PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 111, Number 3, March 1991

A PARTITION RESULT FOR ALGEBRAIC VARIETIES

ANER SHALEV

(Communicated by William Adams)

ABSTRACT. Let K be a finite field. It is shown that, given positive integers d and r, there exists $M = M(d, r)$, such that any variety $V = V(f) \subseteq K^n$, defined by a polynomial f of degree d in $n \geq M$ variables over K, can be partitioned into affine subspaces, each of dimension r. This result, relying on a theorem of R. Brauer, holds in fact for many other fields, including algebraically closed fields. It may provide a partial structural explanation to a divisibility phenomenon discovered by J. Ax.

1. MAIN RESULT

Let K be a field with $q = p^k$ elements. The classical Chevalley-Warning theorem, proved in 1936, states that if $f = f(\overline{x})$ is polynomial in n variables over K of degree $d < n$, then $N(f)$—the number of zeros of f in K^n—is divisible by p ([4, 9]; see also [5, 7]).

This result was remarkably extended by J. Ax in 1964 [2].

Theorem (Ax). *Suppose* $f \in K[x_1, \ldots, x_n]$, $\deg(f) = d$. *Let* r *be a positive integer such that* $n > d \cdot r$. *Then* q^r *divides* $N(f)$.

This theorem is the best possible, in the sense that the condition on n cannot be weakened. Ax also formulated a divisibility result for a system of polynomial equations, which was later sharpened by N. M. Katz [6]. Recently, D. Wan [8] gave a more elementary proof of Katz's theorem, avoiding the use of the p-adic theory of zeta functions. See also [1] for more refined divisibility properties, relying on the "geometry" of the monomials appearing in f and not only on the parameters n and d.

The theorem of Ax shows that the number of (rational) points in varieties defined by a polynomial of fixed degree in a sufficiently large number of variables, is divisible by arbitrarily large qth-powers, where q is the order of the ground field.

It is natural to ask whether there exists any "hidden structure" behind this phenomenon. The most satisfactory structural explanation to a divisibility re-

Received by the editors September 25, 1989 and, in revised form, February 20, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G25, 12E12; Secondary 14A10.

0002-9939/91 $1.00 + $.25 per page

sult is the existence of a certain partition. Obviously, an affine space (i.e., a coset of a linear space) of dimension r over K consists of q^r elements. Therefore, in our case one may wonder whether, for given d and r, any variety $V(f)$, defined by a polynomial f of degree d in a sufficiently large number of variables, may be partitioned into r-dimensional affine spaces.

The purpose of this paper is to prove this hypothesis, not only for finite fields but for a large family of fields, including algebraically closed ones. However, the bounds required for divisibility are usually lower than those insuring the existence of a suitable partition.

One step in this direction was made by R. Brauer in 1945. In order to formulate this result, consider the following field-theoretical property, where ω denotes the natural numbers:

(*) There exists a function $\phi: \omega \to \omega$ such that, if $d \in \omega$ and $n \geq \phi(d)$, then any polynomial of the form

$$a_1 x_1^d + a_2 x_2^d + \cdots + a_n x_n^d = 0$$

over K has a nontrivial zero in K^n.

It is clear that algebraically closed fields, finite fields, and in fact any C_i field (e.g., p-adic fields) satisfy $(*)$.

In [3] Brauer considered a system of homogeneous equations over a field satisfying $(*)$. He proved that if the number of variables n is larger than a certain function of the degrees of the equations and a given parameter r, then the variety defined by the equations contains an r-dimensional linear space. Brauer's theorem is easily modified to the nonhomogeneous case, provided that the equations have no constant terms. Indeed, one should replace every equation of degree d with its homogeneous constituents of degrees $1, 2, \ldots, d$ respectively. Dealing, for simplicity, with one equation, one obtains the following theorem from [3].

Theorem. *Let K be a field satisfying $(*)$. Then, for every d and r, there exists $N = N(d, r)$, such that if f is any polynomial of degree d in $n \geq N$ variables over K with $f(\bar{0}) = 0$, then the variety $V(f) \subseteq K^n$ contains an r-dimensional linear space.*

Remark. If $f(\bar{a}) = 0$ for some $\bar{a} \in K^n$ (not necessarily $\bar{0}$), then, via an affine change of variables, it follows that $V(f)$ contains an r-dimensional affine space U such that $\bar{a} \in U$. Hence Brauer's result shows that $V(f)$ may actually be covered by r-dimensional affine spaces, but these need not be pairwise disjoint.

We can now state and prove our main result.

Theorem 1. *Let K be a field satisfying $(*)$. Then, for every d and r there exists $M = M(d, r)$, such that if f is any polynomial of degree d in $n \geq M$ variables over K, then the variety $V(f) \subseteq K^n$ can be partitioned into r-dimensional affine spaces.*

Proof. Let N be the function appearing in Brauer's theorem. Define $M(d, r)$ inductively by

$$M(1, r) = r + 1; \qquad M(d, r) = N(d, M(d-1, r)) \quad (d \geq 2).$$

Let us prove, by induction on d, that, for all r, $M(d, r)$ is as required.

