On the Waring problem for polynomial rings

Boris Shapiro

jointly with Ralf Fröberg, Giorgio Ottaviani

Université de Genève, March 21, 2016

Introduction

In this lecture we discuss an analog of the classical Waring problem for $\mathbb{C}[x_0, x_1, ..., x_n]$. Namely, we show that a general homogeneous polynomial $p \in \mathbb{C}[x_0, x_1, ..., x_n]$ of degree divisible by $k \geq 2$ can be represented as a sum of at most k^n k-th powers of homogeneous polynomials in $\mathbb{C}[x_0, x_1, ..., x_n]$. Noticeably, k^n coincides with the number obtained by naive dimension count.

PNAS 109(15) (2012), 5600–5602.

Waring problem for natural numbers

In 1770 in his paper Meditationes Algebraicae, the English number theorist E. Waring (1736 – 1798) stated without proof, that every natural number is a sum of at most 9 cubes; every natural number is a sum of at most 19 fourth powers; and so on...

Apparently, he believed that, for every natural number $d \geq 2$, there exists a number N(d) such that every positive integer n can be written as

$$n = a_1^d + ... + a_{N(d)}^d, \quad a_i \in \mathbb{N}.$$

The smallest number with that property is denoted by $g(d)$.

It took more than a century to prove this statement.

Waring problem for natural numbers, cont.

Theorem (D. Hilbert, 1909)

For any $d \geq 2$, $g(d)$ exists.

In fact, from the famous Lagrange's four-square Theorem (1770), we know that $g(2) = 4$. Later Wieferich and Kempner showed that $g(3) = 9$. In 1986, Balasubramanian, Dress and Deshouillers established that $g(4) = 19$.

Conjecture.

$$g(d) = 2d + \left[(3/2)^d\right] - 2.$$

Mahler proved that there are only finitely many values counterexamples to the equality. Due to massive computer checking, it is believed that it is always true and that the conjectured value of $g(d)$ is correct.

Waring problem for natural numbers, final

Davenport proved that any sufficiently large integer can be written as the sum of at most 16 fourth powers. For any $d \geq 2$, it is natural to define $G(d)$ as the least integer such that all sufficiently large integers can be expressed as sum of at most $G(d)$ dth powers of integers. Clearly, $G(d) \leq g(d)$.

Gauss observed that every number congruent to 7 mod(8) is a sum of four squares, which proves that $G(2) = g(2) = 4$. But the inequality can be strict. Indeed, it has been shown, for example, that $G(3) \leq 7$ while $g(3) = 9$ and $G(4) = 16$ while $G(4) = 19$.

At present not much is known about numbers G(d) and this problem is currently a very active area of research in number theory.

Waring problem for rings

Problem 1. *For any ring A and any integer $k > 1$, let $A_k \subset A$ be the set of all sums of kth powers in A. For any $a \in A_k$, let $w_k(a, A)$ be the least s such that a is a sum of s k-th powers. Determine $w_k(A) = \sup_{a \in A_k} w_k(a)$. (It is possible that $w_k(A) = \infty$).*

In many rings it makes sense to talk about generic elements in A_k and, similarly, one can ask to determine the number $\widetilde{w}_k(A) = \sup_{a \in \widetilde{A}_k} w_k(a)$, where $\widetilde{A}_k$ is the appropriate set of generic elements in A_k.

We will refer to the latter question as the *weak Waring problem* as opposed to Problem 1 which we call the *strong Waring problem*.

Set-up

Below we concentrate on $A = \mathbb{C}[x_0, x_1, ..., x_n]$ and for convenience work with homogeneous polynomials usually referred to as forms. In this case it is known that A_k coincides with the space of all forms in $\mathbb{C}[x_0, x_1, ..., x_n]$ whose degree is divisible by k. Thus, the strong Waring problem for $\mathbb{C}[x_0, x_1, ..., x_n]$ is formulated as follows. Denote by S_n^d the linear space of all forms of degree d in $n + 1$ variables (with the 0-form included).

Problem 2. *Find the supremum over the set of all forms $f \in S_n^{kd}$ of the minimal number of forms of degree d needed to represent f as a sum of their k-th powers. In particular, how many forms of degree d is required to represent an arbitrary form $f \in S_n^{2d}$ as a sum of their squares?*

Recall that $\dim S_n^d = \binom{d+n}{n}$ and simple calculations show that

$$\frac{\dim S_n^{kd}}{\dim S_n^d} < k^n \quad \text{and} \quad \lim_{d\to\infty} \frac{\dim S_n^{kd}}{\dim S_n^d} = k^n.$$

Therefore, k^n is the lower bound for the answer to Problem 2 for d large enough. A version of Problem 2 related to the weak Waring problem is as follows.

