which elements are the ordered n–tuples of elements of GF_q, and let $GF_q^* = GF_q\backslash\{0\}$. Given $A\in GL_n(q)$, we call $x\in(GF_q)^n$ a *good vector of* A if both x and Ax have no zero components. Let $P(A,q)$ denote the number of good vectors of A. In [1] the following conjecture was stated for all prime powers and proved for all proper prime powers $q=p^a, a\geq 2$:

Conjecture. *Let $A\in GL_n(q)$, where $q\geq 4$. Then $P(A,q)\geq 1$.*

First we show that the conjecture is correct for all $q\geq n+2\geq 3$ and for all $q\geq n+1\geq 4$, including q being prime (Theorem 1). Next we ask the following question: What is the $\min\{P(A,q)|A\in GL_n(q)\}$? We show that for $n=2k\geq 2$ and $q>2\binom{2n}{3}$, this number is $[(q-1)(q-3)]^k$, while for $n=2k+1\geq 3$ and $q>2\binom{2n}{3}$, this number is $[(q-1)(q-3)]^k(q-2)$. We also describe all matrices $A\in GL_n(q)$ having the minimal number of good vectors.

AMS subject classification code (1991): 06 C 10, 15 A 06, 11 T 99

2.

Theorem 1. *Let $A \in GL_n(q)$, where $q \geq n+2 \geq 3$ or $q \geq n+1 \geq 4$. Then $P(A,q) \geq 1$.*

Proof. We use a probabilistic argument. Let x be a randomly chosen vector obtained by picking each of its coordinates randomly and independently from GF_q^* according to the uniform distribution. For every fixed row of A, the probability that x is orthogonal to the row is at most $\frac{(q-1)^{n-1}}{(q-1)^n} = \frac{1}{q-1}$ since the row contains a nonzero element. Hence the expected number of zero coordinates in Ax is at most $\frac{n}{q-1} < 1$ for $q \geq n+2$. Thus the statement is proven in this case. If $q = n+1$, then this expected value is at most 1. If it is less than 1, the theorem is proven. If it is equal to 1, then the probability of x being orthogonal to every row of A is $\frac{1}{q-1}$, and this happens if and only if each row of A contains precisely two nonzero entries. For $n \geq 3$, the latter implies the existence of $x \in (GF_q^*)^n$ such that Ax has at least two zero components. Since the expected number of zero components of Ax is 1, there must be another vector $y \in (GF_q^*)^n$ such that Ay has no zero coordinates. Thus the theorem is proven for all $q \geq n+1 \geq 4$. ∎

3.

Let $A = (a_{ij})$ and let a_i denote the i–th row of $A, i = 1, \ldots, n$. By e_i we denote the i–th vector in the standard basis of $(GF_q)^n$, i.e. the vector whose i–th component is 1 and the other components are zeros. Let $B = \{b_1, \ldots, b_n, b_{n+1}, \ldots, b_{2n}\}$, where $b_i = e_i$ and $b_{n+i} = a_i, i = 1, 2, \ldots, n$. The set B contains no zero vector since A is nonsingular. Let $B_i = \langle b_i \rangle^{\perp}, i = 1, \ldots, 2n$, be the orthogonal complement of $\langle b_i \rangle$ in $(GF_q)^n$. Then $P(A,q) = \left| \overline{\bigcup_{i=1}^{2n} B_i} \right| = \left| \bigcap_{i=1}^{2n} \overline{B_i} \right|$. By the inclusion–exclusion formula, we have

$$P(A,q) = \sum_{S \subseteq B} (-1)^{|S|} \left| \bigcap_{i \in S} B_i \right| = \sum_{S \subseteq B} (-1)^{|S|} q^{n-r(S)} , \tag{1}$$

