Matrix Choosability

Matt DeVos*

Applied Math Department

Princeton University

Princeton, NJ 08544

matdevos@math.princeton.edu

Abstract

Let F be a finite field with p^c elements, let A be a $n \times n$ matrix over F, and let k be a positive integer. When is it true that for all $X_1, \ldots, X_n \subseteq F$ with $|X_i| = k+1$ and for all $Y_1, \ldots, Y_n \subseteq F$ with $|Y_i| = k$, there exist $x \in X_1 \times \ldots \times X_n$ and $y \in (F \setminus Y_1) \times \ldots \times (F \setminus Y_n)$ such that $Ax = y$? It is trivial that A has this property for $k = p^c - 1$ if $det(A) \neq 0$. The permanent lemma of Noga Alon proves that if $perm(A) \neq 0$, then A has this property for $k = 1$. We will present a theorem which generalizes both of these facts, and then we will apply our theorem to prove "choosability" generalizations of Jaeger's 4-flow and 8-flow theorems in Z_p^k.

1 Introduction

Let F be a field. We define $\mathcal{M}_{n \times m}(F)$ to be the set of all $n \times m$ matrices with entries in F. Let $A \in \mathcal{M}_{n \times m}(F)$, and let $\alpha = (\alpha_1, \ldots, \alpha_m)$, $\beta = (\beta_1, \ldots, \beta_n)$ be sequences of nonnegative integers. We will say that A is (α, β)-*pliant* if for all $X_1, \ldots, X_m \subseteq F$ and $Y_1, \ldots, Y_n \subseteq F$ with every $|X_j| \geq \alpha_j$ and $|Y_i| \leq \beta_i$, there exists a vector $x \in X_1 \times X_2 \times \ldots \times X_m$ and a vector $y \in (F \setminus Y_1) \times (F \setminus Y_2) \times \ldots \times (F \setminus Y_n)$ such that $Ax = y$. If $\alpha = (a, a, \ldots a)$ and

*This research was supported by Navy Aasert grant N00014-98-1-0457

$\beta = (b, b, \ldots b)$, then we will say that A is (a, b)*-pliant*. If A is $(a+1, a)$*-pliant*, we will say that A is a*-pliant*.

Note that any matrix A is 0-pliant. Also, note that if $|F| = p^c$ and $m = n$, then A is $(p^c - 1)$-pliant if and only if A is invertible. If $\alpha' = (\alpha'_1, \ldots, \alpha'_m)$ and $\beta' = (\beta'_1, \ldots, \beta'_n)$ are sequences of nonnegative integers, with $\alpha'_j \geq \alpha_j$ for all $1 \leq j \leq m$ and $\beta'_i \leq \beta_i$ for all $1 \leq i \leq n$, then A is (α, β)-pliant implies that A is (α', β')-pliant.

The following theorem of Noga Alon ([1]) is refered to as the permanent lemma. It has many diverse applications in combinatorics. Our main theorem is a generalization of this theorem.

Lemma 1.1 (Alon's permanent lemma [1]) *Let F be an arbitrary field, and let $A \in \mathcal{M}_{n\times n}(F)$ be such that $perm(A) \neq 0$. Then A is 1-pliant.*

The following conjecture of Jaeger also concerns a solution to the equation $Ax = y$ with coordinate-wise restrictions on x and y.

Conjecture 1.2 (Jaeger) *For any field F with $|F| > 3$, and any $A \in \mathcal{M}_{n\times n}(F)$, if A is invertible then there exist $x = (x_1, \ldots, x_n) \in F^n$ and $y = (y_1, \ldots, y_n) \in F^n$ such that $Ax = y$, and such that $x_i \neq 0 \neq y_i$ for $1 \leq i \leq n$.*

Using the permanent lemma, Alon and Tarsi ([4]) proved that any invertible matrix over a field of characteristic $p > 0$ is $(p, 1)$-pliant. It follows from this that Jaeger's conjecture is true for all fields not of prime order. The following corollary of our main theorem strengthens this result (in particular, we prove that any such matrix is $(p-1)$-pliant).

Corollary 1.3 *Let F be a field of characteristic $p > 0$, and let $A \in \mathcal{M}_{n\times n}(F)$ be invertible. If $k = w_t p^t + \ldots w_1 p + w_0$, where $w_i \in \{0, p-1\}$ for all $0 \leq i \leq t$, then A is k-pliant.*

Let p be a prime. For the vector space Z_p^n, an *additive basis* B is a multiset of elements from Z_p^n such that for all $v \in Z_p^n$, there is a subset of B which sums to v. If a matrix $A \in \mathcal{M}_{n\times m}(Z_p)$ is $(2, p-1) - pliant$, then the multiset of columns of A is an additive basis (of Z_p^n). The following conjecture about additive bases (if true) would have very useful consequences. In particular, for some k, it would establish the existence of a nowhere-zero 3-flow in any k-edge-connected graph.

Conjecture 1.4 (Jaeger, Linial, Payan, Tarsi [8]) *For every prime p, there is a constant $c(p)$ such that the union (as multisets) of any $c(p)$ bases of Z_p^n contains an additive basis.*

A second conjecture is that we may take $c(p) = p$ in Conjecture 1.4. It is known that the union of any $\lceil (p-1)log_e(n) \rceil + p - 2$ bases contains an additive basis. This was proved by Alon, Linial, and Meshulam ([3]) with the help of the permanent lemma.

