Rainy Day Lemmas # 12 and 35

Bruce Reznick
University of Illinois at Urbana-Champaign

East Coast Computer Algebra Day
Wolfram World HQ April 29, 2017

Thank you for coming to the talk. I speak not as a producer of computer algebra, but as a consumer. Richard Hamming, who got his PhD from UIUC in 1942, liked to say that "The purpose of computing is insight, not numbers." In part, the justification of this talk is to present a few examples where insight allows you to do computations which are otherwise unwieldy.

Thank you for coming to the talk. I speak not as a producer of computer algebra, but as a consumer. Richard Hamming, who got his PhD from UIUC in 1942, liked to say that "The purpose of computing is insight, not numbers." In part, the justification of this talk is to present a few examples where insight allows you to do computations which are otherwise unwieldy.

My main interest here is homogeneous polynomials (forms) over $\mathbb{C}$ and their representation as a sum of powers of forms of lower degree. Most of the work I'm talking about is on papers which can be found on my website, or in the other talks from which this one has been Frankenstein'd.

Thank you for coming to the talk. I speak not as a producer of computer algebra, but as a consumer. Richard Hamming, who got his PhD from UIUC in 1942, liked to say that "The purpose of computing is insight, not numbers." In part, the justification of this talk is to present a few examples where insight allows you to do computations which are otherwise unwieldy.

My main interest here is homogeneous polynomials (forms) over $\mathbb{C}$ and their representation as a sum of powers of forms of lower degree. Most of the work I'm talking about is on papers which can be found on my website, or in the other talks from which this one has been Frankenstein'd.

The organization of this talk after the introduction is (basically): canonical forms, sums of powers of linear forms, sums of powers of quadratic forms.

I want to focus on a beautiful conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms (homeogeneous polynomials) $p(x, y)$ of degree m with complex coefficients, and suppose $m = de$, $d, e \in \mathbb{N}$.

Conjecture

Every $p \in H_{de}(\mathbb{C}^2)$ can be written as a sum of at most d d-th powers of forms in $H_e(\mathbb{C}^2)$.

I want to focus on a beautiful conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms (homeogeneous polynomials) $p(x, y)$ of degree m with complex coefficients, and suppose $m = de$, $d, e \in \mathbb{N}$.

Conjecture

Every $p \in H_{de}(\mathbb{C}^2)$ can be written as a sum of at most d d-th powers of forms in $H_e(\mathbb{C}^2)$.

The first point to make is that this assertion is a *universal* statement, not a *generic* one.

I want to focus on a beautiful conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms (homeogeneous polynomials) $p(x, y)$ of degree m with complex coefficients, and suppose $m = de$, $d, e \in \mathbb{N}$.

Conjecture

Every $p \in H_{de}(\mathbb{C}^2)$ can be written as a sum of at most d d-th powers of forms in $H_e(\mathbb{C}^2)$.

The first point to make is that this assertion is a *universal* statement, not a *generic* one.

If $e = 1$, this conjecture is a familiar statement to those who work with Waring rank, and the binary forms of degree d which require d d-th powers of linear forms are precisely those of the shape $\ell^{d-1}\ell'$, where ℓ and ℓ' are non-proportional linear forms. (More on this later.)

If $d = 1$, there is nothing to prove.

If $d = 1$, there is nothing to prove.

If $d = 2$, then $m = 2e$ is even, and p can be factored into linear factors in $\binom{2e-1}{e}$ ways, so that $p = fg$ for $f, g \in H_e(\mathbb{C}^2)$ and

$$p = fg = \left(\frac{f+g}{2}\right)^2 - \left(\frac{f-g}{2}\right)^2 = \left(\frac{f+g}{2}\right)^2 + \left(\frac{f-g}{2i}\right)^2.$$

If $d = 1$, there is nothing to prove.

If $d = 2$, then $m = 2e$ is even, and p can be factored into linear factors in $\binom{2e-1}{e}$ ways, so that $p = fg$ for $f, g \in H_e(\mathbb{C}^2)$ and

$$p = fg = \left(\frac{f+g}{2}\right)^2 - \left(\frac{f-g}{2}\right)^2 = \left(\frac{f+g}{2}\right)^2 + \left(\frac{f-g}{2i}\right)^2.$$

The conjecture is true generically. Using the classical Lasker-Wakeford approach, if $de + 1 = k(e+1) + s$, $0 \leq s \leq e$, then

$$\sum_{j=1}^{k} (\alpha_{j0} x^e + \dots)^d + (\beta_0 x^e + \cdots + \beta_{s-1} x^{e-(s-1)} y^{s-1})^d$$

is a "canonical form" for binary forms of degree de, and

$$k + 1 = \left\lceil \frac{de+1}{e+1} \right\rceil \leq \left\lceil \frac{de+d}{e+1} \right\rceil = d.$$

If $d = 1$, there is nothing to prove.

If $d = 2$, then $m = 2e$ is even, and p can be factored into linear factors in $\binom{2e-1}{e}$ ways, so that $p = fg$ for $f, g \in H_e(\mathbb{C}^2)$ and

$$p = fg = \left(\frac{f+g}{2}\right)^2 - \left(\frac{f-g}{2}\right)^2 = \left(\frac{f+g}{2}\right)^2 + \left(\frac{f-g}{2i}\right)^2.$$

The conjecture is true generically. Using the classical Lasker-Wakeford approach, if $de + 1 = k(e+1) + s$, $0 \leq s \leq e$, then

$$\sum_{j=1}^{k} (\alpha_{j0} x^e + \dots)^d + (\beta_0 x^e + \cdots + \beta_{s-1} x^{e-(s-1)} y^{s-1})^d$$

is a "canonical form" for binary forms of degree de, and

$$k + 1 = \left\lceil \frac{de+1}{e+1} \right\rceil \leq \left\lceil \frac{de+d}{e+1} \right\rceil = d.$$

I will say a bit more about Lasker-Wakeford later.

I will also give you a proof of the first "new" case: $(d, e) = (3, 2)$: every binary sextic is a sum of three cubes of quadratic forms. As we'll see, this proof would be impossible without some kind of computer algebra.

I will also give you a proof of the first "new" case: $(d, e) = (3, 2)$: every binary sextic is a sum of three cubes of quadratic forms. As we'll see, this proof would be impossible without some kind of computer algebra.

The conjecture is easily true if you remove the restriction to forms (but lose the information about degrees). By a 1979 result of Newman-Slater, every complex polynomial in any number of variables is an explicit sum of d d-th powers of polynomials. Let ζ_d denote a primitive d-th root of unity and p be a polynomial in any number of variables. Then the usual orthogonality properties of roots of unity imply that

$$d^2 p = \sum_{k=0}^{d-1} \zeta_d^{-k} (1 + \zeta_d^k p)^d.$$

This equation fails to be helpful if you want both sides to be homogeneous.

