AFST

Annales de la Faculté des Sciences de Toulouse

MATHÉMATIQUES

Reducing the number of equations defining a subset of the n-space over a finite field $^{(*)}$

Stefan Barańczuk $^{(1)}$

Abstract. — Let $f_1, \ldots, f_k$ be polynomials defining an algebraic set in affine n-space over a finite field. Suppose $k > n$. We prove that there exists a system of polynomials $g_1, \ldots, g_n$, each being a linear combination with scalar coefficients of $f_1, \ldots, f_k$, defining the same algebraic set. In particular, one reduces the number of equations without increasing the total degree. We also have the corresponding result for systems of homogeneous polynomials defining algebraic sets in projective spaces.

Résumé. — Soient $f_1, \ldots, f_k$ des polynômes définissant un ensemble algébrique dans un n-espace affine sur un corps fini. Supposons $k > n$. Nous montrons qu'il existe un système de polynômes $g_1, \ldots, g_n$, chacun étant un combinaison linéaire de $f_1, \ldots, f_k$, avec des coefficients scalaires, définissant le même ensemble algébrique. En particulier, on réduit le nombre d'équations sans augmenter le degré total. Nous avons aussi le résultat correspondant pour des systèmes de polynômes homogènes définissant des ensembles algébriques dans des espaces projectifs.

The theorem that any algebraic set in n-dimensional space is the intersection of n hypersurfaces $^{(a)}$ has been proved independently by Storch ([2]), and Eisenbud and Evans ([1]); both short proofs are ring-theoretic, i.e., one reduces the number of generators of radical ideals.

In this note we examine closer the finite fields case of the problem. If just the number of equations needed to describe an algebraic set is in question, then the answer is immediate: it is easy to construct a single polynomial defining it. If, however, the nature of defining polynomials (e.g., their total degree) is to be preserved, this problem becomes more interesting.

$^{(a)}$ The problem dates back to Kronecker. Its rather dramatic story is briefly presented in [1]; for much more detailed vivid account consult N. Schappacher's available online presentation *Political Space Curves*.

Stefan Barańczuk

It turns out that we can avoid dealing with rings; the vector space structure is sufficient and, as in the theorem cited above, our result again produces n equations; moreover, we show that these new equations can be chosen to be linear combinations with *scalar* coefficients of the old ones, so, roughly speaking, they remain of the same type (see Corollaries 3 and 4, with accompanying examples), and our proof is surprisingly elementary.

We fix the following notation:

$\mathbb{F}_q$	the finite field with q elements;
$\mathrm{Map}(X, \mathbb{F}_q)$	the vector space of all functions $f : X \to \mathbb{F}_q$ for a given set X;
$\mathrm{Z}(f_1, \ldots, f_k)$	the set of common zeros of $f_1, \ldots, f_k \in \mathrm{Map}(X, \mathbb{F}_q)$;
$\mathrm{Span}(f_1, \ldots, f_k)$	the subspace of $\mathrm{Map}(X, \mathbb{F}_q)$ generated by $f_1, \ldots, f_k$;
$\mathbb{A}^n(\mathbb{K})$	the affine n-space over a field $\mathbb{K}$;
$\mathbb{P}^n(\mathbb{K})$	the projective n-space over a field $\mathbb{K}$;
$[\alpha_1 : \ldots : \alpha_{n+1}]$	a set of homogeneous coordinates for a point in $\mathbb{P}^n(\mathbb{K})$.

THEOREM 1. — *Let X be a set with at most $\frac{q^{n+1}-q}{q-1}$ elements. If $f_1, \ldots, f_k \in \mathrm{Map}(X, \mathbb{F}_q)$ for some $k > n$ then there exist $g_1, \ldots, g_n \in \mathrm{Span}(f_1, \ldots, f_k)$ such that $\mathrm{Z}(g_1, \ldots, g_n) = \mathrm{Z}(f_1, \ldots, f_k)$.*

This theorem is best possible with respect to the cardinality of X. Indeed, we have the following.

