Sums of powers of binary quadratic forms

Bruce Reznick
University of Illinois at Urbana-Champaign

Joint Mathematical Meetings
AMS Special Session on Gaussian Graphical Models and
Combinatorial Algebraic Geometry
Baltimore, ND January 4, 2017 (slightly corrected 1/10/17)
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 $(n+6)6$ 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 $(3n+5)5$. And, eventually, $(n+6)6 > (3n+5)5$ so there must be dependence at degree $n$.

Bruce Reznick  University of Illinois at Urbana-Champaign  Sums of powers of binary quadratic forms
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 degree $n$. 

Bruce Reznick  University of Illinois at Urbana-Champaign  Sums of powers of binary quadratic forms
Unfortunately,

\[
\left( \frac{1442 + 6}{6} \right) > \left( \frac{3 \times 1442 + 5}{5} \right)
\]

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.
Unfortunately,
\[
\begin{pmatrix}
1442 + 6 \\
6
\end{pmatrix} > \begin{pmatrix}
3 \times 1442 + 5 \\
5
\end{pmatrix}
\]
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.

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,

\[
\left( \frac{1442 + 6}{6} \right) > \left( \frac{3 \times 1442 + 5}{5} \right)
\]

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.

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.
Unfortunately,

\[
\begin{array}{c}
\frac{1442 + 6}{6} > \frac{3 \times 1442 + 5}{5}
\end{array}
\]

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.

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 $\ell$, where $g$ is a cubic which is a sum of two cubes (i.e., $g \neq \ell^2 \ell^2$).

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

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 $\ell$, where $g$ is a cubic which is a sum of two cubes (i.e., $g \neq \ell^2 + \ell^2$).

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

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 $p = f_1f_2f_3$, 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 $\ell^3g$ for some linear form $\ell$, 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 \( \ell \), 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.
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 $\ell$, 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.
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 $\ell$, 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 $F \in C[x_1, \ldots, x_n]$. 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 $G^3 + H^3 = (G + \omega H)(G + \omega^2 H)(G + \omega^3 H)$, where $\omega = e^{2\pi i/3}$, 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 $0 \neq \alpha, \beta \in C$ 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 $3 \alpha \beta (\omega - \omega^2) \neq 0$. 

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.
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 $\omega = e^{2\pi i / 3}$, 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 $3\alpha\beta(\omega - \omega^2) = 3\sqrt{-3} \neq 0$. 

Bruce Reznick  University of Illinois at Urbana-Champaign  Sums of powers of binary quadratic forms
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). We use this a lot.
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 $t > 3$.)
Checking 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 $\infty$ 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 \( \lambda_j \), 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.
The algorithm is this: Given $p$, find the roots $\lambda_j$, 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

$$H(r) := \prod_{\ell=1}^{15} \begin{vmatrix} 1 & 1 & 1 \\ r_{\sigma_\ell}(1) + r_{\sigma_\ell}(2) & r_{\sigma_\ell}(3) + r_{\sigma_\ell}(4) & r_{\sigma_\ell}(5) + r_{\sigma_\ell}(6) \\ r_{\sigma_\ell}(1) r_{\sigma_\ell}(2) & r_{\sigma_\ell}(3) r_{\sigma_\ell}(4) & r_{\sigma_\ell}(5) r_{\sigma_\ell}(6) \end{vmatrix}.$$
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 (and it is) polynomial of degree 45 in the $r_j$’s.
Mathematica can compute $H(r)$ without too much difficulty, and in 11657.87 seconds transform it into a 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 $\sum m_k = 15, \sum km_k = 45$. 

You can use it to check that a generic pencil of sextic contains a finite number of sums of two cubes, but this method doesn’t distinguish repeated factors. So it says that $C_2$ should be a sum of two cubes for any cubic $C$, because $C = \ell_1 \ell_2 \ell_3$ and $\{\ell_2 \ell_1, \ell_2 \ell_3, \ell_2 \ell_3\}$ is dependent. Bad. On the other hand, $(x^3 + y^3)^2 + ax^5 y$ is provably a sum of two cubes if and only if $a^3 \in \{3655 \cdot (13 \pm 5\sqrt{145})\}$. Not sure what that means.
Mathematica can compute $H(r)$ without too much difficulty, and in 11657.87 seconds transform it into a 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 $\sum m_k = 15, \sum km_k = 45$. You can use it to check that a generic pencil of sextic contains a finite number of sums of two cubes, but this method doesn’t distinguish repeated factors. So it says that $C^2$ should be a sum of two cubes for any cubic $C$, because $C = \ell_1 \ell_2 \ell_3$ and $\{\ell_1^2, \ell_2 \ell_3, \ell_2 \ell_3\}$ is dependent. Bad. On the other hand, $(x^3 + y^3)^2 + ax^5y$ is provably a sum of two cubes if and only if