Some notation.
Let $H_d(\mathbb{C}^n)$ denote the set of forms $p(x_1, \ldots, x_n)$ of degree d with coefficients in $\mathbb{C}$. The dimension of the vector space $H_d(\mathbb{C}^n)$ is $N(n,d) := \binom{n+d-1}{d}$. Let $\mathcal{I}(n,d)$ be the index set:

$$\mathcal{I}(n,d) = \left\{ (i_1, \ldots, i_n) : 0 \leq i_k \in \mathbb{Z}, \quad \sum_k i_k = d \right\}.$$

Some notation.
Let $H_d(\mathbb{C}^n)$ denote the set of forms $p(x_1, \ldots, x_n)$ of degree d with coefficients in $\mathbb{C}$. The dimension of the vector space $H_d(\mathbb{C}^n)$ is $N(n,d) := \binom{n+d-1}{d}$. Let $\mathcal{I}(n,d)$ be the index set:

$$\mathcal{I}(n,d) = \left\{ (i_1, \ldots, i_n) : 0 \leq i_k \in \mathbb{Z}, \quad \sum_k i_k = d \right\}.$$

Let $x^i = x_1^{i_1} \cdots x_n^{i_n}$ and $c(i) = \frac{d!}{\prod i_k!}$ denote the multinomial coefficient. If $p \in H_d(\mathbb{C}^n)$, then we can write

$$p(x_1, \ldots, x_n) = \sum_{i \in \mathcal{I}(n,d)} c(i) a(p; i) x^i.$$

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

Theorem

Suppose $F : \mathbb{C}^m \to \mathbb{C}^r$ *is a polynomial map; that is,*

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_r(t_1, \ldots, t_m))$$

where each $f_j \in \mathbb{C}[t_1, \ldots, t_m]$. *Then either (i) or (ii) holds:*

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

Theorem

Suppose $F : \mathbb{C}^m \to \mathbb{C}^r$ *is a polynomial map; that is,*

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_r(t_1, \ldots, t_m))$$

where each $f_j \in \mathbb{C}[t_1, \ldots, t_m]$. *Then either (i) or (ii) holds:*

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

Theorem

Suppose $F : \mathbb{C}^m \to \mathbb{C}^r$ *is a polynomial map; that is,*

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_r(t_1, \ldots, t_m))$$

where each $f_j \in \mathbb{C}[t_1, \ldots, t_m]$. *Then either (i) or (ii) holds:*
(i) The polynomials $\{f_j : 1 \leq j \leq r\}$ *are algebraically dependent and* $F(\mathbb{C}^m)$ *lies in some non-trivial* $\{P = 0\}$ *in* $\mathbb{C}^r$.

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

Theorem

Suppose $F : \mathbb{C}^m \to \mathbb{C}^r$ *is a polynomial map; that is,*

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_r(t_1, \ldots, t_m))$$

where each $f_j \in \mathbb{C}[t_1, \ldots, t_m]$. *Then either (i) or (ii) holds:*
(i) The polynomials $\{f_j : 1 \leq j \leq r\}$ *are algebraically dependent and* $F(\mathbb{C}^m)$ *lies in some non-trivial* $\{P = 0\}$ *in* $\mathbb{C}^r$.
(ii) The polynomials $\{f_j : 1 \leq j \leq r\}$ *are algebraically independent and* $(F(\mathbb{C}^m))^c$ *lies in some non-trivial* $\{P = 0\}$ *in* $\mathbb{C}^r$.

The following amazing theorem is not as well known as it should be. The only accessible proof of (ii) I know is in Ehrenborg-Rota, attributed to Artin and Mattuck. Please let me know of others!

Theorem

Suppose $F : \mathbb{C}^m \to \mathbb{C}^r$ *is a polynomial map; that is,*

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_r(t_1, \ldots, t_m))$$

where each $f_j \in \mathbb{C}[t_1, \ldots, t_m]$. *Then either (i) or (ii) holds:*
(i) The polynomials $\{f_j : 1 \leq j \leq r\}$ *are algebraically dependent and* $F(\mathbb{C}^m)$ *lies in some non-trivial* $\{P = 0\}$ *in* $\mathbb{C}^r$.
(ii) The polynomials $\{f_j : 1 \leq j \leq r\}$ *are algebraically independent and* $(F(\mathbb{C}^m))^c$ *lies in some non-trivial* $\{P = 0\}$ *in* $\mathbb{C}^r$.
Furthermore, the second case occurs if and only there is a point $u \in \mathbb{C}^m$ *at which the Jacobian matrix* $\left[\frac{\partial f_j}{\partial t_k}(u)\right]$ *has rank* r.

When $m = r = N(n, d)$, we may interpret such an F as a map from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ by indexing $\mathcal{I}(n, d)$ as $\{i_j : 1 \leq j \leq N\}$ and making the interpretation in an abuse of notation that

$$F(t, x) = \sum_{j=1}^{N} f_j(t_1 \ldots, t_N) x^{i_j}.$$

When $m = r = N(n, d)$, we may interpret such an F as a map from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ by indexing $\mathcal{I}(n, d)$ as $\{i_j : 1 \leq j \leq N\}$ and making the interpretation in an abuse of notation that

$$F(t, x) = \sum_{j=1}^{N} f_j(t_1 \ldots, t_N) x^{i_j}.$$

Definition

A **canonical form** for $H_d(\mathbb{C}^n)$ is any polynomial map F from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ so that "almost every" $p \in H_d(\mathbb{C}^n)$ is in the range of F.

When $m = r = N(n, d)$, we may interpret such an F as a map from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ by indexing $\mathcal{I}(n, d)$ as $\{i_j : 1 \leq j \leq N\}$ and making the interpretation in an abuse of notation that

$$F(t, x) = \sum_{j=1}^{N} f_j(t_1 \ldots, t_N) x^{i_j}.$$

Definition

A **canonical form** for $H_d(\mathbb{C}^n)$ is any polynomial map F from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ so that "almost every" $p \in H_d(\mathbb{C}^n)$ is in the range of F.

When $m = r = N(n, d)$, we may interpret such an F as a map from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ by indexing $\mathcal{I}(n, d)$ as $\{i_j : 1 \leq j \leq N\}$ and making the interpretation in an abuse of notation that

$$F(t, x) = \sum_{j=1}^{N} f_j(t_1 \ldots, t_N) x^{i_j}.$$

Definition

A **canonical form** for $H_d(\mathbb{C}^n)$ is any polynomial map F from $\mathbb{C}^N$ to $H_d(\mathbb{C}^n)$ so that "almost every" $p \in H_d(\mathbb{C}^n)$ is in the range of F.

If $\{\phi_j\}$ is a basis of $H_d(\mathbb{C}^n)$, e.g. $\phi_j(x) = c(i_j)x^{i_j}$, then $F(t, x) = \sum_{j=1}^{N} t_j \phi_j(x)$ is technically, though not traditionally, a canonical form.

Here's a really simple example: Take a form in $H_2(\mathbb{C}^2)$:

$$p(x, y) = ax^2 + 2bxy + cy^2.$$

As long as $a \neq 0$, we can find $t_j \in \mathbb{C}$ by completing the square so that

$$p(x, y) = (t_1 x + t_2 y)^2 + (t_3 y)^2.$$

Here's a really simple example: Take a form in $H_2(\mathbb{C}^2)$:

$$p(x, y) = ax^2 + 2bxy + cy^2.$$

As long as $a \neq 0$, we can find $t_j \in \mathbb{C}$ by completing the square so that

$$p(x, y) = (t_1 x + t_2 y)^2 + (t_3 y)^2.$$

Using our machinery with $F(t_1, t_2, t_3) = (t_1^2, t_1 t_2, t_2^2 + t_3^2)$, then at "most" choices of t, the Jacobian has rank 3 and, indeed,

$$F(\mathbb{C}^3) = \{(z_1, z_2, z_3) : z_1 \neq 0\} \cup \{(0, 0, z_3)\}.$$

which is case (ii).