PROPOSITION 2. — *For every field $\mathbb{F}_q$ and every positive integer n there are a set X_n of cardinality $\frac{q^{n+1}-q}{q-1}+1$, and maps $f_1, \ldots, f_{n+1} \in \mathrm{Map}(X_n, \mathbb{F}_q)$ such that $\mathrm{Z}(f_1, \ldots, f_{n+1}) = \emptyset$ but $\mathrm{Z}(g_1, \ldots, g_n) \neq \emptyset$ for any $g_1, \ldots, g_n \in \mathrm{Span}(f_1, \ldots, f_{n+1})$.*

We have two immediate corollaries of Theorem 1 of interest in algebraic geometry.

COROLLARY 3. — *Let $n > 0$ and let $\phi : \mathcal{F} \to \mathrm{Map}(\mathbb{A}^n(\mathbb{F}_q), \mathbb{F}_q)$ be a homomorphism of vector spaces over $\mathbb{F}_q$. Any subset of $\mathbb{A}^n(\mathbb{F}_q)$ defined by some members of $\mathcal{F}$ (i.e., the zero locus of their images via ϕ) can be defined using at most n members of $\mathcal{F}$.*

The space $\mathcal{F}$ can be, for example, a space of polynomials in n variables of bounded total degree.

COROLLARY 4. — *Let $n \geqslant 0$ and let $\phi : \mathcal{F} \to \mathrm{Map}(\mathbb{P}^n(\mathbb{F}_q), \mathbb{F}_q)$ be a homomorphism of vector spaces over $\mathbb{F}_q$. Any nonempty subset of $\mathbb{P}^n(\mathbb{F}_q)$ defined by some members of $\mathcal{F}$ (i.e., the zero locus of their images via ϕ) can be defined using at most n members of $\mathcal{F}$.*

The space $\mathcal{F}$ can be a space of homogeneous polynomials in $n+1$ variables of bounded total degree, the space of quadratic (or higher degree) forms in $n + 1$ variables, the space of diagonal forms in $n + 1$ variables, etc.

Before we present the proofs of Theorem 1 and Proposition 2, we separately state their following ingredient.

Let $\mathbb{K}$ be an arbitrary field, and n be a positive integer. Denote by $\mathcal{M}_n$ the set of all matrices in $M_{n,n+1}(\mathbb{K})$ in reduced row echelon form having the rank equal to n, by $N(M)$ the null space of a matrix M, by θ the zero vector in $\mathbb{K}^{n+1}$, and by $\sim$ the equivalence relation which identifies points lying on the same line through the origin.

LEMMA 5. — *The map*

$$\mathcal{M}_n \longrightarrow \mathbb{P}^n(\mathbb{K})$$
$$M \longmapsto (N(M) \setminus \{\theta\})_\sim$$

is bijective.

Proof. — Denote by $\mathcal{N}_n$ the set of all matrices in $M_{n,n+1}(\mathbb{K})$ having the rank equal to n. For every $M \in \mathcal{N}_n$ the dimension of the vector space $N(M) < \mathbb{K}^{n+1}$ equals 1 by the rank-nullity theorem, so $(N(M) \setminus \{\theta\})_\sim \in \mathbb{P}^n(\mathbb{K})$. We thus have the map

$$\mathcal{N}_n \longrightarrow \mathbb{P}^n(\mathbb{K})$$
$$M \longmapsto (N(M) \setminus \{\theta\})_\sim$$

Since matrices of the same size have equal null spaces if and only if they are row equivalent, the induced map

$$\mathcal{N}_n/GL_n(\mathbb{K}) \longrightarrow \mathbb{P}^n(\mathbb{K})$$

is well-defined and injective. It is also surjective, since every vector subspace of $\mathbb{K}^{n+1}$ having dimension equal to 1 is the null space of a matrix in $\mathcal{N}_n$.

Since the canonical map

$$\mathcal{M}_n \longrightarrow \mathcal{N}_n/GL_n(\mathbb{K})$$

is bijective, the lemma follows. $\qquad\square$

Proof of Theorem 1. — It is enough to prove the statement for $k = n+1$ since we may apply induction.