Problem 3. *Find the minimum over all Zariski open subsets in S_n^{kd} of the number of forms of degree d needed to represent forms from these subsets as a sum of their k-th powers. In other words, how many k-th powers of forms of degree d is required to present a general form of degree kd?*

Main result

Our main result is the following.

Theorem

Given a positive integer $k \geq 2$*, then any general form* f *of degree* kd *in* $n+1$ *variables is a sum of at most* k^n k*-th powers. Moreover, for a fixed* n*, this bound is sharp for all sufficiently large* d*.*

Thus k^n gives an upper bound for the answer to Problem 3 for any $n \geq 1$ and $k \geq 2$, and it is optimal for all sufficiently large d, see Remark 1 below.

2 variables

Theorem

(i) *Any form f of even degree $2d$ in 2 variables is a sum of at most two squares;*

(ii) *a general form of even degree $2d$ in 2 variables can be represented as a sum of two squares in exactly $\binom{2d-1}{d}$ ways.*

The proof follows from the identity

$$f = A \cdot B = \left[\frac{1}{2}(A+B)\right]^2 + \left[\frac{i}{2}(A-B)\right]^2$$

and $\binom{2d-1}{d} = \frac{1}{2}\binom{2d}{d}$ is the number of ways f can be presented as the product of two factors A and B of equal degree. Thus, for $n = 1$ and $k = 2$ the answer to Problem 2 is two.

We recall that for any projective variety X, its p-th secant variety is defined as the Zariski closure of the union of the projective spans $< x_1, \ldots, x_p >$, where $x_i \in X$. The following result gives a convenient reformulation of our problem.

Theorem

Given a linear space V, a general polynomial in $S^{kd}V$ is a sum of p k-th powers $g_1^k, \ldots g_p^k$, where $g_i \in S^d V$ if and only if for p general forms $g_i \in S^d V$, $i = 1, \ldots p$, the ideal generated by $g_1^{k-1}, \ldots g_p^{k-1}$ contains $S^{kd}V$. (We shall call such an ideal kd-regular.)

Proof.

The statement is a direct consequence of Terracini's lemma. Consider the subvariety X in the ambient space $\mathcal{P}S^{kd}V$ consisting of the k-th powers of all forms from $S^d V$. The tangent space to X at $g_i^k \in X$ is of the form $\{g_i^{k-1} f | f \in S^d V\}$. Therefore, the p-secant variety of X coincides with the ambient space $\mathcal{P}S^{kd}V$ if and only if the span of the tangent spaces to X at general g_i^k, (which is equal to $\{\sum_{i=1}^p g_i^{k-1} f_i | f_i \in S^d V\}$), coincides with $\mathcal{P}S^{kd}V$ as well.

We will show that if V is an $(n+1)$-dimensional linear space, then the ideal generated by k^n general forms of type g_i^{k-1}, where $g_i \in S^d_n V$ is kd-regular, i.e., contains $S^{kd}V$.

In order to do this, it suffices to find k^n specific polynomials $\{g_1, \ldots g_{k^n}\}$ of degree d such that the ideal generated by the powers g_i^{k-1} is kd-regular.

Below, we will choose as g_i's powers of certain linear forms.

For powers of linear forms one can use a new point of view related to apolarity.

Definition. *A (Macaulay) inverse system is a finite-dimensional space of polynomials which is closed under the differentiation with respect to the variables.*

First, we define a pairing $< \cdot, \cdot >$ between the polynomial rings $\mathbb{C}[V]$ and $\mathbb{C}[V^\vee]$. Let $x_0, ..., x_n$ be a basis of V and $y_0, ..., y_n$ a dual basis of $V^\vee$. Then for each $f(\bar{x}) = f(x_0, ..., x_n) \in \mathbb{C}[V]$, define a differential operator $f(\partial/\partial\bar{y}) := f(\frac{\partial}{\partial y_0}, ..., \frac{\partial}{\partial y_n})$ on $\mathbb{C}[V^\vee]$. Analogously, for each $g(\bar{y}) = g(y_0, ..., y_n) \in \mathbb{C}[V^\vee]$, define a differential operator $g(\partial/\partial\bar{x}) := g(\frac{\partial}{\partial x_0}, ..., \frac{\partial}{\partial x_n})$ on $\mathbb{C}[V]$.

