On the Reducibility and the Lenticular Sets of Zeroes of Almost Newman Lacunary Polynomials

Denys Dutykh, Jean-Louis Verger-Gaugry

Noname manuscript No.
(will be inserted by the editor)

On the Reducibility and the Lenticular Sets of Zeroes of Almost Newman Lacunary Polynomials

Denys Dutykh · Jean-Louis Verger-Gaugry

Received: date / Accepted: date

Abstract The class $\mathcal{B}$ of lacunary polynomials $f(x) := -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s}$ where $s \geq 0$, $m_1 - n \geq n-1$, $m_{q+1} - m_q \geq n-1$ for $1 \leq q < s$, $n \geq 3$, is studied. A polynomial having its coefficients in $\{0,1\}$ except its constant coefficient equal to -1 is called an *almost Newman polynomial*. A general theorem of factorization of the almost Newman polynomials of the class $\mathcal{B}$ is obtained. Such polynomials possess lenticular roots in the open unit disk off the unit circle in the small angular sector $-\pi/18 \leq \arg z \leq \pi/18$ and their non-reciprocal parts are always irreducible. The existence of lenticuli of roots is a peculiarity of the class $\mathcal{B}$. By comparison with the Odlyzko Poonen Conjecture and its variant Conjecture, an "Asymptotic Reducibility Conjecture" is formulated aiming at establishing the proportion of irreducible polynomials in this class. This proportion is conjectured to be $3/4$ and estimated by Monte-Carlo methods; the numerical approximate value 0.756 is obtained. The results extend those on trinomials (Selmer) and quadrinomials (Ljunggren, Mills, Finch and Jones).

Mathematics Subject Classification (2000) 11C08

1 Introduction

In this note, for $n \geq 3$, we study the factorization of the polynomials

$$f(x) := -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} \tag{1}$$

where $s \geq 0$, $m_1 - n \geq n-1$, $m_{q+1} - m_q \geq n-1$ for $1 \leq q < s$. Denote by $\mathcal{B}$ the class of such polynomials, and by $\mathcal{B}_n$ those whose third monomial is exactly

Univ. Grenoble Alpes, Univ. Savoie Mont Blanc, CNRS UMR 5127, LAMA
73000 Chambéry, France
Tel.: +33 (0)4 79 75 85 85
Fax: +33 (0)4 79 75 94 41
E-mail: denys.dutykh@univ-smb.fr, jean-louis.verger-gaugry@univ-smb.fr

x^n, so that

$$\mathcal{B} = \cup_{n\geq 2}\mathcal{B}_n.$$

The case "$s=0$" corresponds to the trinomials $G_n(z) := -1+z+z^n$ studied by Selmer [Sr]: let θ_n be the unique root of the trinomial $G_n(z) := -1+z+z^n$ in $(0,1)$. The algebraic integers $\theta_n^{-1} > 1$ are Perron numbers. The sequence $(\theta_n^{-1})_{n\geq 2}$ tends to 1 if n tends to $+\infty$.

Theorem 1 (Selmer) *Let $n \geq 2$. The trinomials $G_n(x)$ are irreducible if $n \not\equiv 5 \pmod 6$, and, for $n \equiv 5 \pmod 6$, are reducible as product of two irreducible factors whose one is the cyclotomic factor x^2-x+1, the other factor $(-1+x+x^n)/(x^2-x+1)$ being nonreciprocal of degree $n-2$.*

Theorem 2 (Verger-Gaugry [VG2]) *Let $n \geq 2$. The real root $\theta_n = \mathrm{D}(\theta_n) + \mathrm{tl}(\theta_n) \in (0,1)$ of the trinomial G_n admits the following asymptotic expansion:* $\mathrm{D}(\theta_n) = 1$

$$-\frac{\mathrm{Log}\, n}{n}\left(1-\Big(\frac{n-\mathrm{Log}\, n}{n\,\mathrm{Log}\, n+n-\mathrm{Log}\, n}\Big)\Big(\mathrm{Log}\,\mathrm{Log}\, n - n\mathrm{Log}\left(1-\frac{\mathrm{Log}\, n}{n}\right)-\mathrm{Log} n\Big)\right) \tag{2}$$

and

$$\mathrm{tl}(\theta_n) \;=\; \frac{1}{n}O\Big(\Big(\frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\Big)^2\Big), \tag{3}$$

with the constant $1/2$ involved in $O(\ )$.

A simplified form of (2) is the following:

$$\mathrm{D}(\theta_n) = 1-\frac{1}{n}\left(\mathrm{Log}\, n - \mathrm{Log}\,\mathrm{Log}\, n + \frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\right). \tag{4}$$

By definition a *Newman polynomial* is an integer polynomial having all its coefficients in $\{0,1\}$. A polynomial having its coefficients in $\{0,1\}$ except its constant coefficient equal to -1 is called an *almost Newman polynomial*. The polynomials $f \in \mathcal{B}$ are almost Newman polynomials. The following irreducibility Conjecture (called "OP") holds for the asymptotics of the factorization of Newman polynomials.