Denote

$$S = \{[f_1(x) : \ldots : f_{n+1}(x)] : x \in X \setminus \mathrm{Z}(f_1, \ldots, f_{n+1})\}.$$

By Lemma 5 every element s of S defines a unique matrix in $\mathcal{M}_n$; denote this matrix by M_s. Examine the set

$$T = \mathcal{M}_n \setminus \{M_s : s \in S\}.$$

By Lemma 5 the number of elements in $\mathcal{M}_n$ equals the cardinality of $\mathbb{P}^n(\mathbb{F}_q)$, i.e., $\frac{q^{n+1}-1}{q-1}$. The number of elements in S is at most the cardinality of X, i.e., $\frac{q^{n+1}-q}{q-1}$. Hence the cardinality of T is at least $\frac{q^{n+1}-1}{q-1} - \frac{q^{n+1}-q}{q-1} = 1$. So choose a matrix $M \in T$. Our $g_1, \ldots, g_n$ are defined by

$$\begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} = M \begin{bmatrix} f_1 \\ \vdots \\ f_{n+1} \end{bmatrix}.$$

Indeed, the inclusion $\mathrm{Z}(f_1, \ldots, f_{n+1}) \subset \mathrm{Z}(g_1, \ldots, g_n)$ is obvious, and by the definition of T the set $\mathrm{Z}(g_1, \ldots, g_n)$ is disjoint from $X \setminus \mathrm{Z}(f_1, \ldots, f_{n+1})$, i.e., $\mathrm{Z}(g_1, \ldots, g_n) \subset \mathrm{Z}(f_1, \ldots, f_{n+1})$. □

In order to prove Proposition 2 we need the following.

LEMMA 6. — *Let $\mathbb{K}$ be an arbitrary field. For any matrix $A \in M_{n,m}(\mathbb{K})$ where $n \leqslant m$ there exist a matrix $M \in M_{n,m}(\mathbb{K})$ in reduced row echelon form having the rank equal to n, and a matrix $B \in M_{n,n}(\mathbb{K})$ such that $A = BM$.*

Proof. — Denote by $I_{r,k,l}$ the matrix in $M_{k,l}(\mathbb{K})$ having $x_{11} = \cdots = x_{rr} = 1$ and all remaining entries equal to 0. Denote the rank of A by r. Let $G_1 \in GL_n(\mathbb{K})$ and $G_2 \in GL_m(\mathbb{K})$ be matrices transforming A into $I_{r,n,m}$, i.e., $G_1 A G_2 = I_{r,n,m}$. Since $I_{r,n,m} = I_{r,n,n} I_{n,n,m}$, we get $A = G_1^{-1} I_{r,n,n} I_{n,n,m} G_2^{-1}$. Let $G_3 \in GL_n(\mathbb{K})$ be the matrix transforming $I_{n,n,m} G_2^{-1}$ into reduced row echelon form. We have

$$A = G_1^{-1} I_{r,n,n} G_3^{-1} G_3 I_{n,n,m} G_2^{-1}.$$

Put $B = G_1^{-1} I_{r,n,n} G_3^{-1}$ and $M = G_3 I_{n,n,m} G_2^{-1}$. □

Proof of Proposition 2. — For every point $P \in \mathbb{P}^n(\mathbb{F}_q)$ choose a set of homogeneous coordinates for P and denote it by c_P. Define $X_n = \{c_P : P \in \mathbb{P}^n(\mathbb{F}_q)\}$. The cardinality of X_n is $\frac{q^{n+1}-1}{q-1} = \frac{q^{n+1}-q}{q-1} + 1$. Consider $f_1, \ldots, f_{n+1} \in \mathrm{Map}(X_n, \mathbb{F}_q)$ defined in the following way: for every $x \in X_n$ put

$$f_i(x) = \text{the } i\text{th coordinate of } x.$$

We have $\mathrm{Z}(f_1, \ldots, f_{n+1}) = \emptyset$.