In the last section, we will apply the main theorem to prove generalizations of Jaeger's 4-flow and 8-flow theorems (see [7]). For Z_2^k, we have the following results:

Corollary 1.5 *Let G be a 4-edge-connected graph, and for every edge $e \in E(G)$, let $\ell_e \subseteq Z_2^k$ with $|\ell_e| \geq 2^{k-1} + 1$. Then there exists a flow $\phi : E(G) \to Z_2^k$ such that $\phi(e) \in \ell_e$ for all $e \in E(G)$.*

Corollary 1.6 *Let G be a 3-edge-connected graph, and for every edge $e \in E(G)$, let $\ell_e \subseteq Z_2^k$ with $|\ell_e| \geq 2^{k-1} + 2^{k-2} + 1$. Then there exists a flow $\phi : E(G) \to Z_2^k$ such that $\phi(e) \in \ell_e$ for all $e \in E(G)$.*

2 Matrix Choosability

In this section, we will prove our main theorem. Like the proof of the permanent lemma, our proof will require a theorem of Alon and Tarsi called the combinatorial nullstellensatz (see e.g. [1]).

Let $q = q(z_1, \ldots, z_n)$ be a polynomial in $F[z_1, \ldots, z_n]$. For any nonnegative integers $d_1, \ldots, d_n$, we will let $[q]_{z_1^{d_1} z_2^{d_2} \ldots z_n^{d_n}}$ denote the coefficient of $z_1^{d_1} z_2^{d_2} \ldots z_n^{d_n}$ in the expansion of q.

Theorem 2.1 (Alon and Tarsi's combinatorial nullstellensatz [1]) *Let F be an arbitrary field and let $q = q(z_1, \ldots, z_n) \in F[z_1, \ldots, z_n]$. Suppose $deg(q) = \sum_{i=1}^{n} d_i$ where each d_i is a nonnegative integer and $[q]_{z_1^{d_1} z_2^{d_2} \ldots z_n^{d_n}} \neq 0$. Then, if $S_1, \ldots, S_n$ are subsets of F with $|S_i| > d_i$ for each i, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ such that $q(s_1, \ldots s_n) \neq 0$.*

Now, we will require a generalization of the permanent. We will let J_k denote the $k \times k$ matrix of ones. Let F be a field of characteristic p, let $A = (a_{ij}) \in \mathcal{M}_{n\times n}(F)$, and let k be a nonnegative integer such that either $p = 0$ or $k < p$. Then, we define:

$$P_k(A) = \frac{1}{(k!)^n}\, perm \begin{bmatrix} a_{11}J_k & a_{12}J_k & \ldots & a_{1n}J_k \\ a_{21}J_k & a_{22}J_k & \ldots & a_{2n}J_k \\ \vdots & \vdots & . & \vdots \\ a_{n1}J_k & a_{n1}J_k & \ldots & a_{nn}J_k \end{bmatrix}$$

Note that $P_0(A) = 1$ and that $P_1(A) = perm(A)$.

Let A be a matrix with index set $I \times J$, and let $I' \subseteq I$ and $J' \subseteq J$. Then we will let $A[I'|J']$ denote the matrix formed from A by deleting the rows with indices in $I \setminus I'$ and deleting the columns with indices in $J \setminus J'$. If $S \subseteq \{1, \ldots, n\}$, we will let χ_S^n denote the characteristic vector of S (of length n).

Throughout the rest of this section, except where noted, F will be a field of characteristic $p > 0$. Our main result is the following theorem:

Theorem 2.2 *Let $A \in \mathcal{M}_{n\times m}(F)$, and let $w_0, \ldots w_t \in \{0, \ldots, p-1\}$. Let $I_0, \ldots, I_t \subseteq \{1, \ldots, n\}$, $J_0, \ldots, J_t \subseteq \{1, \ldots, m\}$ be such that $|I_k| = |J_k|$ and $P_{w_k}(A[I_k|J_k]) \neq 0$ for all $0 \leq k \leq t$. Then A is (α, β)-pliant where $\alpha = (1, 1, \ldots, 1) + \sum_{k=0}^{t}(w_k p^k)\chi_{J_k}^m$ and $\beta = \sum_{k=0}^{t}(w_k p^k)\chi_{I_k}^n$.*

If $m = n$, then setting $I_0, \ldots, I_t = \{1, \ldots, n\} = J_0, \ldots, J_t$, we have:

Corollary 2.3 *Let $A \in \mathcal{M}_{n\times n}(F)$, and let $k = w_t p^t + \ldots w_1 p + w_0$ with $w_i \in \{0, \ldots, p-1\}$ for $0 \leq i \leq t$. If $P_{w_i}(A) \neq 0$ for all $0 \leq i \leq t$, then A is k-pliant.*

The following corollary is a generalization of the permanent lemma of Alon for finite fields. It follows immediately from the previous corollary, since $P_0(A) = 1$ and $P_1(A) = perm(A)$.

Corollary 2.4 *Let $A \in \mathcal{M}_{n\times n}(F)$ be such that $perm(A) \neq 0$. If $k = w_t p^t + \ldots w_1 p + w_0$, where $w_i \in \{0, 1\}$ for all $0 \leq i \leq t$, then A is k-pliant.*

If $p = 2$, then $det(A) = perm(A)$, so by the previous corollary, we have:

Corollary 2.5 *Let F be a field of characteristic 2 and let $A \in \mathcal{M}_{n\times n}(F)$ be invertible. Then A is k-pliant for any $k \geq 0$.*

We will give a proof of the following lemma in the next section.

