# Sums of powers of binary quadratic forms

Bruce Reznick
University of Illinois at Urbana-Champaign

AMS Central Sectional Meeting
Special Session on Combinatorial Ideals and Applications
North Dakota State University        April 16, 2016

Let $H_m(\mathbb{C}^n)$ denote the vector space of complex forms in $n$ variables with degree $m$. How can a form of degree $m = de$ be written as a sum of $d$-th powers of forms of degree $e$? More specifically, given $p \in H_m(\mathbb{C}^n)$, what is the smallest number $N$ so that there exist forms $f_j \in H_e(\mathbb{C}^n)$ satisfying

$$p = \sum_{j=1}^{N} f_j^d ?$$

Let $H_m(\mathbb{C}^n)$ denote the vector space of complex forms in $n$ variables with degree $m$. How can a form of degree $m = de$ be written as a sum of $d$-th powers of forms of degree $e$? More specifically, given $p \in H_m(\mathbb{C}^n)$, what is the smallest number $N$ so that there exist forms $f_j \in H_e(\mathbb{C}^n)$ satisfying

$$p = \sum_{j=1}^{N} f_j^d ?$$

When $e = 1$, this number $N$ is the *Waring rank* of $p$.

Let $H_m(\mathbb{C}^n)$ denote the vector space of complex forms in $n$ variables with degree $m$. How can a form of degree $m = de$ be written as a sum of $d$-th powers of forms of degree $e$? More specifically, given $p \in H_m(\mathbb{C}^n)$, what is the smallest number $N$ so that there exist forms $f_j \in H_e(\mathbb{C}^n)$ satisfying

$$p = \sum_{j=1}^{N} f_j^d ?$$

When $e = 1$, this number $N$ is the *Waring rank* of $p$.
For the most part, this talk is concerned with $e = 2, n = 2$, but it will be helpful to review the case $e = 1, n = 2$; that is, when the $f_j$'s are binary linear forms.

Let $H_m(\mathbb{C}^n)$ denote the vector space of complex forms in $n$ variables with degree $m$. How can a form of degree $m = de$ be written as a sum of $d$-th powers of forms of degree $e$? More specifically, given $p \in H_m(\mathbb{C}^n)$, what is the smallest number $N$ so that there exist forms $f_j \in H_e(\mathbb{C}^n)$ satisfying

$$p = \sum_{j=1}^{N} f_j^d ?$$

When $e = 1$, this number $N$ is the *Waring rank* of $p$.

For the most part, this talk is concerned with $e = 2, n = 2$, but it will be helpful to review the case $e = 1, n = 2$; that is, when the $f_j$'s are binary linear forms.

We begin with an auto-plagiaristic look at Sylvester's algorithm, limited to representations over $\mathbb{C}$ in this talk. Apologies to everyone who has seen the next few pages before.

### Theorem (Sylvester, 1851)

*Suppose* $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j \in \mathbb{C}[x,y]$ *and* $h(x,y) = \sum_{t=0}^{r} c_t x^{r-t} y^t = \prod_{j=1}^{r} (\beta_j x - \alpha_j y)$ *is a product of pairwise non-proportional linear factors, where* $\alpha_j, \beta_j \in \mathbb{C}$*. 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*

### Theorem (Sylvester, 1851)

*Suppose* $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j \in \mathbb{C}[x,y]$ *and* $h(x,y) = \sum_{t=0}^{r} c_t x^{r-t} y^t = \prod_{j=1}^{r} (\beta_j x - \alpha_j y)$ *is a product of pairwise non-proportional linear factors, where* $\alpha_j, \beta_j \in \mathbb{C}$. *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*

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

Some notes on the proof:

Some notes on the proof:

- This is equivalent to apolarity. Since $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ kills $(\alpha x + \beta y)^d$, if $h(D)$ is defined to be $\prod_{j=1}^r(\beta_j\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$, then

$$h(D)p = \sum_{v=0}^{d-r} \frac{d!}{(d-r-v)!v!}\left(\sum_{i=0}^{d-r} a_{i+v}c_i\right) x^{d-r-v}y^v$$

The coefficients of $h(D)p$ are, up to multiple, the rows in the matrix product, so the matrix condition is $h(D)p = 0$. Each linear factor in $h(D)$ kills a different summand.