Conjecture 1 (Odlyzko - Poonen [OP]) Let $\mathcal{P}_{d,+} := \{1+\sum_{j=1}^{d} a_j x^j \mid a_j = 0 \text{ or } 1, a_d = 1\}$ denote the set of all Newman polynomials of degree d. Denote

$$\mathcal{P}_+ = \bigcup_{d\geq 1}\mathcal{P}_{d,+}.$$

Then, in $\mathcal{P}_+$, almost all polynomials are irreducible; more precisely, if Ω_d denotes the number of irreducible polynomials in $\mathcal{P}_{d,+}$, then

$$\lim_{d\to\infty}\frac{\Omega_d}{2^{d-1}} = \lim_{d\to\infty}\frac{\#\{f\in\mathcal{P}_{d,+} \mid \text{f irreducible}\}}{2^{d-1}} \;=\; 1.$$

The best account of the Conjecture is given by Konyagin [K]: $\Omega_d \gg \frac{2^d}{\mathrm{Log}\, d}$. Replacing the constant coefficients 1 by -1 gives the variant Conjecture (called "variant OP") for the almost Newman polynomials.

Conjecture 2 (Variant OP) Let $\mathcal{P}_{d,-} := \{-1+\sum_{j=1}^{d} a_j x^j \mid a_j = 0 \text{ or } 1, a_d = 1\}$ denote the set of all almost Newman polynomials of degree d. Denote

$$\mathcal{P}_- = \bigcup_{d\geq 1} \mathcal{P}_{d,-}.$$

Then, in $\mathcal{P}_-$, almost all polynomials are irreducible; more precisely,

$$\lim_{d\to\infty} \frac{\#\{f \in \mathcal{P}_{d,-} \mid \text{f irreducible}\}}{2^{d-1}} \;=\; 1.$$

There is a numerical evidence that the OP Conjecture and the variant OP Conjecture are true (Table 1, Sect. 6).

The objectives of this note consist in (i) establishing the type of factorization of the polynomials f of the class $\mathcal{B}$ (Theorem 3), in the context of Schinzel's and Filaseta's theorems on the factorization of lacunary polynomials [S] [S2] [F], (ii) characterizing the geometry of the zeroes of the polynomials f of the class $\mathcal{B}$, in particular in proving the existence of lenticuli of zeroes in the angular sector $-\pi/18 \leq \arg z \leq \pi/18$ inside the open unit disk in Solomyak's fractal (with numerical examples to illustrate Theorem 4), (iii) estimating the probability for a polynomial f in $\mathcal{B}$ to be irreducible (Heuristics called "Asymptotic Reducibility Conjecture") by comparison with the variant OP Conjecture.

Notations used in the sequel: if $P(X) = \sum_{j=0}^{r} a_j x^r \in \mathbb{Z}[X]$, we refer to the reciprocal polynomial of $P(x)$ as $P^*(x) = \sum_{j=0}^{r} a_{r-j} x^r$.The Euclidean norm $\|P\|$ of $P(X) = \sum_{j=0}^{r} a_j x^r \in \mathbb{Z}[X]$ is $\|P\| = \left(\sum_{j=0}^{r} a_j^2\right)^{1/2}$. If α is an algebraic number, $P_\alpha(X)$ denotes its minimal polynomial; if $P_\alpha(X)$ is reciprocal we say that α is reciprocal. A Perron number α is either 1 or a real algebraic integer > 1 such that its conjugates $\alpha^{(i)}$ are strictly less than α in modulus. The integer n is called the *dynamical degree* of the real algebraic integer $\beta > 1$ if $1/\beta$ denotes the unique real zero of $f(x) = -1 + x + x^n + \sum_{q=1}^{s} x^{m_q} \in \mathcal{B}$. $\mathbb{T}$ denotes the unit circle in the complex plane.

Theorem 3 *For any $f \in \mathcal{B}_n$, $n \geq 3$, denote by*

$$f(x) = A(x)B(x)C(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

where $s \geq 1$, $m_1 - n \geq n-1$, $m_{j+1} - m_j \geq n-1$ for $1 \leq j < s$, the factorization of f where A is the cyclotomic part, B the reciprocal noncyclotomic part, C the nonreciprocal part. Then (i) the nonreciprocal part C is nontrivial, irreducible, and never vanishes on the unit circle, (ii) if $\beta > 1$ denotes the real algebraic integer uniquely determined by the sequence $(n, m_1, m_2, \ldots, m_s)$ such that $1/\beta$ is the unique real root of f in (θ_{n-1}, θ_n), the nonreciprocal polynomial $-C^*(X)$ of $C(X)$ is the minimal polynomial of β, and β is a nonreciprocal algebraic integer.

