Exponential polynomials

Paola D'Aquino

Seconda Universita' di Napoli

Cesme, May 2012

Topics

- **Exponential rings, exponential fields and exponential polynomial ring**

- **Ritt's Factorization Theorem**

- **Schanuel's Conjecture and Shapiro's Conjecture**

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) where R is a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a morphism of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E-field if K is a field.

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

4. $K[X]^E$ E-ring of exponential polynomials over (K, E)

Exponential polynomials

Sketch of the construction:

Let R be a partial E-ring, $R = D \oplus \Delta$, where $D = dom(E)$.

Let t^{Δ} be a multiplicative copy of Δ, and consider $R[t^{\Delta}]$.

Extend E to R by defining $E(\delta) = t^{\delta}$, $\delta \in \Delta$.

Decompose $R[t^{\Delta}] = R \oplus t^{\Delta - \{0\}}$. Iterate ω times, and get E total.

1. Let $R = \mathbb{Z}[\overline{X}]$, $D = (0)$ e $\Delta = R$.

   The limit of previous construction is $[\overline{X}]^E$, the free E-ring on $\overline{X}$.

2. Let (K, E) be an E-field and $R = K[\overline{X}]$. Decompose $K[\overline{X}] = K \oplus \Delta$, where $D = K$ and $\Delta = \{f : f(\overline{0}) = 0\}$.

   The limit of previous construction is the E-ring $K[\overline{X}]^E$ of exponential polynomials in $\overline{X}$ over K.

Exponential polynomials

An exponential polynomial in $[x, y]^E$ is represented as

$$P(x, y) = -3x^2y - x^5y^7 + (2xy + 5y^2)e^{(-7x^3+11x^5y^4)}$$

$$+(6 - 2xy^5)e^{(5x+2x^7y^2)e^{5x-10y^2}}$$

Theorem

Let (R, E) be an E-domain. Then $R[\overline{X}]^E$ is an integral domain whose units are $uE(f)$, where u is invertible in R and $f \in R[\overline{X}]^E$.

Definition

An element $f \in R[\overline{X}]^E$ is irreducible if there are no non-units g and h in $R[\overline{X}]^E$ such that $f = gh$.

Exponential polynomials

Definition

Let $f = \sum_{i=1}^{N} a_i t^{\alpha_i}$ be an exponential polynomial. Then *the support* of $f = supp(f) = \mathbb{Q}$-space generated by $\alpha_1, \ldots, \alpha_N$.

Definition

An exponential polynomial $f(x)$ is simple if $\dim supp(f) = 1$.

$$\sin(2\pi x) = \frac{e^{2\pi ix} - e^{-2\pi ix}}{2i}$$

Factorization theory

- Ritt in 1927 studied factorizations of exponential polynomial

$$1 + \beta_1 e^{\alpha_1 z} + \ldots + \beta_k e^{\alpha_k z}$$

  over $\mathbb{C}$, using factorizations in fractional powers of classical polynomials in many variables.

- Gourin (1930) and Macoll (1935) gave a refinement of Ritt's factorization theorem for exponential polynomials of the form

$$p_1(z)e^{\alpha_1 z} + \ldots + p_k(z)e^{\alpha_k z}$$

  with $\alpha_i \in \mathbb{C}$, and $p_i(z) \in \mathbb{C}[z]$.

- D'A. and Terzo (2011) gave a factorization theorem for general exponential polynomials $f(\overline{X}) \in K[\overline{X}]^E$, where K is an algebraically closed field of characteristic 0 with an exponentiation.

Ritt's basic idea

Ritt: reduce the factorization of an exponential polynomial to that of a classical polynomial in many variables in fractional powers.

If $Q(Y_1, \dots, Y_n) \in K[Y_1, \dots, Y_n]$ is an irreducible polynomial over K, it can happen that for some $q_1, \dots, q_n \in \mathbb{N}_+$, $Q(Y_1^{q_1}, \dots, Y_n^{q_n})$ becomes reducible:

Ex: $X - Y$ irreducible, but $X^3 - Y^3 = (X - Y)(X^2 + XY + Y^2)$

Definition

A polynomial $Q(\overline{Y})$ is power irreducible (over K) if for each $\overline{q} \in \mathbb{N}_+^n$, $Q(\overline{Y}^{\overline{q}})$ is irreducible.

A factorization of $Q(\overline{Y})$ gives a factorization of $Q(\overline{Y}^{\overline{q}})$

A factorization of $Q(\overline{Y}^{\overline{q}}) = Q(Y_1^{q_1}, \dots, Y_n^{q_n})$ gives a factorization of $Q(Y_1, \dots, Y_n)$ in fractional powers of $Y_1, \dots, Y_n$.

