Riv. Mat. Univ. Parma, Vol. **7** (2016), 239-246

VINCENZO MANTOVA

Algebraic equations with lacunary polynomials and the Erdős-Rényi conjecture

Abstract. In 1947, Rényi, Kalmár and Rédei discovered some special polynomials $p(x) \in \mathbb{C}[x]$ for which the square $p(x)^2$ has fewer non-zero terms than $p(x)$. Rényi and Erdős then conjectured that if the number of terms of $p(x)$ grows to infinity, then the same happens for $p(x)^2$. The conjecture was later proved by Schinzel, strengthened by Zannier, and a 'final' generalisation was proved by C. Fuchs, Zannier and the author. This note is a survey of the known results, with a focus on the applications of the latest generalisation.

Keywords. Lacunary polynomial, sparse polynomial, fewnomial, Vojta's conjecture, Bertini's irreducibility theorem, multiplicative group.

Mathematics Subject Classification (2010): 11C08, 12E05, 12Y05, 14G05, 14J99, 11U10.

1 - The original conjecture

1.1 - *Sparse square polynomials*

The problem we are going to discuss starts with a question of Rédei: *is there a polynomial $p(x)$ such that the number of terms of $p(x)^2$ is less than the number of terms of $p(x)$?* For the sake of notation, given a field K and a polynomial $p(x) \in K[x]$, let $\mathcal{N}(p)$ be the number of non-zero terms of $p(x)$. In other words, $\mathcal{N}(p)$ is the

Received: January 2, 2016; accepted: March 10, 2016.

minimum natural number such that

$$p(x) = \sum_{i=1}^{\mathcal{N}(p)} a_i x^{n_i},$$

where $a_i \in K$ and $n_i \in \mathbb{N}$.

In [8], Rényi, Kalmár and Rédei gave the following explicit example in $\mathbb{Q}[x]$

$$R_{29}(x) = (4x^4 + 4x^3 - 2x^2 + 2x + 1)(-84x^{24} + 28x^{20} - 10x^{16} + 4x^{12} - 2x^8 + 2x^4 + 1)$$

which satisfies $\mathcal{N}(R_{29}) = 29$, while $\mathcal{N}(R_{29}^2) = 28 < \mathcal{N}(R_{29})$, answering affirmatively the question of Rédei. A polynomial with this property is often called a "sparse square polynomial".

Examples of smaller degrees appeared later in literature:

- $R_{18}(x) = (x^2 + 2x - 2)(x^{15} + 4x^{12} - 8x^9 + 32x^6 - 160x^3 + 896)$ is such that $\mathcal{N}(R_{18}) = 18$ and $\mathcal{N}(R_{18}^2) = 17$ (Chaudry, 1988 [**2**]; an example with the same number of terms was also given by Freud, 1973 [**4**]);
- $R_{13}(x) = (125x^6 + 50x^5 - 10x^4 + 4x^3 - 2x^2 + 2x + 1)(-110x^6 + 1)$ is such that $\mathcal{N}(R_{13}) = 13$ and $\mathcal{N}(R_{13}^2) = 12$ (Coppersmith and Davenport, 1991 [**2**]).

In 2002, with the aid of the computer algebra system CoCoA, Abbott showed that if $p(x) \in \mathbb{C}(x)$ has degree at most 11, then $\mathcal{N}(p^2) \geq \mathcal{N}(p)$ [**1**]. Therefore, R_{13} is a sparse square polynomial of minimal degree. Apparently, it is still not known if the list of polynomials of degree 12 given in [**2**] contains all sparse square polynomials of minimal degree.

1.2 - *Asymptotic behaviour of $\mathcal{N}$ on squares*

Using the polynomial R_{29}, one can easily construct a sequence of polynomials such that the number of terms of their squares is asymptotically infinitesimal with respect to the number of terms of the polynomials themselves. Indeed, we may define

$$R_{29^l}(x) := R_{29}(x) \cdot R_{29}(x^{29}) \cdot \cdots \cdot R_{29}(x^{29^{l-1}}).$$

We have $\mathcal{N}(R_{29^l}) = 29^l$ and $\mathcal{N}(R_{29^l}) \leq 28^l$, so

$$\lim_{l \to \infty} \frac{\mathcal{N}(R_{29^l}^2)}{\mathcal{N}(R_{29^l})} = 0.$$

With additional adjustments to the polynomials R_{29^l}, Erdős proved the following.