A numerical observation: for all the f as in Theorem 3 we have numerically observed the following lower bound (for which we have no proof)

$$\deg(C) \geq \lfloor \frac{m_s - 1}{2} \rfloor. \tag{5}$$

Let us now define the lenticular roots of an f of the class $\mathcal{B}$. In the case "$s = 0$", i.e. for the trinomials $G_n(x) = -1 + x + x^n$, from Proposition 3.7 in [VG], the roots of modulus < 1 of G_n all lie in the angular sector $-\pi/3 < \arg z < +\pi/3$. The set of these "internal" roots has the form of a *lenticulus*, justifying the terminology (Figure 1a for $n = 37$); they are called *lenticular roots*. For extending the notion of "lenticulus of roots" to general polynomials f of the class $\mathcal{B}$, with $s \geq 1$, we view

$$f(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} = G_n(x) + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

(where $n \geq 3$, $s \geq 1$, $m_1 - n \geq n - 1$, $m_{j+1} - m_j \geq n - 1$ for $1 \leq j < s$) as a perturbation of $G_n(x)$ by $x^{m_1} + x^{m_2} + \ldots + x^{m_s}$. The lenticulus of roots of f is then a deformation of the lenticulus of roots of G_n (Figure 1b). In this deformation process, the aisles of the lenticulus may present important displacements, in particular towards the unit circle, whereas the central part remains approximately identical. Therefore it is hopeless to define the lenticulus of roots of f in the full angular sector $-\pi/3 < \arg\omega < +\pi/3$. From the structure of the asymptotic expansions of the roots of G_n [VG2] it is natural to restrict the angular sector to $-\pi/18 < \arg\omega < +\pi/18$. More precisely,

Theorem 4 *Let $n \geq 260$. There exists two positive constants c_n and $c_{A,n}$, $c_{A,n} < c_n$, such that the roots of $f \in \mathcal{B}_n$,*

$$f(x) - 1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

where $s \geq 1$, $m_1 - n \geq n - 1$, $m_{j+1} - m_j \geq n - 1$ for $1 \leq j < s$, lying in $-\pi/18 < \arg z < +\pi/18$ either belong to

$$\{z \mid ||z| - 1| < \frac{c_{A,n}}{n}\}, \quad \textit{or to} \quad \{z \mid ||z| - 1| \geq \frac{c_n}{n}\}.$$

The *lenticulus of zeroes of f* is then defined as

$$\mathcal{L}_\beta := \{\omega \mid |\omega| < 1, -\frac{\pi}{18} < \arg\omega < +\frac{\pi}{18},\ ||\omega| - 1| \geq \frac{c_n}{n}\}$$

where $1/\beta$ is the positive real zero of f. The proof of Theorem 4 requires the structure of the asymptotic expansions of the roots of G_n and is given in [VG3]. Let $\kappa = 0.171573\ldots$ be the maximum of the function $y \mapsto \big(1 - \exp\big(\frac{-\pi}{y}\big)\big)\big(2\exp\big(\frac{\pi}{y}\big) - 1\big)^{-1}$ on $(0, +\infty)$. The following formulation of c_n is given in [VG3]:

$$c_n = -(1 + \frac{1}{n})\operatorname{Log}\kappa + \frac{1}{n} O\Big(\Big(\frac{\operatorname{Log}\operatorname{Log} n}{\operatorname{Log} n}\Big)^2\Big)$$

with $c_n \simeq -\operatorname{Log}\kappa = 1.76274\ldots$ at the first-order. In the present note Theorem 4 is only examplified: in Section 4 we show that the statement of this Theorem

also holds on examples, in particular pentanomials, for dynamical degrees n less than 260.

Concerning the asymptotic probability of irreducibility of the polynomials of the class $\mathcal{B}$ at large degrees, our numerical results in Figure 8, using the Monte-Carlo method, suggest the following

Asymptotic Reducibility Conjecture Let $n \geq 2$ and $N \geq n$. Let $\mathcal{B}_n^{(N)}$ denote the set of the polynomials $f \in \mathcal{B}_n$ such that $\deg(f) \leq N$. Let $\mathcal{B}^{(N)} := \bigcup_{2 \leq n \leq N} \mathcal{B}_n^{(N)}$. The proportion of polynomials in $\mathcal{B} = \cup_{N \geq 2} \mathcal{B}^{(N)}$ which are irreducible is given by the limit, assumed to exist,

$$\lim_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N)}\}} \qquad \text{and its value is expected to be } \frac{3}{4}.$$

2 Quadrinomials ($s = 1$)

Since every $f \in \mathcal{B}$ is nonreciprocal and such that $f(1) \neq 0$, f is never divisible by the cyclotomic nonreciprocal polynomial $-1 + x$. When $f \in \mathcal{B}$ is a quadrinomial, the following Theorems provide all the possible factorizations of f.

Theorem 5 (Ljunggren) *If $f \in \mathcal{B}$, as*

$$f(x) = -1 + x + x^n + x^{m_1},$$

has no zeroes which are roots of unity, then $f(x)$ is irreducible. If $f(x)$ has exactly q such zeroes, then $f(x)$ can be decomposed into two rational factors, one of which is cyclotomic of degree q with all these roots of unity as zeroes, while the other is irreducible (and nonreciprocal).

Ljunggren's Theorem 5 is not completely correct. Mills corrected it (Theorem 8). Finch and Jones completed the results (Theorem 9).

Theorem 6 (Ljunggren) *If $f \in \mathcal{B}$, with $s = 1$, as*

$$f(x) = -1 + x + x^n + x^{m_1}$$

with $e_1 = \gcd(m_1, n-1), e_2 = \gcd(n, m_1 - 1)$, then all possible roots of unity of $f(x)$ are simple zeroes, which are to be found among the zeroes of

$$x^{e_1} = \pm 1, \qquad x^{e_2} = \pm 1, \qquad x = -1.$$

Theorem 7 (Ljunggren) *If $f \in \mathcal{B}$, as*

$$f(x) = -1 + x + x^n + x^{m_1},$$

is such that both n and m_1 are odd integers, then $f(x)$ is irreducible.

