Waring rank and the underlying field

Bruce Reznick
University of Illinois at Urbana-Champaign

SIAM Conference on Applied Algebraic Geometry
Polynomial Optimization and Moments
NIMS, Daejeon, South Korea August 6, 2015

Suppose $p(x,y) = \sum \binom{d}{i} a_i x^{d-i} y^i$ is a homogeneous form of degree d over a field $F \subset \mathbb{C}$ and suppose K is an intermediate field, $F \subseteq K \subseteq \mathbb{C}$.

Suppose $p(x,y) = \sum \binom{d}{i} a_i x^{d-i} y^i$ is a homogeneous form of degree d over a field $F \subset \mathbb{C}$ and suppose K is an intermediate field, $F \subseteq K \subseteq \mathbb{C}$.
We define the *K-length of p*, $L_K(p)$ to be the minimum integer r so that there exists a representation

$$p(x,y) = \sum_{i=1}^{r} \lambda_i (\alpha_i x + \beta_i y)^d, \qquad \lambda_i, \alpha_i, \beta_i \in K.$$

Of course, $L_{\mathbb{C}}(p)$ is the Waring rank of p.

Suppose $p(x,y) = \sum \binom{d}{i} a_i x^{d-i} y^i$ is a homogeneous form of degree d over a field $F \subset \mathbb{C}$ and suppose K is an intermediate field, $F \subseteq K \subseteq \mathbb{C}$.
We define the *K-length of p*, $L_K(p)$ to be the minimum integer r so that there exists a representation

$$p(x,y) = \sum_{i=1}^{r} \lambda_i (\alpha_i x + \beta_i y)^d, \qquad \lambda_i, \alpha_i, \beta_i \in K.$$

Of course, $L_{\mathbb{C}}(p)$ is the Waring rank of p.
If $K \subset \mathbb{C}$, then $L_K(p)$ may be larger. For example,

$$p(x,y) = (x + \sqrt{2}y)^d + (x - \sqrt{2}y)^d \in \mathbb{Q}[x,y],$$

and $L_K(p) = 2$ if $\sqrt{2} \in K$ and (it turns out) $L_K(p) = d$ if $\sqrt{2} \notin K$.
More generally, if $K_1 \subset K_2$, then $L_{K_1}(p) \geq L_{K_2}(p)$.

Here are some known results about $L_K(p)$, followed by some of the new results in this talk.

Here are some known results about $L_K(p)$, followed by some of the new results in this talk.
I'll say that two linear forms are *distinct* if they (or their d-th powers) are not proportional. A representation is *honest* if the summands are pairwise distinct. Two honest representations are *different* if the summands are not permutations of each other.

Here are some known results about $L_K(p)$, followed by some of the new results in this talk.
I'll say that two linear forms are *distinct* if they (or their d-th powers) are not proportional. A representation is *honest* if the summands are pairwise distinct. Two honest representations are *different* if the summands are not permutations of each other.

- Any $d+1$ distinct d-th powers are linearly independent, hence if p has two different representations, of length k and ℓ, then $k+\ell \geq d+2$.

Here are some known results about $L_K(p)$, followed by some of the new results in this talk.
I'll say that two linear forms are *distinct* if they (or their d-th powers) are not proportional. A representation is *honest* if the summands are pairwise distinct. Two honest representations are *different* if the summands are not permutations of each other.

- Any $d+1$ distinct d-th powers are linearly independent, hence if p has two different representations, of length k and ℓ, then $k+\ell \geq d+2$.
- Sylvester gave an algorithm in 1851 for computing $L_K(p)$, subject to being able to determine whether there exist forms in certain subspaces which split completely into distinct factors over K. (This can be expressed in terms of apolarity, but discussions of particular forms need the algorithm.) More later.

- Sylvester proved a version of "Newton's generalization of Descartes' Rule of Signs" in 1864 which implies that if p itself is a product of d real linear factors (whether distinct or not), then $L_{\mathbb{R}}(p) \geq d$. More later.

- Sylvester proved a version of "Newton's generalization of Descartes' Rule of Signs" in 1864 which implies that if p itself is a product of d real linear factors (whether distinct or not), then $L_{\mathbb{R}}(p) \geq d$. More later.
- For all $F \subseteq K$, $L_K(p) \leq d$.