where $r(S)$ is the rank of S. We will use some notions and results about geometric lattices (see [3] for the relevant definitions). In the geometric lattice L we consider, B is the set of atoms and, in general, the elements are of the form $B \cap X$ as X ranges over all subspaces of $(GF_q)^n$, $\wedge$ is intersection, and $\vee$ is calculated from the sum of subspaces. We call a minimal dependent subset of B a *circuit*. If the subset $\{b_{i_1}, b_{i_2}, \ldots, b_{i_k}\}$ is a circuit with $i_1 < i_2 < \ldots < i_k$, then the subset $\{b_{i_2}, b_{i_3}, \ldots, b_{i_k}\}$ is called a *broken circuit*. The polynomial $P(A,q)$ is a well known polynomial in q called the *characteristic polynomial of* L. (See e.g. [3].) The properties of $P(A,q)$ are described in the following theorem, the proof of which can be found in [3].

Theorem 2. *Let L be a geometric lattice of rank m. The characteristic polynomial is*

$$f(L, \lambda) = \lambda^m + f_1 \lambda^{m-1} + f_2 \lambda^{m-2} + \ldots + f_m ,$$

where $(-1)^i f_i$ is a positive integer for $1 \leq i \leq m$, equal to the number of independent subsets of i atoms not containing any broken circuit. ∎

Using Theorem 2, we can rewrite (1) as

$$P(A,q) = q^n - c_1 q^{n-1} + c_2 q^{n-2} - \ldots + (-1)^n c_n \ , \tag{2}$$

where c_k, for $k=1,\ldots,n$, is the number of independent subsets of k vectors of B containing no broken circuits. This description of the c_i's implies that

$$1 \leq c_i \leq \binom{2n}{i}, \text{ for } i = 1,\ldots,n. \tag{3}$$

By Theorem 1, we know that for $q \geq n+2 \geq 3$ and for $q \geq n+1 \geq 4$, there is at least one good vector for any $A \in GL_n(q)$. The next theorem shows which matrices have the least number of good vectors when q is sufficiently large.

Theorem 3. Part 1: *Let $n=2k \geq 2, q=p^a$, p prime, $a \geq 1$, and $A \in GL_n(q)$. Then if $n=2$ and $q \geq 3$, or $n \geq 4$ and $q > 2\binom{2n}{3}$,*

(i) $P(A,q) \geq [(q-1)(q-3)]^k$;

(ii) $P(A,q) = [(q-1)(q-3)]^k$ if and only if A is a block diagonal matrix

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & 0 & \\ & 0 & \ddots & \\ & & & A_k \end{pmatrix},$$

where A_i is a 2 by 2 nonsingular matrix over GF_q^*, or A is a matrix which can be brought to this form by some permutations of its rows and columns.

Part 2: *Let $n=2k+1 \geq 3$ and $A \in GL_n(q)$ with q as above. If $n=3$ and $q \geq 3$, or if $n \geq 5$ and $q > 2\binom{2n}{3}$, then*

(i) $P(A,q) \geq [(q-1)(q-3)]^k (q-2)$;

(ii) $P(A,q) = [(q-1)(q-3)]^k (q-2)$ if and only if, upon permuting rows and columns, we obtain a block diagonal matrix

$$\begin{pmatrix} A_1 & & & \\ & A_2 & 0 & \\ & 0 & \ddots & \\ & & & A_k \end{pmatrix},$$

where each A_i with $1 \leq i \leq k-1$ is a 2 by 2 nonsingular matrix over GF_q^* while A_k is a 3 by 3 nonsingular matrix of one of the following two forms, where zeros occur only where they have been specified:

$$\begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & a_{32} & a_{33} \end{pmatrix}, \quad \begin{pmatrix} \alpha a_{31} & \alpha a_{32} & 0 \\ \beta a_{31} & 0 & \beta a_{33} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \quad \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ \alpha a_{21} & \alpha a_{22} & a_{33} \end{pmatrix}. \tag{4}$$

Proof. We first treat the cases $n=2$ and $n=3$. These play an important role in the general case.