Theorem 8 (Mills) *Let $f \in \mathcal{B}$,*

$$f(x) = -1 + x + x^n + x^{m_1}$$

decomposed as $f(x) = A(x)B(x)$ where every root of $A(x)$ and no root of $B(x)$ is a root of unity. Then $A(x)$ is the greatest common divisor of $f(x)$ and $f^*(x) = x^{m_1} f(1/x)$, then reciprocal cyclotomic, and the second factor $B(x)$ is irreducible, then nonreciprocal, except when $f(x)$ has the following form:

$$-1 + x^r + x^{7r} + x^{8r} = (x^{2r} + 1)(x^{3r} + x^{2r} - 1)(x^{3r} - x^r + 1).$$

In the last case, the factors $x^{3r} + x^{2r} - 1$ and $x^{3r} - x^r + 1$ are (nonreciprocal) irreducible.

Theorem 9 (Finch - Jones) *Let $f \in \mathcal{B}$,*

$$f(x) = -1 + x + x^n + x^{m_1}.$$

Let $e_1 = \gcd(m_1, n-1), e_2 = \gcd(n, m_1 - 1)$. The quadrinomial $f(x)$ is irreducible over $\mathbb{Q}$ if and only if

$$m_1 \not\equiv 0 \pmod{2e_1}, \qquad n \not\equiv 0 \pmod{2e_2}.$$

3 Noncyclotomic reciprocal factors

In this paragraph we investigate the possible irreducible factors, in the factorization of a polynomial $f \in \mathcal{B}_n$, with n large enough, which vanish on the lenticular zeroes, or a subcollection of them. Examples are given in Section 4. In Proposition 1 it is proved that the degrees of the noncyclotomic reciprocal factors, *if they exist*, and therefore the degrees of such f, should be fairly large. Proposition 1 does not say that the degrees of the noncyclotomic reciprocal factors are large. For simplicity's sake the value c_n (defining the lenticulus of zeroes of f) is taken to be equal to $-\mathrm{Log}\,\kappa$.

Proposition 1 *If $f(x) := -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} \in \mathcal{B}_n$, $s \geq 1$, $n \geq 260$, admits a reciprocal noncyclotomic factor in its factorization which has a root of modulus $\geq 1 + (1-c)(-\frac{\mathrm{Log}\,\kappa}{n}) + c(\theta_n^{-1} - 1)$, for some $0 \leq c \leq 1$, then the number $s+3$ of its monomials satisfies:*

$$s + 3 \geq \left(1 + \frac{1}{n}\mathrm{Log}\,\frac{n^c}{\kappa^{(1-c)}}\right)^{n-1} + 1$$

and its degree has the following lower bound

$$m_s = \deg f \geq (\left(1 + \frac{1}{n}\mathrm{Log}\,\frac{n^c}{\kappa^{(1-c)}}\right)^{n-1} - 1)(n-1) + 1. \tag{6}$$

Proof The Perron number θ_n^{-1} is the dominant root of $-1+x+x^n$, and θ_{n-1}^{-1} of $-1+x+x^{n-1}$. Since $f \in \mathcal{B}_n$, $s \geq 1$, by Lemma 5.1 (ii) in [FLP] (cf Section 5.4), the dominant (positive real) zero of $f^*(x)$ lies in the interval $(\theta_n^{-1}, \theta_{n-1}^{-1})$. The (external) lenticulus of zeroes of f^* is defined as the image of that of f by $z \to 1/z$. The existence of $c \in [0,1]$ and a reciprocal noncylotomic factor vanishing at the zeroes of the subcollection of the lenticulus of f defined by c, implies that this reciprocal noncylotomic factor also vanishes at the zeroes of the lenticulus of f^*, external to the unit disk, in the same proportion.

Lemma 1 (Mignotte - Ştefănescu [MS]) *Let* $P(x) = x^q + a_{q-k}x^{q-k} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \setminus \mathbb{Z}$. *Then the moduli of the roots of* P *are bounded by*

$$(|a_0| + |a_1| + \ldots + |a_{q-k}|)^{1/k}. \tag{7}$$

The number of monomials in $f \in \mathcal{B}_n$, $n \geq 2$, is equal to $s+3$. Then the sum $|a_0| + |a_1| + \ldots + |a_{q-k}|$ of Proposition 1, applied to $P(x) = f(x)$ with $q = m_s$, is equal to $s+2$, and k is $\geq n-1$. If we assume that f contains an irreducible reciprocal noncyclotomic factor B having a root of modulus $\geq 1 + (1-c)(-\frac{\mathrm{Log}\,\kappa}{n}) + c(\theta_n^{-1} - 1)$, for some $0 \leq c \leq 1$ then we should have, by Lemma 1 and (4),

$$(s+2)^{1/k} \geq 1 + \frac{1}{n}(-\mathrm{Log}\,\kappa^{(1-c)} + c\,\mathrm{Log}\,n).$$

Therefore

$$\frac{1}{k}\mathrm{Log}\,(s+2) \geq \mathrm{Log}\left(1 + \frac{1}{n}\mathrm{Log}\,\frac{n^c}{\kappa^{(1-c)}}\right)$$

which implies

$$\mathrm{Log}\,(s+2) \geq \mathrm{Log}\left(\left(1 + \frac{1}{n}\mathrm{Log}\,\frac{n^c}{\kappa^{(1-c)}}\right)^{n-1}\right)$$

and the result. Moreover

$$\begin{aligned} m_s &= (m_s - m_{s-1}) + (m_{s-1} - m_{s-2}) + \ldots + (m_2 - m_1) + (m_1 - n) + (n-1) + 1 \\ &\geq (s+1)(n-1) + 1, \end{aligned}$$

from which (6) is deduced.