The case $d = 1$ is clear (since $V(f)$ itself is an affine space of dimension r). Now, let f be a polynomial of degree $d \geq 2$ in $n \geq M(d, r)$ variables. If $V(f) = \varnothing$ we are done (there is nothing to partition), so let us assume $V(f) \neq \varnothing$. Put $s = M(d-1, r)$. By Brauer's theorem, $V(f)$ contains an affine space U of dimension s. After an affine change of variables we may assume that U is given by the $n - s$ linear constraints $x_{s+1} = 0$, $x_{s+2} = 0, \ldots, x_n = 0$. This means that the function $K^s \to K$ defined by the polynomial $f_0 = f(x_1, \ldots, x_s, 0, \ldots, 0)$ is identically zero. Therefore f_0 is the zero polynomial (if K is finite, we will have to assume here, as we may, that f is reduced). We conclude that every monomial which appears in f involves some of the vanishing variables $x_{s+1}, \ldots, x_n$. Hence, any substitution $x_{s+1} \leftarrow a_{s+1}, \ldots, x_n \leftarrow a_n$ (where $a_i \in K$) will reduce the degree of f.

Now, given $\bar{a} = (a_{s+1}, \ldots, a_n) \in K^{n-s}$, consider the polynomial $f_{\bar{a}} = f(x_1, \ldots, x_s, a_{s+1}, \ldots, a_n)$. Its degree is $\leq d - 1$, and its number of variables is $s = M(d-1, r)$. By induction hypothesis, $V(f_{\bar{a}}) \subseteq K^s$ is partitioned into affine spaces, each of dimension r. Letting $\bar{a} \in K^{n-s}$ take all its possible values, we get the required partition of the original variety $V(f)$. □

Remark. A similar result holds for algebraic varieties defined by more than one polynomial: if the number of variables is greater than a certain function of the degrees of the defining polynomials and a given parameter r, then the variety obtained can be partitioned into r-dimensional affine spaces. The proof is essentially the same.

2. Numerical estimates

In this section we consider the problem of the evaluation of the functions $N_K(d, r)$ and $M_K(d, r)$ associated with a finite field K, defined by

$$N_K(d, r) = \min\{n: \text{if } f \in K[x_1, \ldots, x_n],\ \deg(f) \leq d,\ \text{and } V(f) \neq \varnothing,\ \text{then } V(f) \text{ contains an } r\text{-dimensional affine space}\}.$$

$$M_K(d, r) = \min\{n: \text{if } f \in K[x_1, \ldots, x_n] \text{ and } \deg(f) \leq d,\ \text{then } V(f) \text{ may be partitioned into } r\text{-dimensional affine spaces}\}.$$

Although we shall not get much information on the behaviour of $M_K(d, r)$ (except for a certain astronomical upper bound), our estimates for $N_K(d, r)$ are more satisfactory; they show that, for a finite field K and fixed $d < |K|$, $N(d, r) = O(r^{d-1})$. Similar estimations may be carried out for algebraically closed fields as well.

It should be noted that Brauer's proof does not include any specific evaluation of the function $N(d, r)$; however, in our estimation we apply some of his ideas. We also use Warning's second theorem [9], showing that if $|K| = q$, then any system of equations in n variables over K, whose sum of degrees is d, has at least q^{n-d} solutions, provided it has a solution.

Theorem 2. *Suppose* $d < |K| < \infty$. *Then for all* r,

$$\frac{1}{d}\binom{r+d}{d-1} + r - 1 < N_K(d, r) \leq \binom{r+d}{d-1} + r.$$

Consequently, fixing d, *we obtain* $N_K(d, r) = O(r^{d-1})$.

Proof. We first prove the upper bound.

Let f be a polynomial of degree $\leq d$ in n variables, and suppose $n \geq \binom{r+d}{d-1} + r$. We assume, by induction, that $V(f)$ contains an affine space U' of dimension $r-1$, and we would like to extend it to an r-dimensional affine space U, lying in $V(f)$. We may assume that $\overline{0} \in U'$ (so that U' is a linear space).

Let $\overline{u}_1, \ldots, \overline{u}_{r-1}$ be a basis for U'. We introduce r new variables $y_1, \ldots, y_r$ and form the expression

$$f(y_1\overline{u}_1 + \cdots + y_{r-1}\overline{u}_{r-1} + y_r\overline{x}) = \sum_{\overline{m}} f_{\overline{m}}(\overline{x}) y_1^{m_1} \cdots y_r^{m_r}. \tag{1}$$

Clearly, if, for a certain substitution $\overline{x} \leftarrow \overline{u} (\in K^n)$, all the $f_{\overline{m}}$'s vanish, then $U' + K\overline{u} \subseteq V(f)$. If, in addition, $\overline{u} \notin U'$, then $U = U' + K\overline{u}$ will be as required.

So consider the system of equations in $x_1, \ldots, x_n$ over K;

$$f_{\overline{m}}(\overline{x}) = 0 \quad \text{for all } \overline{m} = (m_1, \ldots, m_r),\ m_i \geq 0,\ \sum m_i \leq d. \tag{2}$$

We have to show that it has a solution in $K^n \setminus U'$.

