Journal of Pure and Applied Algebra 219 (2015) 5117–5136

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

On the number of points of algebraic sets over finite fields

Gilles Lachaud, Robert Rolland *

Université d'Aix-Marseille, Institut de Mathématiques de Marseille, Luminy Case 907, F13288 Marseille Cedex 9, France

ARTICLE INFO

Article history:
Received 30 July 2014
Received in revised form 7 April 2015
Available online 27 May 2015
Communicated by I.M. Duursma

MSC:
14G15; 14G05

ABSTRACT

We determine upper bounds on the number of rational points of an affine or projective algebraic set defined over an extension of a finite field by a system of polynomial equations, including the case where the algebraic set is not defined over the finite field by itself. A special attention is given to irreducible but not absolutely irreducible algebraic sets, which satisfy better bounds. We study the case of complete intersections, for which we give a decomposition, coarser than the decomposition in irreducible components, but more directly related to the polynomials defining the algebraic set. We describe families of algebraic sets having the maximum number of rational points in the affine case, and a large number of points in the projective case.

RÉSUMÉ

Nous déterminons des majorations du nombre de points d'un ensemble algébrique affine ou projectif, défini sur une extension d'un corps fini par un système d'équations polynomiales, y compris dans le cas où l'ensemble algébrique n'est pas défini sur le corps fini lui-même. Une attention particulière est portée aux ensembles algébriques irréductibles mais non absolument irréductibles, pour lesquels nous obtenons de meilleures bornes. Nous étudions le cas des intersections complètes, pour lesquelles nous construisons une décomposition moins fine que la décomposition en composantes irréductibles, mais plus directement liée aux polynômes qui définissent l'ensemble algébrique. Enfin, nous construisons des familles d'ensembles algébriques atteignant le nombre maximum de points rationnels dans le cas affine, et comportant de nombreux points dans le cas projectifs.

0. Introduction

Let X be an algebraic subset of the affine or projective space, defined over an extension of a given finite field $\mathbb{F}_q$. Our purpose is to give several bounds on the maximum number of points of X, with coordinates

* Corresponding author.
E-mail addresses: gilles.lachaud@univ-amu.fr (G. Lachaud), robert.rolland@acrypta.fr (R. Rolland).

http://dx.doi.org/10.1016/j.jpaa.2015.05.008
0022-4049/

in $\mathbb{F}_q$ (unless explicitly stated, we do not assume that X is defined over $\mathbb{F}_q$). These bounds are expressed in terms of the degree of X, and they are obtained by applying various versions of Bézout's Theorem. Hence, the notions of degree and cumulative degree are essential tools in our computations, and they are introduced in Section 1. We establish a general upper bound in Section 2 (Theorem 2.1). We improve this general bound if X is irrational, that is, not defined over $\mathbb{F}_q$, by introducing the *greatest k-closed subset* in X. Surprisingly, we obtain in this case a bound of order $q^{\dim X-1}$ (Corollary 2.11). In Section 3 we assume that X is relatively irreducible, and study the decomposition of X in absolutely irreducible components of X. This decomposition leads to a better upper bound (Corollary 3.6) than the general upper bound given in Section 2, and also to a bound of order $q^{\dim X-1}$. We also show that the set of rational points of X is contained in the singular locus of X, and moreover $X(k) = \emptyset$ if X is normal (Proposition 3.8). We assume in Section 4 that X is an (ideal-theoretic) complete intersection, for which an exact formula for the degree is known. We describe a decomposition of X directly related to a system $(f_1, \ldots, f_r)$ of polynomials defining X, namely the *coarse decomposition* (Proposition 4.5). The decomposition in irreducible components is finer than the coarse decomposition, but the later can be explicitly constructed from $(f_1, \ldots, f_r)$. This leads to an upper bound on the number of rational points of X, improving the general upper bound if every polynomial among $(f_1, \ldots, f_r)$ is relatively irreducible, but at least one is not absolutely irreducible (Proposition 4.3). In Section 5 we construct a family of affine algebraic sets over $\mathbb{F}_q$ (the *tubular sets*) reaching the general upper bound given in Section 2. The corresponding projective family has also a large number of points but does not reach the general upper bound (Theorem 5.1). It is worthwhile to precise that our results generalize and improve those previously obtained in the case of hypersurfaces defined over $\mathbb{F}_q$, for which the best bounds are given in [14] in the affine case, and in [19] and [21] in the projective case. Also note that some of our methods can be seen as similar, although in a more explicit and precise way, to the general approach of Heath-Brown in [15, Th. 3].

1. The cumulative degree

Let k be a field and K the algebraic closure of k. We are interested in the solutions in the affine space k^n of a system

$$f_i(T_1, \ldots, T_n) = 0 \qquad (1 \le i \le r) \tag{1}$$

with $f_i \in K[T_1, \ldots, T_n]$, and $r \le n$. We are also concerned about solutions in the projective space $\mathbb{P}^n(k)$ of a system

$$f_i(T_0, \ldots, T_n) = 0 \qquad (1 \le i \le r) \tag{2}$$

with homogeneous polynomials $f_i \in K[T_0, \ldots, T_n]$. These systems define respectively a K-algebraic subset X in the affine space $\mathbb{A}^n = K^n$ and in the projective space $\mathbb{P}^n = \mathbb{P}^n(K)$. If $\mathfrak{a}$ is an ideal of $K[T_1, \ldots, T_n]$, the subset of zeros of $\mathfrak{a}$ is denoted by $V(\mathfrak{a})$. Hence, $X = V(\mathfrak{a})$ where $\mathfrak{a}$ is the ideal generated by $f_1, \ldots, f_r$. If S is a subset of $\mathbb{A}^n$ or $\mathbb{P}^n$, the *ideal of* S, denoted by $I(S)$, is the radical ideal of polynomials vanishing on S. Hence, $I(X)$ is the radical $\mathfrak{r}(\mathfrak{a})$ of $\mathfrak{a}$.

Let $Z_1, \ldots, Z_t$ be the irreducible components of X, in such a way that

$$X = Z_1 \cup \cdots \cup Z_t.$$

We put $m = \dim X = \max_{1 \le i \le t} \dim Z_i$. Then $m \ge n - r$ since, by the Generalized Principal Ideal Theorem [4, Ch. VIII, §3, Prop. 4]:

$$\min_{1 \le i \le t} \dim Z_i \ge n - r.$$