Associate polynomial

Let $f(\overline{X}) = \sum_{h=1}^{m} a_h t^{b_h}$, where $a_h \in K[\overline{X}]$ and $b_h \in \Delta$ and let $\{\beta_1, \ldots, \beta_l\}$ be a $\mathbb{Z}$-basis of *supp*(f).

Modulo a monomial we consider f as polynomial in $e^{\beta_1}, \ldots, e^{\beta_l}$, with coefficients in $K[\overline{X}]$. Let $Y_i = e^{\beta_i}$, for $i = 1, \ldots, l$.

$$f(\overline{X}) \in K[\overline{X}]^E \rightsquigarrow Q(Y_1, \ldots, Y_l) \in K[\overline{X}][Y_1, \ldots, Y_l]$$

monomial: $Y_1^{m_1} \cdot \ldots \cdot Y_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$, i.e. an invertible element in $K[\overline{X}]^E$

Simple exponential polynomials correspond to a single variable classical polynomials

Factorization theorem

If $Q(\overline{Y}) = Q_1(\overline{Y}) \cdot \ldots \cdot Q_r(\overline{Y})$ then $f(\overline{X}) = f_1(\overline{X}) \cdot \ldots \cdot f_r(\overline{X})$

and for any $\overline{q}$ positive integers

if $Q(\overline{Y}^{\overline{q}}) = R_1(\overline{Y}) \cdot \ldots \cdot R_p(\overline{Y})$ then $f(\overline{X}) = g_1(\overline{X}) \cdot \ldots \cdot g_p(\overline{X})$.

All the factorizations of $f(\overline{X})$ are obtained in this way.

Lemma

Let $f(\overline{X})$ and $g(\overline{X})$ be in $\in K[\overline{X}]^E$. If $g(\overline{X})$ divides $f(\overline{X})$ then $supp(ag)$ is contained in $supp(bf)$, for some units a, b.

Remark: If f is a simple polynomial and g divides f then g is also simple.

Factorization theorem

Problem: How many tuples $\overline{q}$ are there such that $Q(\overline{Y}^{\overline{q}})$ is reducible?

Have to avoid $Y - Z$ since $Y^{\frac{1}{k}} - Z^{\frac{1}{k}}$ is a factor for all $k > 0$

Theorem

There is a uniform bound for the number of irreducible factors of

$$Q(Y_1^{q_1}, \dots, Y_l^{q_l})$$

for $Q(Y_1, \dots, Y_l)$ irreducible with more than two terms and arbitrary $q_1, \dots, q_l \in \mathbb{N}_+$. The bound depends only on

$$M = max\{d_{Y_1}, \dots, d_{Y_l}\}.$$

Factorization Theorem

Theorem (Ritt)

Let $f(z) = \lambda_1 e^{\mu_1 z} + ... + \lambda_N e^{\mu_N z}$, where $\lambda_i, \mu_i \in \mathbb{C}$. Then f can be written uniquely up to order and multiplication by units as

$$f(z) = S_1 \cdot \ldots \cdot S_k \cdot I_1 \cdot \ldots \cdot I_m$$

where S_j are simple polynomials with $supp(S_{j_1}) \neq supp(S_{j_2})$ for $j_1 \neq j_2$, and I_h are irreducible exponential polynomials.

Factorization Theorem

Theorem (D'A-Terzo)

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials Q_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials P_j where $supp(P_{j1}) \neq supp(P_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Corollary

If f is irreducible and the dimension of $supp(f) > 1$ then f is prime

Schanuel's conjecture

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$,

$l.d.(\alpha_1, \ldots, \alpha_n)$ =linear dimension of $< \alpha_1, \ldots, \alpha_n >_{\mathbb{Q}}$

$tr.d._{\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ =transcendence degree of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}$.

$$\textbf{(SC)} \quad tr.d._{\mathbb{Q}}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) \geq l.d.(\alpha_1, \ldots, \alpha_n)$$

Generalized Schanuel Conjecture Assume (R, E) is an E-ring and $char(R) = 0$. Let $\lambda_1, \ldots, \lambda_n \in R$ then

$$tr.d._{\mathbb{Q}}(\lambda_1, \ldots, \lambda_n, e^{\lambda_1}, \ldots, e^{\lambda_n}) - l.d.(\lambda_1, \ldots, \lambda_n) \geq 0$$

Known cases

Generalization of Lindemann-Weierstrass Theorem:
Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers which are linearly independent over $\mathbb{Q}$.Then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraic independent over $\mathbb{Q}$.