Why can't we just constant-count in the non-obvious cases? Historically, the simplest example occurs in $H_4(\mathbb{C}^3)$. Since $N(3,4) = \binom{6}{2} = 15$, can a general ternary quartic can be written as

$$p(x_1, x_2, x_3) = \sum_{k=1}^{5} (\alpha_{k1} x_1 + \alpha_{k2} x_2 + \alpha_{k3} x_3)^4 ?$$

This would be a canonical form, if the partials with respect to the α_{kj}'s at some chosen value span $H_4(\mathbb{C}^3)$. Using "apolarity", which I don't have time to explain, this is equivalent to there being no non-zero quartic which is singular at the $\alpha_k = (\alpha_{k1}, \alpha_{k2}, \alpha_{k3})$'s.

Why can't we just constant-count in the non-obvious cases? Historically, the simplest example occurs in $H_4(\mathbb{C}^3)$. Since $N(3,4) = \binom{6}{2} = 15$, can a general ternary quartic can be written as

$$p(x_1, x_2, x_3) = \sum_{k=1}^{5} (\alpha_{k1}x_1 + \alpha_{k2}x_2 + \alpha_{k3}x_3)^4?$$

This would be a canonical form, if the partials with respect to the α_{kj}'s at some chosen value span $H_4(\mathbb{C}^3)$. Using "apolarity", which I don't have time to explain, this is equivalent to there being no non-zero quartic which is singular at the $\alpha_k = (\alpha_{k1}, \alpha_{k2}, \alpha_{k3})$'s.

However, as Clebsch argued in the 1860's, since $N(3,2) = 6$, any choice of five α_k's pass through a non-zero quadratic $h(x_1, x_2, x_3)$, and h^2 is such a singular quartic. Thus, a sum of five 4th powers is not a canonical form for ternary quartics.

A few years later, Sylvester gave another proof. Given

$$p(x_1, x_2, x_3) = \sum_{r+s+t=4} \frac{4!}{r!s!t!} a_{rst} x_1^r x_2^s x_3^t,$$

define the catalecticant H_p as a quadratic form in 6 variables (or a 6×6 symmetric matrix defined **linearly** in terms of p).

$$H_p = \begin{pmatrix} a_{400} & a_{220} & a_{202} & a_{310} & a_{301} & a_{211} \\ a_{220} & a_{040} & a_{022} & a_{130} & a_{121} & a_{031} \\ a_{202} & a_{022} & a_{004} & a_{112} & a_{103} & a_{013} \\ a_{310} & a_{130} & a_{112} & a_{220} & a_{211} & a_{121} \\ a_{301} & a_{121} & a_{103} & a_{211} & a_{202} & a_{112} \\ a_{211} & a_{031} & a_{013} & a_{121} & a_{112} & a_{022} \end{pmatrix}$$

(This also has an apolar interpretation as $q^2(D)p$.)

Under this definition, $H_{(\alpha_k \cdot)^4}$ is a perfect square. Thus if p is a sum of five fourth powers, then $rank(H_p) \leq 5$, so H_p is singular. This can't happen for a general ternary quartic, where the determinant is non-zero. The vanishing of the determinant is precisely the algebraic relation of the 15 coefficients in a sum of five fourth powers. Clebsch's proof and Sylvester's proof are really the same, but that would take another talk.

Under this definition, $H_{(\alpha_k \cdot)^4}$ is a perfect square. Thus if p is a sum of five fourth powers, then $rank(H_p) \leq 5$, so H_p is singular. This can't happen for a general ternary quartic, where the determinant is non-zero. The vanishing of the determinant is precisely the algebraic relation of the 15 coefficients in a sum of five fourth powers. Clebsch's proof and Sylvester's proof are really the same, but that would take another talk.

In his original paper, Sylvester apologized for introducing this term: "Meicatalecticizant would more completely express the meaning of that which, for the sake of brevity, I denominate the catalecticant." Sylvester was very interested in the technical aspects of poetry and a "catalectic" verse is one in which the last line is missing a foot.

Under this definition, $H_{(\alpha_k \cdot)^4}$ is a perfect square. Thus if p is a sum of five fourth powers, then $rank(H_p) \leq 5$, so H_p is singular. This can't happen for a general ternary quartic, where the determinant is non-zero. The vanishing of the determinant is precisely the algebraic relation of the 15 coefficients in a sum of five fourth powers. Clebsch's proof and Sylvester's proof are really the same, but that would take another talk.

In his original paper, Sylvester apologized for introducing this term: "Meicatalecticizant would more completely express the meaning of that which, for the sake of brevity, I denominate the catalecticant." Sylvester was very interested in the technical aspects of poetry and a "catalectic" verse is one in which the last line is missing a foot.

To his credit, in the same paper, Sylvester introduced the term "unimodular" in its current meaning.

Our 19th century ancestors saw that funny things happen in sums of powers of linear forms. when $(n, d) = (3, 4), (4, 4), (5, 4), (5, 3)$. In the early 1990s, Alexander and Hirschowitz proved that these are the only cases in which this can happen. This is the basis of another talk, and probably one that's better than this one, especially if someone else gives it.

Our 19th century ancestors saw that funny things happen in sums of powers of linear forms. when $(n, d) = (3, 4), (4, 4), (5, 4), (5, 3)$. In the early 1990s, Alexander and Hirschowitz proved that these are the only cases in which this can happen. This is the basis of another talk, and probably one that's better than this one, especially if someone else gives it.

The attribution "Lasker-Wakeford" comes from *The theory of determinants, matrices and invariants* by H. W. Turnbull, who was one of the last "pre-Hilbert" invariant theorists. This 1960 book is a Rosetta Stone for understanding 19th century algebra. Turnbull described this theorem as "paradoxical and very curious". It is the "apolar" version of the earlier result.

Theorem (Lasker-Wakeford)

If $F : \mathbb{C}^N \to H_d(\mathbb{C}^n)$, then F is a canonical form if and only if there is a point $u \in \mathbb{C}^N$ so that there is no non-zero form q which is apolar to all N forms $\{\frac{\partial F}{\partial t_1}(u), \ldots, \frac{\partial F}{\partial t_N}(u)\}$.

And now, a biographical interlude.

Emanuel Lasker (1868-1941) received his Ph.D. under Max Noether at Göttingen in 1902. He first developed the concept of a primary ideal and proved the primary decomposition theorem for an ideal of a polynomial ring in terms of primary ideals.

And now, a biographical interlude.

Emanuel Lasker (1868-1941) received his Ph.D. under Max Noether at Göttingen in 1902. He first developed the concept of a primary ideal and proved the primary decomposition theorem for an ideal of a polynomial ring in terms of primary ideals.

He is probably better known for being the world chess champion for 27 years (1894-1921), which spanned the life of ...

Edward Kingsley Wakeford (1894-1916).

And now, a biographical interlude.

Emanuel Lasker (1868-1941) received his Ph.D. under Max Noether at Göttingen in 1902. He first developed the concept of a primary ideal and proved the primary decomposition theorem for an ideal of a polynomial ring in terms of primary ideals.

He is probably better known for being the world chess champion for 27 years (1894-1921), which spanned the life of ...

Edward Kingsley Wakeford (1894-1916).

If you remember European history, those dates will give you pause.