Example: let $f \in \mathcal{B}_n$, with $n = 400$, for which it is assumed that there exists a reciprocal noncyclotomic factor of f vanishing on the subcollection of roots of the lenticulus of f given by $c = 0.95$. Then, by (6), the degree m_s of f should be above 121 786.

The case where the summit (real > 1) of the lenticulus of zeroes of f^* is a zero of a reciprocal noncyclotomic factor of f never occurs by the following Proposition.

Proposition 2 *If* $f(x) := -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} \in \mathcal{B}_n$, $s \geq 1$, $n \geq 3$, *is factorized as* $f(x) = A(x)B(x)C(x)$ *as in Theorem 3, then the unique positive real root of* $f(x)$ *is a root of the nonreciprocal part* $C(x)$.

Proof By Descartes's rule the number of positive real roots of f should be less than the number of sign changes in the sequence of coefficients of the polynomials f. The number of sign changes in f is 1. If say $1/\beta$ is the unique root of f in $(0,1)$, and assumed to be a root of a factor of B then β and $1/\beta \neq \beta$ would be two real roots of f, what is impossible.

4 Lenticuli of zeroes: an example with $s = 12$, and various pentanomials (with $s = 2$)

In this paragraph let us examplify the fact that the roots of any

$$f(x) := -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s}$$

where $s \geq 1$, $m_1 - n \geq n-1$, $m_{q+1} - m_q \geq n-1$ for $1 \leq q < s, n \geq 3$, are separated into two parts, those which lie in a narrow annular neighbourhood of the unit circle, and those forming a lenticulus of roots ω inside an angular sector $-\gamma < \arg\omega < \gamma$ with γ say $< +\pi/3$ off the unit circle. This dichotomy phenomenon becomes particularly visible when n and s are large. This lenticulus is shown to be a deformation of the lenticulus determined by the trinomial $-1 + x + x^n$ made of the first three terms of f; the lenticulus of zeroes of $-1 + x + x^n$ is constituted by the zeroes of real part $> 1/2$, equivalently which lie in the angular sector $-\pi/3 < \arg(z) < \pi/3$, symmetrically with respect to the real axis, for which the number of roots is equal to $1 + 2\lfloor n/6 \rfloor$ ([VG2] Prop. 3.7).

The value of γ is taken equal to $\pi/18$ as soon as n is large enough, due to the structure of the asymptotic expansions of the roots of G_n [VG2], so that the number of roots of the lenticulus of roots of f can be asymptotically defined by the formula

$$1 + \lfloor \frac{1}{3} \lfloor \frac{n}{6} \rfloor \rfloor \quad \pm 1. \tag{8}$$

At small values of n, the value of $\gamma = \pi/18$ is also kept as a critical threshold to estimate the number of elements in the lenticulus of roots of f by (8). It can be shown [VG3] that the lenticulus of roots of f is a set of zeroes of the nonreciprocal irreducible factor in the factorization of f. Even though it seems reasonable to expect many roots of f on the unit circle, it is not the case: all the roots α of the nonreciprocal irreducible component of $f(x)$ are never on the unit circle: $|\alpha| \neq 1$, as proved in Proposition 5.

(i) Example of a polynomial in $\mathcal{B}_{37}$ with $s = 12$: let

$$f(x) := -1 + x + x^{37} + x^{81} + x^{140} + x^{184} + x^{232} + x^{285} + x^{350} + x^{389} + x^{450} + x^{514} + x^{550}$$
$$+ x^{590} + x^{649} = G_{37}(x) + x^{81} + \ldots + x^{649}. \tag{9}$$

The zeroes are represented in Figure 1b, those of $G_{37}(x) = -1 + x + x^{37}$ in Figure 1a. The polynomial f is irreducible. The zeroes of $f(x)$ are either lenticular or lie very close to the unit circle. The lenticulus of zeroes of f

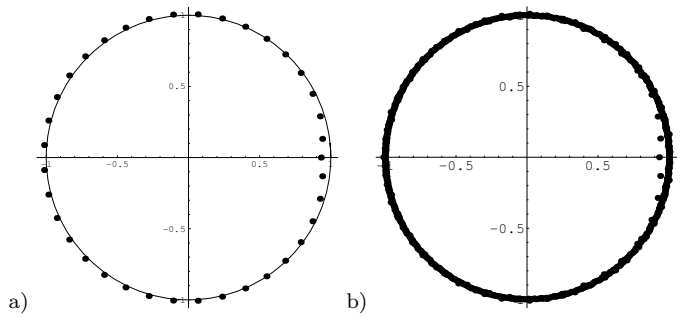

Fig. 1 a) The 37 zeroes of $G_{37}(x) = -1 + x + x^{37}$, b) The 649 zeroes of $f(x) = G_{37}(x) + \ldots + x^{649}$ given by (9). The lenticulus of roots of f (having 3 simple zeroes) is obtained by a very slight deformation of the restriction of the lenticulus of roots of G_{37} to the angular sector $|\arg z| < \pi/18$, off the unit circle. The other roots (nonlenticular) of f can be found in a narrow annular neighbourhood of $|z| = 1$.