Lemma 2.6 (Alon, Linial, Meshulam [3]) *If $A \in \mathcal{M}_{n\times n}(F)$, then $P_{p-1}(A) = det(A)^{p-1}$.*

Corollary 1.3 (restated for convenience) now follows from Corollary 2.3, since $P_0(A) = 1$ and $P_{p-1}(A) = det(A)^{p-1}$.

Corollary 1.3 Let $A \in \mathcal{M}_{n\times n}(F)$ be invertible. If $k = w_t p^t + \ldots w_1 p + w_0$, where $w_i \in \{0, p-1\}$ for all $0 \leq i \leq t$, then A is k-pliant.

Corollary 2.7 *Let $A \in \mathcal{M}_{n\times m}(F)$. Suppose that there exist $S_1, S_2 \subseteq \{1, \ldots, m\}$ such that $A[\{1, \ldots, n\}|S_i]$ is invertible for $i = 1, 2$, and such that $S_1 \cap S_2 = \emptyset$. Then for any $t > 1$, we have that A is $((p-1)p^{t-1} + 1, p^t - 1)$-pliant.*

Proof: Let $w_0, \ldots, w_{t-1} = p - 1$. Then set $I_0, \ldots, I_{t-1} = \{1, \ldots, n\}$, set $J_{t-1} = S_1$, set $J_0, \ldots, J_{t-2} = S_2$, and apply Theorem 2.2. This gives us a pair of sequences (α, β) such that A is (α, β)-pliant. The corollary follows easily from the fact that $\alpha_j \leq (p-1)p^{t-1} + 1$ for all $1 \leq j \leq m$ and $\beta_i = p^t - 1$ for all $1 \leq i \leq n$. □

Corollary 2.8 *Let $A \in \mathcal{M}_{n\times m}(F)$. Suppose that there exist $S_1, S_2, S_3 \subseteq \{1, \ldots, m\}$ such that $A[\{1, \ldots, n\}|S_i]$ is invertible for $i = 1, 2, 3$ and such that $S_1 \cap S_2 \cap S_3 = \emptyset$. Then for any $t > 2$, we have that W is $((p-1)(p^{t-1} + p^{t-2}) + 1, p^t - 1)$-pliant.*

Proof: Let $w_0, \ldots, w_{t-1} = p - 1$. Then set $I_0, \ldots, I_{t-1} = \{1, \ldots, n\}$, set $J_{t-1} = S_1$, set $J_{t-2} = S_2$, set $J_0, \ldots, J_{t-3} = S_3$, and apply Theorem 2.2. This gives us a pair of sequences (α, β) such that A is (α, β)-pliant. The corollary follows easily from the fact that $\alpha_j \leq (p-1)(p^{t-1} + p^{t-2}) + 1$ for all $1 \leq j \leq m$ and $\beta_i = p^t - 1$ for all $1 \leq i \leq n$. □

The proof of Theorem 2.2 also extends to fields of characteristic zero, but the results here are most interesting for $n \times n$ matrices.

Theorem 2.9 *Let F be a field of characteristic zero, and let $A \in \mathcal{M}_{n\times n}(F)$. If $P_k(A) \neq 0$, then A is k-pliant.*

The following corollary follows immediately from the above theorem. This corollary also has an elementary combinatorial proof.

Corollary 2.10 *Let F be a field of characteristic zero, and let $A \in \mathcal{M}_{n\times n}(F)$ be nonnegative. If $perm(A) \neq 0$, then A is k-pliant for any $k \geq 0$.*

Now, we will proceed with the proofs of this section. First we will prove two lemmas and then we will use these lemmas to prove the main theorem.

We define $\mathcal{T}_n^k$ to be the set of all $n \times n$ matrices with nonnegative integer entries and with the additional property that the entries in each row and column sum to k.

Lemma 2.11 *If $A = (a_{ij}) \in \mathcal{M}_{n\times n}(F)$ then*

$$P_k(A) = (k!)^n \sum_{(t_{ij})\in\mathcal{T}_n^k} \prod_{1\leq i,j\leq n} \frac{(a_{ij})^{t_{ij}}}{t_{ij}!}$$

Proof: Let

$$B = (b_{gh}) = \begin{bmatrix} a_{11}J_k & \dots & a_{1n}J_k \\ \vdots & \cdot & \vdots \\ a_{n1}J_k & \dots & a_{nn}J_k \end{bmatrix}$$