1. $\lambda = 1$ transcendence of e (Hermite 1873)
2. $\lambda = 2\pi i$ transcendence of π (Lindemann 1882)
3. $\overline{\lambda} = (\pi, i\pi)$ then tr.d.$(\pi, i\pi, e, e^{i\pi}) = 2$, i.e. π, e^{π} are algebraically independent over $\mathbb{Q}$ (Nesterenko 1996)
4. (SC) is true for power series $\mathbb{C}[[t]]$ (Ax 1971)

The Schanuel machine

- $\overline{\lambda} = (1, \pi i)$,

$$\textbf{SC} \Rightarrow t.d(1, i\pi, e, e^{i\pi}) \geq l.d.(1, i\pi).$$

Then e, π, are algebraically independent over $\mathbb{Q}$;

- $\overline{\lambda} = (1, i\pi, e)$

$$\textbf{SC} \Rightarrow t.d(1, i\pi, e, e, e^{i\pi}, e^{e}) \geq l.d.(1, i\pi, e).$$

Then π, e, e^{e} are algebraically independent over $\mathbb{Q}$;

- $\overline{\lambda} = (1, i\pi, i\pi^2, e, e^{e}, e^{i\pi^2})$,

$$\textbf{SC} \Rightarrow t.d(1, i\pi, i\pi^2, e, e^{e}, e^{i\pi^2}, e, e^{i\pi}, e^{i\pi^2}, e^{e}, e^{e^{e}}, e^{e^{i\pi^2}})$$

$$\geq l.d.(1, i\pi, i\pi^2, e, e^{e}, e^{i\pi^2}).$$

Then $\pi, e, e^{e}, e^{e^{e}}, e^{i\pi^2}, e^{e^{i\pi^2}}$ are algebraically independent / $\mathbb{Q}$.

Algebraic consequences of Schanuel's Conjecture

Theorem (Macintyre)

Suppose S is an E-ring satisfying (SC), and S_0 is the E-subring of S generated by 1. Then the natural E-morphism $\varphi : [\emptyset]^E \to S_0$ is an E-isomorphism, i.e. S_0 is isomorphic to E-free ring on the empty set.

Corollary

(SC) There is an algorithm which decides if two exponential constants coincide.

Algebraic consequences of Schanuel's Conjecture

Theorem (Terzo)

(SC) Let $[x,y]^E$ be the free E-ring generated by $\{x,y\}$ and let ψ be the E-morphism:

$$\psi : [x,y]^E \to (\mathbb{C}, exp)$$

defined by $\psi(x) = \pi$ and $\psi(y) = i$. Then there exists a unique isomorphism

$$f : [x,y]^E / Ker\psi \to \langle i, \pi \rangle^E$$

and

$$Ker\psi = \langle e^{xy} + 1, y^2 + 1 \rangle^E.$$

Corollary

(SC) The only algebraic relations among π, e and i over $\mathbb{C}$ are

$$e^{i\pi} = -1 \text{ and } i^2 = -1$$

Algebraic consequences of Schanuel's Conjecture

Theorem (Terzo)

(SC) Let $[x]^E$ be the free E-ring generated by $\{x\}$ and let R be the E-subring of $(\mathbb{R}, exp)$ generated by π. Then the E-morphism

$$\varphi : [x]^E \to (R, exp)$$

$$x \mapsto \pi$$

is an E-isomorphism.

Corollary

(SC)

1. There is an algorithm for deciding if two exponential polynomials in π and i are equal in $\mathbb{C}$.
2. There is an algorithm for deciding if two exponential polynomials in π are equal in $\mathbb{R}$.

$K[\overline{X}]^E$ is sharply Schanuel

$[\overline{X}]^E$ satisfies Schanuel Conjecture

THEOREM (D., Macintyre and Terzo)

Let (K, E) be an exponential field satisfying Schanuel Conjecture. Suppose that

$\gamma_1, \ldots, \gamma_n \in K[\overline{X}]^E - K$ are $\mathbb{Q}$-linearly independent over K.

Then

$$t.d._K K(\gamma_1, \ldots, \gamma_n, E(\gamma_1), \ldots, E(\gamma_n)) \geq n + 1.$$

Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

$$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}$$

$$g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial.

This conjecture comes out of complex analysis (and early work of Polya, Ritt and many other). It was formulated by H.S. Shapiro in a paper entitled:

The expansion of mean-periodic functions in series of exponentials.