The memorial article by J. H. Grace about Wakeford in the 1917/1918 volume of *Proceedings of the London Mathematical Society* may be the angriest obituary I've ever read in a scholarly journal, and it can be found in its entirety on my webpage:

The memorial article by J. H. Grace about Wakeford in the 1917/1918 volume of *Proceedings of the London Mathematical Society* may be the angriest obituary I've ever read in a scholarly journal, and it can be found in its entirety on my webpage:

http://www.math.uiuc.edu/∼reznick/wakeford.pdf

"He [EKW] was slightly wounded early in 1916, and soon after coming home was busy again with Canonical Forms.... [H]e discovered a paper of Hilbert's which contained the very theorem he had long been in want of – first vaguely, and later quite definitely. This was in March; April found him, full of the most joyous and reverential admiration for the great German master, working away in fearful haste to finish the dissertation ...

The memorial article by J. H. Grace about Wakeford in the 1917/1918 volume of *Proceedings of the London Mathematical Society* may be the angriest obituary I've ever read in a scholarly journal, and it can be found in its entirety on my webpage:

http://www.math.uiuc.edu/∼reznick/wakeford.pdf

"He [EKW] was slightly wounded early in 1916, and soon after coming home was busy again with Canonical Forms.... [H]e discovered a paper of Hilbert's which contained the very theorem he had long been in want of – first vaguely, and later quite definitely. This was in March; April found him, full of the most joyous and reverential admiration for the great German master, working away in fearful haste to finish the dissertation ...

He returned to the front in June and was killed in July.... He only needed a chance, and he never got it."

The question of canonical forms for binary forms as a sum of powers of linear forms was completely settled by Sylvester in 1851.

Theorem (Sylvester's Canonical Forms)

(i) A general binary form of odd degree $d = 2k - 1$ can be written uniquely (i.e., up to indexing and roots of unity) as

$$\sum_{j=1}^{k} (\alpha_j x + \beta_j y)^{2k-1}.$$

(ii) A general binary form of even degree $d = 2k$ can be written uniquely as

$$\lambda \cdot x^{2k} + \sum_{j=1}^{k} (\alpha_j x + \beta_j y)^{2k}.$$

for some $\lambda \in \mathbb{C}$.

In 1869, James Joseph Sylvester (1814-1897) reflected on the discovery of his canonical forms, done while he was working as an actuary in the office next to Arthur Cayley's.

In 1869, James Joseph Sylvester (1814-1897) reflected on the discovery of his canonical forms, done while he was working as an actuary in the office next to Arthur Cayley's.

"I discovered and developed the whole theory of canonical binary forms for odd degrees, and, as far as yet made out, for even degrees too, at one evening sitting, with a decanter of port wine to sustain nature's flagging energies, in a back office in Lincoln's Inn Fields. The work was done, and well done, but at the usual cost of racking thought — a brain on fire, and feet feeling, or feelingless, as if plunged in an ice-pail. *That night we slept no more.*"

In 1869, James Joseph Sylvester (1814-1897) reflected on the discovery of his canonical forms, done while he was working as an actuary in the office next to Arthur Cayley's.

"I discovered and developed the whole theory of canonical binary forms for odd degrees, and, as far as yet made out, for even degrees too, at one evening sitting, with a decanter of port wine to sustain nature's flagging energies, in a back office in Lincoln's Inn Fields. The work was done, and well done, but at the usual cost of racking thought — a brain on fire, and feet feeling, or feelingless, as if plunged in an ice-pail. *That night we slept no more.*"

The "λx^{2k}" must be what Sylvester meant by "as far as yet made out". As if anticipating modern mathematics, Sylvester proved his theory with one brilliant algorithm.

Theorem (Sylvester)

Suppose $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j$ *and* $\{\alpha_k x + \beta_k y\}$ *is a set of non-proportional linear factors. Let* $h(x,y) = \sum_{t=0}^{r} c_t x^{r-t} y^t$ $= \prod_{j=1}^{r} (\beta_j x - \alpha_j y)$. *Then there exist* $\lambda_k \in \mathbb{C}$ *so that*

$$p(x,y) = \sum_{k=1}^{r} \lambda_k (\alpha_k x + \beta_k y)^d$$

if and only if

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_r \\ a_1 & a_2 & \cdots & a_{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-r} & a_{d-r+1} & \cdots & a_d \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Theorem (Sylvester)

Suppose $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j$ *and* $\{\alpha_k x + \beta_k y\}$ *is a set of non-proportional linear factors. Let* $h(x,y) = \sum_{t=0}^{r} c_t x^{r-t} y^t$ $= \prod_{j=1}^{r} (\beta_j x - \alpha_j y)$. *Then there exist* $\lambda_k \in \mathbb{C}$ *so that*

$$p(x,y) = \sum_{k=1}^{r} \lambda_k (\alpha_k x + \beta_k y)^d$$

if and only if

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_r \\ a_1 & a_2 & \cdots & a_{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-r} & a_{d-r+1} & \cdots & a_d \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Theorem (Sylvester)

Suppose $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j$ *and* $\{\alpha_k x + \beta_k y\}$ *is a set of non-proportional linear factors. Let* $h(x,y) = \sum_{t=0}^{r} c_t x^{r-t} y^t$ $= \prod_{j=1}^{r} (\beta_j x - \alpha_j y)$. *Then there exist* $\lambda_k \in \mathbb{C}$ *so that*

$$p(x,y) = \sum_{k=1}^{r} \lambda_k (\alpha_k x + \beta_k y)^d$$

if and only if

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_r \\ a_1 & a_2 & \cdots & a_{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-r} & a_{d-r+1} & \cdots & a_d \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

(This is an algorithm, because you start with $r = 1$ and increment until you find a null-vector which gives a square-free h.)

If $d = 2s - 1$ and $r = s$, then the matrix is $s \times (s + 1)$ and has a non-trivial null-vector. The corresponding h (given in terms of the coefficients of p) has distinct factors unless its discriminant vanishes, giving the canonical form in odd degree.

If $d = 2s - 1$ and $r = s$, then the matrix is $s \times (s + 1)$ and has a non-trivial null-vector. The corresponding h (given in terms of the coefficients of p) has distinct factors unless its discriminant vanishes, giving the canonical form in odd degree.
If $d = 2s$ and $r = s$, then the matrix is square, and in general, there exists λ so that $p(x, y) - \lambda x^{2s}$ has a matrix with a non-trivial null-vector as above, giving the canonical form in even degree.
It can be shown without too much difficulty that if $r = d$, so there is a single equation, then there is a null-vector whose resulting form is square-free, and thus, every binary form of degree d is a sum of at most d d-th powers of linear forms.

If $d = 2s - 1$ and $r = s$, then the matrix is $s \times (s + 1)$ and has a non-trivial null-vector. The corresponding h (given in terms of the coefficients of p) has distinct factors unless its discriminant vanishes, giving the canonical form in odd degree.
If $d = 2s$ and $r = s$, then the matrix is square, and in general, there exists λ so that $p(x, y) - \lambda x^{2s}$ has a matrix with a non-trivial null-vector as above, giving the canonical form in even degree.
It can be shown without too much difficulty that if $r = d$, so there is a single equation, then there is a null-vector whose resulting form is square-free, and thus, every binary form of degree d is a sum of at most d d-th powers of linear forms.
It is not hard to see that $x^{d-1}y$ is not a sum of $d - 1$ powers, because

$$\begin{pmatrix} 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \implies c_0 = c_1 = 0.$$