By definition, $P_k(A) = 1/(k!)^n perm(B)$. Consider the terms in the expansion of $perm(B)$. All of the terms in this expansion are of the form $a_{11}^{t_{11}} \dots a_{1n}^{t_{1n}} a_{21}^{t_{21}} \dots a_{nn}^{t_{nn}}$ for some $(t_{ij}) \in \mathcal{T}_n^k$. Now, for a fixed $(t_{ij}) \in \mathcal{T}_n^k$, we will count the number of times the term $a_{11}^{t_{11}} \dots a_{1n}^{t_{1n}} a_{21}^{t_{21}} \dots a_{nn}^{t_{nn}}$ appears in this expansion. In other words, we will count the number of ways we can choose an $nk \times nk$ permutation matrix $R = (r_{gh})$ such that $\prod_{1\leq g,h\leq nk}(b_{gh})^{r_{gh}} = a_{11}^{t_{11}} \dots a_{1n}^{t_{1n}} a_{21}^{t_{21}} \dots a_{nn}^{t_{nn}}$. To do this, we will choose the permutation matrix in stages. First, we will choose for each column h the a_{ij} such that $\prod_{1\leq g\leq nk}(b_{gh})^{r_{gh}} = a_{ij}$. This can be done in $\prod_{j=1}^n \binom{k}{t_{1j}, t_{2j}, \dots, t_{nj}}$ ways. Now, independently we may choose for each row g the a_{ij} such that $\prod_{1\leq h\leq nk}(b_{gh})^{r_{gh}} = a_{ij}$. This can be done in $\prod_{i=1}^n \binom{k}{t_{i1}, t_{i2}, \dots, t_{in}}$ ways. Now, for each a_{ij}, we have chosen a $t_{ij} \times t_{ij}$ submatrix of the $a_{ij}I_k$ submatrix of B, and we need to choose exactly one element from each row and column of these submatrices to specify the permutation matrix completely. This gives us an additional factor of $\prod_{1\leq i,j\leq n} t_{ij}!$. Thus, the term $a_{11}^{t_{11}} \dots a_{1n}^{t_{1n}} a_{21}^{t_{21}} \dots a_{nn}^{t_{nn}}$ occurs exactly $(k!)^{2n} \prod_{1\leq i,j\leq n} 1/t_{ij}!$ ways, which completes the proof. $\square$

For every sequence of nonnegative integers $\gamma = (\gamma_1, \ldots, \gamma_n)$, and any $n \times m$ matrix $A = (a_{ij})$, we define the polynomial

$$\Theta_{\gamma,A} = \Theta_{\gamma,A}(z_1, \ldots, z_m) = \prod_{i=1}^{n}(a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{im}z_m)^{\gamma_i}$$

Lemma 2.12 *Let F be a field of characteristic p, and let $A \in \mathcal{M}_{n\times n}(F)$. Let k be an integer, and assume that either $p = 0$ or $k < p$. Then, if $\gamma = (k, k, \ldots, k) \in Z^n$, we have $[\Theta_{\gamma,A}]_{z_1^k z_2^k \ldots z_n^k} = P_k(A)$.*

Proof: For $1 \le i \le n$, we have that $q_i = (a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{im}z_m)^k$ is a homogeneous polynomial of degree k. If $d_1, \ldots, d_n$ are nonnegative integers and $\sum_{i=1}^{n} d_i = k$, then the coefficient of $z_1^{d_1} z_2^{d_2} \ldots z_n^{d_n}$ in the expansion of q_i is precisely $\binom{k}{d_1, d_2, \ldots, d_n} a_{i1}^{d_1} a_{i2}^{d_2} \ldots a_{im}^{d_m}$. Thus, we can expand $[\Theta_{\gamma,A}]_{z_1^k \ldots z_n^k}$ as follows:

$$[\Theta_{\gamma,A}]_{z_1^k \ldots z_n^k} = \sum_{(t_{ij})\in \mathcal{T}_n^k} \prod_{i=1}^{n} \binom{k}{t_{i1}, t_{i2}, \ldots, t_{in}} (a_{i1}^{t_{i1}} a_{i2}^{t_{i2}} \ldots a_{im}^{t_{im}}) = P_k(A)$$

□

Proof of Theorem 2.2: Let F be a field of characteristic $p > 0$, let $A \in \mathcal{M}_{n\times m}(F)$, let $w_0, \ldots, w_t \in \{0, \ldots, p-1\}$, and let $I_0, \ldots, I_t \subseteq \{1, \ldots, n\}$, $J_0, \ldots, J_t \subseteq \{1, \ldots, m\}$ be such that $|I_k| = |J_k|$ and $P_{w_k}(A[I_k|J_k]) \ne 0$ for all $0 \le k \le t$. Now, define $\alpha = \sum_{k=0}^{t}(w_k p^k)\chi_{J_k}^m$ and $\beta = \sum_{k=0}^{t}(w_k p^k)\chi_{I_k}^n$. Next, let $X_1, \ldots, X_m \subseteq F$ and $Y_1, \ldots, Y_n \subseteq F$ be given, and assume that $|X_j| \ge \alpha_j + 1$ for all $1 \le j \le m$ and that $|Y_i| = \beta_i$ for all $1 \le i \le n$. It will suffice to show that there exists $x \in X_1 \times X_2 \times \ldots \times X_m$ and $y \in (F \setminus Y_1) \times (F \setminus Y_2) \times \ldots \times (F \setminus Y_n)$ such that $Ax = y$. Next we define a polynomial:

$$\eta = \eta(z_1, \ldots, z_m) = \prod_{i=1}^{n} \prod_{u\in Y_i} (a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{im}z_m - u)$$

Now, observe that η is not identically zero on $X_1 \times X_2 \times \ldots \times X_m$ if and only if there exists $x \in X_1 \times X_2 \times \ldots \times X_m$ and $y \in (F \setminus Y_1) \times (F \setminus Y_2) \times \ldots \times (F \setminus Y_n)$ such that $Ax = y$. Since $deg(\eta) = \sum_{i=1}^{n} \beta_i = \sum_{j=1}^{m} \alpha_j$, by Theorem 1, it is enough to prove that $[\eta]_{z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m}} \ne 0$. Now, observe that since $z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m}$ is a term of top degree, we have that $[\eta]_{z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m}} = [\Theta_{\beta,A}]_{z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m}}$. By this equation, and by our hypothesis, to prove the theorem, it will suffice to prove the following claim:

Claim:

$$[\Theta_{\beta,A}]_{z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}} = \prod_{k=0}^{t}(P_{w_k}(A[I_k|J_k]))^{p^k}$$

We will prove the claim by induction on t. If $t=-1$, we have

$$[\Theta_{\beta,A}]_{z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}} = 1 = \prod_{k=0}^{t}(P_{w_k}(A[I_k|J_k]))^{p^k}$$

For the general case, let $\ell = |I_t| = |J_t|$. For convenience, we will assume (without loss) that $J_t = \{1,\ldots,\ell\}$. Let $\alpha' = \alpha - (w_t p^t)\chi^m_{J_t}$, and let $\beta' = \beta - (w_t p^t)\chi^n_{I_t}$. Then we have

$$[\Theta_{\beta,A}]_{z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}} = [\Theta_{\beta',A}\prod_{i\in I_t}(a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{im}z_m)^{w_t p^t}]_{z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}}$$

Now, consider the monomials in the expansion of $q = \prod_{i\in I_t}(a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{im}z_m)^{w_t p^t}$. Since F is a field of characteristic p, the degree of z_j in a monomial in the expansion of q will be a multiple of p^t. Since $\sum_{k=0}^{t-1} w_k p^k < p^t$, and $(\alpha_1,\ldots,\alpha_m) = \sum_{k=1}^{t}(w_k p^k)\chi^m_{J_k}$, the only monomial in the expansion of q which can contribute to the coefficient of $z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}$ is $\prod_{j\in J_t} z_j^{w_t p^t} = z_1^{w_t p^t} z_2^{w_t p^t}\ldots z_\ell^{w_t p^t}$. Let $\gamma = (w_t, w_t, \ldots, w_t) \in Z^\ell$, then

$$\begin{aligned}
[\Theta_{\beta,A}]_{z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_m^{\alpha_m}} &= [\Theta_{\beta',A}]_{z_1^{\alpha'_1}z_2^{\alpha'_2}\ldots z_m^{\alpha'_m}}[\prod_{i\in I_t}(a_{i1}z_1+\ldots+a_{im}z_m)^{w_t p^t}]_{z_1^{w_t p^t}z_2^{w_t p^t}\ldots z_\ell^{w_t p^t}} \\
&= \prod_{k=0}^{t-1}(P_{w_k}(A[I_k|J_k]))^{p^k}([\prod_{i\in I_t}(a_{i1}z_1+\ldots+a_{i\ell}z_\ell)^{w_t}]_{z_1^{w_t}z_2^{w_t}\ldots z_\ell^{w_t}})^{p^t} \\
&= \prod_{k=0}^{t-1}(P_{w_k}(A[I_k|J_k]))^{p^k}([\Theta_{\gamma,A[I_t|J_t]}]_{z_1^{w_t}\ldots z_\ell^{w_t}})^{p^t} \\
&= \prod_{k=0}^{t-1}(P_{w_k}(A[I_k|J_k]))^{p^k}(P_{w_t}(A[I_t|J_t]))^{p^t} = \prod_{k=0}^{t}(P_{w_k}(A[I_k|J_k]))^{p^k}
\end{aligned}$$

□

3 Relating Generalized Permanents

Let p be a prime, and let $W \in \mathcal{M}_{n\times n}(Z_p)$ be an invertible matrix. Then it is clear that W^{-1} is k-pliant if and only if W is $(p-1-k)$-pliant. Thus, it is natural to ask whether $P_k(W)$ and $P_{p-1-k}(W^{-1})$ are related. Indeed, this is the case. Our main theorem of this section is the following:

Theorem 3.1 *Let F be a field of characteristic $p > 0$, and let $W \in \mathcal{M}_{n\times n}(F)$ be invertible. Then*

$$P_k(W^{-1}) = \frac{P_{p-1-k}(W)}{det(W)^{p-1}}$$

To prove our main theorem, we will need to consider another permanent-type function $\mathbf{p}(\cdot)$. Matrices which evaluate to a nonzero element under $\mathbf{p}(\cdot)$ are of independent interest, so we will mention a couple of conjectures concerning them.

For convenience, we will frequently use curly braces to help define our matrices. These braces will always have the obvious connotation. If $A \in \mathcal{M}_{n\times(p-1)n}(F)$, let

$$\mathbf{p}(A) = (-1)^n \; perm \left.\begin{bmatrix} A \\ A \\ \vdots \\ A \end{bmatrix}\right\} p-1$$

Note that if $W \in \mathcal{M}_{n\times n}(F)$, then since $(-1)^n = 1/(p-1)!^n$, we have that $\mathbf{p}[\underbrace{W \dots W}_{p-1}] = P_{p-1}(W)$.

Alon, Linial, and Meshulam have made the following conjecture, which would imply Conjecture 1.4 (with $c(p) = p$) via the polynomial technique of the combinatorial nullstellensatz. Actually, this conjecture would also imply the stronger statement that if $W_1, \dots, W_p \in \mathcal{M}_{n\times n}(Z_p)$ are invertible, then $[W_1 W_2 \dots W_p]$ is $(2, p-1)$-pliant.