Theorem 1.1 (Erdős, 1949 [**3**]). *There exist constants $c_2 > 0$ and $0 < c_1 < 1$ such that for all $l \in \mathbb{N}^*$, there is a $p_l(x) \in \mathbb{C}[x]$ satisfying*

$$\mathcal{N}(p_l) = l, \quad \mathcal{N}(p_l^2) < c_2 l^{c_1}.$$

In the same year, Verdenius proved that one can take $c_1 = \log_{13}(8)$ [**11**], and also produced a sequence (q_l) where $\mathcal{N}(q_l^3) < c_4 l^{c_3}$, again with $c_4 > 0$ and $0 < c_3 < 1$.

Although $\mathcal{N}(p^2)$ may be way smaller than $\mathcal{N}(p)$, Rényi and Erdős conjectured that for any sequence p_l of polynomials, if $\mathcal{N}(p_l) \to \infty$, then $\mathcal{N}(p_l^2) \to \infty$. We reformulate this as follows.

Conjecture 1.1. *For all $l \in \mathbb{N}$ there exists $c = c(l)$ with the following property: if $p(x) \in \mathbb{C}[x]$ is such that $\mathcal{N}(p^2) \leq l$, then $\mathcal{N}(p) \leq c$.*

Informally, we shall say that a polynomial p is *lacunary* (or *sparse*, or *fewnomial*) if $\mathcal{N}(p)$ is bounded, whereas the degree of p may be arbitrarily large. In this language, Conjecture 1.1 says that if the square of a polynomial p is lacunary, then p itself is lacunary.

2 - Known results on lacunary polynomials

2.1 - *Schinzel's and Zannier's theorems*

Conjecture 1.1 was proved by Schinzel, who actually obtained a stronger and explicit result. For the sake of exposition, the bound is slightly simplified with respect to the original one proved by Schinzel.

Theorem 2.1 (Schinzel, 1987 [**9**]). *For all $d, l \in \mathbb{N}^*$, and for all $p \in \mathbb{C}[x]$, if $\mathcal{N}(p^d) \leq l$, then $\mathcal{N}(p) \leq (4d)^{2^l d}$.*

This includes the original conjecture for $d = 2$. Moreover, in the same paper Schinzel proved that the conjecture does not hold if one replaces $\mathbb{C}$ with a field of positive characteristic: if d is not a power of the characteristic of the field, one can construct polynomials with an arbitrarily large number of terms whose d-th powers have at most $2d$ terms. In 2009, Schinzel and Zannier improved the bound of Theorem 2.1 to $1 + (4d)^{l-2}$ [**10**].

Always in [**9**], Schinzel also put forward a new conjecture: fixed a polynomial $f(y) \in \mathbb{C}[y]$, if $\mathcal{N}(f(p)) \leq l$, is there a bound for $\mathcal{N}(p)$? This specialises to the previous conjecture for $f(y) = y^d$. This was proved by Zannier in two steps. Again, for the sake of exposition, the conclusions are slightly simplified.

Theorem 2.2 (Zannier, 2007 [**12**]). *For all $l \in \mathbb{N}$, and for all $f \in \mathbb{C}[y] \setminus \mathbb{C}$, $p \in \mathbb{C}[x]$, if $\mathcal{N}(f(p)) \leq l$, then:*

- *either $\mathcal{N}(p) \leq 2$,*
- *or $\deg(f) \leq 2l(l-1)$.*

Theorem 2.3 (Zannier, 2008 [**13**]). *For all $l \in \mathbb{N}$ there exists $c_5 = c_5(l)$ such that for all $f \in \mathbb{C}[y] \setminus \mathbb{C}$, if $\mathcal{N}(f(p)) \leq l$, then $\mathcal{N}(p) \leq c_5$.*

We remark that the central argument in the proof of Theorem 2.3 yields a bound that depends on l and $\deg(f)$, which is already sufficient to answer Schinzel's original conjecture; however, when combined with the conclusion of Theorem 2.2, it yields a bound that is completely uniform in f. Moreover, the proof is constructive, so the bound c_5 is effective, although it is not explicitly calculated.

