The coefficient tuples of univariate polynomials whose roots form arithmetic progressions define an irreducible algebraic variety

José António Perdigão Dias da Silva, Dep. Matemática.; Fac. de Ciências, Bloco C6, Univ. de Lisboa, 1700 Lisboa, Portugal.
João Gouveia, Dep. Math. Univ. Coimbra, 3001-454 Coimbra, Portugal, jsgouveia@netcabo.pt
Alexander Kovačec, Dep. Math. Univ. Coimbra, 3001-454 Coimbra, Portugal, kovacec@mat.uc.pt

- - - -

Motivated by questions in additive number theory we prove the following

1 Theorem Let $n \in \mathbb{Z}_{\geq 2}$ Define set $V \subseteq \mathbb{C}^n$ by

$$V = \{(\tilde{a}_1, \ldots, \tilde{a}_n) : \text{ the roots of } T^n + \tilde{a}_1 T^{n-1} + \ldots + \tilde{a}_n \text{ define an arithmetic progression}\}.$$

Then V is an irreducible algebraic variety.

Proof. Define polynomials $q(T, x, y) \in \mathbb{C}[T, x, y]$ and $a_0 = 1, a_k(x, y) \in \mathbb{C}[x, y]$, $k = 1, \ldots, n$, by

$$q(T, x, y) = (T - x)(T - (x + y))(T - (x + 2y)) \ldots (T - (x + (n - 1)y)) = \textstyle\sum_{k=0}^{n} a_k(x, y)T^{n-k}.$$

Evidently $a_k(x, y) \in \mathbb{C}[x, y]$ is homogeneous of degree k and $V = \{(a_1(\tilde{x}, \tilde{y}), \ldots, a_n(\tilde{x}, \tilde{y})) : \tilde{x}, \tilde{y} \in \mathbb{C}\}$. Let $c_1, \ldots, c_n$ be a new set of indeterminates and define for the polynomial $n-$tuple $A = (a_1, \ldots, a_n)$ the set $I_A = \{h \in \mathbb{C}[c_1, \ldots, c_n] : h(a_1(x, y), \ldots, a_n(x, y)) = 0\}$. By [CLS, p338c-5, 339c1], I_A is the prime ideal of syzygies for A. (The facts in [CLS p. 338, 339] we refer to, do not need the G-invariance hypotheses there made.)

We shall show $V = \mathbf{V}(I_A)$. Clearly $V \subseteq \mathbf{V}(I_A)$. For the converse, consider the ideal

$$J_A := \langle a_1(x, y) - c_1, \ldots, a_n(x, y) - c_n\rangle \lhd \mathbb{C}[x, y; c_1, \ldots, c_n].$$

By pp113c11,340c1, I_A is the second elimination ideal of J_A, that is $I_A = J_A \cap \mathbb{C}[c_1, \ldots, c_n]$. Also let $I'_A = J_A \cap \mathbb{C}[y, c_1, \ldots, c_n]$ be the first elimination ideal of J_A.

Some calculation reveals that

$$a_1(x, y) = -nx - (\tfrac{n^2}{2} - \tfrac{n}{2})y, \text{ and } \quad a_2(x, y) = (\tfrac{n^2}{2} - \tfrac{n}{2})x^2 + (\tfrac{n^3}{2} - n^2 + \tfrac{n}{2})xy + (\tfrac{n^4}{8} - \tfrac{5}{12}n^3 + \tfrac{3}{8}n^2 - \tfrac{n}{12})y^2$$

From here in turn one obtains that

$$\begin{aligned} q(y, c_1, c_2) &:= (-\frac{n^3}{24} + \frac{n}{24})y^2 + (\frac{1}{2} - \frac{1}{2n})c_1^2 - c_2 \\ &= (a_2 - c_2) + \left(\frac{n-1}{2}x + (\frac{n^2}{4} - \frac{n}{2} + \frac{1}{4})y + \frac{1-n}{2n}c_1\right)(a_1 - c_1). \end{aligned}$$

This shows that $q(y, c_1, c_2) \in \langle a_1 - c_1, a_2 - c_2\rangle \subseteq J_A$, and hence $q \in I'_A$.