Conjecture 3.2 (Alon, Linial, Meshulam [3]) *Let $A = [W_1 W_2 \dots W_p] \in \mathcal{M}_{n\times pn}(Z_p)$, and assume that W_i is invertible for $1 \le i \le p$. Then there exists a $n \times (p-1)n$ submatrix B of A such that $\mathbf{p}(B) \neq 0$.*

Jeff Kahn has made the following conjecture about permanents, which would imply Conjecture 1.2:

Conjecture 3.3 (Kahn [11]) *Let F be an arbitrary field, and let $W \in \mathcal{M}_{n\times n}(F)$ be invertible. Then there is an $n \times n$ submatrix W' of $[WW]$ such that $perm(W') \neq 0$.*

The following conjecture seems to be a natural extension of Conjecture 3.2. If true, this conjecture would imply that if $|F| = p^c$ and $W_1, \ldots, W_p \in \mathcal{M}_{n\times n}(F)$ are invertible, then $[W_1 W_2 \ldots W_p]$ is $(p^{c-1}+1, p^c-1)$-pliant. This conjecture would also imply Kahn's Conjecture 3.3 for finite fields (apply to $[W^\top W^\top I_n \ldots I_n]$).

Conjecture 3.4 *Let F be a field of characteristic $p > 0$, and let $A = [W_1 W_2 \ldots W_p] \in \mathcal{M}_{n\times pn}(F)$. If W_i is invertible for $1 \le i \le p$, then we may partition the columns of A into two matricies $B \in \mathcal{M}_{n\times(p-1)n}(F)$ and $V \in \mathcal{M}_{n\times n}(F)$ so that $\mathbf{p}(B) \neq 0 \neq det(V)$.*

Now, we will proceed with the proofs of this section. First, we will prove a simple lemma concerning permanents of matrices over finite fields. We will use this lemma to prove Lemma 2.6. Then, we will use Lemma 2.6 to prove a theorem which gives us a change of basis formula for $\mathbf{p}(\cdot)$. Finally, we will apply this theorem to give the main result, Theorem 3.1. Throughout the rest of this section, F will always be a field of characteristic $p > 0$.

Lemma 3.5 *Let $A = (a_{ij}) \in \mathcal{M}_{n\times n}(F)$. If A has p columns which are identical, then $perm(A) = 0$.*

This lemma is a simple fact which has been observed by several authors. We include the proof here for the sake of completeness.

Proof: We assume that the last p columns of A are identical, and let $J = \{1, \ldots, n-p\}$. If we expand the last p columns of A, we have

$$perm(A) = \sum_{I\subseteq\{1,\ldots,n\};|I|=n-p} perm(A[I|J])\,(p!) \prod_{i\in\{1,\ldots,n\}\setminus I} (a_{in}) = 0$$

$\square$

Proof of Lemma 2.6: Let $W = (w_{ij}) \in \mathcal{M}_{n\times n}(F)$ be given. If $A \in \mathcal{M}_{n\times n}(F)$, then $perm(A)$ is a multilinear function with respect to the columns of A, and $perm(A)$ vanishes if A has p identical columns. Thus, if A has a set of $p-1$ identical columns, adding a multiple of one of these columns to a column of A outside this set, gives us a new matrix A' such that $perm(A') = perm(A)$. We will call this a characteristic p column operation. Now, we may choose a matrix $C = (c_{ij}) \in \mathcal{M}_{n\times n}(F)$ such that W may be transformed into C by (ordinary) elementary column operations and such that CR is lower triangular for some permutation matrix R. Then, by characteristic p column operations (each operation we perform to a column is performed on all $p-1$ copies of it), we have

$$\begin{aligned} P_{p-1}(W) &= \frac{1}{(p-1)!^n}\, perm \begin{bmatrix} w_{11}J_{p-1} & \dots & w_{1n}J_{p-1} \\ \vdots & . & \vdots \\ w_{n1}J_{p-1} & \dots & w_{nn}J_{p-1} \end{bmatrix} \\ &= \frac{1}{(p-1)!^n}\, perm \begin{bmatrix} c_{11}J_{p-1} & \dots & c_{1n}J_{p-1} \\ \vdots & . & \vdots \\ c_{n1}J_{p-1} & \dots & c_{nn}J_{p-1} \end{bmatrix} \\ &= det(C)^{p-1} = det(W)^{p-1} \end{aligned}$$

□

Theorem 3.6 *Let $A \in \mathcal{M}_{n\times(p-1)n}(F)$, and let $W \in \mathcal{M}_{n\times n}(F)$ be given. Then $\mathbf{p}(WA) = det(W)^{p-1}\mathbf{p}(A)$.*

Proof: Since both sides of the equation $\mathbf{p}(WA) = det(W)^{p-1}\mathbf{p}(A)$ are multilinear in the columns of A, it will suffice to prove the theorem in the case when A is a 0,1 matrix, and each column of A contains exactly one entry which is a 1. If we can permute the columns of A to obtain the matrix $[I_nI_n\dots I_n]$, then

$$\mathbf{p}(WA) = \mathbf{p}([WW\dots W]) = P_{p-1}(W) = det(W)^{p-1}P_{p-1}(I_n) = det(W)^{p-1}\mathbf{p}(A)$$

Otherwise, A must have one column which occurs p times, so we find $\mathbf{p}(WA) = 0 = det(W)^{p-1}\mathbf{p}(A)$. □

Lemma 3.7 *if $W = (w_{ij}) \in \mathcal{M}_{n\times n}(F)$, then $\mathbf{p}[\underbrace{I_n\dots I_n}_{p-1-k}\underbrace{W\dots W}_{k}] = P_k(W)$.*

