COMBINATORICA 9 (4) (1989) 393—395

COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

NOTE

A NOWHERE-ZERO POINT IN LINEAR MAPPINGS

N. ALON and M. TARSI

Received March 29, 1988

We state the following conjecture and prove it for the case where q is a proper prime power: *Let A be a nonsingular n by n matrix over the finite field GF_q, $q \geqq 4$, then there exists a vector x in $(GF_q)^n$ such that both x and Ax have no zero component.*

In this note we consider the following conjecture:

Conjecture 1. *Let A be a nonsingular n by n matrix over the finite field GF_q, $q \geqq 4$, then there exists a vector x in $(GF_q)^n$ such that both x and Ax have no zero component.*

Notice that there are easy examples showing that the assertion of the conjecture is false for $q \leqq 3$. We have reached this conjecture while trying to generalize some simple properties of sparse graphs to more general matroids. Specifically: a graph whose edge set is the union of two forests is clearly 4-colorable. In general, the chromatic number of a matroid whose element set is the union of two independent sets can be bigger. This claim can be verified by checking the chromatic polynomial of the uniform matroid $U_{n,2n}$ (see [4] for the relevant definitions). However, if such a matroid is representable over a field GF_q for which conjecture 1 holds then its chromatic number is at most q, since the conjecture implies that its critical number over GF_q is 1 ([4], Chapter 15.5).

The conjecture also seems, to be of interest for its own. The case $q=5$ was stated as an open problem by F. Jaeger [3]. All we could do so far is to prove the following partial result given in Theorem 1 below. Our proof resembles the ones given in [2], [1], but contains several additional ideas.

Theorem 1. *Conjecture 1 holds for the case where q is not a prime, that is $q=p^k$ for a prime p and $k \geqq 2$.*

Proof. Let $A=\{a_{i,j}\}$ be an n by n nonsingular matrix over GF_q, where $q=p^k$, $k \geqq 2$ and p is a prime. Define the polynomial $P_A(X_1, X_2, \ldots, X_n)$ as follows:

$$P_A(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} \Big(\sum_{j=1}^{n} a_{i,j} X_j\Big).$$

Denote by L the set of all ordered partitions of n into the sum of n non-negative integer parts, that is:

$$L = \Big\{\alpha = (\alpha_1, \ldots, \alpha_n) \,\Big|\, \sum_{j=1}^{n} \alpha_j = n, \alpha_j \text{ is an integer } \geqq 0\Big\}.$$

Research supported in part by Allon Fellowship and by a Bat Sheva de Rothschild grant.
AMS subject classifications (1980): 05 B 35, 05 B 25, 12 C 05.

Let A_α be the n by n matrix whose columns are α_j copies of the j'th column of A for every $1\leqq j\leqq n$. E.g., $A_{(1,1,\dots,1)}=A$ and $A_{(2,0,1,1,\dots,1)}$ is obtained as the second column of A is replaced by a copy of the first one. Also define for every $\alpha=(\alpha_1,\dots,\alpha_n)\in L$ c_α to be the coefficient of $\prod_{j=1}^n X_j^{\alpha_j}$ in the expansion of $P_A(X_1,\dots,X_n)$. It is a straightforward routine to verify:

Claim 1. *For every* $\alpha=(\alpha_1,\dots,\alpha_n)\in L$

$$\operatorname{Per}(A_\alpha)=c_\alpha\prod_{j=1}^n(\alpha_j!),$$

where $\operatorname{Per}(A_\alpha)$ *is the permanent of the matrix* A_α.

The α_j's are natural numbers and by $\alpha_j!$ we mean its value modulo p as an element of GF_p considered as a subfield of GF_q. For a natural number m greater or equal to p, $m!\equiv 0 \pmod p$, which yields:

Claim 2. *Let* $\alpha=(\alpha_1,\dots,\alpha_n)\in L$. *If for some* j $\alpha_j\geqq p$ *then* $\operatorname{Per}(A_\alpha)=0$.

Let A' be the matrix obtained from A by adding the j_1'th column multiplied by a scalar $s\in GF_q$ to the j_2'th column, for some $1\leqq j_1,\ j_2\leqq n$. Clearly $\operatorname{Per}(A')=$ $=\operatorname{Per}(A)+s\operatorname{Per}(A_{\alpha=(\alpha_1,\dots,\alpha_n)})$ where $\alpha_{j_1}=2$, $\alpha_{j_2}=0$ and $\alpha_j=1$ for $j\neq j_1,j_2$. Recursively the permanent of every matrix obtained from A by repeated applications of elementary column operations can be represented as a linear combination $\sum_{\alpha\in L}s_\alpha\operatorname{Per}(A_\alpha)$, where $s_\alpha\in GF_q$. Since A is nonsingular the identity matrix is obtained from A by elementary column operations and hence $1=\sum_{\alpha\in L}s_\alpha\operatorname{Per}(A_\alpha)$. Applying Claim 2 we obtain:

$$1=\sum_{\alpha\in L'}s_\alpha\operatorname{Per}(A_\alpha)$$

where L' is the subset of L consisting of the partitions $\alpha=(\alpha_1,\dots,\alpha_n)$ for which $\alpha_j<p$, $1\leqq j\leqq n$. Therefore, there exists, $\alpha\in L'$ with $\operatorname{Per}(A_\alpha)\neq 0$. By Claim 1 this implies:

Claim 3. *In the expansion of* $P_A(X_1,\dots,X_n)$ *there is a monomial* $c_\alpha\prod_{j=1}^n X_j^{\alpha_j}$ *with* $c_\alpha\neq 0$ *and* $\alpha_j<p$ *for every* j.

Define now

$$P'_A(X_1,\dots,X_n)=\Big(\prod_{j=1}^n X_j\Big)P_A(X_1,\dots,X_n).$$

For a vector $x=(x_1,\dots,x_n)\in(GF_q)^n$ $P'_A(x)=P'_A(x_1,\dots,x_n)$ is the product of all the $2n$ components of both x and Ax. Theorem 1 is thus equivalent to the existence of a vector x for which $P'_A(x)\neq 0$.

It is easy to show (by induction on n) that a polynomial in n variables over GF_q gives the value 0 for every substitution if and only if it can be reduced to the zero polynomial (i.e., the one with all the coefficients equal to 0) by the relations $X^q=X$ for every variable X. In the expansion of $P'_A(X_1,\dots,X_n)$ there is, according to Claim 3, a monomial $c_\alpha\Pi X_j^{\beta_j}$ with $c_\alpha\neq 0$ and all β_j at most p $(\beta_j=\alpha_j+1)$. Since $q=p^k>p$ this monomial cannot be the subject to a reduction by any relation

$X_j^q = X_j$. On the other hand $P'_A(X_1, \ldots, X_n)$ is homogeneous and thus a term similar to this monomial cannot be obtained out of another by these relations. It turns out that $P'_A(X_1, \ldots, X_n)$ cannot be reduced to the zero polynomial and thus there exists a vector x as required. ∎

Remarks

By modifying the above proof we can prove the following extension of Theorem 1, which may help in settling the general case of Conjecture 1.

Proposition 1. *Let A be a nonsingular n by n matrix over a field F of characteristic p. Let $F_1, F_2, \ldots, F_n \subset F$ be arbitrary subsets of F, each of cardinality p, and let $f_1, f_2, \ldots, f_n$ be elements of F. Then there exists a vector $x = (x_1, x_2, \ldots, x_n)$ with $x_j \in F_j$ such that the i'th component of Ax is different from f_i.*

The proof is almost identical to that of Theorem 1. Only $P'_A(X_1, \ldots, X_n)$ should be replaced by:

$$\prod_{j=1}^{n} \prod_{f \notin F_j} (X_j - f) \prod_{i=1}^{n} \left(\left(\sum_{j=1}^{n} a_{i,j} X_j\right) - f_i\right)$$

Although this polynomial is not homogeneous, the proof considers only terms of maximal degree and the result follows. ∎

Even stronger restrictions can be forced on the components of x and Ax using the following statement, in which nonsingularity is replaced by permanent $\neq 0$. The (similar) proof is omitted.

Proposition 2. *Let A be an n by n matrix over a field F and suppose* $\mathrm{Per}(A) \neq 0$. *Let $F_1, F_2, \ldots, F_n \subset F$ be arbitrary subsets of F, each of cardinality 2, and let $f_1, f_2, \ldots, f_n$ be elements of F. Then there exists a vector $x = (x_1, x_2, \ldots, x_n)$ with $x_i \in F_i$ such that the j'th component of Ax is different from f_j.* ∎

Propositions 1 and 2 can be used to show that if $q = p^k$, $k \geqq 2$ and A is a nonsingular n by n matrix over GF_q then there are many vectors $x \in (GF_q)^n$ such that both x and Ax have no zero component. For example, for $q = 4$ one can easily show that there are at least $(3/2)^n$ such vectors x. We omit the details.

References

[1] N. Alon, E. E. Bergmann, D. Coppersmith and A. M. Odlyzko, Balancing sets of vectors, *IEEE Transactions on Information Theory*, in press.

[2] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combinatorial Theory*, Ser. A **24** (1978), 251—253.

[3] F. Jaeger, Problem presented in the 6th *Hungar. Comb. Coll.*, *Eger*, Hungary **1981**, and: *Finite and Infinite Sets* (eds.: Hajnal, A., Lovász, L,, Sós, V. T.). North Holland, Amsterdam, 1982 II, 879.

[4] D. J. A. Welsh, *Matroid Theory*, Academic Press, San Francisco, **1976**.

Noga Alon and Michael Tarsi

School of Mathematical Sciences
Sackler Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv
69978 Israel