Lemma 1. *Let $A \in GL_2(q)$, with $q \geq 3$. Then $P(A,q) \geq (q-1)(q-3)$, with equality if and only if no entry of A is zero.*

Proof. When $n=2$, there are three possible geometric lattices generated by the vectors e_1, e_2, a_1, a_2, namely a two-point line, a three-point line, and a four-point line. The respective characteristic polynomials are $\lambda^2-2\lambda+1=(\lambda-1)^2$, $\lambda^2-3\lambda+2=(\lambda-1)(\lambda-2)$ and $\lambda^2-4\lambda+3=(\lambda-1)(\lambda-3)$. Of these, the last is least when evaluated at q. Since the four-point line arises precisely when no entry of A is zero, this proves the lemma. ∎

Lemma 2. *Let $A \in GL_3(q)$, with $q \geq 3$. Then $P(A,q) \geq (q-1)(q-2)(q-3)$, and equality holds if and only if the rows and columns of A can be permuted to produce a matrix of one of the forms given in (4).*

Proof. $P(A,q)$ is the characteristic polynomial of the rank-3 geometric lattice generated by the six vectors $e_1, e_2, e_3, a_1, a_2, a_3$. It is straightforward to check that if we evaluate at q the characteristic polynomials of rank-3 geometric lattices with 6 points and no 5-point line, the minimum obtained is $q^3-6q^2+11q-6=(q-1)(q-2)(q-3)$. Furthermore, only two geometries have this characteristic polynomial, namely the geometry formed by deleting a point from the Fano plane, and the geometry consisting of a three-point line intersecting a four-point line. These geometries arise precisely from the matrices described in the statement. ∎

Turning to the general case, we want to describe all nonsingular matrices $A \in GL_n(q)$ for which $P(A,q)$ takes the smallest values provided that q is sufficiently large. Since the leading term in $P(A,q)$ is q^n, the same for all $A \in GL_n(q)$, then an extremal matrix A should maximize c_1. According to Theorem 2, c_1 is the number of independent 1–subsets of B containing no broken circuits. Since B contains no zero vector, every vector of B forms an independent 1–subset. Therefore the greatest value of c_1 is $\binom{2n}{1}$ and the corresponding matrix A has no row which is a scalar multiple of a vector $e_i, i=1,\ldots,n$. We denote the class of such matrices A by $\mathscr{F}_1$ and the next question we ask is: for which $A \in \mathscr{F}_1$ is the second coefficient c_2 of $P(A,q)$ the smallest? Call this set of matrices $\mathscr{F}_2$; thus $\mathscr{F}_2 \subseteq \mathscr{F}_1$. According to Theorem 2, c_2 is the number of independent 2–subsets of B which contain no broken circuits. Since $A \in \mathscr{F}_1$, any two vectors of B are independent and a 2–subset of B contains a broken circuit if and only if it is a broken circuit. Therefore

$$c_2 = \binom{2n}{2} - |\{S \subseteq B : S \text{ is a 2-element broken circuit}\}| .$$

Clearly, c_2 is smallest if and only if the number of 2-element broken circuits of B is greatest, and our next step is to identify such sets B. The non-trivial lines (i.e. those containing more than two points) of the geometric lattice generated by B are of three types: $\{e_i, e_j, a_r\}$, $\{e_i, a_r, a_s\}$, and $\{e_i, e_j, a_r, a_s\}$ where $i<j$ and $r<s$. Lines of the first type give rise to a single 2-element broken circuit, namely $\{e_j, a_r\}$; those of the second type contribute the 2-element broken circuit $\{a_r, a_s\}$; however those of the third type give rise to three 2-element broken circuits, namely $\{e_j, a_r\}$, $\{e_j, a_s\}$ and $\{a_r, a_s\}$. This motivates the claim: The maximum number of 2-element broken circuits is $\lfloor 3n/2 \rfloor$. The following ideas and terminology will clarify the proof