- Sylvester proved a version of "Newton's generalization of Descartes' Rule of Signs" in 1864 which implies that if p itself is a product of d real linear factors (whether distinct or not), then $L_{\mathbb{R}}(p) \geq d$. More later.
- For all $F \subseteq K$, $L_K(p) \leq d$.
- There is a quintic $p(x, y) = 3x^5 - 20x^3y^2 + 10xy^4$ with the property that $L_{\mathbb{Q}(\sqrt{-1})}(p) = 3$, $L_{\mathbb{Q}(\sqrt{-2})}(p) = 4$, and $L_{\mathbb{R}}(p) = 5$. There cannot be three different lengths for degrees < 5.

- Sylvester proved a version of "Newton's generalization of Descartes' Rule of Signs" in 1864 which implies that if p itself is a product of d real linear factors (whether distinct or not), then $L_{\mathbb{R}}(p) \geq d$. More later.
- For all $F \subseteq K$, $L_K(p) \leq d$.
- There is a quintic $p(x, y) = 3x^5 - 20x^3y^2 + 10xy^4$ with the property that $L_{\mathbb{Q}(\sqrt{-1})}(p) = 3$, $L_{\mathbb{Q}(\sqrt{-2})}(p) = 4$, and $L_{\mathbb{R}}(p) = 5$. There cannot be three different lengths for degrees < 5.

The new results are part of an ongoing project with my new graduate student Neriman Tokcan, whom I hope will be able to present a lot more from her thesis to AG17.

- Sylvester proved a version of "Newton's generalization of Descartes' Rule of Signs" in 1864 which implies that if p itself is a product of d real linear factors (whether distinct or not), then $L_{\mathbb{R}}(p) \geq d$. More later.
- For all $F \subseteq K$, $L_K(p) \leq d$.
- There is a quintic $p(x, y) = 3x^5 - 20x^3y^2 + 10xy^4$ with the property that $L_{\mathbb{Q}(\sqrt{-1})}(p) = 3$, $L_{\mathbb{Q}(\sqrt{-2})}(p) = 4$, and $L_{\mathbb{R}}(p) = 5$. There cannot be three different lengths for degrees < 5.

The new results are part of an ongoing project with my new graduate student Neriman Tokcan, whom I hope will be able to present a lot more from her thesis to AG17.

Let ζ_m denote a primitive m-th root of unity. It is an amusing algebraic number theory exercise to show that for $m \geq 3$, $\zeta_m \notin \mathbb{Q}(\zeta_{m\pm 1})$.

- If $k \geq 3$ and $p_{2k-1}(x,y) = x^{k-1}y^{k-1}(x-y)$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k-1}) = k$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k-1}) = k+1$, and $L_{\mathbb{R}}(p_{2k-1}) = 2k-1$.

- If $k \geq 3$ and $p_{2k-1}(x,y) = x^{k-1}y^{k-1}(x-y)$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k-1}) = k$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k-1}) = k+1$, and $L_{\mathbb{R}}(p_{2k-1}) = 2k-1$.
- If $k \geq 3$ and $p_{2k}(x,y) = x^k y^k$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k}) = k+1$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k}) = k+2$, and $L_{\mathbb{R}}(p_{2k}) = 2k$.

- If $k \geq 3$ and $p_{2k-1}(x,y) = x^{k-1}y^{k-1}(x-y)$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k-1}) = k$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k-1}) = k+1$, and $L_{\mathbb{R}}(p_{2k-1}) = 2k-1$.
- If $k \geq 3$ and $p_{2k}(x,y) = x^k y^k$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k}) = k+1$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k}) = k+2$, and $L_{\mathbb{R}}(p_{2k}) = 2k$.
- Thus, three different lengths are possible for all degrees ≥ 5. It is an open and seemingly difficult algebraic/Diophantine question to determine whether four lengths are possible.