contains 3 zeroes, compared to 13 for the cardinal of the lenticulus of zeroes of the trinomial $-1 + x + x^{37}$. It is obtained by a slight deformation of the restriction of the lenticulus of zeroes of $-1 + x + x^{37}$ to the angular sector $|\arg z| < \pi/18$.

(ii) Examples of pentanomials ($s = 2$) The examples show different factorizations of polynomials $f \in \mathcal{B}_n$ for various values of n, having a small number of roots in their lenticulus of roots; in many examples the number of factors is small (one, two or three). The last examples exhibit polynomials $f \in \mathcal{B}$ having a larger number of zeroes in the lenticuli of roots (5, 7 and 27). Denser lenticuli of roots (for $n \geq 1000$ for instance) are difficult to visualize on a Figure for the reason that the lenticuli of roots are extremely close to the unit circle, and *apparently* become embedded in the annular neighbourhood of the nonlenticular roots.

(1) Dynamical degree $n = 5$: let $f(x) = -1 + x + x^5 + x^9 + x^{15}$. It is reducible and its factorization admits only one irreducible cyclotomic factor, the second factor being irreducible nonreciprocal:

$$f(x) = (1 + x + x^2)(-1 + 2x - x^2 - x^3 + 2x^4 - 2x^6 + 2x^7 - x^9 + x^{10} - x^{12} + x^{13}).$$

Let $f(x) = -1 + x + x^5 + x^9 + x^{18}$. In the factorization of f two irreducible cyclotomic factors appear and where the third factor is irreducible and nonreciprocal:

$$f(x) = (1 - x + x^2)(1 + x + x^2)(-1 + x + x^2 - x^3 + x^5 - x^6 + x^8 - x^{12} + x^{14}).$$

In both cases, the lenticulus of zeroes of $f(x)$ is the lenticulus of its nonreciprocal factor. It is reduced to the unique real positive zero of f: $0.7284\ldots$, resp. $0.7301\ldots$, close to real positive zero $0.7548\ldots$ of G_5 which is the only element of the lenticulus of roots of G_5.

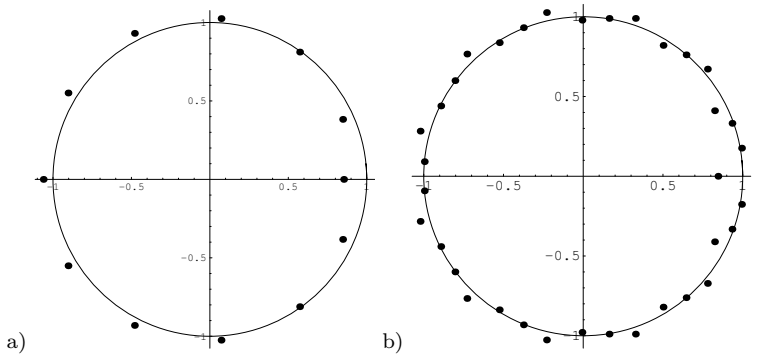

Fig. 2 a) The 12 zeroes of G_{12}, b) The 35 simple zeroes of $f(x) = -1+x+x^{12}+x^{23}+x^{35}$. By definition, only one root is lenticular, the one on the real axis, though the "complete" lenticulus of roots of $-1+x+x^{12}$, slightly deformed, can be guessed.

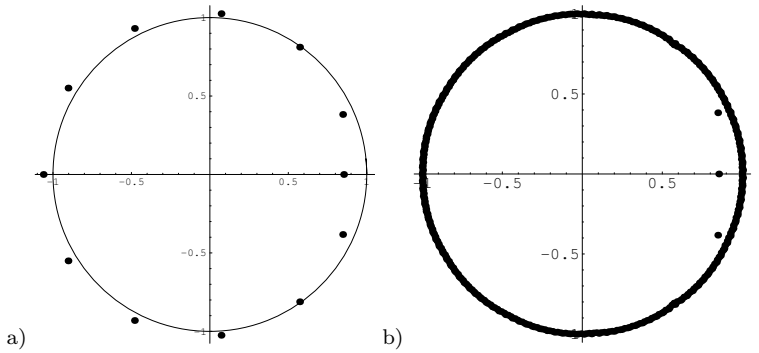

Fig. 3 a) The 12 zeroes of G_{12}, b) The 385 zeroes of $f(x) = -1+x+x^{12}+x^{250}+x^{385}$. The lenticulus of roots of the trinomial $-1+x+x^{12}$ can be guessed, slightly deformed and almost "complete". It is well separated from the other roots, and off the unit circle. Only one root of f is considered as a lenticular zero, the one on the real axis: $0.8525\ldots$. The thickness of the annular neighbourhood of $|z| = 1$ which contains the nonlenticular zeroes of f is much smaller than in Figure 2b.

