DEGREES OF HIGH-DIMENSIONAL SUBVARIETIES OF DETERMINANTAL VARIETIES

B.A. SETHURAMAN

Abstract. Let $n = p^a b$, where p is a prime, and g.c.d.$(p, b) = 1$. In $\mathbf{P}^{n^2-1}$, let X_r be the variety defined by $\mathrm{rank}((x_{i,j})) \leq n - r$. We show that any subvariety of X_r of codimension less than $p^a r$ must have degree a multiple of p. We also show that the bounds on the codimension in our results are strict by exhibiting subvarieties of the appropriate codimension whose degrees are prime to p.

1. Introduction.

This note is motivated by the following question, which arose rather naturally in some investigations into the structure of division algebras with involution: Let n be a power of 2, $n > 1$. In $\mathbf{P}^{n^2-1}$, let X be the hypersurface defined by $\det((x_{i,j})) = 0$. Does X contain a subvariety of *odd* degree whose codimension (in $\mathbf{P}^{n^2-1}$) is *less* than n?

It is known that for any n, the minimum codimension of any linear subvariety of X is n (see [5, Chapter 2], for instance), our question is thus a natural generalization when n is a power of 2.

We show here that the answer to the question is negative. In fact, we show that for any prime p and for any n a power of p ($n > 1$), if V is any subvariety of the hypersurface X of codimension less than n, then the degree of V must be divisible by p. More generally, we show that if X_r is the variety defined by $\mathrm{rank}((x_{i,j})) \leq n-r$, and if $n = p^a b$, with g.c.d.$(p, b) = 1$, then any subvariety of X_r of codimension less than $p^a r$ must have degree a multiple of p. We also show that the bounds on the codimension in our results are strict by exhibiting subvarieties of the appropriate codimension whose degrees are prime to p.

Our proof is based on the following (see [1, Example 13.1(b)]): Let F be a field such that all its finite field extensions have degree a power of p for some prime p, and let K be its algebraic closure. If V and W are two irreducible subvarieties of $\mathbf{P}^m_K$ defined over F such that $\dim(V) + \dim(W) \geq m$ and g.c.d.$(p, \deg(V)\deg(W)) = 1$, then $V \cap W$ has an F-rational point.

We wish to thank Bill Watkins for some very useful conversations, and Bob Guralnick for bringing to our attention the paper [G]. We also wish to point out that David Saltman has an alternative proof of Theorem 1 below. Finally, the original question (see above) that motivated this paper arose while the author was visiting Tata Institute of Fundamental Research in Bombay, India, and we wish to thank the School of Mathematics there for its generous hospitality.

1991 *Mathematics Subject Classification.* Primary 14M12.
Key words and phrases. Determinantal Varieties, Degree.
Supported in part by an N.S.F. grant.

2. The prime-power case.

The case where n is a prime-power is simpler than the more general case, and we consider this first.

Theorem 1. *Let K be an algebraically closed field, and let n be a power of a prime p, say $n = p^a$ $(a > 0)$. In $\mathbf{P}_K^{n^2-1}$, let X_r be the variety of matrices of rank at most $n - r$ $(r = 1, 2, \ldots, n-1)$. Let V be any subvariety of X_r whose codimension (in $\mathbf{P}_K^{n^2-1}$) is less than nr. Then the degree of V must be divisible by p.*

Proof. Assume that X_r contains a subvariety V whose codimension is less than nr and whose degree is prime to p. It is well-known that the degree of a projective variety V is just the sum of the degrees of its irreducible components of the same dimension as V (this follows, for instance, from an easy modification of the proof of [4, Prop. 7.6(b)]). Hence at least one irreducible component of V of the same dimension as V must have degree prime to p. In what follows, we will replace V by this irreducible component.

Let X be a transcendence base for K/P, where P is the prime field of K. Let E_0 be the inseparable closure of $P(X)$ in K, and let E_1 be the fixed field of any p-sylow subgroup of $\mathrm{Gal}(K/E_0)$. (Every finite extension of E_1 thus has degree a power of p.) Let E be the field extension of E_1 obtained by adjoining the coefficients of any finite generating set of the ideal of V in $K[x_0, x_1, \ldots, x_{n^2-1}]$. Since there are only finitely many coefficients, E/E_1 is a finite extension, and V is defined over E.