Let $g_1, \ldots, g_n \in \mathrm{Span}(f_1, \ldots, f_{n+1})$, i.e.,

$$\begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} = A \begin{bmatrix} f_1 \\ \vdots \\ f_{n+1} \end{bmatrix}$$

for some matrix $A \in M_{n,n+1}(\mathbb{F}_q)$. By Lemma 6 there exist a matrix $M \in M_{n,n+1}(\mathbb{F}_q)$ in reduced row echelon form having the rank equal to n, and a

matrix $B \in M_{n,n}(\mathbb{F}_q)$ such that $A = BM$. Hence by Lemma 5 we get that there is $x \in X_n$ belonging to $\mathrm{Z}(g_1, \ldots, g_n)$. $\qquad\square$

Proof of Corollary 3. — For any positive integer n we have $\frac{q^{n+1}-q}{q-1} \geqslant q^n = |\mathbb{A}^n(\mathbb{F}_q)|$. Applying Theorem 1 and some elementary algebra, we get the assertion. $\qquad\square$

Remark 7. — It has been suggested by the reviewer of this paper to include the following example to demonstrate that although the bound $\frac{q^{n+1}-q}{q-1} \geqslant q^n$ used in the proof of Corollary 3 is rather crude, the result is sharp for any q. Consider the system of n polynomials $f_i(x_1, \ldots, x_n) = x_i$. While $\mathrm{Z}(f_1, \ldots, f_k) = \{\theta\}$, any system of $n-1$ combinations of them has at least q common zeros.

Proof of Corollary 4. — Let $\{f_1, \ldots, f_k\}$ be the image via ϕ of a subset of $\mathcal{F}$. Let $\alpha \in \mathrm{Z}(f_1, \ldots, f_k)$. Denote by $\bar{f}_1, \ldots, \bar{f}_k$ the images of $f_1, \ldots, f_k$ via the restriction homomorphism

$$r : \mathrm{Map}(\mathbb{P}^n(\mathbb{F}_q), \mathbb{F}_q) \longrightarrow \mathrm{Map}(\mathbb{P}^n(\mathbb{F}_q) \setminus \{\alpha\}, \mathbb{F}_q)$$
$$f \longmapsto f|_{\mathbb{P}^n(\mathbb{F}_q)\setminus\{\alpha\}}.$$

For any positive integer n we have

$$|\mathbb{P}^n(\mathbb{F}_q) \setminus \{\alpha\}| = |\mathbb{P}^n(\mathbb{F}_q)| - 1 = \frac{q^{n+1}-1}{q-1} - 1 = \frac{q^{n+1}-q}{q-1}.$$

So we apply Theorem 1 to get $\overline{g_1}, \ldots, \overline{g_n} \in \mathrm{Span}(\bar{f}_1, \ldots, \bar{f}_k)$ such that $\mathrm{Z}(\overline{g_1}, \ldots, \overline{g_n}) = \mathrm{Z}(\bar{f}_1, \ldots, \bar{f}_k)$. Let $A \in M_{k,n}(\mathbb{F}_q)$ be such that

$$\begin{bmatrix} \overline{g_1} \\ \vdots \\ \overline{g_n} \end{bmatrix} = A \begin{bmatrix} \bar{f}_1 \\ \vdots \\ \bar{f}_k \end{bmatrix}.$$

Define $g_1, \ldots, g_n \in \mathrm{Map}(\mathbb{P}^n(\mathbb{F}_q), \mathbb{F}_q)$ by

$$\begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} = A \begin{bmatrix} f_1 \\ \vdots \\ f_k \end{bmatrix}.$$

We are done, since

$$\mathrm{Z}(f_1, \ldots, f_k) = \{\alpha\} \cup \mathrm{Z}(\bar{f}_1, \ldots, \bar{f}_k),$$
$$\text{and} \quad \mathrm{Z}(g_1, \ldots, g_n) = \{\alpha\} \cup \mathrm{Z}(\overline{g_1}, \ldots, \overline{g_n}). \qquad\square$$

Stefan Barańczuk

Acknowledgements

Bibliography

[1] D. Eisenbud & E. G. Evans, Jr, "Every algebraic set in n-space is the intersection of n hypersurfaces", *Invent. Math.* **19** (1973), p. 107-112.

[2] U. Storch, "Bemerkung zu einem Satz von M. Kneser", *Arch. Math.* **23** (1972), p. 403-404.