2.2 - *Rational functions*

C. Fuchs and Zannier applied a similar reasoning when the polynomial p is replaced by a rational function g. We define the number of terms of $g(x) \in \mathbb{C}[x]$ as the minimum number of terms required to write $g(x)$ as the ratio of two polynomials, possibly not coprime. Formally, we define

$$\mathcal{N}^{\#}(g) := \min\left\{ \mathcal{N}(p) + \mathcal{N}(q) \ : \ p, q \in \mathbb{C}[x],\ g(x) = \frac{p(x)}{q(x)} \right\}.$$

The fact that p and q may not be coprime is crucial and makes $\mathcal{N}$ and $\mathcal{N}^{\#}$ take different values on polynomials; for instance,

$$\mathcal{N}(1 + \ldots + x^{n-1}) = n, \quad \mathcal{N}^{\#}(1 + \ldots + x^{n-1}) = \mathcal{N}^{\#}\left(\frac{1-x^n}{1-x}\right) = 4.$$

Fuchs and Zannier proved an equivalent of Theorem 2.2 for rational functions, using $\mathcal{N}^{\#}$ in place of $\mathcal{N}$. The statement is simplified for the sake of exposition.

Theorem 2.4 (C. Fuchs-Zannier, 2012 [**6**]). *For all $l \in \mathbb{N}$, and for all $f \in \mathbb{C}(y) \setminus \mathbb{C}$, $g \in \mathbb{C}(x)$, if $\mathcal{N}^{\#}(f(g)) \leq l$, then:*

- *either $\mathcal{N}^{\#}(g) \leq 6$,*
- *or $\deg(f) \leq 2016 \cdot 5^l$.*

The equivalent of Theorem 2.3 holds for rational functions, and it was proved later as a special case of a much more general theorem on lacunary polynomials.

Theorem 2.5 (C. Fuchs-Mantova-Zannier, 2014 [**5**]). *For all $l \in \mathbb{N}$ there exists $c_6 = c_6(l)$ such that for all $f \in \mathbb{C}(y) \setminus \mathbb{C}$, $g \in \mathbb{C}(x)$, if $\mathcal{N}(f(g)) \leq l$, then $\mathcal{N}(g) \leq c_6$.*

2.3 - *Arbitrary algebraic equations*

It turns out that the above statement are special cases of the following theorem.

Theorem 2.6 ([**5**]). *For all $d, l \in \mathbb{N}^*$, there exists $c_7 = c_7(d, l)$ such that for all $f \in \mathbb{C}[x, y], p \in \mathbb{C}[x]$, if f is monic of degree d in y, $\mathcal{N}(f) \leq l$, and $f(x, p(x)) = 0$, then $\mathcal{N}(p) \leq c_7$.*

(Note that here $\mathcal{N}(f)$ means that we think of f as a polynomial in $\mathbb{C}(y)[x]$.) The above statement says that if $p(x)$ is algebraic and integral over some lacunary polynomials, then p is lacunary as well. Again, the proof of the theorem is constructive, but no explicit bound is given. Apart from explicit constants, one can recover the previous theorems on taking $f(x, y) = y^d - h(x)$ or $f(x, y) = g(y) - h(x)$.

Note that the assumption that f is monic is crucial. As soon as we admit f non-monic in y, we have the counterexample

$$f(x, y) = (1 - x)y - (1 - x^n), \quad p(x) = 1 + \ldots + x^{n-1}, \quad f(x, p(x)) = 0.$$

On the other hand, in the above example we have $\mathcal{N}^{\#}(p) = 4$. Indeed, with a standard variable substitution, one may easily deduce the following statement from Theorem 2.6.

Theorem 2.7 ([**5**]). *For all $d, l \in \mathbb{N}^*$, and for all $f \in \mathbb{C}(x)[y], g \in \mathbb{C}(x)$, if f has degree d in y, $\mathcal{N}^{\#}(f) \leq l$, and $f(x, g(x)) = 0$, then $\mathcal{N}^{\#}(g) \leq c_7(d, l^d) + l$.*

Together with Theorem 2.4, the above statement implies Theorem 2.5 as a special case.