We claim that E has a cyclic extension of degree p^a. For, let $[E : E_1] = p^t$. It is well known that P has cyclic extensions of any degree, so let L_0 be any cyclic extension of P of degree p^{a+t}. Since $P(X)/P$ is purely transcendental, $E_0/P(X)$ is purely inseparable, and E_1/E_0 is a compositum of extensions of degree prime to p, L_0 and E_1 are linearly disjoint over P, so $L_1 = L_0E_1$ is a cyclic extension of E_1 of degree p^{a+t}. Now let $L = L_1E$, so L is a Galois extension of E. The restriction map $r\colon \mathrm{Gal}(L/E) \to \mathrm{Gal}(L_1/E_1)$ is injective, since any element in the kernel must fix both L_1 and E. This shows that L/E is cyclic. The image has fixed field $E \cap L_1$, and since $[E \cap L_1 : E_1] \leq [E : L_1] = p^t$, we find that $[L : E] = |r(\mathrm{Gal}(L/E))| \geq p^a$. It is clear then that L has a subextension that is cyclic over E of degree exactly p^a.

Abusing notation, write L for any cyclic extension of E of degree p^a, and write $M_n(E)$ as $\overset{n-1}{\underset{i=0}{\oplus}} Lu^i$, where conjugation by the powers of u induces $\mathrm{Gal}(L/E)$ on L and $u^n = 1$. By [G, Lemma 3.2], every non-zero matrix in the E-subspace $W = \overset{r-1}{\underset{i=0}{\oplus}} Lu^i$ has rank greater than $n - r$. (This generalizes the $r = 1$ statement that the matrices arising from the non-zero elements of K are invertible.) Also, W has dimension nr. Write W' for the linear subvariety of $\mathbf{P}_K^{n^2-1}$ corresponding to $W \otimes_E K$. W' is of dimension $nr - 1$. Since V and W' are irreducible, [1, Example 13.1(b)] shows that $V \cap W'$ must have an E-rational point. But the E-rational points of W' are precisely those that arise from non-zero elements of the E-space W. This is a contradiction, since the non-zero elements of W all have rank greater than $n - r$. □

3. The general case.

The case where n is not a power of a prime needs a more careful analysis of the question of existence of subspaces of matrix algebras of a given dimension and large minimal rank.

We first prove an elementary lemma.

Lemma 2. *Let Y be an irreducible variety in $\mathbf{P}^n_K$, where K is some algebraically closed field. Let s be a new indeterminate, and let F denote the algebraic closure of $K(s)$. Then, the closed set Y' in $\mathbf{P}^n_F$ consisting of all points with coordinates in F that satisfy the same equations as Y is an irreducible variety of the same degree and dimension as Y.*

Proof. (Sketch.) Let $I \lhd K[x_0, \ldots, x_n]$ be the ideal of Y. It is sufficient to show that IF ($= I \otimes_K F$) is a prime ideal of $F[x_0, \ldots, x_n]$. For, if this holds, then it is immediate that IF is the ideal of Y', so Y' will be irreducible. Moreover, the isomorphism $F[x_0, \ldots, x_n]/IF \cong K[x_0, \ldots, x_n]/I \otimes_K F$ shows that the F-dimension of the homogeneous subspaces of $F[x_0, \ldots, x_n]/IF$ of a given degree will be the same as the K-dimension of the corresponding homogeneous subspaces of $K[x_0, \ldots, x_n]/I$, so the Hilbert polynomials of Y and Y' will coincide.

It is sufficient to show that $K[x_0, \ldots, x_n]/I \otimes_K F$ is a domain. By Noether Normalization, $K[x_0, \ldots, x_n]/I$ is integral over the (polynomial) ring generated by some linear combination of the x_i, so $K[x_0, \ldots, x_n]/I$ is contained in the algebraic closure of $K(x_0, ..., x_n)$. It is thus sufficient to show that the algebraic closure of $K(x_0, ..., x_n)$ and the algebraic closure of $K(s)$ are linearly disjoint over K, but this is well known. □

We are now ready to prove our theorem.

Theorem 3. *Let K be an algebraically closed field. Let $n = p^a b$, where g.c.d.$(p, b) = 1$, $a > 0$, $b > 1$. Let V be a subvariety of X_r ($r = 1, 2, \ldots, p^a - 1$), whose codimension in $\mathbf{P}^{n^2-1}_K$ is less than $p^a r$. Then the degree of V must be divisible by p. (In particular, the degree of any subvariety of $X = X_1$ whose codimension is smaller than p^a must be divisible by p.)*

Note: The codimension of X_r is r^2 ([3, Prop. 12.2]), so when $r \geq p^a$, X_r cannot have a subvariety whose codimension less than $p^a r$.