Proof: Let J' denote the $(p-1)\times(p-1-k)$ matrix of ones, and let J'' denote the $(p-1)\times k$ matrix of ones. Then the matrix

$$\left.\begin{bmatrix} I_n & \dots & I_n & W & \dots & W \\ \vdots & . & \vdots & \vdots & . & \vdots \\ \underbrace{I_n \quad \dots \quad I_n}_{p-1-k} & & & \underbrace{W \quad \dots \quad W}_{k} & & \end{bmatrix}\right\} p-1$$

may be transformed into the following matrix by permuting rows and columns

$$A = \begin{bmatrix} J' & & & 0 & w_{11}J'' & w_{12}J'' & \dots & w_{1n}J'' \\ & J' & & & w_{21}J'' & w_{22}J'' & \dots & w_{2n}J'' \\ & & \ddots & & \vdots & \vdots & . & \vdots \\ 0 & & & J' & w_{n1}J'' & w_{n2}J'' & \dots & w_{nn}J'' \end{bmatrix}$$

It follows that $\mathbf{p}[\underbrace{I_n \dots I_n}_{p-1-k} \underbrace{W \dots W}_{k}] = (-1)^n perm(A)$. If we expand $perm(A)$ along the first $p-1-k$ columns, we find that $perm(A) = (p-1)(p-2)\dots(k+1)perm(A')$, where A' is the matrix obtained from A by deleting the first $p-1-k$ rows and deleting the first $p-1-k$ columns. Repeating this operation, until the first $n(p-1-k)$ columns are deleted, we find that

$$perm(A) = ((p-1)(p-2)\dots(k+1))^n perm \begin{bmatrix} w_{11}J_k & \dots & w_{1n}J_k \\ \vdots & . & \vdots \\ w_{n1}J_k & \dots & w_{nn}J_k \end{bmatrix}$$

Thus, we have:

$$\mathbf{p}[\underbrace{I_n \dots I_n}_{p-1-k} \underbrace{W \dots W}_{k}] = (-1)^n perm(A) = \frac{1}{(p-1)!^n} perm(A) = P_k(W)$$

□

Proof of Theorem 3.1: Let $W \in \mathcal{M}_{n\times n}(F)$ be invertible. Then

$$\begin{aligned} P_{p-1-k}(W) &= \mathbf{p}[\underbrace{I_n \dots I_n}_{k} \underbrace{W \dots W}_{p-1-k}] \\ &= det(W)^{p-1}\mathbf{p}[\underbrace{W^{-1} \dots W^{-1}}_{k} \underbrace{I_n \dots I_n}_{p-1-k}] \\ &= det(W)^{p-1} P_k(W^{-1}) \end{aligned}$$

□

The following corollary was first proved by G. Kogan and J.A. Makowsky ([9]). It is also a special case of a theorem of Yang Yu ([11]). It follows immediately from the preceding theorem, since $perm(W) = P_1(W)$.

Corollary 3.8 (Kogan and Makowsky [9]) *Let F be a field of characteristic 3, and let $W \in \mathcal{M}_{n\times n}(F)$ be invertible. Then $perm(W^{-1}) = perm(W)/det(W)^2$.*

4 Z_p^k Flows in Graphs

In this section, we will apply two of our corollaries to the main theorem to prove generalizations of Jaeger's 4-flow and 8-flow theorems (see [7]). We will follow Jaeger's original proofs by constructing trees whose edge sets have empty intersection. However, instead of using these trees to route a flow, we will use them to apply a suitable corollary of our main theorem.

Theorem 4.1 *Let p be a prime, let G be a directed 3-edge-connected graph, and for every $e \in E(G)$, let $\ell_e \subseteq Z_p^k$, with $|\ell_e| \geq (p-1)(p^{k-1}+p^{k-2})+1$. Then, there exists a flow $\phi : E(G) \to Z_p^k$ such that $\phi(e) \in \ell_e$ for all $e \in E(G)$.*

Theorem 4.1 does not appear to be very sharp in general, but for $p = 2$, this theorem is tight for $k \geq 2$, and for any cubic graph H which is 3-edge-connected and not 3-edge-colorable. More precisely, for any such cubic graph H, and any $k \geq 2$, there exists an assignment of lists $\ell_e \subseteq Z_2^k$ to each edge $e \in E(H)$ such that $|\ell_e| = 2^{k-1}+2^{k-2}$ and such that no flow $\phi : E(H) \to Z_2^k$ can satisfy $\phi(e) \in \ell_e$ for all $e \in E(H)$. The construction is as follows: let $L \subseteq Z_2^k$ be the set of all vectors $v = (v_1, \ldots, v_k) \in Z_2^k$ such that $v_1 = 1$ or $v_2 = 1$, and let $\ell_e = L$ for all $e \in E(H)$. Then, $|\ell_e| = 2^{k-1}+2^{k-2}$ for all $e \in E(H)$. Now, for any flow $\phi : E(H) \to Z_2^k$, the restriction of ϕ to the first 2 coordinates of Z_2^k is also a flow. Since H does not have a nowhere zero $Z_2 \times Z_2$ flow, for some edge $e \in E(H)$, we must have $\phi(e) \notin L = \ell_e$.