Let $(\tilde{c}_1, \ldots, \tilde{c}_n) \in V(I_A)$. By p118c7, I_A is the first elimination ideal of I'_A. Inspecting q, we see by p117c-8 that there exists an $\tilde{y}$ such that $(\tilde{y}, \tilde{c}_1, \ldots, \tilde{c}_n) \in V(I'_A)$. Again by that fact, but now inspecting $a_1 - c_1 = -nx - \binom{n}{2}y - c_1 \in J_A$, we see that there exists $\tilde{x}$ such that $(\tilde{x}, \tilde{y}, \tilde{c}_1, \ldots, \tilde{c}_n) \in V(J_A)$. Thus we have shown that, given $(\tilde{c}_1, \ldots, \tilde{c}_n) \in \mathbf{V}(I_A)$, there exists $\tilde{x}, \tilde{y} \in \mathbb{C}$ such that $a_1(\tilde{x}, \tilde{y}) - \tilde{c}_1 = 0, \ldots, a_n(\tilde{x}, \tilde{y}) - \tilde{c}_n = 0$; hence $(\tilde{c}_1, \ldots, \tilde{c}_n) \in V$. This establishes $V = V(I_A)$ and so V is a variety. Since I_A is prime by p338c-5, and hence radical (p206c7), we find $I(V) = I(\mathbf{V}(I_A)) = I_A$ by p174c-3 &p180c3. By p195c-0 this shows that V is irreducible. □

Using p340c2, one gets via a symbolic computation the following:

2 Fact a. A monic polynomials of degree 3, $T^3 + \tilde{a}_1 T^2 + \tilde{a}_2 T + \tilde{a}_3 \in \mathbb{C}[T]$ has roots defining an arithmetic progression if and only if

$$27\tilde{a}_3 - 9\tilde{a}_1\tilde{a}_2 + 2\tilde{a}_1^3 = 0.$$

b. A monic polynomials of degree 4, $T^4 + \tilde{a}_1 T^3 + \tilde{a}_2 T^2 + \tilde{a}_3 T + \tilde{a}_4 \in \mathbb{C}[T]$ has roots defining an arithmetic progression if and only if

$$8\tilde{a}_3 - 4\tilde{a}_2\tilde{a}_1 + \tilde{a}_1^3 = 0, \text{ and } 1600\tilde{a}_4 - 144\tilde{a}_2^2 + 8\tilde{a}_2\tilde{a}_1^2 + 11\tilde{a}_1^4 = 0.$$

□

These computations can be extended indefinitely.

As a step towards a system parametrized by n, tying polynomials $a_k(x, y)$ to well studied objects may be useful.

3 Proposition Polynomials $a_{n,k}(x, y) = a_k(x, y)$ occuring in n-th degree polynomial $q(T, x, y)$ above, admit the following development in terms of the Stirling numbers $s(\cdot, \cdot)$ of the first kind:

$$a_{n,k}(x, y) = (-1)^k \sum_{j=0}^{k} x^{k-j} y^j \binom{n-j}{k-j} (-)^j s(n, n-j).$$

Proof. We work with fixed n. Letting $e_k(...)$ stand for the k-th elementary symmetric function of n arguments we have by Viète's formulae and definiton of e_k that

$$\begin{aligned}
a_k(x, y) &= (-)^k e_k(x, x+y, x+2y, \ldots, x+(n-1)y) \\
&= (-)^k \sum_{0 \le l_1 < l_2 < \ldots < l_k \le n-1} (x + l_1 y)(x + l_2 y) \ldots (x + l_k y) \\
&= (-)^k \sum_{0 \le l_1 < l_2 < \ldots < l_k \le n-1} \left(\sum_{j=0}^{k} x^{k-j} y^j \sum_{1 \le i_1 < i_2 < \ldots < i_j \le k} l_{i_1} l_{i_2} \ldots l_{i_j} \right) \\
&= (-)^k \sum_{j=0}^{k} x^{k-j} y^j \left(\sum_{0 \le l_1 < l_2 < \ldots < l_k \le n-1} \sum_{1 \le i_1 < i_2 < \ldots < i_j \le k} l_{i_1} l_{i_2} \cdots l_{i_j} \right) \\
&\stackrel{1}{=} (-)^k \sum_{j=0}^{k} x^{k-j} y^j \binom{n-j}{k-j} \sum_{0 \le l_1 < \ldots < l_j \le n-1} l_1 l_2 \cdots l_j.
\end{aligned}$$