$$a^3 \in \left\{ \frac{3^6}{5^5} \cdot (13 \pm 5\sqrt{145}) \right\}.$$
Mathematica can compute $H(r)$ without too much difficulty, and in 11657.87 seconds transform it into a 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 $\sum m_k = 15$, $\sum km_k = 45$.

You can use it to check that a generic pencil of sextic contains a finite number of sums of two cubes, but this method doesn’t distinguish repeated factors. So it says that $C^2$ should be a sum of two cubes for any cubic $C$, because $C = l_1l_2l_3$ and $\{l_1^2, l_2l_3, l_2l_3\}$ is dependent. Bad. On the other hand, $(x^3 + y^3)^2 + ax^5y$ is provably a sum of two cubes if and only if

$$a^3 \in \left\{ \frac{3^6}{5^5} \cdot (13 \pm 5\sqrt{145}) \right\}.$$ 

Not sure what that means.
Here is a nice conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms of degree $m$ with complex coefficients, and suppose $m = de, \ d, e \in \mathbb{N}$. 

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 $d$-th powers of linear forms are precisely those of the shape $(ax + by)^{d-1} (a'x + b'y)$, $ab' \neq a'b$; ie $\ell^{d-1} \ell'$. If $d = 1$, there is nothing to prove.
Here is a nice conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms 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 $d$ $d$-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 $(ax + by)^{d-1}(a'x + b'y)$, $ab' \neq a'b$; i.e., $\ell^{d-1}\ell'$. If $d = 1$, there is nothing to prove.
Here is a nice conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms 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 $d$ $d$-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.
Here is a nice conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms 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 $d$ $d$-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 $(ax + by)^{d-1}(a'x + b'y)$, $ab' \neq a'b'$; ie $\ell^{d-1}\ell'$.
Here is a nice conjecture due to Boris Shapiro. Let $H_m(\mathbb{C}^2)$ denote the vector space of binary forms 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 $d$ $d$-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 $(ax + by)^{d-1}(a'x + b'y), ab' \neq a'b'$; i.e. $\ell^{d-1}\ell'$.
- If $d = 1$, there is nothing to prove.
If $d = 2$, then $m = 2e$ is even, and $p$ can be factored into linear factors, so that $p = fg$ for $f, g \in H_e(C^2)$ and

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

is a sum of two squares (one could write this with "\(i\)" inside.)
If \( d = 2 \), then \( m = 2e \) is even, and \( p \) can be factored into linear factors, so that \( p = fg \) for \( f, g \in H_e(C^2) \) and

\[
p = fg = \left( \frac{f + g}{2} \right)^2 - \left( \frac{f - g}{2} \right)^2
\]

is a sum of two squares (one could write this with “\( i \)” inside.)

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

\[
\sum_{j=1}^{k}(\alpha_j x^e + \ldots)^d + (\beta_0 x^e + \ldots + \beta_{s-1} x^{e-(s-1)} y^{s-1})^d
\]

is a canonical form for binary forms of degree \( de \), and

\[
\left\lceil \frac{de + 1}{e + 1} \right\rceil \leq \left\lceil \frac{de + d}{e + 1} \right\rceil = d.
\]
The conjecture is true if you remove the restriction to forms (but lose the information about degrees). In fact, every polynomial is a sum of $d$ $d$-th powers of polynomials by a result of Newman-Slater. Let $\zeta_d$ 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

$$d^2 p = \sum_{k=0}^{d-1} \zeta_d^{-k} (1 + \zeta_d^k p)^d.$$
The conjecture is true if you remove the restriction to forms (but lose the information about degrees). In fact, every polynomial is a sum of $d$th powers of polynomials by a result of Newman-Slater. Let $\zeta_d$ 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

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

I now sketch an algorithmic proof for the simplest non-obvious case — $d = 3$, $e = 2$ — that is, every complex binary sextic is a sum of three cubes of quadratic forms.
Part of an ongoing project with Hal Schenck and Boris Shapiro I think.