Some notes on the proof:

- This is equivalent to apolarity. Since $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ kills $(\alpha x + \beta y)^d$, if $h(D)$ is defined to be $\prod_{j=1}^r (\beta_j\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$, then

$$h(D)p = \sum_{v=0}^{d-r} \frac{d!}{(d-r-v)!v!} \left( \sum_{i=0}^{d-r} a_{i+v}c_i \right) x^{d-r-v}y^v$$

  The coefficients of $h(D)p$ are, up to multiple, the rows in the matrix product, so the matrix condition is $h(D)p = 0$. Each linear factor in $h(D)$ kills a different summand.

- This is also an algorithm! Given $p$, for increasing $r$, look for null vectors $c$ corresponding to apolar forms with distinct roots. In effect, look for the small linear recurrences satisfied by the $a_j's$.

Some notes on the proof:

- This is equivalent to apolarity. Since $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ kills $(\alpha x + \beta y)^d$, if $h(D)$ is defined to be $\prod_{j=1}^r(\beta_j\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$, then

$$h(D)p = \sum_{v=0}^{d-r}\frac{d!}{(d-r-v)!v!}\left(\sum_{i=0}^{d-r}a_{i+v}c_i\right)x^{d-r-v}y^v$$

  The coefficients of $h(D)p$ are, up to multiple, the rows in the matrix product, so the matrix condition is $h(D)p = 0$. Each linear factor in $h(D)$ kills a different summand.

- This is also an algorithm! Given $p$, for increasing $r$, look for null vectors $c$ corresponding to apolar forms with distinct roots. In effect, look for the small linear recurrences satisfied by the $a_j's$.
- If $h$ has repeated factors, see Gundelfinger's Theorem (1886): $(\beta x - \alpha y)^\ell$ gives a summand $(\alpha x + \beta y)^{d-(\ell-1)}q(x,y)$, where $q$ is an arbitrary form of degree $\ell - 1$.

Here is a (reverse-engineered) example of Sylvester's Theorem in action. Let

$$p(x,y) = x^3 + 12x^2y - 6xy^2 + 10y^3 =$$

$$\binom{3}{0} \cdot 1\ x^3 + \binom{3}{1} \cdot 4\ x^2y + \binom{3}{2} \cdot (-2)xy^2 + \binom{3}{3} \cdot 10\ y^3$$

We have

$$\begin{pmatrix} 1 & 4 & -2 \\ 4 & -2 & 10 \end{pmatrix}$$

Here is a (reverse-engineered) example of Sylvester's Theorem in action. Let

$$p(x,y) = x^3 + 12x^2y - 6xy^2 + 10y^3 =$$

$$\binom{3}{0}\cdot 1\ x^3 + \binom{3}{1}\cdot 4\ x^2y + \binom{3}{2}\cdot(-2)xy^2 + \binom{3}{3}\cdot 10\ y^3$$

We have

$$\begin{pmatrix} 1 & 4 & -2 \\ 4 & -2 & 10 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Here is a (reverse-engineered) example of Sylvester's Theorem in action. Let

$$p(x,y) = x^3 + 12x^2y - 6xy^2 + 10y^3 =$$

$$\binom{3}{0}\cdot 1\ x^3 + \binom{3}{1}\cdot 4\ x^2y + \binom{3}{2}\cdot(-2)xy^2 + \binom{3}{3}\cdot 10\ y^3$$

We have

$$\begin{pmatrix} 1 & 4 & -2 \\ 4 & -2 & 10 \end{pmatrix}\cdot\begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and $2x^2 - xy - y^2 = (2x+y)(x-y)$, so that

$$p(x,y) = \lambda_1(x-2y)^3 + \lambda_2(x+y)^3.$$

In fact, $p(x,y) = -(x-2y)^3 + 2(x+y)^3$.

The next simple example is $p(x,y) = 3x^2y$. Note that

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \implies c_0 = c_1 = 0$$

so that $h(x,y) = c_2y^2$ has repeated factors, and $p$ is not a sum of two cubes. Similarly, $x^{d-1}y$ requires $d$ $d$-th powers.