Here is an example of Sylvester's algorithm in action. Let

$$p(x,y) = 3x^5 - 20x^3y^2 + 10xy^4 =$$

$$\binom{5}{0} \cdot 3\, x^5 + \binom{5}{1} \cdot 0\, x^4y + \binom{5}{2} \cdot (-2)\, x^3y^2$$

$$+ \binom{5}{3} \cdot 0\, x^2y^3 + \binom{5}{4} \cdot 2\, xy^4 + \binom{5}{5} \cdot 0\, y^5;$$

$$\begin{pmatrix} 3 & 0 & -2 & 0 \\ 0 & -2 & 0 & 2 \\ -2 & 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Here is an example of Sylvester's algorithm in action. Let

$$p(x,y) = 3x^5 - 20x^3y^2 + 10xy^4 =$$
$$\binom{5}{0} \cdot 3\, x^5 + \binom{5}{1} \cdot 0\, x^4y + \binom{5}{2} \cdot (-2)\, x^3y^2$$
$$+\binom{5}{3} \cdot 0\, x^2y^3 + \binom{5}{4} \cdot 2\, xy^4 + \binom{5}{5} \cdot 0\, y^5;$$
$$\begin{pmatrix} 3 & 0 & -2 & 0 \\ 0 & -2 & 0 & 2 \\ -2 & 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

We have $h(x,y) = y(x^2+y^2) = y(y-ix)(y+ix)$.
Accordingly, there exist $\lambda_k \in \mathbb{C}$ so that

$$p(x,y) = \lambda_1 x^5 + \lambda_2 (x+iy)^5 + \lambda_3 (x-iy)^5.$$

Indeed, $\lambda_1 = \lambda_2 = \lambda_3 = 1$, as may be checked.

It would take us too far afield to spend much time on this, but the number of summands required depends on the field in which one allows coefficients. A few years ago, I proved that the quintic from the last page is a sum of three fifth powers over a field F iff $i \in F$, but is a sum of four fifth powers over $\mathbb{Q}(\sqrt{-2})$ and at best a sum of at least five fifth powers over $\mathbb{Q}$. I also showed that any binary form of degree d in $F[x, y]$ can be written as a linear combination of d d-th powers of linear forms over F.

It would take us too far afield to spend much time on this, but the number of summands required depends on the field in which one allows coefficients. A few years ago, I proved that the quintic from the last page is a sum of three fifth powers over a field F iff $i \in F$, but is a sum of four fifth powers over $\mathbb{Q}(\sqrt{-2})$ and at best a sum of at least five fifth powers over $\mathbb{Q}$. I also showed that any binary form of degree d in $F[x, y]$ can be written as a linear combination of d d-th powers of linear forms over F.
My PhD student Neriman Tokcan and I have shown in a forthcoming paper that this phenomenon of three different "lengths" occurs in all degrees ≥ 5. Our examples are $x^k y^k (x - y)$ for $k \geq 2$ and $x^k y^k$ for $k \geq 3$.

It would take us too far afield to spend much time on this, but the number of summands required depends on the field in which one allows coefficients. A few years ago, I proved that the quintic from the last page is a sum of three fifth powers over a field F iff $i \in F$, but is a sum of four fifth powers over $\mathbb{Q}(\sqrt{-2})$ and at best a sum of at least five fifth powers over $\mathbb{Q}$. I also showed that any binary form of degree d in $F[x, y]$ can be written as a linear combination of d d-th powers of linear forms over F.

My PhD student Neriman Tokcan and I have shown in a forthcoming paper that this phenomenon of three different "lengths" occurs in all degrees ≥ 5. Our examples are $x^k y^k (x - y)$ for $k \geq 2$ and $x^k y^k$ for $k \geq 3$.

Another theorem of Sylvester (this time from 1863) implies that if $p(x, y)$ is a hyperbolic real form of degree d (that is, p splits over $\mathbb{R}$), then p cannot be written as a sum of fewer than d real d-th powers.

Getting back to constant-counting, it is easy to see that if $m < r$, then any polynomial map $F : \mathbb{C}^m \to \mathbb{C}^r$ must have the property that $\{f_j(t_1, \ldots t_m)\}$ must be algebraically dependent. In fact, Hilbert proved this, and it was considered a highly abstract theorem at the time. Folks in the 19th century really didn't know the dimension of a vector space!

Getting back to constant-counting, it is easy to see that if $m < r$, then any polynomial map $F : \mathbb{C}^m \to \mathbb{C}^r$ must have the property that $\{f_j(t_1, \ldots t_m)\}$ must be algebraically dependent. In fact, Hilbert proved this, and it was considered a highly abstract theorem at the time. Folks in the 19th century really didn't know the dimension of a vector space!

To simplify matters, Suppose $d = \max(\deg f_j)$ and k is a positive integer. There are $\binom{r+k}{r}$ "monomials" $f_1^{k_1} \ldots f_r^{k_r}$ with $\sum_j k_j \leq k$. This number grows like $k^r/r!$ in k. On the other hand, these polynomials live in the vector space of polynomials in $(t_1, \ldots, t_m)$ of degree $\leq dk$, which has dimension $\binom{m+dk}{m}$, and grows like $(dk)^m/m!$ in k. Since $r > m$, $\binom{r+k}{r} > \binom{m+dk}{m}$ for sufficiently large k, and so the monomials are linearly dependent. This gives the algebraic dependence of the f_j's.

Here's an example of how the proof overstates the degrees needed. Suppose you want to describe ternary quadratic forms which factor as

$$(x + ay + bz)(x + cy + dz) = x^2 + \sum_{i,j,k} c_{ijk} x^i y^j z^k$$

Here's an example of how the proof overstates the degrees needed. Suppose you want to describe ternary quadratic forms which factor as

$$(x + ay + bz)(x + cy + dz) = x^2 + \sum_{i,j,k} c_{ijk} x^i y^j z^k$$

Ignoring x^2, the c_{ijk}'s give five polynomials in the four variables (a, b, c, d): $a + c, b + d, ac, bd, ad + bc$. Using a more careful version of the previous argument, even accounting for two linear and three quadratic polynomials, the best we can say is that there has to be an algebraic relation of degree 22. (Yes, I used Mathematica.)

Here's an example of how the proof overstates the degrees needed. Suppose you want to describe ternary quadratic forms which factor as

$$(x + ay + bz)(x + cy + dz) = x^2 + \sum_{i,j,k} c_{ijk} x^i y^j z^k$$

Ignoring x^2, the c_{ijk}'s give five polynomials in the four variables (a, b, c, d): $a + c, b + d, ac, bd, ad + bc$. Using a more careful version of the previous argument, even accounting for two linear and three quadratic polynomials, the best we can say is that there has to be an algebraic relation of degree 22. (Yes, I used Mathematica.)

However any such quadratic form has rank two, so

$$\begin{vmatrix} 1 & (a+c)/2 & (b+d)/2 \\ (a+c)/2 & ac & (ad+bc)/2 \\ (b+d)/2 & (ad+bc)/2 & bd \end{vmatrix} = 0.$$

Let's talk about cubes.
I'd like to begin with a simple question. Consider a sum of two cubes of quadratic forms:

$$\sum_{j=1}^{2}(\alpha_{j0}x^2+\alpha_{j1}xy+\alpha_{j2}y^2)^3=\sum_{k=0}^{6}c_k x^{6-k}y^k,$$

Let's talk about cubes.
I'd like to begin with a simple question. Consider a sum of two cubes of quadratic forms:

$$\sum_{j=1}^{2}(\alpha_{j0}x^2+\alpha_{j1}xy+\alpha_{j2}y^2)^3=\sum_{k=0}^{6}c_k x^{6-k}y^k,$$

One can view the seven c_k's as cubic polynomials in the six $\alpha'_{j\ell}s$, and since $7>6$, we know that the c_k's must be algebraically dependent. There are $\binom{n+6}{6}$ monomials in the c_j's of degree n; these are forms of degree $3n$ in the $\alpha'_{j\ell}s$, which comprise a vector space of dimension $\binom{3n+5}{5}$. And, eventually,

$$\binom{n+6}{6}>\binom{3n+5}{5}$$

so there must be dependence at some degree n.