- If $k \geq 3$ and $p_{2k-1}(x,y) = x^{k-1}y^{k-1}(x-y)$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k-1}) = k$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k-1}) = k+1$, and $L_{\mathbb{R}}(p_{2k-1}) = 2k-1$.
- If $k \geq 3$ and $p_{2k}(x,y) = x^k y^k$, then $L_{\mathbb{Q}(\zeta_{k+1})}(p_{2k}) = k+1$, $L_{\mathbb{Q}(\zeta_k)}(p_{2k}) = k+2$, and $L_{\mathbb{R}}(p_{2k}) = 2k$.
- Thus, three different lengths are possible for all degrees ≥ 5. It is an open and seemingly difficult algebraic/Diophantine question to determine whether four lengths are possible.
- If $q(x) = x^2y^2(x^2-y^2)$, then $L_K(q) = 4$ iff $\zeta_3 \in K$ and $L_K(q) \leq 5$ iff there exist $i \in K$ or there exist $u, v \in K$, $u, 1/u, v, 1/v$ distinct, such that

$$(u + 1/u)(v + 1/v) = -1.$$

Otherwise, $L_K(q) = 6$.

Theorem (Sylvester, 1851)

Suppose $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j \in K[x,y] \subset \mathbb{C}[x,y]$ *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 distinct linear factors,* $\alpha_j, \beta_j \in K$.

Theorem (Sylvester, 1851)

Suppose $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j \in K[x,y] \subset \mathbb{C}[x,y]$ *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 distinct linear factors,* $\alpha_j, \beta_j \in K$.
Then there exist $\lambda_k \in K$ *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 $p(x,y) = \sum_{j=0}^{d} \binom{d}{j} a_j x^{d-j} y^j \in K[x,y] \subset \mathbb{C}[x,y]$ *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 distinct linear factors,* $\alpha_j, \beta_j \in K$.
Then there exist $\lambda_k \in K$ *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 an algorithm! Given p, for increasing r, write the coefficients of p in the Hankel matrix, and look for null vectors c which are the coefficients of forms h which split into distinct linear factors over K.

Some notes on the proof:

- This is an algorithm! Given p, for increasing r, write the coefficients of p in the Hankel matrix, and look for null vectors c which are the coefficients of forms h which split into distinct linear factors over K.
- Note $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ 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

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

Some notes on the proof:

- This is an algorithm! Given p, for increasing r, write the coefficients of p in the Hankel matrix, and look for null vectors c which are the coefficients of forms h which split into distinct linear factors over K.
- Note $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ 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

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

Some notes on the proof:

- This is an algorithm! Given p, for increasing r, write the coefficients of p in the Hankel matrix, and look for null vectors c which are the coefficients of forms h which split into distinct linear factors over K.
- Note $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ 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

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

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, and dimension counting takes care of the rest. This is the apolarity approach.

Some notes on the proof:

- This is an algorithm! Given p, for increasing r, write the coefficients of p in the Hankel matrix, and look for null vectors c which are the coefficients of forms h which split into distinct linear factors over K.
- Note $(\beta\frac{\partial}{\partial x} - \alpha_j\frac{\partial}{\partial y})$ 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

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

  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, and dimension counting takes care of the rest. This is the apolarity approach.
- We call h (of any degree) a *Sylvester form* for p.

- Sylvester worked before the field concept was known and, implicitly, everything was taken over $\mathbb{C}$. His ideas carry over to K, with the observation that if $p \in K[x,y], \alpha_k, \beta_k \in K$ and

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

with $\lambda_k \in \mathbb{C}$, then, in fact, $\lambda_k \in K$.

- Sylvester worked before the field concept was known and, implicitly, everything was taken over $\mathbb{C}$. His ideas carry over to K, with the observation that if $p \in K[x,y], \alpha_k, \beta_k \in K$ and

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

with $\lambda_k \in \mathbb{C}$, then, in fact, $\lambda_k \in K$.
- Sylvester's Theorem has an elementary proof using the theory of constant-coefficient linear recurrence sequences.