Proof. Assume that X_r has a subvariety V of codimension less than $p^a r$ whose degree is prime to p. As in the beginning of the proof of Theorem 1, we may replace V by an irreducible component of the same dimension whose degree is also prime to p. Further, if K is the algebraic closure of a finite field, Lemma 2 shows that the degrees and dimensions of V and X_r will not change if we extend scalars to the algebraic closure of $K(s)$, where s is a new indeterminate. Thus, in the positive characteristic case, we may assume that K has positive transcendence degree over its prime field P.

Now let X be a transcendence base for K/P, and let E_0, E_1, and E be as in the proof of Theorem 1. We will show that $M_n(E)$ has an E-subspace W of dimension $p^a r$, all of whose non-zero elements have rank greater than $n - r$. Assuming the existence of such a subspace, the rest of the proof is exactly as in Theorem 1: W', the linear variety in $\mathbf{P}^n_K$ corresponding to $W \otimes_E K$, must intersect V in an E-rational point, but such a rational point must come from some non-zero element of

W, contradicting the fact that every non-zero element of W has rank greater than $n - r$.

Now for the existence of W. At its core, the idea is similar to [G, Lemma 3.2], but we need to work harder to set things up since E does not possess any field extensions (let alone cyclic extensions) of degree n.

As in the proof of Theorem 1, let $[E : E_1] = p^t$. Let L be an extension of $P(X)$ that is Galois over $P(x)$ with Galois group $\mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \cdots \times \mathbb{Z}/p^a\mathbb{Z}$, where there $1 + t$ factors of the form $\mathbb{Z}/p^a\mathbb{Z}$. In the case $P = \mathbb{Q}$, it is well known that $\mathbb{Q}$ has such an extension, and since $\mathbb{Q}(X)/\mathbb{Q}$ is purely transcendental, $\mathbb{Q}(X)$ also has such an extension. In the positive characteristic case, note that we have assumed that K/P has positive transcendence degree. It is also well known, and can be derived readily from the Grunwald-Wang theorem ([6, Theorem 32.18]), that the rational function in one variable over a finite field admits Galois extensions with any given finite abelian group. Thus, the existence of L is assured in all characteristics.

Let $L = L_0 \otimes_{P(X)} L_1 \otimes_{P(X)} \cdots \otimes_{P(X)} L_{1+t}$, where $L_0/P(X)$ has Galois group $\mathbb{Z}/b\mathbb{Z}$, and the remaining $L_i/P(X)$ have Galois group $\mathbb{Z}/p^a\mathbb{Z}$. Let $L_i = P(X)(\beta_i)$, and let f_i be the minimum polynomial of the β_i over $P(X)$. (Thus, f_0 is of degree b, while the remaining f_i have degree p^a.) We claim that for $i = 1, 2, \ldots, 1 + t$, at least one f_i must remain irreducible over E. For, assume that each such f_i factors non-trivially over E. Since each f_i factors into a product of linear factors over L_i, the coefficients of the factors of f_i over E must lie in L_i. Let $H_i \subseteq L_i$ be the field extension of $P(X)$ generated by the coefficients of the factors of f_i over E. The assumption that the factorization is non-trivial shows that H_i strictly contains $P(X)$. Since the L_i are linearly disjoint over $P(X)$, and since $[H_i : P(X)] \geq p$, the compositum $H = H_1 \cdot H_2 \cdots H_{1+t}$ is an extension of $P(X)$ of degree at least p^{1+t}. Since $E_0/P(X)$ is purely inseparable, and since E_1/E_0 is a compositum of prime to p extensions, the compositum $E_1 H$ is an extension of E_1 of degree at least p^{1+t}. Finally, since each $H_i \subseteq E$, we find $E_1 H \subseteq E$, a contradiction, as $[E : E_1] \geq p^t$.

Assume that f_1 remains irreducible over E, so $L_1 E$ is a field extension of E of degree p^a. In what follows, we will work with the field $L_0 \otimes_{P(X)} L_1$, which is cyclic of degree n over $P(X)$. We will abuse notation and write L for this field. We will denote a generator of $\mathrm{Gal}(L/P(X))$ by σ.

View L as embedded in $M_N(P(X))$, and write $M_n(P(X))$ as $\bigoplus_{i=0}^{n-1} L u^i$, where $u^n = 1$, and $ulu^{-1} = \sigma(l)$ for all $l \in L$. Let B be the matrix corresponding to the element β_0. Since $1, \beta_0, \ldots, \beta_0^{b-1}$ is a basis for L/L_1, the L_1 vector spaces $\{L_1 B^i u^j\}$ $(i = 0, 1, \ldots, b-1,\ j = 0, 1, \ldots, n-1)$ are L_1-linearly independent and span $M_n(P(X))$. That is, $M_n(P(X))$ is isomorphic to $\bigoplus_{i=0}^{b-1} \bigoplus_{j=0}^{n-1} L_1 B^i u^j$ as L_1 vector spaces.