Proof of Theorem 4.1: Since the additive group of $F = GF(p^k)$ is isomorphic to Z_p^k, we may work in F. Thus, we will consider $\ell_e \subseteq F$ for all $e \in E(G)$, and we will construct a flow $\phi : E(G) \to F$. Choose $u \in V(G)$ and let A be the matrix obtained from the $V(G) \times E(G)$ incidence matrix of G by deleting the row corresponding to u.

Now, consider the graph G' obtained by doubling every edge of G. This graph is 6-edge-connected, so by a theorem of Nash-Williams ([10]), we may choose 3 edge-disjoint spanning trees T_1', T_2', T_3' of G'. Let T_1, T_2, T_3 denote the corresponding trees in G. Now, $A[V(G) \setminus \{u\}|E(T_i)]$ is invertible for $i = 1, 2, 3$ and $E(T_1) \cap E(T_2) \cap E(T_3) = \emptyset$. Thus, by Corollary 2.8, we have that A is $((p-1)(p^{k-1}+p^{k-2})+1, p^k-1)$-pliant. Thus, we may choose a vector $x \in F^{E(G)}$ such that $x_e \in \ell_e$ for all $e \in E(G)$ and such that $Ax = 0$. Define $\phi(e) = x_e$

for all $e \in E(G)$. For all $v \in V(G) \setminus \{u\}$, we have that $\sum_{e\in\delta^+(v)} \phi(e) - \sum_{e\in\delta^-(v)} \phi(e) = 0$. It follows that this condition also holds at u, and we conclude that ϕ is a flow. $\square$

Proof of Corollary 1.6: Set $p = 2$ in the above theorem. $\square$

Theorem 4.2 *Let p be a prime, let G be a directed 4-edge-connected graph, and for every $e \in E(G)$, let $\ell_e \subseteq Z_p^k$, with $|\ell_e| \geq (p-1)p^{k-1} + 1$. Then, there exists a flow $\phi : E(G) \to Z_p^k$ such that $\phi(e) \in \ell_e$ for all $e \in E(G)$.*

Again, this theorem does not seem to be very tight for general p, but for $p = 2$, the theorem is tight in a very strong sense. Indeed, for $p = 2$, for any $k \geq 1$, and for any graph H with at least one non-loop edge, there is an assignment $\ell_e \subseteq Z_2^k$ for every edge $e \in E(H)$ such that $|\ell_e| = 2^{k-1}$ for every $e \in E(H)$, and such that no flow $\phi : E(H) \to Z_2^k$ can satisfy $\phi(e) \in \ell_e$ for all $e \in E(H)$. The construction is as follows: let L_0 denote the set of all vectors $v = (v_1, \ldots, v_k) \in Z_2^k$ such that $v_1 = 0$, and let L_1 denote the set of all vectors $v = (v_1, \ldots, v_k) \in Z_2^k$ such that $v_1 = 1$. Choose a non-loop edge $f \in E(H)$ and let $\ell_f = L_1$. For all other edges $e \in E(H) \setminus \{f\}$, let $\ell_e = L_0$. Now, for any flow $\phi : E(H) \to Z_2^k$, the restriction of ϕ to the first coordinate of Z_2^k is a flow. It follows that $\phi(e) \notin \ell_e$ for some $e \in E(H)$.

Proof of Theorem 4.2: The proof of this theorem is essentially the same as that of the preceeding theorem, so we will only mention the differences. Since G is 4-edge-connected, we may choose 2 edge-disjoint spanning trees, T_1, T_2 of G. In the truncated adjacency matrix A, we will then have $A[V(G) \setminus \{u\}|E(T_i)]$ invertible for $i = 1, 2$. Since $E(T_1) \cap E(T_2) = \emptyset$, we may apply corollary 2.7 and proceed as above. $\square$

Proof of Corollary 1.5: Set $p = 2$ in the above theorem. $\square$

Acknowledgement

The author thanks Noga Alon and Paul Seymour for enlightening discussions.

References

[1] N. Alon, *Combinarorial Nullstellensatz*, Combinatorics, Probability, Comput., 8 (1999), no. 1-2, 7-29.

[2] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, in: "Combinatorics, Paul Erdös is Eighty", Bolyai Society, Mathematical Studies, Keszthely, Hungary, 1993, 33-50.

[3] N. Alon, N. Linial and R. Meshulam, *Additive bases of vector spaces over prime fields*, J. Combinatorial Theory Ser. A 57 (1991), 203-210.

[4] N. Alon and M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica 9 (1989), 393-395.

[5] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica 12 (1992), 125-134.

[6] J. Edmonds, *Minimum partition of a matroid into independent subsets*, J. Res. Nat. Bur. Standards 69B (1965), 67-72.

[7] F. Jaeger, *Flows and generalized coloring theorems in graphs*, J. Combinatorial Theory Ser. B 26 (1979), 205-216.

[8] F. Jaeger, N. Linial, C. Payan and M. Tarsi, *Group connectivity of graphs- a nonhomogeneous analogue of nowhere-zero flow*, J. Combinatorial Theory Ser. B 56 (1992), 165-182.

[9] G. Kogan and J.A. Makowsky, *Computing permanents over fields of characteristic 3: Where and why it becomes difficult*, Computational Complexity, to appear.

[10] C.S.J.A. Nash-Williams, *Edge disjoint spanning trees of finite graphs*, J. London Math. Soc. 36 (1961), 445-450.

[11] Yang Yu, *The permanent rank of a matrix*, J. Combinatorial Theory Ser. A 85 (1999), 237-242.