- Sylvester worked before the field concept was known and, implicitly, everything was taken over $\mathbb{C}$. His ideas carry over to K, with the observation that if $p \in K[x,y], \alpha_k, \beta_k \in K$ and

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

with $\lambda_k \in \mathbb{C}$, then, in fact, $\lambda_k \in K$.
- Sylvester's Theorem has an elementary proof using the theory of constant-coefficient linear recurrence sequences.
- In the even case, the determinant of the square matrix is the *catalecticant*. Sylvester apologized for introducing this term:

- Sylvester worked before the field concept was known and, implicitly, everything was taken over $\mathbb{C}$. His ideas carry over to K, with the observation that if $p \in K[x,y], \alpha_k, \beta_k \in K$ and

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

  with $\lambda_k \in \mathbb{C}$, then, in fact, $\lambda_k \in K$.
- Sylvester's Theorem has an elementary proof using the theory of constant-coefficient linear recurrence sequences.
- In the even case, the determinant of the square matrix is the *catalecticant*. 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.

- Sylvester worked before the field concept was known and, implicitly, everything was taken over $\mathbb{C}$. His ideas carry over to K, with the observation that if $p \in K[x,y], \alpha_k, \beta_k \in K$ and

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

  with $\lambda_k \in \mathbb{C}$, then, in fact, $\lambda_k \in K$.
- Sylvester's Theorem has an elementary proof using the theory of constant-coefficient linear recurrence sequences.
- In the even case, the determinant of the square matrix is the *catalecticant*. 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 1851 paper, Sylvester introduced the term "unimodular" in its current meaning.

Here is an 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 an 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 an 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 $h(x,y) = 2x^2 - xy - y^2 = (2x+y)(x-y)$, so that

Here is an 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 $h(x,y) = 2x^2 - xy - y^2 = (2x+y)(x-y)$, so that

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

In fact (and not coincidentally), $p(x,y) = -(x-2y)^3 + 2(x+y)^3$.

Another simple, but important, 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 $h(x,y) = c_0x^2 + c_1xy + c_2y^2$ has repeated factors, and p is not a sum of two cubes.

Another simple, but important, 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 $h(x,y) = c_0x^2 + c_1xy + c_2y^2$ has repeated factors, and p is not a sum of two cubes.

Similarly, $x^{d-1}y$ requires d d-th powers, but these are essentially the only such examples of $L_{\mathbb{C}}(p) = d$ for a d-ic form p.

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 fixed $\ell = \alpha_0 x + \beta_0 y$, there exists λ so that $p(x, y) - \lambda \ell^{2s}$ has a matrix with a non-trivial null-vector, generally corresponding to h with distinct factors. Thus:

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 fixed $\ell = \alpha_0 x + \beta_0 y$, there exists λ so that $p(x,y) - \lambda \ell^{2s}$ has a matrix with a non-trivial null-vector, generally corresponding to h with distinct factors. Thus:

(i) A general binary form p of odd degree $2s-1$ can be written over $\mathbb{C}$ (uniquely) as

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

(ii) Given any fixed linear form ℓ, a general binary form p of even degree $2s$ can be written over $\mathbb{C}$ as

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

One concrete application is related to the "Hilbert Identities", used in solving Waring's Problem over $\mathbb{Z}$.

Theorem

The representations of $(x^2+y^2)^t$ *of length* $t+1$ *over* $\mathbb{C}$ *are:*

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

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

One concrete application is related to the "Hilbert Identities", used in solving Waring's Problem over $\mathbb{Z}$.

Theorem

The representations of $(x^2+y^2)^t$ *of length* $t+1$ *over* $\mathbb{C}$ *are:*

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

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

$$L_K((x^2+y^2)^t) = t+1 \iff \tan\left(\frac{\pi}{t+1}\right)\in K.$$

One concrete application is related to the "Hilbert Identities", used in solving Waring's Problem over $\mathbb{Z}$.

Theorem

The representations of $(x^2+y^2)^t$ *of length* $t+1$ *over* $\mathbb{C}$ *are:*

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

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

$$L_K((x^2+y^2)^t) = t+1 \iff \tan\left(\frac{\pi}{t+1}\right)\in K.$$

The earliest version I have found of this identity is for real θ, by Avner Friedman, from the 1950s. It can also be derived from an 1863 quadrature formula of Mehler.

Newton was very interested in non-real roots of real polynomials, proving that they have to occur in conjugate pairs. Sylvester in 1864 proved one of Newton's conjectured generalizations of Descartes' Rule of Signs, not unlike Sturm's theorem. All known proofs rely on Rolle's Theorem.