Now consider $M_n(E) = M_n(P(X)) \otimes_{P(X)} E$. Since $L_1 B^i u^j \otimes_{P(X)} E$ is just $(L_1 \otimes_{P(X)} E) B^i u^j$, and since $L_1 \otimes_{P(X)} E$ is just the compositum $L_1 E$, we get the decomposition of $M_n(E)$ into the direct sum of $L_1 E$ spaces $\bigoplus_{i=0}^{b-1} \bigoplus_{j=0}^{n-1} (L_1 E) B^i u^j$.

Now let W be the $L_1 E$ subspace $\bigoplus_{j=0}^{r-1} (L_1 E) u^j$. We claim that for any non-zero matrix $M = z_0 + z_1 u + \cdots + z_{r-1} u^{r-1}$ in W $(z_i \in L_1 E)$, the matrices $\{M B^i u^j\}$ $(i = 0, 1, \ldots, b-1,\ j = 0, 1, \ldots, n-r)$ are $L_1 E$-linearly independent.

For, say $\Sigma\lambda_{i,j}MB^iu^j = 0$, $\lambda_{i,j} \in L_1E$. Note that $MB^i = (z_0 + z_1u + \cdots + z_{r-1}u^{r-1})B^i = z_0 + z_1\sigma(B^i)u + \cdots + z_{r-1}\sigma^{r-1}(B^i)u^{r-1}$. Note, too, that each $z_k\sigma^k(B^i)$ is in $L \otimes_{P(X)} E$. Now in the equation $\Sigma\lambda_{i,j}MB^iu^j = 0$, let J be the largest value of j for which some $\lambda_{i,J} \neq 0$ ($i = 0, 1, \ldots, b-1$), and let T be the largest index for which $z_T \neq 0$ in the expression $M = z_0 + z_1u + \cdots + z_{r-1}u^{r-1}$. Since $T \leq r-1$ and $J \leq n-r$, the decomposition of $M_n(E)$ $(= M_n(P(X)) \otimes_{P(X)} E)$ into the direct sum $\overset{n-1}{\underset{i=0}{\oplus}} (L \otimes_{P(X)} E)u^i$ shows that the coefficient of u^{T+J} should be zero. This coefficient is $\lambda_{0,J}z_T + \lambda_{1,J}z_T\sigma^T(B) + \cdots + \lambda_{b-1,J}z_T\sigma^T(B^{b-1})$. Since z_T is in L_1E and is non-zero, it is invertible. Thus we find $\lambda_{0,J} + \lambda_{1,J}\sigma^T(B) + \cdots + \lambda_{b-1,J}\sigma^T(B^{b-1}) = 0$. Premultiplying by u^{-T} and postmultiplying by u^T, we find $u^{-T}\lambda_{0,J}u^T + u^{-T}\lambda_{1,J}u^TB + \cdots + u^{-T}\lambda_{b-1,J}u^TB^{b-1} = 0$. Since $u^{-T}L_1Eu^T \subseteq L_1E$, the linear independence of the powers of B over L_1E shows that each $\lambda_{i,J}$ must be zero—a contradiction to our choice of J.

It follows that the right ideal $M \cdot M_n(E)$ has L_1E dimension $\geq b(n-r+1)$, and hence has E dimension $\geq (p^ab)(n-r+1)$. Let V be an n-dimensional E-space on which M acts, and let $V' \subseteq V$ be the kernel of M. The kernel of the left multiplication by M map on $M_n(E)$ consists of all matrices whose columns are in V', and this kernel is hence isomorphic to n copies of V'. It follows that $\mathrm{rank}(M) \geq n-r+1$ as claimed.

Since $\dim(W) = p^ar$, W indeed has the property we desire. □

4. Examples.

We show in this section that the bounds on the codimension in Theorems 1 and 3 are strict, that is, there exist subvarieties of X_r of codimension exactly p^ar whose degrees are prime to p. When $n = p^a$, the various linear subvarieties of codimension nr (such as those consisting of matrices whose first r rows are zero) provide the necessary examples, so we need to study the case $n = p^ab$, $b > 1$.