The next simple example is $p(x, y) = 3x^2y$. Note that

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \implies c_0 = c_1 = 0$$

so that $h(x, y) = c_2y^2$ has repeated factors, and $p$ is not a sum of two cubes. Similarly, $x^{d-1}y$ requires $d$ $d$-th powers.

It can be shown more generally that the Waring rank of $p$ is less than its degree, unless $p = \ell_1^{d-1}\ell_2^1$ for different linear $\ell_i$'s.

If $d = 2s - 1$ and $r = s$, then the matrix in Sylvester's Theorem is $s \times (s+1)$ and has a non-trivial null-vector. The corresponding $h$ has distinct factors unless its discriminant vanishes. If $d = 2s$ and $r = s$, then the matrix is square, and for a fixed linear form $\ell$, there generally exists $\lambda \in \mathbb{C}$ so that $p(x,y) - \lambda \ell^{2s}$ has a non-trivial null-vector, generally corresponding to $h$ with distinct factors.

If $d = 2s - 1$ and $r = s$, then the matrix in Sylvester's Theorem is $s \times (s + 1)$ and has a non-trivial null-vector. The corresponding $h$ has distinct factors unless its discriminant vanishes. If $d = 2s$ and $r = s$, then the matrix is square, and for a fixed linear form $\ell$, there generally exists $\lambda \in \mathbb{C}$ so that $p(x, y) - \lambda \ell^{2s}$ has a non-trivial null-vector, generally corresponding to $h$ with distinct factors.

### Theorem (Sylvester's Theorem, canonical form version)

*(i) A general binary form $p$ of odd degree $2s - 1$ can be written as*

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

*(ii) Given any fixed linear form $\ell$, a general binary form $p$ of even degree $2s$ can be written as*

$$p(x, y) = \lambda \ell^{2s}(x, y) + \sum_{j=1}^{s} (\alpha_j x + \beta_j y)^{2s}.$$

The following result is from my 2013 paper on canonical forms in *Pac. J. Math.* The basis of the numerology below is simply constant-counting.

The following result is from my 2013 paper on canonical forms in *Pac. J. Math.* The basis of the numerology below is simply constant-counting.

### Theorem

*A general binary form of degree $de$ can be written as a sum of $\lceil \frac{de+1}{e+1} \rceil$ $d$-th powers of binary forms of degree $e$. (That is, if possible at all, a general binary form is a sum of at most $d$ $d$-th powers of forms.)*

The following result is from my 2013 paper on canonical forms in *Pac. J. Math.* The basis of the numerology below is simply constant-counting.

### Theorem

*A general binary form of degree $de$ can be written as a sum of $\lceil \frac{de+1}{e+1} \rceil$ $d$-th powers of binary forms of degree $e$. (That is, if possible at all, a general binary form is a sum of at most $d$ $d$-th powers of forms.)*

The following result is from my 2013 paper on canonical forms in *Pac. J. Math.* The basis of the numerology below is simply constant-counting.

**Theorem**

*A general binary form of degree $de$ can be written as a sum of $\lceil \frac{de+1}{e+1} \rceil$ $d$-th powers of binary forms of degree $e$. (That is, if possible at all, a general binary form is a sum of at most $d$ $d$-th powers of forms.)*
*In fact, if $de + 1 = N(e + 1) + k$, $1 \le k \le e + 1$, then one can take $N$ binary forms of degree $e$ and specify one's favorite $k$ monomials in the $(N + 1)$-st.*

The following result is from my 2013 paper on canonical forms in *Pac. J. Math.* The basis of the numerology below is simply constant-counting.

**Theorem**

*A general binary form of degree $de$ can be written as a sum of $\lceil \frac{de+1}{e+1} \rceil$ $d$-th powers of binary forms of degree $e$. (That is, if possible at all, a general binary form is a sum of at most $d$ $d$-th powers of forms.)*
*In fact, if $de + 1 = N(e + 1) + k$, $1 \le k \le e + 1$, then one can take $N$ binary forms of degree $e$ and specify one's favorite $k$ monomials in the $(N + 1)$-st.*

Roughly speaking, the appeal to constant-counting, when combined with these theorems, shows that "most" forms of degree $2d$ are a sum of roughly $\frac{2}{3}d$ $d$-th powers of quadratic forms.