Newton was very interested in non-real roots of real polynomials, proving that they have to occur in conjugate pairs. Sylvester in 1864 proved one of Newton's conjectured generalizations of Descartes' Rule of Signs, not unlike Sturm's theorem. All known proofs rely on Rolle's Theorem.

Theorem (Sylvester, 1864)

Suppose $p(x, y)$ is a real form of degree d with τ real linear factors (including multiplicity) and

$$p(x, y) = \sum_{j=1}^{r} \lambda_j (\cos \theta_j x + \sin \theta_j y)^d$$

where $-\frac{\pi}{2} < \theta_1 < \cdots < \theta_r \leq \frac{\pi}{2}$, $r \geq 2$ and $\lambda_j \neq 0$.

Newton was very interested in non-real roots of real polynomials, proving that they have to occur in conjugate pairs. Sylvester in 1864 proved one of Newton's conjectured generalizations of Descartes' Rule of Signs, not unlike Sturm's theorem. All known proofs rely on Rolle's Theorem.

Theorem (Sylvester, 1864)

Suppose $p(x, y)$ is a real form of degree d with τ real linear factors (including multiplicity) and

$$p(x, y) = \sum_{j=1}^{r} \lambda_j (\cos \theta_j x + \sin \theta_j y)^d$$

where $-\frac{\pi}{2} < \theta_1 < \cdots < \theta_r \leq \frac{\pi}{2}$, $r \geq 2$ and $\lambda_j \neq 0$.
If there are σ sign changes in the tuple $(\lambda_1, \lambda_2, \ldots, \lambda_r, (-1)^d \lambda_1)$, then $\tau \leq \sigma$ $(\leq r)$.

Newton was very interested in non-real roots of real polynomials, proving that they have to occur in conjugate pairs. Sylvester in 1864 proved one of Newton's conjectured generalizations of Descartes' Rule of Signs, not unlike Sturm's theorem. All known proofs rely on Rolle's Theorem.

Theorem (Sylvester, 1864)

Suppose $p(x, y)$ is a real form of degree d with τ real linear factors (including multiplicity) and

$$p(x, y) = \sum_{j=1}^{r} \lambda_j (\cos\theta_j x + \sin\theta_j y)^d$$

where $-\frac{\pi}{2} < \theta_1 < \cdots < \theta_r \leq \frac{\pi}{2}$, $r \geq 2$ and $\lambda_j \neq 0$.
If there are σ sign changes in the tuple $(\lambda_1, \lambda_2, \ldots, \lambda_r, (-1)^d \lambda_1)$, then $\tau \leq \sigma$ $(\leq r)$.
In particular, if $\tau = d$, then $d \leq r$, so $L_{\mathbb{R}}(p) = d$.

We turn to the new material and give illustrative examples, rather than the full proof in all degrees.

We turn to the new material and give illustrative examples, rather than the full proof in all degrees.
Under the invertible linear map $(x, y) \mapsto (x + iy, x - iy)$, x^4y^4 becomes $(x^2 + y^2)^4$, so it's not surprising that the results are well-behaved. Does x^4y^4 have a representation of length 4?

We turn to the new material and give illustrative examples, rather than the full proof in all degrees.
Under the invertible linear map $(x, y) \mapsto (x + iy, x - iy)$, x^4y^4 becomes $(x^2 + y^2)^4$, so it's not surprising that the results are well-behaved. Does x^4y^4 have a representation of length 4? Consider $\binom{8}{4}x^4y^4$. Then the Hankel matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which is non-singular; no Sylvester forms!

For length 5, we have

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \iff c_1 = c_2 = c_3 = c_4 = 0.$$

For length 5, we have

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \iff c_1 = c_2 = c_3 = c_4 = 0.$$

The general Sylvester form is $c_0x^5 + c_5y^5$. If this splits over K, then it must factor as $c_0 \prod_{k=0}^{4}(x + \zeta_5^k \lambda y)$ for some λ, and if these roots are in K, then so is $(\zeta_5\lambda)/\lambda = \zeta_5$. Since $x^5 - y^5$ is a Sylvester form, $L_K(x^4y^4) = 5$ iff $\zeta_5 \in K$.

For length 6, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The general Sylvester form is $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$; in particular, $xy(x^4 - y^4)$, which splits over $\mathbb{Q}(\zeta_4)$. There are many other such fields as well.