Remark

The factorization theorem implies that we need to consider only two cases of the Shapiro problem.

CASE 1. At least one of the exponential polynomial is a simple polynomial.

CASE 2. At least one of the exponential polynomials is irreducible.

Over $\mathbb{C}$ answer is positive unconditionally

Theorem (van der Poorten and Tijdeman, 1975)

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in \mathbb{C}$, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Ingredients of the proof

Theorem (Ritt)

If every zero of an exponential polynomial $f(z)$ is a zero of $g(z)$ then $f(z)$ divides $g(z)$.

Theorem (Skolem, Mahler, Lech)

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, be an exponential polynomial, where $\alpha, \beta \in K$ where K is a field of characteristic 0. If $f(z)$ vanishes for infinitely many integers $z = z_i$, then there exists an integer d and certain set of least residues modulo $d, d_1, \ldots, d_l$ such that $f(z)$ vanishes for all integers $z \equiv d_i (mod\ d)$, for $i = 1, \ldots, l$, and $f(z)$ vanishes only finitely often on other integers.

Case 1.

Setting: Over (K, E) algebraically closed field with an exponentiation, $char(K) = 0$, $ker(E) = \omega\mathbb{Z}$, E surjective
answer is positive unconditionally

Lemma (DMT)

Let $h(z) = \lambda_1 e^{\mu_1 z} + \ldots + \lambda_N e^{\mu_N z}$, where $\lambda_j, \mu_j \in K$. If h vanishes over all integers then $sin(\pi z)$ divides h.

We use Vandermonde determinant.

Theorem (DMT)

Let f be a simple exponential polynomial, and let g be an arbitrary exponential polynomial such that f and g have infinitely many common roots. Then there exists an exponential polynomial which divides both f and g.

Schanuel → Shapiro

THEOREM (A. Skhop, 2010)

(SC) Let f and g be exponential polynomials as above with $c_i, b_j, \lambda_i, \mu_j \in \mathbb{Q}^{alg}$. If f and g have no common factors except monomials then f and g have only finitely many common zeros.

THEOREM (D'A, Macintyre, Terzo, 2011)

Schanuel's conjecture implies **Shapiro's conjecture.**

The proof uses no logic, but substantial work by Bombieri, Masser and Zannier, and work of Evertse, Schlickewei and Schmidt on linear functions of elements of finite rank groups.

Case 2.

Consider the following system:

$$\left\{ \begin{array}{ll} f(z) = \lambda_1 e^{\mu_1 z} + \ldots + \lambda_N e^{\mu_N z} & = 0 \\ g(z) = l_1 e^{m_1 z} + \ldots + l_M e^{m_M z} & = 0 \end{array} \right. \tag{1}$$

where $\lambda_i, \mu_i, l_j, m_j \in K$.

Let $D = l.d.(supp(f) \cup supp(g))$, $b_1, \ldots, b_D$ a $\mathbb{Z}$-basis, and $Y_i = e^{b_i z}$ for $i = 1, \ldots, D$.

To system (1) associate:

$$\left\{ \begin{array}{ll} F(Y_1, \ldots, Y_D) & = 0 \\ G(Y_1, \ldots, Y_D) & = 0 \end{array} \right. \tag{2}$$

where $F(Y_1, \ldots, Y_D), G(Y_1, \ldots, Y_D) \in \mathbb{Q}(\bar{\lambda}, \bar{l})[Y_1, \ldots, Y_D]$.

Case 2.

Let $L = \mathbb{Q}(\bar{\lambda}, \bar{l})^{alg}$, $t.d._{\mathbb{Q}}(L) < \infty$. Let S be the infinite set of non zero common solutions of system (1).

Remark

If $s \in S$ then $(e^{b_1 s}, \ldots, e^{b_D s})$ is a solution of system (2).

Theorem (D'A, Macintyre and Terzo)

(SC) The $\mathbb{Q}$-vector space generated by S is finite dimensional.

(SC) gives bounds on linear dimensions and transcendence degrees of finite subsets of S and their exponentials.

Let V be an irreducible component of the subvariety of the algebraic group G_m^D defined by (2) over L containing $(e^{b_1 s}, \ldots, e^{b_D s})$ for infinitely many $s \in S$.

Ingredients

Definition

An irreducible subvariety W of V is anomalous in V if W is contained in an algebraic subgroup Γ of G_m^D with

$$\dim W > max\{0, \dim V - \mathrm{codim}\Gamma\}$$

Theorem (Bombieri, Masser, Zannier (2007))

Let V be an irreducible variety in G_m^D of positive dimension defined over $\mathbb{C}$. There is a finite collection Φ_V of proper tori H such that $1 \leq D - dimH \leq dimV$ and every maximal anomalous subvariety W of V is a component of the intersection of V with a coset $H\theta$ for some $H \in \Phi_V$ and $\theta \in G_m^D$.