We need another elementary lemma:

Lemma 4. *Let K be an algebraically closed field, and let $Y \subseteq \mathbf{P}^n_K$ be an irreducible variety. In $\mathbf{P}^m_K$ ($m > n$), let Y' be the closed set given by all points whose first $n+1$ homogeneous coordinates satisfy the same equations as Y. Then Y' is irreducible, deg(Y') = deg(Y), and dim(Y') = dim(Y) + $m - n$.*

Proof. (Sketch.) This can be proved geometrically, or else can be proved via Hilbert polynomials using induction on $m - n$. Here is a sketch of the second approach. Let $I \triangleleft K[x_0, x_1, \ldots, x_n]$ be the ideal of Y. It is easy to see that $J = I \cdot K[x_0, \ldots, x_{n+1}]$ is also prime, so J is the ideal of Y' and Y' is irreducible. (Note that both I and J are homogeneous.) One has the exact sequence of graded $K[x_0, \ldots, x_{n+1}]$ modules $0 \longrightarrow K[x_0, \ldots, x_{n+1}]/J\ (-1) \longrightarrow K[x_0, \ldots, x_{n+1}]/J \longrightarrow K[x_0, \ldots, x_{n+1}]/(J, x_{n+1}) \longrightarrow 0$, where the second map is multiplication by x_{n+1}, and one also has the isomorphism of graded rings $K[x_0, \ldots, x_{n+1}]/(J, x_{n+1}) \cong K[x_0, \ldots, x_n]/I$. It follows that the Hilbert polynomial of Y is the difference between the Hilbert polynomial of Y' evaluated at t and evaluated at $t-1$, from which the results on the degree and dimension follow. □

Now for our examples. For simplicity, we first consider the case where $r = 1$. Let $t = p^a(b-1)+1$, and let Z be the subvariety of $\mathbf{P}^{n^2-1}$ given by the condition that the rank of the $t \times n$ submatrix formed by the first t rows has rank $\leq p^a(b-1)$. Z, of course, is contained in X_1. If $Y \subseteq \mathbf{P}^{nt-1}$ is the subvariety given by the condition rank $\leq p^a(b-1)$, then by Lemma 4, $\deg(Z) = \deg(Y)$ and $\operatorname{codim}_{\mathbf{P}^{n^2-1}}(Z) = \operatorname{codim}_{\mathbf{P}^{nt-1}}(Y)$. By [3, Prop. 12.2], $\operatorname{codim}_{\mathbf{P}^{nt-1}}(Y) = p^a b - p^a(b-1) = p^a$, and by [3, Example 19.10], $\deg(Y) = \binom{n}{t-1} = \binom{p^a b}{p^a}$. In the binomial expansion of $(x+y)^{p^a b} = (x^{p^a} + y^{p^a})^b$ in characteristic p, the coefficient of x^{p^a} is non-zero since p does not divide b, so $\deg(Y)$ is prime to p.

For $r > 1$, we let $t = p^a(b-1)+r$, and we let Z be the subvariety of $\mathbf{P}^{n^2-1}$ given by the condition that the submatrix formed by the first t rows has rank $\leq p^a(b-1)$. As before, we work with the variety $Y \subseteq \mathbf{P}^{nt-1}$ given by rank $\leq p^a(b-1)$ to find that $\operatorname{codim}(Z) = p^a r$. Also, by Lemma 4 and [3, Example 19.10],

$$\deg(Z) = \deg(Y) = \prod_{i=0}^{r-1} \frac{\binom{p^a b+i}{p^a(b-1)}}{\binom{p^a(b-1)+i}{p^a(b-1)}}.$$

By considering the characteristic p binomial expansions of $(x+y)^{p^a b+i} = (x+y)^i(x^{p^a}+y^{p^a})^b$ and $(x+y)^{p^a(b-1)+i} = (x+y)^i(x^{p^a}+y^{p^a})^{b-1}$, and using the fact that $i < r < p^a$, we see that each of the $2r$ binomial coefficients in the formula above is prime to p.

References

[1] W. Fulton, Intersection Theory, Springer-Verlag 1984.
[2] R. Guralnick, *Invertible presevers and algebraic groups,* Linear Algebra and its Applications, **212/213** (1994) 249–257.
[3] J. Harris, Algebraic Geometry, A First Course, Springer-Verlag, 1992.
[4] R. Hartshorne, Algebraic Geometry, Springer-Verlag, 1977.
[5] S. Pierce et al., *A survey of linear preserver problems,* Linear and Multilinear Algebra, **33** (1992) 1–130.
[6] Reiner, Maximal Orders, Academic Press, 1975.

E-mail address: al.sethuraman@csun.edu

Department of Mathematics, California State University, Northridge, Northridge, CA 91330 USA