For length 6, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The general Sylvester form is $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$; in particular, $xy(x^4 - y^4)$, which splits over $\mathbb{Q}(\zeta_4)$. There are many other such fields as well.

On the other hand, x^4y^4 has 8 real linear factors, so $L_{\mathbb{R}}(x^4y^4) = 8$.

For length 6, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The general Sylvester form is $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$; in particular, $xy(x^4 - y^4)$, which splits over $\mathbb{Q}(\zeta_4)$. There are many other such fields as well.

On the other hand, x^4y^4 has 8 real linear factors, so $L_{\mathbb{R}}(x^4y^4) = 8$.

We do not know whether there exists a non-real field K so that no form of the kind $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$ splits over K.

For length 6, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The general Sylvester form is $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$; in particular, $xy(x^4 - y^4)$, which splits over $\mathbb{Q}(\zeta_4)$. There are many other such fields as well.

On the other hand, x^4y^4 has 8 real linear factors, so $L_{\mathbb{R}}(x^4y^4) = 8$.

We do not know whether there exists a non-real field K so that no form of the kind $c_0x^6 + c_1x^5y + c_5xy^5 + c_6y^6$ splits over K.

This discussion generalizes uneventfully to x^ky^k.

Now we consider $x^3y^3(x-y)$, or equivalently $\binom{7}{4}x^3y^3(x-y)$. The matrix for length 4 is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \end{pmatrix}.$$

Now we consider $x^3y^3(x-y)$, or equivalently $\binom{7}{4}x^3y^3(x-y)$. The matrix for length 4 is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \end{pmatrix}.$$

It is almost comically easy to see that the only Sylvester forms are multiples of $x^4+x^3y+x^2y^2+xy^3+y^4=\frac{x^5-y^5}{x-y}$, which splits over K if and only if $\zeta_5 \in K$, and so this is the necessary and sufficient condition for $L_K(x^3y^3(x-y))=4$.

For length 5, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}$$

The Sylvester forms are

$$r_1 x^5 + r_2(x^4 y + x^3 y^2 + x^2 y^3 + x y^4) + r_3 y^5$$

For length 5, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}$$

The Sylvester forms are

$$r_1x^5 + r_2(x^4y + x^3y^2 + x^2y^3 + xy^4) + r_3y^5$$

One such instance is $(r_1, r_2, r_3) = (0, 1, 0)$: $xy(x + y)(x^2 + y^2)$, which splits over $\mathbb{Q}(\zeta_4)$.

For length 5, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}$$

The Sylvester forms are

$$r_1x^5 + r_2(x^4y + x^3y^2 + x^2y^3 + xy^4) + r_3y^5$$

One such instance is $(r_1, r_2, r_3) = (0, 1, 0)$: $xy(x + y)(x^2 + y^2)$, which splits over $\mathbb{Q}(\zeta_4)$.
It seems quite hard to determine over which fields a Sylvester form can split, even in these extremely simple cases.

For length 5, the matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}$$

The Sylvester forms are

$$r_1x^5 + r_2(x^4y + x^3y^2 + x^2y^3 + xy^4) + r_3y^5$$

One such instance is $(r_1, r_2, r_3) = (0, 1, 0)$: $xy(x + y)(x^2 + y^2)$, which splits over $\mathbb{Q}(\zeta_4)$.
It seems quite hard to determine over which fields a Sylvester form can split, even in these extremely simple cases.

As before, $x^3y^3(x - y)$ has seven real factors, so

$$L_{\mathbb{R}}(x^3y^3(x - y)) = 7.$$

These arguments generalize uneventfully to $x^ky^k(x - y)$.

Based on the examples $x^k y^k$ and $x^k y^k (x - y)$, all experienced PhD advisors will be able to guess what Neriman decided to look at first:

Based on the examples $x^k y^k$ and $x^k y^k (x - y)$, all experienced PhD advisors will be able to guess what Neriman decided to look at first:

$$x^2 y^2 (x^2 - y^2).$$

Based on the examples $x^k y^k$ and $x^k y^k (x-y)$, all experienced PhD advisors will be able to guess what Neriman decided to look at first:

$$x^2 y^2 (x^2 - y^2).$$

This has six real linear factors, so its length over $\mathbb{R}$ is 6.