of this claim. Consider the set of all 3-element circuits; thus these have the forms $\{e_i,e_j,a_r\}$ and $\{e_i,a_r,a_s\}$ where $i<j$ and $r<s$. Counting 2-element broken circuits amounts to counting the sets $\{e_j,a_r\}$ and $\{a_r,a_s\}$ we obtain from the 3-element circuits. Call a vector a_r a *weight-2 vector* if $\{e_i,e_j,a_r\}$ is a circuit for some e_i and e_j. (The terminology comes from coding theory.) Call a set $\{a_r,a_s\}$ arising from a circuit $\{e_i,a_r,a_s\}$ the *trace* of the circuit. Note that each trace should be counted once as a 2-element broken circuit (even though it may arise from either one or two 3-circuits) while each weight-2 vector a_r occurs in precisely one 3-circuit of the form $\{e_i,e_j,a_r\}$, and hence in precisely one 2-element broken circuit of the form $\{e_j,a_r\}$. Thus we want to count the traces and weight-2 vectors. Two further terms will be convenient. Generalizing the idea of weight-2 above, the *weight* of a vector a_i is the number of nonzero components of a_i. The *support* of a_i is the collection of distinct elements among $e_1,\dots,e_n$ which occur with nonzero coefficients when a_i is expressed as a linear combination of $e_1,\dots,e_n$. Thus the weight of a_i is the cardinality of its support. Consider a simple graph whose vertex set is the set of all 3-circuits in B with an edge joining two 3-circuits if and only if the 3-circuits have a vector a_r in common. The bound $\lfloor 3n/2\rfloor$ on 2-element broken circuits, claimed above, follows from the examination of the connected components of this graph given in Lemmas 3 through 5 below. Each trace $\{a_r,a_s\}$ arises from a vertex (or possibly two) $\{e_i,a_r,a_s\}$ in exactly one component; each weight-2 vector a_r arises from a vertex $\{e_i,e_j,a_r\}$ of exactly one component. Thus we want to examine traces and weight-2 vectors in components. For a component C, let $t(C)$ denote the set of traces of circuits in C, and let $w_2(C)$ denote the set of weight-2 vectors occurring as elements of vertices of C. Abusing terminology slightly, vectors a_i occurring as elements of vertices (3-circuits) of C will be called *vectors of C*. Finally, $A(C)$ will denote the set of vectors of C. Obviously the sets of vectors of distinct components are disjoint.

Lemma 3. *For any component C, we have $|t(C)|\le|A(C)|$.*

Proof. The traces of C correspond to at least $|t(C)|$ distinct standard basis vectors. Thus at least $|t(C)|$ distinct standard basis vectors are in the span of $A(C)$. Therefore the inequality follows from elementary linear algebra. ∎

Lemma 4. *Any component C contains at most two weight-2 vectors. Furthermore if C has two weight-2 vectors a_r and a_s, then either they have identical supports or there is a weight-3 vector a_t such that both $\{a_r,a_t\}$ and $\{a_s,a_t\}$ are traces.*

Proof. We first treat the case in which C contains two weight-2 vectors with the same support. For simplicity of notation, assume these vectors are a_1 and a_2, and that their common support is e_1,e_2. For any other vector a_u of C, consider all paths which start with a circuit containing either a_1 or a_2 and end at a circuit containing a_u. Out of all such paths we choose one of minimum length. We observe that no interior vertex of such a path is of the form $\{e_i,e_j,a_k\}$. Indeed, if this were the case, then both the predecessor and the successor of $\{e_i,e_j,a_k\}$ would contain a_k by the definition of edges in our graph. Then we could bypass $\{e_i,e_j,a_k\}$ (since its neighbors have a_k in common) and thereby shorten the path. Similarly the first and last vertices of the path are not of the form $\{e_i,e_j,a_k\}$. Therefore we may assume that the shortest path is of the form

$$\{e_3,a_2,a_3\},\{e_4,a_3,a_4\},\dots,\{e_{u-1},a_{u-2},a_{u-1}\},\{e_u,a_{u-1},a_u\}$$