(3) Dynamical degree $n = 12$: the lenticulus of zeroes of G_{12} is shown in Figure 2a and Figure 3a. It contains 5 zeroes. Let $f(x) = -1+x+x^{12}+x^{23}+x^{35}$, resp. $f(x) = -1+x+x^{12}+x^{250}+x^{385}$. Both polynomials are irreducible. In both cases the lenticulus of zeroes of $f(x)$ (Figure 2b, Figure 3b) only contains one point, the real root $0.8447\ldots$, resp. $0.8525\ldots$, close to the real positive zero $0.852551\ldots$ of G_{12}: the lenticulus of f is a slight deformation of the restriction of the lenticulus of G_{12} to the angular sector $|\arg z| < \pi/18$. Comparing Figure 2b and Figure 3b, the higher degree of f, 385 instead of 35, has two consequences: i) the densification of the annular neighbourhood of $|z| = 1$ by the zeroes of f, 2) the decrease of the thickness of the annular neighbourhood containing the nonlenticular roots of f. This phenomenon is general (cf Section 5.3).

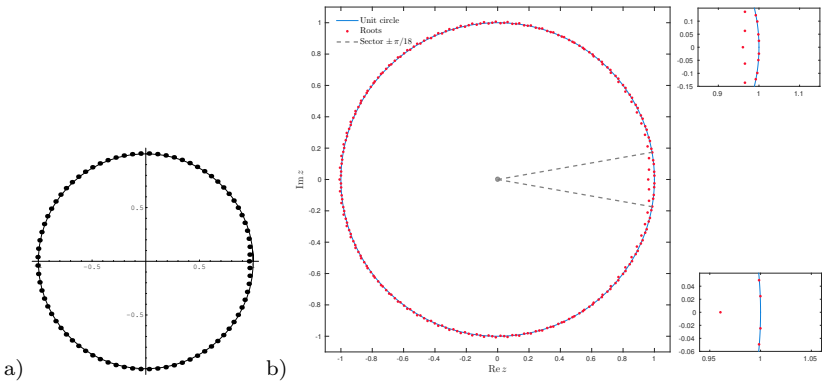

Fig. 4 a) Zeroes of G_{81}, b) Zeroes of $f(x) = -1+x+x^{81}+x^{165}+x^{250}$. On the right the distribution of the roots of f is zoomed twice in the angular sector $-\pi/18 < \arg(z) < \pi/18$. The number of lenticular roots of f is equal to 5.

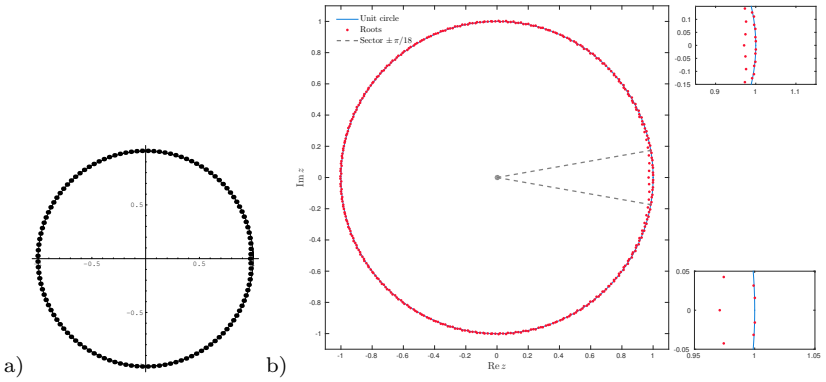

Fig. 5 a) Zeroes of G_{121}, b) Zeroes of $f(x) = -1+x+x^{121}+x^{250}+x^{385}$. On the right the distribution of the roots of f is zoomed twice in the angular sector $-\pi/18 < \arg(z) < \pi/18$. The lenticulus of roots of f has 7 zeroes.

(6) Dynamical degree $n = 81$: let

$$f(x) = -1+x+x^{81}+x^{165}+x^{250}.$$

It is irreducible. The lenticulus of zeroes of $-1+x+x^{81}$ contains 27 points (Figure 4a) , while that of $f(x)$ (Figure 4b) contains 5 points, in particular the real root 0.9604…, close to the real positive root 0.9608… of G_{81}.

(7) Dynamical degree $n = 121$: let

$$f(x) = -1+x+x^{121}+x^{250}+x^{385}.$$

It is irreducible. The lenticulus of zeroes of $-1+x+x^{121}$ contains 41 points (Figure 5a) , whereas the lenticulus of roots of $f(x)$ (Figure 5b) contains 7 points, in particular the real root 0.9709…, close to the real positive root 0.971128… of G_{121}.