Unfortunately,

$$\binom{1441+6}{6} > \binom{3\times 1441+5}{5}$$

is the first time this occurs. Various smart computational algebraic geometers I've asked over the years have been unable to brute force this relation. It tends to kill the kernel.

Unfortunately,

$$\binom{1441+6}{6} > \binom{3\times 1441+5}{5}$$

is the first time this occurs. Various smart computational algebraic geometers I've asked over the years have been unable to brute force this relation. It tends to kill the kernel.

Is there a better way to do this? The answer is yes, and it turns out that there is a relation of degree $n = 15$ in the c_j's, admittedly with more than 1000 terms.

Unfortunately,

$$\binom{1441+6}{6} > \binom{3\times 1441+5}{5}$$

is the first time this occurs. Various smart computational algebraic geometers I've asked over the years have been unable to brute force this relation. It tends to kill the kernel.

Is there a better way to do this? The answer is yes, and it turns out that there is a relation of degree $n = 15$ in the c_j's, admittedly with more than 1000 terms.

This quindecic form is derived from a simple characterization of binary sextics which are a sums of two cubes of binary quadratics.

Let's go to the characterization. There are two equivalent statements.

Theorem

Suppose p is a binary sextic. Then p is a sum of two cubes of quadratics if and only if:
(i) p is a perfect cube or $p = f_1 f_2 f_3$, where the f_i's are linearly dependent but non-proportional quadratic forms.
(ii) There exists an invertible linear change of variables after which p equals either $g(x^2, y^2)$ or $\ell^3 g$ for some linear form ℓ, where g is a cubic which is a sum of two cubes (i.e., $g \neq \ell_1^2 \ell_2$.)

Theorem

Suppose p is a binary sextic. Then p is a sum of two cubes of quadratics if and only if:
(i) p is a perfect cube or $p = f_1 f_2 f_3$, where the f_i's are linearly dependent but non-proportional quadratic forms.
(ii) There exists an invertible linear change of variables after which p equals either $g(x^2, y^2)$ or $\ell^3 g$ for some linear form ℓ, where g is a cubic which is a sum of two cubes (i.e., $g \neq \ell_1^2 \ell_2$.)

The proof of (i) is part of a more general result about sums of two cubes of forms.
The proof of (ii) relies on the ancient art of simultaneous diagonalization: if q and r are two binary quadratic forms, then either they share a common factor, or they can be simultaneously diagonalized.
(Also note: an even form under $(x, y) \mapsto (x + y, x - y)$ becomes a symmetric form, and *vice versa*.)

Theorem (Either mine, or very old and obscure, or both)

Suppose $F \in \mathbb{C}[x_1, \ldots, x_n]$. Then $F = G^3 + H^3$ for forms G, H if and only if either $F = K^3$, or $F = G_1 G_2 G_3$, where the G_j's are non-proportional, but linearly dependent factors.

Proof.

First $G^3 + H^3 = (G + H)(G + \omega H)(G + \omega^2 H)$, where $\omega = e^{\frac{2\pi i}{3}}$, and if two of the factors $G + \omega^j H$ are proportional, then so are G and H, and hence F is a cube. In any event, please observe that $(G + H) + \omega(G + \omega H) + \omega^2(G + \omega^2 H) = 0$.

Theorem (Either mine, or very old and obscure, or both)

Suppose $F \in \mathbb{C}[x_1, \ldots, x_n]$. Then $F = G^3 + H^3$ for forms G, H if and only if either $F = K^3$, or $F = G_1 G_2 G_3$, where the G_j's are non-proportional, but linearly dependent factors.

Proof.

First $G^3 + H^3 = (G + H)(G + \omega H)(G + \omega^2 H)$, where $\omega = e^{\frac{2\pi i}{3}}$, and if two of the factors $G + \omega^j H$ are proportional, then so are G and H, and hence F is a cube. In any event, please observe that $(G + H) + \omega(G + \omega H) + \omega^2(G + \omega^2 H) = 0$.
Conversely, if F has such a factorization, there exist $0 \neq \alpha, \beta \in \mathbb{C}$ so that $F = G_1 G_2(\alpha G_1 + \beta G_2)$. It is easily checked that

$$3\alpha\beta(\omega - \omega^2)F = (\omega^2 \alpha G_1 - \omega \beta G_2)^3 - (\omega \alpha G_1 - \omega^2 \beta G_2)^3.$$

Note that $3\alpha\beta(\omega - \omega^2) = 3\sqrt{-3}\ \alpha\beta \neq 0$. □

In any particular case, if $\deg F = 3r$, there are, up to multiple, only $\frac{(3r)!}{3!(r!)^3}$ ways to write F as a product of three factors of degree r, so checking this condition is algorithmic.

In any particular case, if $\deg F = 3r$, there are, up to multiple, only $\frac{(3r)!}{3!(r!)^3}$ ways to write F as a product of three factors of degree r, so checking this condition is algorithmic.

In particular, if $F(x, y)$ is a binary cubic form, then it has three linear factors $\ell_j(x, y) = \alpha_j x + \beta_j y$, and these are always dependent. Thus, as Sylvester and our 19th century predecessors knew, a binary cubic F is a sum of two cubes unless it has a square factor (and isn't a cube).

The second case uses a simple old lemma whose proof is omitted.

Lemma

Two quadratic forms $q_1(x, y)$ and $q_2(x, y)$ either have a common linear factor, or can be simultaneously diagonalized; that is, $q_j(ax + by, cx + dy) = \rho_j x^2 + \sigma_j y^2$.

The second case uses a simple old lemma whose proof is omitted.

Lemma

Two quadratic forms $q_1(x, y)$ and $q_2(x, y)$ either have a common linear factor, or can be simultaneously diagonalized; that is, $q_j(ax + by, cx + dy) = \rho_j x^2 + \sigma_j y^2$.

Thus, if $p = q_1^t + q_2^t$, where q_j is quadratic, then either the q_j's have a common linear factor (and $p = \ell^t g$, where g is a sum of two linear t-th powers), or after a linear change of variables,

$$p(ax + by, cx + dy) = \sum_{j=1}^{2} (\rho_j x^2 + \sigma_j y^2)^t;$$

That is, $p(ax + by, cx + dy) = g(x^2, y^2)$, where g again is a sum of two linear t-th powers (typical for $t = 3$, not for $t > 3$.)

Finding if p is even after a change of variables is also algorithmic.

$$p(x,y) = \prod_{j=0}^{2d-1} (x - \lambda_j y) \implies$$

$$p(ax+by, cx+dy) = p(a,-c) \prod_{j=0}^{2d-1} \left(x - \left(\frac{\lambda_j d - b}{a - \lambda_j c} \right) y \right)$$

$$:= p(a,-c) \prod_{j=0}^{2d-1} (x - \mu_j y).$$

Thus, the roots of p (taking ∞ if $y \mid p$) are mapped by a Möbius transformation. If $\tilde{p}(x,y) = p(ax+by, cx+dy)$ is even, then $T(z) = -z$ is an involution on the roots, say $T(\mu_{2j}) = \mu_{2j+1}$. It follows that there is an involutory Möbius transformation U permuting the d pairs of roots of p; to be specific:

$$\lambda_{2j+1} = \frac{2ad - (ad+bc)\lambda_{2j}}{(ad+bc) - 2cd\lambda_{2j}}.$$

The algorithm is this: Given p, find the roots λ_j, and for each quadruple $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3}, \lambda_{i_4}$, define the Möbius transformation U so that $U(\lambda_{i_1}) = \lambda_{i_2}$, $U(\lambda_{i_2}) = \lambda_{i_1}$ and $U(\lambda_{i_3}) = \lambda_{i_4}$ and see if it permutes the others. There are instances in which more than one U may work; for example, if p is both even and symmetric.