(or $\{e_3,a_1,a_3\},\{e_4,a_3,a_4\},\ldots,\{e_{u-1},a_{u-2},a_{u-1}\},\{e_u,a_{u-1},a_u\}$ if this yields a shorter path) where we have relabeled the elements to simplify notation. Note that the vectors $a_1,a_2,\ldots,a_u$ are distinct since the path has minimum length. Since a_3 is distinct from a_1 and a_2, it follows that e_3 is distinct from e_1 and e_2 (justifying the relabeling) and so a_3 has weight 3. Since all elements in the support of a_3 can be written in terms of a_1,a_2,a_3, it follows that $e_4 \notin \{e_1,e_2,e_3\}$, and so a_4 has weight 4. Continuing in this manner, it follows that all vectors of C other than a_1 and a_2 have weights greater than 2. Now assume that C contains at least two weight-2 vectors a_1 and a_s, and that any two weight-2 vectors of C have different supports. Consider a path of minimum length between circuits containing a_1 and a_s, say $\{e_{i_2},a_1,a_2\}$ and $\{e_{i_s},a_{s-1},a_s\}$. Without loss of generality, we assume that a_1 has support e_1,e_2. Since a_1 has weight 2 and a_2 has a different support, e_{i_2} is distinct from e_1 and e_2, and so a_2 has weight 3. Looking at successive vertices in the path $\{e_{i_2},a_1,a_2\},\ldots,\{e_{i_s},a_{s-1},a_s\}$, note that either

(a) the weight of a_k is one greater than that of a_{k-1}, or

(b) the weight of a_k is one less than that of a_{k-1} and either $\{e_1,a_{k-1},a_k\}$ or $\{e_2,a_{k-1},a_k\}$, but not both, is a circuit, or

(c) a_{k-1} and a_k share common support and either $\{e_1,a_{k-1},a_k\}$ or $\{e_2,a_{k-1},a_k\}$, but not both, is a circuit.

Indeed, let $h\geq 3$ be the least index such that the weight of a_{h-1} is at least as big as the weight of a_h. Then all vectors $a_1,\ldots,a_h$ are distinct due to the minimality of the path, and all vectors $e_1,e_2,e_{i_2},\ldots,e_{i_{h-1}}$ are distinct since they form the support of a_{h-1}. Vector e_{i_h} must belong to the supports of both a_{h-1} and a_h. It must be distinct from vectors $e_{i_2},\ldots,e_{i_{h-1}}$, otherwise we obtain linear dependence among distinct vectors $a_1,\ldots,a_h$. Therefore $e_{i_h}\in\{e_1,e_2\}$. Since condition (b) allows the weight to go down only once as we consider successive a_k's, a_s can have weight-2 if and only if the path has length 1, say $\{e_3,a_1,a_2\},\{e_1,a_2,a_3\}$, and the elements are of the form $a_1=\delta\alpha e_1+\delta\beta e_2$, $a_2=\alpha e_1+\beta e_2+\gamma e_3$ and $a_3=\epsilon\beta e_2+\epsilon\gamma e_3$, where none of the coefficients are zero. From this it is easy to see that there are only two weight-2 vectors in the component C. ∎

We now prove the inequality claimed above for 2-element broken circuits, recast in terms of traces and weight-2 vectors, for each component.

Lemma 5. *For any component C with $|A(C)|$ even, we have*

$$|t(C)|+|w_2(C)|\leq\frac{3|A(C)|}{2},$$

with equality if and only if $|A(C)|=2$, $|t(C)|=1$ and $|w_2(C)|=2$.
If $|A(C)|$ is odd, then we have

$$|t(C)|+|w_2(C)|\leq\frac{3|A(C)|-1}{2},$$

with equality if and only if either

(a) $|A(C)|=1$, $|t(C)|=0$ *and* $|w_2(C)|=1$, *or*

(b) $|A(C)|=3$, $|t(C)|=2$ *and* $|w_2(C)|=2$.