## Corollary

*(i) A general binary form of degree $d = 6s$ can be written as*

$$(\lambda x^2)^{3s} + \sum_{j=1}^{2s} (\alpha_j x^2 + \beta_j xy + \gamma_j y^2)^{3s}$$

*(ii) A general binary form of degree $d = 6s + 2$ can be written as*

$$\sum_{j=1}^{2s+1} (\alpha_j x^2 + \beta_j xy + \gamma_j y^2)^{3s+1}.$$

*(iii) A general binary form of degree $d = 6s + 4$ can be written as*

$$(\lambda_1 x^2 + \lambda_2 y^2)^{3s+2} + \sum_{j=1}^{2s+1} (\alpha_j x^2 + \beta_j xy + \gamma_j y^2)^{3s+2}$$

Why is this a harder question than the Waring rank? For one thing, if $\{\ell_1, ..., \ell_n\}$ are $n$ pairwise non-proportional binary linear forms, then $\{\ell_1^d, ...\ell_n^d\}$ is linearly independent if and only if $n \le d + 1$. There are no non-trivial linear dependencies among powers of binary forms. On the other hand, we have the familiar

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2.$$

Why is this a harder question than the Waring rank? For one thing, if $\{\ell_1, \dots, \ell_n\}$ are $n$ pairwise non-proportional binary linear forms, then $\{\ell_1^d, \dots \ell_n^d\}$ is linearly independent if and only if $n \le d + 1$. There are no non-trivial linear dependencies among powers of binary forms. On the other hand, we have the familiar

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2.$$

Furthermore, there doesn't seem to be an apolarity argument. Even a single quadratic form to the $d$-th power, say $(xy)^d$, is not apolar to any form of degree smaller than $d + 1$. I can't find an obvious form of degree $\le 2d$ which is apolar to the sum of two $d$-th powers of quadratic forms. Suggestions are welcome.

Another indication of the difficulty lies in the existence of Hilbert Identities, which is another talk altogether. For purposes of this talk, I will note the following crypto-19th century result:

Another indication of the difficulty lies in the existence of Hilbert Identities, which is another talk altogether. For purposes of this talk, I will note the following crypto-19th century result:

### Theorem

*The representations of* $(x^2+y^2)^t$ *as a sum of* $t+1$ $2t$*-th powers are given by*

$$\binom{2t}{t}(x^2+y^2)^t$$

$$= \frac{2^{2t}}{t+1}\sum_{j=0}^{t}\left(\cos(\tfrac{j\pi}{t+1}+\theta)x+\sin(\tfrac{j\pi}{t+1}+\theta)y\right)^{2t},$$

$$\theta \in \mathbb{C}.$$

Another indication of the difficulty lies in the existence of Hilbert Identities, which is another talk altogether. For purposes of this talk, I will note the following crypto-19th century result:

### Theorem

*The representations of $(x^2+y^2)^t$ as a sum of $t+1$ $2t$-th powers are given by*

$$\binom{2t}{t}(x^2+y^2)^t$$

$$= \frac{2^{2t}}{t+1}\sum_{j=0}^{t}\left(\cos(\tfrac{j\pi}{t+1}+\theta)x+\sin(\tfrac{j\pi}{t+1}+\theta)y\right)^{2t},$$

$$\theta \in \mathbb{C}.$$

This expression gives lots of non-trivial linear combinations of $t$-th powers of quadratic forms. The earliest known version (for real $\theta$) is by Avner Friedman, from the 1950s. It must be older.

A form of degree two is trivially the sum of the first powers of one quadratic form.

A form of degree two is trivially the sum of the first powers of one quadratic form.

Let $p$ be a binary quartic form. Since $\lceil \frac{5}{3} \rceil = 2$, we hope to write a general $p$ as a sum of two squares of quadratic forms.

A form of degree two is trivially the sum of the first powers of one quadratic form.

Let $p$ be a binary quartic form. Since $\lceil \frac{5}{3} \rceil = 2$, we hope to write a general $p$ as a sum of two squares of quadratic forms.