Second case of Shapiro's Conjecture

Remark

BMZ result holds for every algebraically closed field K with $char(K) = 0$

For a finite sequence $\overline{s} = s_1, \ldots, s_k \in S$ consider the variety $W_{\overline{s}} \subseteq V^k$ generated by $(e^{\overline{b}s_1}, \ldots, e^{\overline{b}s_k})$, where $\overline{b} = b_1, \ldots, b_D$.

For big k, either dim $W_{\overline{s}} = 0$ or $W_{\overline{s}}$ is anomalous.

If for infinitely many k's dim $W_{\overline{s}} = 0$ then we are done.

Otherwise, we are forced into anomalous case, and using BMZ we get finite dimensionality of the set of solutions.

Corollary (DMT)

If $\widehat{G}$ is the divisible hull of G the group generated by all $e^{\mu_j s}$'s where $s \in S$ then $\widehat{G}$ has finite rank.

Theorem (DMT)

(SC) Let $f(z)$ be an irreducible polynomial and suppose the following system

$$\begin{cases} f(z) = \lambda_1 e^{\mu_1 z} + \ldots + \lambda_N e^{\mu_N z} & = 0 \\ g(z) = l_1 e^{m_1 z} + \ldots + l_M e^{m_M z} & = 0 \end{cases}$$

has infinitely common zeros. Then f divides g.

Degenerate solutions

Definition

A solution $(\alpha_1, \ldots, \alpha_n)$ of a linear equation

$$a_1 x_1 + \ldots + a_n x_n = 1$$

over a field K is non degenerate if for every proper non empty subset I of $\{1, \ldots, n\}$ we have $\sum_{i \in I} a_i \alpha_i \neq 0$.

Theorem (Evertse, Schlickewei, Schmidt)

Let K be a field, $char(K) = 0$, n a positive integer, and Γ a finitely generated subgroup of rank r of $(K^\times)^n$. There exists a positive integer $R = R(n, r)$ such that for any non zero $a_1, \ldots, a_n$ elements in K, the equation $a_1 x_1 + \ldots + a_n x_n = 1$ does not have more than R non degenerate solutions $(\alpha_1, \ldots, \alpha_n)$ in Γ.

Associated linear equation

By finite dimensionality of S, $l.d.(S) = p$, where $p \in \mathbb{N}$. Denote by $\{s_1, \ldots, s_p\}$ a $\mathbb{Q}$-basis of S. For any $s \in S$ we have:

$$s = \sum_{l=1}^{p} c_l s_l$$

where $c_l \in \mathbb{Q}$.

$$0 = f(s) = \lambda_1 e^{\mu_1(\sum_{l=1}^{p} c_l s_l)} + \ldots + \lambda_N e^{\mu_N(\sum_{l=1}^{p} c_l s_l)} = \sum_{j=1}^{N} \lambda_j \prod_{l=1}^{p} (e^{\mu_j s_l})^{c_l}$$

Any solution $s \in S$ produces a solution $\overline{\omega}$ of the linear equation associated to f,

$$\lambda_1 X_1 + \ldots + \lambda_N X_N = 0$$

where $\omega_i = e^{\mu_i(\sum_{l=1}^{p} c_l s_l)}$, $i = 1, \ldots, N$ and $\overline{\omega} \in \widehat{G}$.

Proof of main result

Induction of length of $g(z)$.

- $M = 2$ (g simple);
- $N, M > 2$, we associate to

$$g(z) \rightsquigarrow l_1 X_1 + \ldots + l_M X_M.$$

By (ESS) result we have that there are infinitely many degenerate solutions. By PHP there exist a subset $I = \{i_1, \ldots, i_r\}$ of $\{1, \ldots, M\}$ such that $i_r > 2$ and

$$l_{i_1} X_{i_1} + \ldots + l_{i_r} X_{i_r} = 0$$

has infinitely many zeros.
$g(z) = g_1(z) + g_2(z)$, where $g_1(z) = l_{i_1} e^{m_{i_1} z} + \ldots + l_{i_r} e^{m_{i_r} z}$, and $g_2(z) = g(z) - g_1(z)$. By inductive hypothesis and by the irreducibility of f, we have that f divides g_1 and f divides g_2, and hence f divides g.