Proof. The cases of $|A(C)|$ being either 1 or 2 are obvious, and the case $|A(C)|=3$ follows from the ideas in the proof of Lemma 4. For $|A(C)|=4$, the bound of

6 follows since $|t(C)| \le |A(C)| = 4$ and $|w_2(C)| \le 2$. Furthermore the ideas in the proof of Lemma 4 show that when $|A(C)| = 4$, we have that $|w_2(C)| = 2$ implies that $|t(C)| \le 3$. Hence equality never occurs in this case. The case $|A(C)| = 5$ is similar. All cases with $|A(C)| \ge 6$ follow directly from Lemma 3 and the inequality $|w_2(C)| \le 2$ of Lemma 4. ∎

Applying Lemma 5 to the components of the graph gives us the desired inequality about 2-element broken circuits in $B = \{e_1, \ldots, e_n, a_1, \ldots, a_n\}$ and allows us to describe the cases of equality as follows.

Lemma 6. *The maximum number of broken circuits in $B = \{e_1, \ldots, e_n, a_1, \ldots, a_n\}$ is $\lfloor 3n/2 \rfloor$. The cases of equality arise precisely when by permuting the rows and columns of A, a matrix of the form in Theorem 3 can be obtained.* ∎

From here on, the differences between the cases of even n and odd n are minimal, and so we shall focus on the even case. We just argued that, by proper permutations of its rows and columns, the matrix A can be brought to a block diagonal form

$$A' = \begin{pmatrix} A_1 & & & \\ & A_2 & 0 & \\ & 0 & \ddots & \\ & & & A_k \end{pmatrix}, \tag{5}$$

where $A_i \in GL_2(q)$ and A_i has no zero entries. Notice that $P(A,q) = P(A',q)$.

Thus our attempt to find all $A \in GL_n(q)$ for which c_1 is the greatest (class $\mathcal{F}_1$), and then out of all matrices of $\mathcal{F}_1$ to choose the ones for which c_2 is the least (class $\mathcal{F}_2$) led to the complete characterization of the matrices. If $A \in \mathcal{F}_2$, then

$$P(A,q) = q^n - \binom{2n}{1} q^{n-1} + \left[\binom{2n}{2} - \frac{3n}{2}\right] q^{n-2} - c_3 q^{n-3} + \ldots + (-1)^n c_n.$$

In order to compute $P(A,q)$ we use Lemma 1 (similarly, use both Lemmas 1 and 2 for the odd case).

Let $A \in \mathcal{F}_2$, and we may assume that A has a block diagonal form (5) with $A_i \in GL_2(q)$, and A_i having no zero entries. A vector $x = (x_1, x_2, \ldots, x_{n-1}, x_n)$ is a good vector of A if and only if (x_{2i-1}, x_{2i}) a good vector of $A_i, i = 1, \ldots, k$ (recall $n = 2k$). By Lemma 1 there are exactly $(q-1)(q-3)$ choices for (x_{2i-1}, x_{2i}) for each $i = 1, 2, \ldots, k$. Hence there are $[(q-1)(q-3)]^k$ good vectors of $A \in \mathcal{F}_2$. Therefore Theorem 3 is proved for all sufficiently large q, i.e. for all $q \ge q_0$, where q_0 is some constant depending on n. An estimate on q_0 can be taken as an upper bound M for the absolute values of the roots of the polynomial $H(q) = P(A,q) - P(A^*,q)$ where $A \in GL_n(q) \setminus \mathcal{F}_2, A^* \in \mathcal{F}_2$. Then for all $q > M$, we have $H(q) > 0$. In order to compute M in terms of the coefficients of $H(q)$ we use the following proposition due to Fujiwara [2]; for a reference in English see Wilf [4]:

Lemma 7. *All the roots of the polynomial $f(z) = f_0 z^n + f_1 z^{n-1} + \ldots + f_n$ lie in the circle $|z| \le R = 2\max\left\{\left|\frac{f_i}{f_0}\right|^{1/i} : 1 \le i \le n\right\}$.* ∎

Let $P(A,q)=q^n-c_1q^{n-1}+c_2q^{n-2}-\ldots+(-1)^nc_n$ and $P(A^*,q)=q^n-c_1^*q^{n-1}+c_2^*q^{n-2}-\ldots+(-1)^nc_n^*$. Then $H(q)=h_1q^{n-1}+h_2q^{n-2}+\ldots+h_n$, where $h_i=(-1)^i(c_i-c_i^*), i=1,\ldots,n$. The coefficient h_1 is 0 if $A\in\mathscr{F}_1\backslash\mathscr{F}_2$, and satisfies $1\le h_1<\binom{2n}{1}$ if $A\in GL_n(q)\backslash\mathscr{F}_1$. From (3) we have

$$0\le|h_i|\le\binom{2n}{i}, \text{ for } i=2,\ldots,n. \tag{6}$$

If $h_1\neq 0$, then by Lemma 7, we get

$$R_1=2\max\left\{\left|\frac{h_{1+i}}{h_1}\right|^{1/i}:1\le i\le n-1\right\}. \tag{7}$$

If $h_1=0$, then $h_2\ge 1$ (since $A\in\mathscr{F}_1\backslash\mathscr{F}_2$) and so by Lemma 7, we get

$$R_2=2\max\left\{\left|\frac{h_{2+i}}{h_2}\right|^{1/i}:1\le i\le n-2\right\} \tag{8}$$

Lemma 8. *$R_1\le 2\binom{2n}{2}$, and $R_2\le 2\binom{2n}{3}$.*

Proof. Using (6), (7), and (8) we have:

$$R_1\le 2\max\left\{\binom{2n}{1+i}^{1/i}:i=1,\ldots,n-1\right\},$$

and

$$R_2\le 2\max\left\{\binom{2n}{2+i}^{1/i}:i=1,\ldots,n-2\right\}.$$

It is a straightforward verification that both sequences $\binom{2n}{i+1}^{1/i}, i=1,\ldots,n-1$, and $\binom{2n}{2+i}^{1/i}, i=1,\ldots,n-2$ are decreasing. Hence their first terms are the largest, and this proves the lemma. ∎

Since $\max\{R_1,R_2\}=R_2=2\binom{2n}{3}$ for $n\ge 3$, then $P(A,q)>P(A^*,q)$ for all $q>2\binom{2n}{3}$ and all $A\in GL_n(q)\backslash\mathscr{F}_2$. This ends the proof of Theorem 3. ∎

Acknowledgment. The authors are grateful to the anonymous referee who suggested the probabilistic proof of Theorem 1 and a slight strengthening of the original statement. The original proof was different and covered the case $q\ge n+2\ge 3$ only.

References

[1] N. ALON, and M. TARSI: A nowhere zero point in linear mappings, *Combinatorica* **9(4)** (1989), 393–395.

[2] M. FUJIWARA: Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung, *Tôhoku Math. J.* **10** (1916), 167–171.

[3] G.–C. ROTA: On the Foundations of Combinatorial Theory I: Theory of Möbius Functions, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2**, 340–368, 1964.

[4] H. S. WILF: *Mathematics for the Physical Sciences* (Wiley, New York, 1978).

R. D. Baker

Department of Mathematical Sciences
University of Delaware
Newark, Delaware 19716, USA
baker@math.udel.edu

J. Bonin

Department of Mathematics
The George Washington University
Washington, DC 20052, USA
jbonin@gwuvm.gwu.edu

Felix Lazebnik

Department of Mathematical Sciences
University of Delaware
Newark, Delaware 19716, USA
fellaz@math.udel.edu

E. Shustin

School of Mathematical Sciences
Tel Aviv University
69 978 Tel Aviv, Israel
shustin@math.tau.ac.il