But this is easy, because of the identity

$$FG = \left(\frac{F+G}{2}\right)^2 + \left(\frac{F-G}{2i}\right)^2.$$

Factor $p$ as a product of linear forms (possibly with repeats):

$$p = \ell_1\ell_2\ell_3\ell_4 = \left(\frac{\ell_1\ell_2 + \ell_3\ell_4}{2}\right)^2 + \left(\frac{\ell_1\ell_2 - \ell_3\ell_4}{2i}\right)^2.$$

A form of degree two is trivially the sum of the first powers of one quadratic form.

Let $p$ be a binary quartic form. Since $\lceil \frac{5}{3} \rceil = 2$, we hope to write a general $p$ as a sum of two squares of quadratic forms.

But this is easy, because of the identity

$$FG = \left(\frac{F+G}{2}\right)^2 + \left(\frac{F-G}{2i}\right)^2.$$

Factor $p$ as a product of linear forms (possibly with repeats):

$$p = \ell_1\ell_2\ell_3\ell_4 = \left(\frac{\ell_1\ell_2 + \ell_3\ell_4}{2}\right)^2 + \left(\frac{\ell_1\ell_2 - \ell_3\ell_4}{2i}\right)^2.$$

By using $F^2 + G^2 = (\cos\theta F + \sin\theta G)^2 + (-\sin\theta F + \cos\theta G)^2$, we can also arrange one of the coefficients to disappear, as in the canonical form.

We turn to the first non-trivial case, and a theorem. Observe that $\left\lceil \frac{7}{3} \right\rceil = 3$, so a *general* binary sextic is a sum of three cubes of quadratic forms. We shall show that *every* sextic is a sum of at most three cubes; there are no exceptions, such as $x^{d-1}y$ for sums of powers of linear forms. We also give an algorithm for finding some of these representations.

We turn to the first non-trivial case, and a theorem. Observe that $\left\lceil \frac{7}{3} \right\rceil = 3$, so a *general* binary sextic is a sum of three cubes of quadratic forms. We shall show that *every* sextic is a sum of at most three cubes; there are no exceptions, such as $x^{d-1}y$ for sums of powers of linear forms. We also give an algorithm for finding some of these representations.

It's useful to consider the case of the sum of two cubes of linear forms. The coefficients of $\sum_{i=1}^{2}(\alpha_i x^2 + \beta_i xy + \gamma_i y^2)^3$ comprise seven forms in six variables, and so satisfy a non-trivial polynomial that's hard to find. On the other hand, there are two simple criteria on the sum itself.

## Theorem

*Suppose $p \in H_6(\mathbb{C}^2)$. Then p to be sum of two cubes of quadratics if and only if either (i) or (ii) hold:*

### Theorem

*Suppose $p \in H_6(\mathbb{C}^2)$. Then $p$ to be sum of two cubes of quadratics if and only if either (i) or (ii) hold:*
*(i) $p = f_1 f_2 f_3$, where the $f_i$'s are linearly dependent but non-proportional quadratic forms.*

### Theorem

*Suppose $p \in H_6(\mathbb{C}^2)$. Then $p$ to be sum of two cubes of quadratics if and only if either (i) or (ii) hold:*
*(i) $p = f_1 f_2 f_3$, where the $f_i$'s are linearly dependent but non-proportional quadratic forms.*
*(ii) There either exists a linear change of variables so that $p(ax + by, cx + dy) = g(x^2, y^2)$, or $p = \ell^3 g$ for some linear form $\ell$, where $g$ is a cubic which is a sum of two cubes (i.e., not $\ell_1^2 \ell_2^1$.)*

### Theorem

*Suppose $p \in H_6(\mathbb{C}^2)$. Then $p$ to be sum of two cubes of quadratics if and only if either (i) or (ii) hold:*
*(i) $p = f_1 f_2 f_3$, where the $f_i$'s are linearly dependent but non-proportional quadratic forms.*
*(ii) There either exists a linear change of variables so that $p(ax + by, cx + dy) = g(x^2, y^2)$, or $p = \ell^3 g$ for some linear form $\ell$, where $g$ is a cubic which is a sum of two cubes (i.e., not $\ell_1^2 \ell_2^1$.)*

The proof of the second 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.
The proof of the first is part of a more general result about sums of two cubes of forms, given below.