Don't get me wrong. Complications abound. Here's a simple one. Consider the even sextic

$$p(x, y) = x^6 - x^4y^2 - x^2y^4 + y^6 = (x^2 - y^2)^2(x^2 + y^2).$$

Here, $p(x, y) = g(x^2, y^2)$, where $g(x, y) = (x - y)^2(x + y)$ (having a square factor) is unfortunately not a sum of two cubes. On the other hand, if $\gamma = \frac{2}{\sqrt{3}}i$, then

$$p(x, y) = (x^2 + 2xy + y^2)(x^2 + y^2)(x^2 - 2xy + y^2) \implies$$
$$2p(x, y) = (x^2 + \gamma xy + y^2)^3 + (x^2 - \gamma xy + y^2)^3.$$

Now let's suppose our given cubic p is a sum of two cubes, factor it and expand it in the usual way. Write p as

$$\sum_{k=0}^{6} c_k x^{6-k} y^k = c_0 \left(x^6 + \sum_{k=1}^{6} e_k x^{6-k} y^k \right) = c_0 \prod_{j=1}^{6} (x + r_j y),$$

where the e_k's are the elementary symmetric functions.

Now let's suppose our given cubic p is a sum of two cubes, factor it and expand it in the usual way. Write p as

$$\sum_{k=0}^{6} c_k x^{6-k} y^k = c_0 \left(x^6 + \sum_{k=1}^{6} e_k x^{6-k} y^k \right) = c_0 \prod_{j=1}^{6} (x + r_j y),$$

where the e_k's are the elementary symmetric functions.
There are 15 ways to divide the 6 r_j's into 3 pairs of roots, and the condition that the quadratic factors be dependent for some choice of factorization is equivalent to the vanishing of

$$H(r) := \prod_{\ell=1}^{15} \begin{vmatrix} 1 & 1 & 1 \\ r_{\sigma_\ell(1)} + r_{\sigma_\ell(2)} & r_{\sigma_\ell(3)} + r_{\sigma_\ell(4)} & r_{\sigma_\ell(5)} + r_{\sigma_\ell(6)} \\ r_{\sigma_\ell(1)} r_{\sigma_\ell(2)} & r_{\sigma_\ell(3)} r_{\sigma_\ell(4)} & r_{\sigma_\ell(5)} r_{\sigma_\ell(6)} \end{vmatrix}.$$

This is an I-really-hope-it's-symmetric polynomial of degree 45 in the r_j's.

It *is* symmetric.

Mathematica can compute $H(r)$ without too much difficulty, and in 11657.87 seconds transform it into a symmetric function in the e_k's of degree 15. Now write $e_k = c_k/c_0$, make the substitution and multiply by c_0^{15} to get the relation. It has 1360 terms, so I won't write it here. I also need to express it in terms of the fundamental invariants of the binary sextic, and haven't done so yet. It is *isobaric* in the old sense, each monomial $\prod c_k^{m_k}$ has $\sum m_k = 15, \sum k m_k = 45$.

It *is* symmetric.

Mathematica can compute $H(r)$ without too much difficulty, and in 11657.87 seconds transform it into a symmetric function in the e_k's of degree 15. Now write $e_k = c_k/c_0$, make the substitution and multiply by c_0^{15} to get the relation. It has 1360 terms, so I won't write it here. I also need to express it in terms of the fundamental invariants of the binary sextic, and haven't done so yet. It is *isobaric* in the old sense, each monomial $\prod c_k^{m_k}$ has $\sum m_k = 15, \sum k m_k = 45$.

You can use it to check that a generic pencil of sectic contains a finite number of sums of two cubes, but it is easy to get some very ugly equations. For example, $(x^2+y^2)^3 + ax^5y$ is a sum of two cubes if and only if

$$a \in \left\{ 0, \pm_1 \frac{12\sqrt{3}}{125} \times (25 \pm_2 \sqrt{-15}) \right\}.$$

The non-zero values have modulus $\frac{96\sqrt{30}}{125}$.

Part of an ongoing project with Samuel Lundqvist, Alessandro Oneto and Boris Shapiro.

Theorem

There is an algorithm for writing every binary sextic in $\mathbb{C}[x, y]$ as a sum of three cubes of quadratic forms.

Write the binary sextic (warning: different notation) as

$$p(x, y) = \sum_{k=0}^{6} \binom{6}{k} a_k x^{6-k} y^k.$$

Part of an ongoing project with Samuel Lundqvist, Alessandro Oneto and Boris Shapiro.

Theorem

There is an algorithm for writing every binary sextic in $\mathbb{C}[x, y]$ as a sum of three cubes of quadratic forms.

Write the binary sextic (warning: different notation) as

$$p(x, y) = \sum_{k=0}^{6} \binom{6}{k} a_k x^{6-k} y^k.$$

Part of an ongoing project with Samuel Lundqvist, Alessandro Oneto and Boris Shapiro.

Theorem

There is an algorithm for writing every binary sextic in $\mathbb{C}[x, y]$ as a sum of three cubes of quadratic forms.

Write the binary sextic (warning: different notation) as

$$p(x, y) = \sum_{k=0}^{6} \binom{6}{k} a_k x^{6-k} y^k.$$

Given $p \neq 0$, we may always make an invertible change of variables to ensure that $p(0, 1)p(1, 0) \neq 0$; hence, assume $a_0 a_6 \neq 0$.

Part of an ongoing project with Samuel Lundqvist, Alessandro Oneto and Boris Shapiro.

Theorem

There is an algorithm for writing every binary sextic in $\mathbb{C}[x, y]$ as a sum of three cubes of quadratic forms.

Write the binary sextic (warning: different notation) as

$$p(x, y) = \sum_{k=0}^{6} \binom{6}{k} a_k x^{6-k} y^k.$$

Given $p \neq 0$, we may always make an invertible change of variables to ensure that $p(0, 1)p(1, 0) \neq 0$; hence, assume $a_0 a_6 \neq 0$.

By an observation of *ad hoc*,

$$q(x, y) = x^2 + \frac{2a_1}{a_0}\, x\, y + \frac{5a_0 a_2 - 4a_1^2}{a_0^2}\, y^2$$

$$\implies a_0 q^3(x, y) = a_0 x^6 + 6a_1 x^5 y + 15a_2 x^4 y^2 + \ldots$$

Thus there always exists a cubic c such that

$$p(x,y) - a_0 q(x,y)^3 = y^3 c(x,y).$$

Usually, $(p - a_0 q^3)/y^3 = c$ is a sum of 2 cubes of linear forms, from which it follows that p is a sum of 3 cubes. As we've seen, this only fails if c has a square factor. Trusting Mathematica, the discriminant of $c(x,y)$ is a non-zero polynomial in the a_i's of degree 18, divided by a_0^{14} for general p.

We now consider the remaining cases in which this first approach fails. Such a failure will have the shape

$$p(x,y) = (ax^2 + bxy + cy^2)^3 + y^3(rx + sy)^2(tx + uy)$$

where $ru - st \neq 0$, so that $c(x,y)$ genuinely is not a sum of two cubes.