For form f and g of the same degree, we define the pairing

$$< f, g >:= f\left(\frac{\partial}{\partial\bar{y}}\right) \cdot g(\bar{y})|_{\bar{y}=0} = g\left(\frac{\partial}{\partial\bar{x}}\right) \cdot f(\bar{x})|_{\bar{x}=0}.$$

Definition. *The inverse system of a homogeneous ideal* $I \subset \mathbb{C}[V]$ *is its orthogonal complement with respect to the above pairing. In other words, it is given by*

$$I^{\perp} = \left\{ g(\bar{y}) \in \mathbb{C}[V^{\vee}] | f\left(\frac{\partial}{\partial \bar{y}}\right) \cdot g(y) = 0 \quad \text{for any} \quad f(\bar{x}) \in I \right\}.$$

Since $I^{\perp}$ is the space of solutions of a system of homogeneous linear differential equations with constant coefficients, it is a Macaulay inverse system. The space $I^{\perp}$ is graded. The dimension of the quotient algebra $A = \mathbb{C}[V^{\vee}]/I$ equals $\dim I^{\perp}$. Moreover, the dimension of the i-th graded component A_i of A equals the dimension of the i-th graded component of $I^{\perp}$.

Back to our considerations!

The space $T_{g^k}X^\perp$ orthogonal to $T_{g^k}X = \{g^{k-1}f | f \in S^d V\}$ is given by $T_{g^k}X^\perp = \{h \in S^{kd}V^\vee | h \cdot g^{k-1} = 0 \in S^d V^\vee\}$, i.e., is the space of polynomials in $V^\vee$ apolar to g^{k-1}. Moreover, when $g = l^m$, $l \in V$, the classical theory of apolarity provides a better result.

Lemma

A form $f \in S^m V^\vee$ is apolar to l^{m-k}, i.e., $l^{m-k} f = 0$ if and only if all the derivatives of f of order $\leq k$ vanish at $l \in V$.

Using the above Lemma one can reduce the Main Theorem to the following statement.

Theorem

For a given integer $k \geq 2$, a form of degree kd in $(n+1)$ variables which has all derivatives of order $\leq d$ vanishing at k^n general points vanishes identically.

Our final effort will be settle the latter Theorem. Denote by $x_0, \ldots, x_n$ a basis of V. Let $\xi_i = e^{2\pi i\sqrt{-1}/k}$ for $i = 0, \ldots, k-1$ be the (set of all) k-th roots of unity. By semicontinuity, it is enough to find k^n special points in $\mathcal{P}V \simeq \mathbf{P}^n$ such that a polynomial of degree kd in $\mathbf{P}^n$ which has all derivatives of order $\leq d$ vanishing at these points must necessarily vanish identically. As such points we choose the points $(1, \xi_{i_1}, \xi_{i_2}, \ldots, \xi_{i_n})$, where $0 \leq i_j \leq k-1$, $1 \leq j \leq n$.

The following result proves even more than was claimed in Theorem 6.

Theorem

For a given integer $k \geq 2$, a form of degree $kd + k - 1$ in $(n+1)$ variables which has all derivatives of order $\leq d$ vanishing at k^n general points vanishes identically.

Proof:

As above we choose as our configuration the k^n points $(1, \xi_{i_1}, \xi_{i_2}, \ldots, \xi_{i_n})$, where $0 \leq i_j \leq k-1$, $1 \leq j \leq n$. Consider first the case $n = 1$. If a form $f(x_0, x_1)$ of degree $kd + k - 1$ has its derivatives of order $\leq d$ vanishing at all $(1, \xi_i)$, then f should be divisible by $(x_1 - \xi_i x_0)^{d+1}$ for $i = 0, \ldots k-1$ and, therefore, if f is not vanishing identically, then its degree should be at least $k(d+1)$, which is a contradiction.

For $n \geq 2$, consider the arrangement of $\binom{n}{2}k$ hyperplanes given by $x_i = \xi_s x_j$, where $1 \leq i < j \leq n$, $0 \leq s \leq k-1$. One can easily check that this arrangement has the property that each hyperplane contains exactly k^{n-1} points. Furthermore, each point is contained in exactly $\binom{n}{2}$ hyperplanes. Indeed, consider, for example, the hyperplane $\mathcal{H}$ given by $x_n = \xi_i x_{n-1}$. The natural parametrization of $\mathcal{H}$ is by $(x_0, \ldots, x_{n-1}) \mapsto (x_0, x_1, \ldots, x_{n-1}, \xi_i x_{n-1})$ and the k^{n-1} points which lie on $\mathcal{H}$ correspond, according to this parametrization, exactly to $(1, \xi_{i_1}, \xi_{i_2}, \ldots, \xi_{i_{n-1}})$ for $0 \leq i_j \leq k-1$, $1 \leq j \leq n-1$. In other words, they correspond exactly to our arrangement of points in the previous dimension n.