### Theorem

*Suppose $F \in \mathbb{C}[x_1, \ldots, x_n]$. Then $F$ is a sum of two cubes in $\mathbb{C}[x_1, \ldots, x_n]$ if and only if it is itself a cube, or has a factorization $F = G_1 G_2 G_3$, into non-proportional, but linearly dependent factors.*

### Proof.

First $F = G^3 + H^3 = (G + H)(G + \omega H)(G + \omega^2 H)$, where $\omega = e^{\frac{2\pi i}{3}}$. 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 case,

$$(G + H) + \omega(G + \omega H) + \omega^2(g + \omega^2 H) = 0.$$

### Theorem

*Suppose $F \in \mathbb{C}[x_1, \dots, x_n]$. Then $F$ is a sum of two cubes in $\mathbb{C}[x_1, \dots, x_n]$ if and only if it is itself a cube, or has a factorization $F = G_1 G_2 G_3$, into non-proportional, but linearly dependent factors.*

### Proof.

First $F = G^3 + H^3 = (G + H)(G + \omega H)(G + \omega^2 H)$, where $\omega = e^{\frac{2\pi i}{3}}$. 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 case,

$$(G + H) + \omega(G + \omega H) + \omega^2(g + \omega^2 H) = 0.$$

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

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

□

(From an ongoing project with Hal Schenck and Boris Shapiro.)

(From an ongoing project with Hal Schenck 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, The method can give infinitely many different representations, except for some singular cases.*

(From an ongoing project with Hal Schenck 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, The method can give infinitely many different representations, except for some singular cases.*

(From an ongoing project with Hal Schenck 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, The method can give infinitely many different representations, except for some singular cases.*

Here is a sketch of the proof. Write the binary sextic as

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

(From an ongoing project with Hal Schenck 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, The method can give infinitely many different representations, except for some singular cases.*

Here is a sketch of the proof. Write the binary sextic 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 $a_0 a_6 \neq 0$.

(From an ongoing project with Hal Schenck 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, The method can give infinitely many different representations, except for some singular cases.*

Here is a sketch of the proof. Write the binary sextic 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*, if

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

then the coefficients of $x^6, x^5 y, x^4 y^2$ in $p$ and $a_0 q^3$ agree.

Thus there always exists a cubic $c$ such that

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

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. This algorithm can only fail if $c$ has a square factor. The discriminant of $c$ is a non-zero polynomial in the $a_i$'s of degree 18, divided by $a_0^{14}$, assuming that Mathematica is reliable.

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. This algorithm can only fail if $c$ has a square factor. The discriminant of $c$ is a non-zero polynomial in the $a_i$'s of degree 18, divided by $a_0^{14}$, assuming that Mathematica is reliable.

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 $a_0(T) \neq 0$.

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, the discriminant is a polynomial of degree 72 in $T$ with coefficients in $\{a, b, c, r, s, t, u\}$ and more than 72,000 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 trusting in "Solve".)

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, the discriminant is a polynomial of degree 72 in $T$ with coefficients in $\{a,b,c,r,s,t,u\}$ and more than 72,000 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 trusting in "Solve".)

Hence by avoiding finitely many values of $T$, the algorithm 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

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

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

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

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

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

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

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

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.

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.

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.

We do not know how to completely characterize the sets of sums of three cubes for a given $p$ and what other symmetries those sets might have.

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.

We do not know how to completely characterize the sets of sums of three cubes for a given $p$ and what other symmetries those sets might have.

Clearly these tools from *Ècole de calcul ad hoc* will not generalize to higher degree. It is natural to ask about representations of octics as sums of three fourth powers of quadratic forms. (I think Boris has some results along those lines.) One would, in fact, expect that there is a canonical number of different representations and there would be some exceptional cases. For example, I think that $\ell_1^4\ell_2^3\ell_3^1$ is not a sum of three fourth powers unless the $\ell_j$'s are the same. No proofs yet.

I thank the organizers for the invitation to speak and the audience for its patience and attention.