First, observe that by substituting $\overline{x} = \overline{0}$ in (1), we can conclude that the polynomial $g(y_1, \ldots, y_r) = \sum f_{\overline{m}}(\overline{0}) y_1^{m_1} \cdots y_r^{m_r}$ defines the zero function $K^r \to K$ (since $U' \subseteq V(f)$). Its degree is less than or equal to d, and is therefore strictly less than $|K|$. It follows that $g = 0$, so $f_{\overline{m}}(\overline{0}) = 0$ for all $\overline{m}$. This shows that system (2) has at least one solution, namely—the zero one. Now, observe that $\deg(f_{\overline{m}}) \leq m_r$. Therefore, if D denotes the sum of the degrees of equations (2), then $D \leq \sum_{\overline{m}} m_r = \sum_M \deg_{y_r}(M)$, where M ranges over the set of all the $\binom{r+d}{d}$ monomials of degree $\leq d$ in $y_1, \ldots, y_r$, denoted here by $\mathrm{Mon}(d, r)$. It follows that

$$D \leq \sum_{M \in \mathrm{Mon}(d, r)} \deg_{y_r}(M) = \binom{r+d}{d-1},$$

where the equality on the right can be easily verified. By Warning's second

theorem, system (2) has at least q^{n-D} solutions, where $|K| = q$. The last calculation and the choice of n yield $n - D \geq n - \binom{r+d}{d-1} \geq r$, so that $q^{n-D} \geq q^r > |U'|$. Therefore one of these solutions must lie outside U'. This completes the proof of the right inequality.

For the left one we use a simple probabilistic argument.

Note that a polynomial $f = f(x_1, \ldots, x_n)$ over K of degree $\leq d < q$ vanishes on the linear space U defined by $x_{r+1} = x_{r+2} = \cdots = x_n = 0$ if and only if all its $\binom{r+d}{d}$ coefficients of the monomials in $x_1, \ldots, x_r$ of degree d or less vanish. This event occurs with probability $q^{-\binom{r+d}{d}}$ in the space of all the $q^{\binom{n+d}{d}}$ possible polynomials f. Obviously, this probability does not change if one replaces U with any other r-dimensional affine space. Now, if $n = N_K(d, r)$, then by definition every such polynomial f will vanish on a certain r-dimensional affine space, provided it has a zero. Since the probability of f having a zero is clearly greater than or equal to q^{-1}, we obtain

$$A_K(n, r) \cdot q^{-\binom{r+d}{d}} \geq q^{-1},$$

where $A_K(n, r)$ denotes the number of r-dimensional affine subspaces of K^n. It is well known that

$$A_K(n, r) = q^{n-r} \cdot \frac{(q^n - 1) \cdot \cdots \cdot (q^n - q^{r-1})}{(q^r - 1) \cdot \cdots \cdot (q^r - q^{r-1})} < q^{n(r+1)-r^2}.$$

We conclude that $q^{n(r+1)-r^2} \cdot q^{-\binom{r+d}{d}} > q^{-1}$, so that $n(r+1) > \binom{r+d}{d} + r^2 - 1$, and $n > \frac{1}{r+1}\binom{r+d}{d} + \frac{r^2-1}{r+1} = \frac{1}{d}\binom{r+d}{d-1} + r - 1$, as required. □

Remark. The upper bound given in Theorem 2 remains valid without the restriction on d. To see this, one should reduce the right-hand side of expression (1) (using the identities $y_i^q = y_i$), and form the corresponding system of equations. Clearly, this system must have a solution (the zero one), and its sum of degrees is less than or equal to D—the sum of degrees of (2)—which is in turn bounded above by $\binom{r+d}{d-1}$. This yields the desired conclusion.

Corollary. *For fixed d we have $M_K(d, r) \leq O(r^{(d-1)!})$.*

Proof. Combine the last remark with the proof of Theorem 1, showing that $M_K(1, r) = r + 1$ and $M_K(d, r) \leq N_K(d, M_K(d-1, r))$ $(d \geq 2)$. □

This bound is clearly much larger than the one appearing in Ax's divisibility theorem, which is linear in r. However, if $d \geq 2$, one cannot expect $M_K(d, r)$ (and even $N_K(d, r)$) to be linear in r, as shown in Theorem 2. Nevertheless, it would be interesting to understand the asymptotic behaviour of $M_K(d, r)$.

ACKNOWLEDGMENT

I am grateful to D. Kazhdan for stimulating discussions.

References

1. A. Adolphson and S. Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci. École Norm. Sup. (4) **20** (1987), 545–556.
2. J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.
3. R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. **51** (1945), 749–755.
4. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.
5. M. J. Greenberg, *Lectures on forms in many variables*, Benjamin, Amsterdam and New York, 1969.
6. N. M. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.
7. W. M. Schmidt, *Equations over finite fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin and New York, 1976.
8. D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. **111** (1989), 1–8.
9. E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.

Institute of Mathematics and Computer Sciences, The Hebrew University, Jerusalem 91904, Israel

Current address: Mathematical Institute, University of Oxford, 24-29 St. Giles, Oxford 0X1 3LB, United Kingdom