Based on the examples $x^k y^k$ and $x^k y^k (x-y)$, all experienced PhD advisors will be able to guess what Neriman decided to look at first:

$$x^2 y^2 (x^2 - y^2).$$

This has six real linear factors, so its length over $\mathbb{R}$ is 6.

To see that this does not have length 3, its catalecticant is non-singular.

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

For length 4, the matrix is

$$\begin{pmatrix} 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

and the Sylvester forms are $a(x^4 + x^2y^2 + y^4) + bxy(x^2 + y^2)$.

For length 4, the matrix is

$$\begin{pmatrix} 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

and the Sylvester forms are $a(x^4 + x^2y^2 + y^4) + bxy(x^2 + y^2)$.

When can this split over K? If $a = 0$, the answer is iff $i \in K$. If $a \neq 0$, we may take $a = 1$ and dehomogenize by setting $y = 1$. Observe that x is a root iff $1/x$ is a root. Let $w = x + 1/x$, so that

$$x^4 + bx^3 + x^2 + bx + 1 = x^2(w^2 + bw - 1)$$
$$= x^2(w - w_1)(w - w_2) = (x^2 - w_1x + 1)(x^2 - w_2x + 1),$$
$$w_1w_2 = -1.$$

For length 4, the matrix is

$$\begin{pmatrix} 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

and the Sylvester forms are $a(x^4 + x^2y^2 + y^4) + bxy(x^2 + y^2)$.

When can this split over K? If $a = 0$, the answer is iff $i \in K$. If $a \neq 0$, we may take $a = 1$ and dehomogenize by setting $y = 1$. Observe that x is a root iff $1/x$ is a root. Let $w = x + 1/x$, so that

$$x^4 + bx^3 + x^2 + bx + 1 = x^2(w^2 + bw - 1)$$
$$= x^2(w - w_1)(w - w_2) = (x^2 - w_1x + 1)(x^2 - w_2x + 1),$$
$$w_1w_2 = -1.$$

We see that there are four distinct roots iff there exist $u, v \in K$ so that $u, v, \frac{1}{u}, \frac{1}{v}$ are distinct and $(u + \frac{1}{u})(v + \frac{1}{v}) = -1$.

It is easy enough to find fields K so that $(u+\frac{1}{u})(v+\frac{1}{v})=-1$ has four distinct solutions in K. Pick u for example, and then solve for v. By choosing $u=\frac{m}{n}$, we need

$$v+\frac{1}{v}=\frac{-mn}{m^2+n^2}.$$

Then

$$v\in\mathbb{Q}(\sqrt{-(4m^4+7m^2n^2+4n^4)})=$$

$$\mathbb{Q}(\sqrt{-(2m^2+mn+2n^2)(2m^2-mn+2n^2)}).$$

It is easy enough to find fields K so that $(u+\frac{1}{u})(v+\frac{1}{v})=-1$ has four distinct solutions in K. Pick u for example, and then solve for v. By choosing $u=\frac{m}{n}$, we need

$$v+\frac{1}{v}=\frac{-mn}{m^2+n^2}.$$

Then

$$v\in\mathbb{Q}(\sqrt{-(4m^4+7m^2n^2+4n^4)})=$$

$$\mathbb{Q}(\sqrt{-(2m^2+mn+2n^2)(2m^2-mn+2n^2)}).$$

By taking $m,n\leq 10^3$, we find $L_{\mathbb{Q}(\sqrt{-N})}(x^2y^2(x^2-y^2))=4$ when $N\in\{6,10,51,85\}$.

It is easy enough to find fields K so that $(u+\frac{1}{u})(v+\frac{1}{v})=-1$ has four distinct solutions in K. Pick u for example, and then solve for v. By choosing $u=\frac{m}{n}$, we need

$$v+\frac{1}{v}=\frac{-mn}{m^2+n^2}.$$

Then

$$v\in\mathbb{Q}(\sqrt{-(4m^4+7m^2n^2+4n^4)})=$$

$$\mathbb{Q}(\sqrt{-(2m^2+mn+2n^2)(2m^2-mn+2n^2)}).$$

By taking $m,n\le 10^3$, we find $L_{\mathbb{Q}(\sqrt{-N})}(x^2y^2(x^2-y^2))=4$ when $N\in\{6,10,51,85\}$.