3 - Applications

3.1 - *A non-standard interpretation*

The last theorems of the previous section have a rather natural non-standard interpretation. Recall that in non-standard analysis one has a map * which sends the standard objects, such as $\mathbb{N}$ or $\mathbb{R}$, into non-standard counterparts, in a way that preserves all the first-order formulas.

Given a map * such that ${}^*\mathbb{N} \neq \mathbb{N}$, our informal notion of lacunary polynomial can be given a precise meaning. We define the *ring $\mathcal{L}$ of lacunary polynomials* in ${}^*(\mathbb{C}[x])$ as the subring of polynomials whose number of terms is actually finite:

$$\mathcal{L} := \{a_1 x^{n_1} + \ldots + a_l x^{n_l} \ : \ l \in \mathbb{N},\ a_i \in {}^*\mathbb{C},\ n_i \in {}^*\mathbb{N}\}.$$

Note how the number of terms l is a standard, hence finite, natural number, while the degrees n_i are non-standard, hence possibly infinite. One can easily verify that the original Erdős-Rényi conjecture is equivalent to saying that if $p(x) \in {}^*\mathbb{C}[x]$ satisfies $p(x)^2 \in \mathcal{L}$, then $p(x) \in \mathcal{L}$.

Similarly, Theorem 2.6 translates to the following.

Theorem 3.1 ([5]). *The ring $\mathcal{L}$ is integrally closed in ${}^*(\mathbb{C}(x))$.*

The translation of Theorem 2.7 is the following.

Theorem 3.2 ([5]). *The fraction field of $\mathcal{L}$ is relatively algebraically closed in ${}^*(\mathbb{C}(x))$.*

The above statements had been proposed independently by Fornasiero.

3.2 - *Integral points*

A crucial observation in [5] is that one may think of a lacunary polynomial $p(x)$ as the specialisation in $(x^{n_1}, \ldots, x^{n_l})$, for some arbitrary $n_i \in \mathbb{N}$, of a polynomial $P(t_1, \ldots, t_l)$ of bounded degree in each variable. In turn, we may think of the polynomial $f(x, y)$ of Theorem 2.6 as the specialisation of a polynomial in several variables. This yields the following result about covers of $\mathbb{G}_{\mathrm{m}}^l$.

Given $f \in \mathbb{C}[t_1, \ldots, t_l, y] \setminus \mathbb{C}$ monic in y, let W be the quasi-projective variety defined by $f(t_1, \ldots, t_l, y) = 0$ and $t_1 \cdot \cdots \cdot t_l \neq 0$. Let $\pi : W \to \mathbb{G}_{\mathrm{m}}^l$ be the projection onto the first l coordinates.

If we think of $\mathbb{C}(x)$ as a function field over $\mathbb{C}$, and let $S = \{0, \infty\}$ be the set containing the zero and the pole of x, then the S-integral points of W are precisely the points of the form

$$(\alpha_1 x^{n_1}, \ldots, \alpha_l x^{n_l}, p(x)),$$

with $\alpha_i \in \mathbb{C}^*$, $n_i \in \mathbb{Z}$ and $p(x) \in \mathbb{C}[x^{\pm 1}]$, such that

$$f(\alpha_1 x^{n_1}, \ldots, \alpha_l x^{n_l}, p(x)) = 0.$$

Note that an integral point can be also seen as regular map $\rho : \mathbb{G}_{\mathrm{m}} \to W$.

Theorem 2.6 then implies the following.

Theorem 3.3 ([**5**]). *There exists a finite set Ψ of regular maps $\psi : V \times \mathbb{G}_{\mathrm{m}}^{s} \to W$, with $V = V_\psi$ a quasi-projective variety and $s = s_\psi$ a natural number, such that for all regular $\rho : \mathbb{G}_{\mathrm{m}} \to W$, there exist $\psi \in \Psi$, $\xi \in V_\psi$ and a regular $\gamma : \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{s_\psi}$ such that*

$$\rho(x) = \psi(\xi, \gamma(x))$$

for all $x \in \mathbb{G}_{\mathrm{m}}$.