Let $p_T(x, y) = p(x, Tx + y)$ and write

$$p_T(x, y) = \sum_{k=0}^{6} \binom{6}{k} a_k(T) x^{6-k} y^k.$$

Here, a_k is a polynomial in T of degree $6 - k$ and $a_6(T) = a_6 \neq 0$. There are at most 6 values of T which must be avoided to ensure that $a_0(T) \neq 0$.

Repeating the same construction as above to p_T, we find that the discriminant is a polynomial of degree 72 in T with coefficients in $\{a, b, c, r, s, t, u\}$ and tens of thousands of terms. It turns out, tediously, that for every *non-trivial* choice of (a, b, c, d, r, s, t, u), this discriminant gives a non-zero polynomial in T. (Cased out, not completely trusting in "Solve". Sorry, Danny.)

Hence by avoiding finitely many values of T, the previous argument will work successfully on p_T to give it as a sum of three cubes. We then reverse the invertible transformations and get an expression for p itself.

For example, suppose $p(x,y) = x^6 + x^5y + x^4y^2 + x^3y^3 + x^2y^4 + xy^5 + y^6$. Then

$$p(x,y) - \left(x^2 + \tfrac{1}{3}xy + \tfrac{2}{9}y^2\right)^3 =$$

$$\frac{7}{729}y^3(54x^3 + 81x^2y + 99xy^2 + 103y^3).$$

An application of Sylvester's algorithm shows that

$$54x^3 + 81x^2y + 99xy^2 + 103y^3 =$$

$$m_1(78x + (173 - \sqrt{20153})y)^3 + m_2(78x + (173 + \sqrt{20153})y)^3,$$

$$m_1 = \frac{20153 + 134\sqrt{20153}}{354209128}, \qquad m_2 = \frac{20153 - 134\sqrt{20153}}{354209128}$$

For example, suppose $p(x,y) = x^6 + x^5y + x^4y^2 + x^3y^3 + x^2y^4 + xy^5 + y^6$. Then

$$p(x,y) - \left(x^2 + \tfrac{1}{3}xy + \tfrac{2}{9}y^2\right)^3 =$$
$$\frac{7}{729}y^3(54x^3 + 81x^2y + 99xy^2 + 103y^3).$$

An application of Sylvester's algorithm shows that

$$54x^3 + 81x^2y + 99xy^2 + 103y^3 =$$
$$m_1(78x + (173 - \sqrt{20153})y)^3 + m_2(78x + (173 + \sqrt{20153})y)^3,$$
$$m_1 = \frac{20153 + 134\sqrt{20153}}{354209128}, \qquad m_2 = \frac{20153 - 134\sqrt{20153}}{354209128}$$

This gives a simple sextic p as a sum of three cubes in an ugly way and gives no hint about the existence of the formula

$$p(x,y) = \sum_{\pm} \left(\tfrac{9\pm\sqrt{-3}}{18}\right)(x^2 + \tfrac{1\pm\sqrt{-3}}{2}xy + y^2)^3.$$

An alternative approach is to observe that for a sextic p, there is usually a quadratic q so that $p - q^3$ is even. (Look at the coefficients of x^5y, x^3y^3, xy^5 and solve the equations for the coefficients of q.) Then $p - q^3$ is a cubic in $\{x^2, y^2\}$ and so is usually a sum of two cubes of even quadratic form. If this doesn't work, apply it to p_T.

An alternative approach is to observe that for a sextic p, there is usually a quadratic q so that $p - q^3$ is even. (Look at the coefficients of x^5y, x^3y^3, xy^5 and solve the equations for the coefficients of q.) Then $p - q^3$ is a cubic in $\{x^2, y^2\}$ and so is usually a sum of two cubes of even quadratic form. If this doesn't work, apply it to p_T.

We do not know how to completely characterize the symmetries of the sets of sums of three cubes for a given p. Or if a real binary sextic is a sum of three cubes of real quadratic forms. (Question of Lek-Heng Lim at a conference in China.)

An alternative approach is to observe that for a sextic p, there is usually a quadratic q so that $p - q^3$ is even. (Look at the coefficients of x^5y, x^3y^3, xy^5 and solve the equations for the coefficients of q.) Then $p - q^3$ is a cubic in $\{x^2, y^2\}$ and so is usually a sum of two cubes of even quadratic form. If this doesn't work, apply it to p_T.

We do not know how to completely characterize the symmetries of the sets of sums of three cubes for a given p. Or if a real binary sextic is a sum of three cubes of real quadratic forms. (Question of Lek-Heng Lim at a conference in China.)

This heavy reliance on tools from *Ècole de calcul ad hoc* can only take you so far. There are two natural next steps; based on the observation that $8 = 4 \times 2$ and $9 = 3 \times 3$. Is every binary octic a sum of four 4th powers of quadratic forms? Is every binary nonic a sum of three cubes of quadratic forms? One more fun fact: according to the Oxford English Dictionary (as well as wikipedia), an obsolete term for the 4th power is *zenzizenzic*.

The octic (or *zenzizenzizenzic*) case is interesting because a canonical form for the octics gives them as a sum of three fourth powers, and the Conjecture is still true even if some singular cases require one more.

The octic (or *zenzizenzizenzic*) case is interesting because a canonical form for the octics gives them as a sum of three fourth powers, and the Conjecture is still true even if some singular cases require one more.

In my earlier canonical form project, I noted that $7 = 3 + 4$ and a general binary sextic is a sum of a cubic squared plus a quadratic cubed, but I don't have an algorithm for it.

$$p(x, y) = f^2(x, y) + g^3(x, y) =$$
$$(t_1x^3 + t_2x^2y + t_3xy^2 + t_4y^3)^2 + (t_5x^2 + t_6xy + t_7y^2)^3.$$

Also, $15 = 3 \times 3 + 1 \times 6$, and

$$p(x_1, x_2, x_3) = \sum_{k=1}^{3} (\alpha_{k1}x_1 + \alpha_{k2}x_2 + \alpha_{k3}x_3)^4 + (q(x_1, x_2, x_3))^2,$$

for quadratic q is a quadratic form for ternary quartics.

Here are some references of papers referred to in the talk. These are all available on my website

Homogeneous polynomial solutions to constant coefficient PDE's over fields, *Adv. Math.*, 117 (1996), 179-192 (MR97a:12006).

On the length of binary forms, *Quadratic and Higher Degree Forms*, (K. Alladi, M. Bhargava, D. Savitt, P. Tiep, eds.), Developments in Math. 31 (2013), Springer, New York, pp. 207-232, http://arxiv.org/pdf/1007.5485.pdf, MR3156559.

Some new canonical forms for polynomials, *Pac. J. Math.*, 266 (2013), 185220, http://arxiv.org/abs/1203.5722, MR3105781.

(with Neriman Tokcan) Binary forms with three different relative ranks, http://front.math.ucdavis.edu/1608.08560, to appear in *Proc. Amer. Math. Soc.*

(with Samuel Lundqvist, Alessandro Oneto and Boris Shapiro), On generic and maximal k-ranks of binary forms, in preparation.

Thank you for your attention. I want to thank Danny Lichtblau for the invitation to speak.

Thank you for your attention. I want to thank Danny Lichtblau for the invitation to speak.

I also want to thank him for arranging such comfortable accommodations. I woke up this morning and I almost felt like I was home.

$$\int_\Omega f_u \, dt.$$