Our proof now proceeds by a double induction on the number of variables n and degree d. Assume that the statement holds for all d and up to n variables. (The case $n = 1$ is settled above.)

Let us perform a step of induction in d. First we settle the case $d \leq \binom{n}{2} - 1$. Consider a polynomial f of degree $kd + k - 1$ satisfying our assumptions. Restricting f to each of the above $\binom{n}{2}k$ hyperplanes $x_i = \xi_s x_j$, where $1 \leq i < j \leq n$, $0 \leq s \leq k-1$, we obtain the same situation in dimension n. By the induction hypothesis f vanishes on each such hyperplane and, therefore, must be divisible by H, where H is the product of the linear forms $x_i = \xi_s x_j$ defining all the chosen hyperplanes. (Obviously, $\deg H = \binom{n}{2}k$.) Thus, f vanishes identically since $k\left(\binom{n}{2} - 1\right) + k - 1 < \binom{n}{2}k$. For higher degrees we argue as follows. Take a form f of degree $kd + k - 1$ satisfying our assumptions. Restricting as above f to each of the above $\binom{n}{2}k$ hyperplanes $x_i = \xi_s x_j$, we obtain the same situation in dimension n.

Again, by the induction hypothesis f vanishes on each such hyperplane and must be divisible by H. We get

$$f = H\tilde{f},$$

where $\deg \tilde{f} = k\left(d - \binom{n}{2}\right) + k - 1$ and $\tilde{f}$ has all derivatives of order $\leq d - \binom{n}{2}$ vanishing at the same k^n points $(1, \xi_{i_1}, \xi_{i_2}, \dots, \xi_{i_n})$. Indeed, in any affine coordinate system centered at any of these points, f has no terms of degree $\leq d$. Since H has its lowest term in degree $\binom{n}{2}$ it follows that $\tilde{f}$ has no terms in degree $\leq d - \binom{n}{2}$. By the induction hypothesis $\tilde{f}$ is identically zero.

Notice that we have also obtained the following result of independent interest.

Corollary

Any form of degree kd in $(n+1)$ variables can be expressed as a linear combination of the polynomials $(x_0 + \xi_{i_1}x_1 + \xi_{i_2}x_2 + \ldots + \xi_{i_n}x_n)^{(k-1)d}$ with coefficients being polynomials of degree d.

Open problems

Remark 1. Although k^n is the correct asymptotic bound, it seems to be sharp only for considerably large values d. In particular, computer experiments show that for $k = 2,\ n = 3$ and $d \leq 20$ seven general polynomials of degree d suffice to generate the space of polynomials in degree $2d$. All eight polynomials are required only for $d \geq 21$. Similarly, for $n = 4$ and $d \leq 75$ experiments suggest that 15 (instead of the expected 16) general polynomials of degree d suffice to generate the space of polynomials in degree $2d$. Analogously, all 16 polynomials are required for $d \geq 76$. The ultimate challenge of this project is to solve completely Problem 8 for triples (n, k, d), and, in particular, to find the complete list of exceptional triples for which the answer to Problem 8 is larger than the one obtained by dimension count. Obviously, this list should include the list of exceptional cases obtained earlier by J. Alexander and A. Hirschowitz.

General Conjecture

Main conjecture of G. Ottaviani. The d-th Waring rank of a generic form of degree kd in $n+1$ variables is given by:

$$rk_d(n+1,k) = \begin{cases} \min\{s \mid s\binom{n+k}{n} - \binom{s}{2} \geq \binom{n+k}{n}\}, & \text{for } d = 2 \\ \left\lceil \frac{\binom{n+kd}{n}}{\binom{n+k}{n}} \right\rceil, & \text{for } d \geq 3. \end{cases}$$

Open problems, cont. 1

Remark 3. What about the strong Waring problem over $\mathbb{C}$?

By a result of Blekherman –Teitler, the maximal rank over $\mathbb{C}$ is at most twice the generic rank over $\mathbb{C}$, i.e.,

$$rk_d^{max}(n+1,k) \leq 2rk_d(n+1,k)$$

Remark 4. What about the strong Waring problem over $\mathbb{R}$?

By a very recent result of C. Scheiderer, for $n=2$, $k=2$ and any d,

$$rk_d^{max,\mathbb{R}}(3,2) = d+1 \text{ or } d+2,$$

while $rk_d^{max}(3,2) \leq 8$.

THANK YOU FOR YOUR ATTENTION!