I do not claim that these are the only such small imaginary quadratic fields, but I also don't know how to prove anything else, in either direction.

It is easy enough to find fields K so that $(u+\frac{1}{u})(v+\frac{1}{v})=-1$ has four distinct solutions in K. Pick u for example, and then solve for v. By choosing $u=\frac{m}{n}$, we need

$$v+\frac{1}{v}=\frac{-mn}{m^2+n^2}.$$

Then

$$v\in\mathbb{Q}(\sqrt{-(4m^4+7m^2n^2+4n^4)})=$$

$$\mathbb{Q}(\sqrt{-(2m^2+mn+2n^2)(2m^2-mn+2n^2)}).$$

By taking $m,n\le 10^3$, we find $L_{\mathbb{Q}(\sqrt{-N})}(x^2y^2(x^2-y^2))=4$ when $N\in\{6,10,51,85\}$.

I do not claim that these are the only such small imaginary quadratic fields, but I also don't know how to prove anything else, in either direction.

Note that $|u+1/u|\ge 2$ for real u, so Sylvester 1864 is partially validated: $L_{\mathbb{R}}(p)>4$.

To ask a somewhat larger question, let V be a subspace of the binary forms of degree d over a field K. When is there $0 \neq h \in V$ which splits into distinct factors over K?

To ask a somewhat larger question, let V be a subspace of the binary forms of degree d over a field K. When is there $0 \neq h \in V$ which splits into distinct factors over K?
When V has codimension one, the theorem $L_K(p) \leq d$ easily implies that such an h always exists.

To ask a somewhat larger question, let V be a subspace of the binary forms of degree d over a field K. When is there $0 \neq h \in V$ which splits into distinct factors over K?

When V has codimension one, the theorem $L_K(p) \leq d$ easily implies that such an h always exists.

When V has codimension two, I know two possible obstacles. First, V could simply consist of multiples of some $(\alpha x + \beta y)^2$.

To ask a somewhat larger question, let V be a subspace of the binary forms of degree d over a field K. When is there $0 \neq h \in V$ which splits into distinct factors over K?
When V has codimension one, the theorem $L_K(p) \leq d$ easily implies that such an h always exists.
When V has codimension two, I know two possible obstacles.
First, V could simply consist of multiples of some $(\alpha x + \beta y)^2$.
Descartes' Rule of Signs gives another approach for real forms. Let

$$V_{k,d} = \left\{ \sum_{i=0}^{d} a_i x^{d-i} y^i \ : \ a_k = a_{k+1} = 0 \right\}.$$

If $0 \neq h \in V_{k,d}$, then the consecutive zero coefficients means that h has at most $d-2$ real roots, and so cannot split over $\mathbb{R}$.
Similarly if $ad \neq bc$, $a, b, c, d \in \mathbb{R}$, and $p(\frac{ax+by}{cx+dy}) \in V_{k,d}$.

To ask a somewhat larger question, let V be a subspace of the binary forms of degree d over a field K. When is there $0 \neq h \in V$ which splits into distinct factors over K?
When V has codimension one, the theorem $L_K(p) \leq d$ easily implies that such an h always exists.
When V has codimension two, I know two possible obstacles.
First, V could simply consist of multiples of some $(\alpha x + \beta y)^2$.
Descartes' Rule of Signs gives another approach for real forms. Let

$$V_{k,d} = \left\{ \sum_{i=0}^{d} a_i x^{d-i} y^i \ : \ a_k = a_{k+1} = 0 \right\}.$$

If $0 \neq h \in V_{k,d}$, then the consecutive zero coefficients means that h has at most $d-2$ real roots, and so cannot split over $\mathbb{R}$.
Similarly if $ad \neq bc$, $a, b, c, d \in \mathbb{R}$, and $p(\frac{ax+by}{cx+dy}) \in V_{k,d}$.
The question I leave you with is this: **are there versions of Descartes' Rule of Signs over other fields which give similar information?**

Thanks to the organizers for the invitation and to the audience for their attention.