\begin{align*}
\text{Theorem} & \\
\text{There is an algorithm for writing every binary sextic in } & \\
\mathbb{C}[x, y] & \text{as a sum of three cubes of quadratic forms.}
\end{align*}

Write the binary sextic (warning: different notation) as

\[ p(x, y) = 6 \sum_{k=0}^{6} \left(6^k a_k x^{6-k} y^k\right). \]

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

By an observation of \textit{ad hoc},

\[ q(x, y) = x^2 + 2a_1 a_0 xy + 5a_0 a_2 - 4a_2 a_0 y^2 \]

\[ \Rightarrow a_0 q^3(x, y) = a_0 x^6 + 6a_1 x^5 y + 15a_2 x^4 y^2 + \ldots \]
Part of an ongoing project with Hal Schenck and Boris Shapiro I think.

**Theorem**

*There is an algorithm for writing every binary sextic in \( \mathbb{C}[x, y] \) as a sum of three cubes of quadratic forms.*
Part of an ongoing project with Hal Schenck and Boris Shapiro I think.

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

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, $q(x, y) = x^2 + 2 a_1 a_0 x y + 5 a_0 a_2 - 4 a_1^2 a_2 y^2 = \Rightarrow a_0 q^3(x, y) = a_0 x^6 + 6 a_1 x^5 y + 15 a_2 x^4 y^2 + ...$.
Part of an ongoing project with Hal Schenck and Boris Shapiro I think.

**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 Hal Schenck and Boris Shapiro I think.

**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

$$p(x, y) - a_0 q(x, y)^3 = y^3 c(x, y).$$
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. The discriminant of $c(x, y)$ is a non-zero polynomial in the $a_i$’s of degree 18, divided by $a_0^{14}$, assuming that Mathematica is reliable, so this works for general $p$. 

We now consider the remaining cases in which this first approach fails. Such a failure will have the shape
\[ p(x, y) = (ax^2 + bxy + cy^2)^3 + y^3 (rx + sy)(tx + uy), \]
where $ru - st \neq 0$, so that $c(x, y)$ genuinely is not a sum of two cubes.
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. The discriminant of $c(x, y)$ is a non-zero polynomial in the $a_i$’s of degree 18, divided by $a_0^{14}$, assuming that Mathematica is reliable, so this works 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 trusting in “Solve”.)

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.
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 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 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 trusting in “Solve”.)

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

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

An application of Sylvester’s algorithm shows that

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

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

\[
54x^3 + 81x^2y + 99xy^2 + 103y^3 = m_1(78x + (173 - \sqrt{20153})y)^3 + m_2(78x + (173 + \sqrt{20153})y)^3,
\]

\[
m_1 = \frac{20153 + 134\sqrt{20153}}{354209128}, \quad m_2 = \frac{20153 - 134\sqrt{20153}}{354209128}
\]

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

\[
p(x, y) = \sum_{\pm} \left( \frac{9\pm\sqrt{-3}}{18} \right) (x^2 + \frac{1\pm\sqrt{-3}}{2}xy + y^2)^3.
\]
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 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 $x^5 y$, $x^3 y^3$, $x y^5$ 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 sets of sums of three cubes for a given $p$ and what other symmetries those sets might have.

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 sets of sums of three cubes for a given $p$ and what other symmetries those sets might have.

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 cubic (thanks GM!) 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.

To sum up:

**Conjecture**

*Every* \( p \in H_m(\mathbb{C}^2) \) *can be written as a sum of* \( d \) *d-th powers of forms in* \( H_e(\mathbb{C}^2) \). *This is true for* \( d = 1, d = 2, e = 1 \) *and for* \( (d, e) = (3, 2) \).
The octic (or \textit{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.

To sum up:

\begin{center}
\textbf{Conjecture}
\end{center}

\begin{quote}
Every $p \in H_m(\mathbb{C}^2)$ can be written as a sum of $d$ $d$-th powers of forms in $H_e(\mathbb{C}^2)$. This is true for $d = 1, d = 2, e = 1$ and for $(d, e) = (3, 2)$.
\end{quote}
Thank you for your attention. I also very much to thank Josephine, Rainer and Seth for the opportunity to speak here.
Thank you for your attention. I also very much to thank Josephine, Rainer and Seth for the opportunity to speak here.

\[
\int_{\Omega} f_u \ dt.
\]