This implies Vojta's conjecture for the special case of the S-integral points on W. Indeed, if the S-integral points of positive height are Zariski-dense in W (equivalently, if the union of the images of the non-constant regular maps $\rho : \mathbb{G}_{\mathrm{m}} \to W$ is Zariski-dense in W), then one may find a finite regular dominant map $V \times \mathbb{G}_{\mathrm{m}}^{s} \to W$ with $s > 0$. This implies that W is not of log-general type (see e.g. [**7**]).

3.3 - *Bertini for covers of multiplicative groups*

Via a standard argument involving symmetric functions, one can show that Theorem 2.6 also yields information about the irreducible factors of $f(x, y)$, rather than just its roots as a polynomial in y. Using the same formalism of the previous subsection, one can prove a form of 'Bertini irreducibility theorem' for covers of $\mathbb{G}_{\mathrm{m}}^{l}$.

Indeed, let $f \in \mathbb{C}[t_1, \ldots, t_l, y] \setminus \mathbb{C}$ monic in y, W be the quasi-projective variety defined by $f(t_1, \ldots, t_l, y) = 0$ and $t_1 \cdot \cdots \cdot t_l \neq 0$, and $\pi : W \to \mathbb{G}_{\mathrm{m}}^{l}$ be the projection onto the first l coordinates. Let e be the degree of π. Let $[e] : \mathbb{G}_{\mathrm{m}}^{l} \to \mathbb{G}_{\mathrm{m}}^{l}$ be the map taking each point to its e-th power. Theorem 2.6 then implies the following.

Theorem 3.4 ([**5**]). *If the pullback $[e]^* W$ is irreducible, there exists a finite set $\mathcal{E}$ of proper algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^{l}$ such that for all H connected algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^{l}$ and all $\theta \in \mathbb{G}_{\mathrm{m}}^{l}$, if $\pi^{-1}(\theta H)$ is reducible, then $H \subseteq \bigcup \mathcal{E}$.*

Acknowledgments. The author acknowledges the support by the ERC-AdG 267273 "Diophantine Problems".

References

[**1**] J. Abbott, *Sparse squares of polynomials*, Math. Comp. **71** (2002), no. 237, 407-413 (electronic).

[**2**] D. Coppersmith and J. H. Davenport, *Polynomials whose powers are sparse*, Acta Arith. **58** (1991), no. 1, 79-87,

[3] P. ERDŐS, *On the number of terms of the square of a polynomial*, Nieuw Arch. Wiskunde (2) **23** (1949), 63-65.

[4] R. FREUD, *On the minimum number of terms in the square of a polynomial*, Mat. Lapok **24** (1973), 95-98.

[5] C. FUCHS, V. MANTOVA and U. ZANNIER, *On fewnomials, integral points and a toric version of Bertini's theorem*, arXiv:1412.4548 [math.NT], preprint (2014).

[6] C. FUCHS and U. ZANNIER, *Composite rational functions expressible with few terms*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 1, 175-208.

[7] Y. KAWAMATA, *Characterization of abelian varieties*, Compositio Math. **43** (1981), no. 2, 253-276.

[8] A. RÉNYI, *On the minimal number of terms of the square of a polynomial*, Hungarica Acta Math. **1** (1947), 30-34.

[9] A. SCHINZEL, *On the number of terms of a power of a polynomial*, Acta Arith. **49** (1987), no. 1, 55-70.

[10] A. SCHINZEL and U. ZANNIER, *On the number of terms of a power of a polynomial*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **20** (2009), no. 1, 95-98.

[11] W. VERDENIUS, *On the number of terms of the square and the cube of polynomials*, Indagationes Math. **11** (1949), 459-465.

[12] U. ZANNIER, *On the number of terms of a composite polynomial*, Acta Arith. **127** (2007), no. 2, 157-167.

[13] U. ZANNIER, *On composite lacunary polynomials and the proof of a conjecture of Schinzel*, Invent. Math. **174** (2008), no. 1, 127-138.

VINCENZO MANTOVA
School of Mathematics
University of Leeds
Leeds, LS2 9JT, United Kingdom
e-mail: v.l.mantova@leeds.ac.uk