Here '$\stackrel{1}{=}$' follows by observing that in the penultimate line we add a given product $l_1 l_2 \cdots l_j$ just as often as $J = \{l_1, \ldots, l_j\}$ occurs as a subset of a k-set K satisfying $J \subseteq K \subseteq \{0, \ldots, n-1\}$; so by elementary combinatorics it occurs $\binom{n-j}{k-j}$ times. Now recall that the Stirling numbers of the 1st kind can be found in the books, see e.g. [A, p153], as defined by the equation

$$x(x-1)\ldots(x-(n-1)) = \sum_{j=0}^{n} s(n, n-j) x^{n-j}.$$

So applying Viète on the left and comparing coefficients of x^{n-j}, we find $s(n, n-j) = (-)^j \sum_{0 \le l_1 < \ldots < l_j \le n-1} l_1 l_2 \cdots l_j$, concluding the proof. □

We can also explain the occurence of polynomial functions of n and their degrees as appearing as coefficients of the terms $x^j y^l$ in $a_1(x, y), a_2(x, y)$ in the proof of theorem 1.

4 Proposition For fixed $j \in \mathbb{Z}_{\ge 1}$, the map $\mathbb{Z}_{\ge 0} \ni n \mapsto s(n, n-j) \in \mathbb{Z}$ is a polynomial function of degree $2j$; in particular the coefficient of $x^{k-j} y^j$ in $a_{n,k}(x, y)$ as a function of n is a polynomial of degree $k + j$.

Proof. The proof is by induction on j. Write $p_j(n) := |s(n, n-j)|$. From the last lines of the previous proof we find, that $p_1(n) = |s(n, n-1)| = \sum_{0 \le l_1 \le n-1} l_1 = n(n-1)/2 = \frac{n^2}{2} - \frac{n}{2}$, a polynmial of degree 2 as claimed. We also have $p_j(n+1) = p_j(n) + n p_{j-1}(n)$, or $p_j(n+1) - p_j(n) = n p_{j-1}(n)$, for all $n \ge 0$. Hence $p_j(n+1) = \sum_{l=0}^{n} (p_j(l+1) - p_j(l)) = \sum_{l=0}^{n} l p_{j-1}(l)$. Since by induction hypothesis $\deg(x p_{j-1}(x)) = 2j - 1$, the first claim follows from well known formulae for the power sums via Bernoulli numbers: see [IR, p230c-6]; the second because the map $n \mapsto \binom{n-j}{k-j}$ is polynomial in n of degree $k - j$. □

The question whether the maps $n \mapsto s(n, n-j)$ have a nice polynomial representation in some basis remains to be investigated. A really simple parametrization in the standard basis is unlikely. For small degrees we find already 'large' primes. For example, we have

$$p_5(x) = -\frac{x^2}{80} - \frac{x^3}{960} + \frac{x^4}{36} - \frac{5x^5}{2304} - \frac{229x^6}{11520} + \frac{31x^7}{5760} + \frac{5x^8}{1152} - \frac{5x^9}{2304} + \frac{x^{10}}{3840}.$$

The explicit form of these polynomials can be found after calculating sufficiently many values of $s(n, n-j)$ and using the `InterpolationPolynomial` command in MATHEMATICA or the like. They suggest that the leading coefficient is always $(2^j j!)^{-1}$, while the coefficient of the lowest degree monomial is linked sometimes to the Bernoulli numbers.

References

[A] M. Aigner, *Kombinatorik* I, Springer 1975. (∃ English translation, Springer 1987(?))
[CLS] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms,* Springer 1997.
[IR] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer 1982.