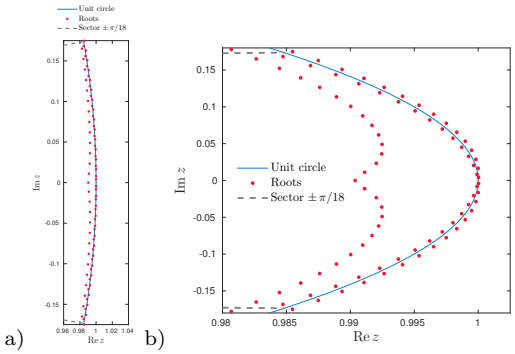

Fig. 6 The representation of the 27 zeroes of the lenticulus of $f(x) = -1 + x + x^{481} + x^{985} + x^{1502}$ in the angular sector $-\pi/18 < \arg z < \pi/18$ in two different scalings in x and y (in a) and b)). In this angular sector the other zeroes of f can be found in a thin annular neighbourhood of the unit circle. The real root $1/\beta > 0$ of f is such that β satisfies: $1.00970357\ldots = \theta_{481}^{-1} < \beta = 1.0097168\ldots < \theta_{480}^{-1} = 1.0097202\ldots$.

5 Factorization of the lacunary polynomials of the class $\mathcal{B}$

In a series of papers Schinzel [S] [S2] [S3] [S4] has studied the reducibility of lacunary polynomials, their possible factorizations, the asymptotics of their numbers of irreducible factors, reciprocal, nonreciprocal, counted with multiplicities or not, for large degrees. Dobrowolsky [D] has also contributed in this domain in view of understanding the problem of Lehmer. First let us deduce the following Theorem on the class $\mathcal{B}$, from Schinzel's Theorems.

Theorem 10 *Suppose $f(x) \in \mathcal{B}$ of the form*

$$-1 + x + x^n + x^{m_1} + \ldots + x^{m_s}, \quad n \geq 2,\ s \geq 1.$$

Then the number $\omega(f)$, resp. $\omega_1(f)$, of irreducible factors, resp. of irreducible noncyclotomic factors, of $f(x)$ counted without multiplicities in both cases, satisfy

(i)

$$\omega(f) \ll \sqrt{\frac{m_s \operatorname{Log}(s+3)}{\operatorname{Log}\operatorname{Log} m_s}} \qquad (m_s \to \infty),$$

(ii) for every $\epsilon \in (0,1)$,

$$\omega_1(f) = o(m_s^{\epsilon})\,(\operatorname{Log}(s+3))^{1-\epsilon}, \qquad (m_s \to \infty).$$

Proof Theorem 1 and Theorem 2, with the "Note added in proof" p. 319, in Schinzel [S4].

5.1 Cyclotomic parts

Let us first mention some results on the existence of cyclotomic factors in the factorization of the polynomials of the class $\mathcal{B}$. Then, in Proposition 4, we prove the existence of infinitely many polynomials $f \in \mathcal{B}$ which are divisible by a given cyclotomic polynomial Φ_p, for every prime number $p \geq 3$.

Lemma 2 *Suppose $f(x) \in \mathcal{B}$ of the form*

$$-1+x+x^n+x^{m_1}+\ldots+x^{m_s}, \quad n \geq 2,\ s \geq 1,$$

and divisible by a cyclotomic polynomial. Then there is an integer $m = p_1^{q_1} \ldots p_r^{q_r}$ having all its prime factors $p_i \leq s+3$ such that $\Phi_m(x)$ divides $f(x)$.

Proof Lemma 3.2 in [FFN].

The divisibility of $f \in \mathcal{B}$ by cyclotomic polynomials $\Phi_p(x)$, where p are prime numbers, implies conditions on those p's by Proposition 3.

Lemma 3 (Boyd) *Let p be a prime number. Suppose $f(x) \in \mathcal{B}$ of the form*

$$\sum_{j=0}^{m_s} a_j x^j = -1+x+x^n+x^{m_1}+\ldots+x^{m_s}, \quad n \geq 2,\ s \geq 1.$$

Denote $c_i = \sum_{k \equiv i(p)} a_k$. Then

$$\Phi_p(x) | f(x) \iff c_0 = c_1 = \ldots = c_{p-1}.$$

Proof $\Phi_p(x)$ divides $f(x)$ if and only if (X^p-1) divides $(X-1)f(x)$.

Proposition 3 *Suppose $f(x) \in \mathcal{B}$ of the form*

$$f(x) = \sum_{j=0}^{m_s} a_j x^j = -1+x+x^n+x^{m_1}+\ldots+x^{m_s}, \quad n \geq 2,\ s \geq 1,$$

and that $\Phi_p(x) | f(x)$ for some prime number p. Then

$$p \mid (s+1).$$

Proof Using Lemma 3, since $f(1) = s+1 = \sum_k a_k = \sum_{i=0}^{p-1} \sum_{k \equiv i(p)} a_k = p \cdot c_0$, we deduce the claim.

A necessary condition for $f(x)$ to be divisible by $\Phi_p(x)$ is that s should be congruent to -1 modulo p.

Proposition 4 *Let $p \geq 3$ be a prime number. Let $n \geq 2$. There exist infinitely many $f \in \mathcal{B}_n$ such that*

$$\Phi_p(x) | f(x).$$

Proof Let ζ_p denote the primitive root of unity $e^{2i\pi/p}$. Let us assume that $f(x) \in \mathcal{B}_n$ vanishes at ζ_p, as

$$f(\zeta_p) = -1 + \zeta_p + \zeta_p^n + \zeta_p^{m_1} + \ldots + \zeta_p^{m_s} = 0.$$

We consider the residues modulo p of the $(s+1)$-tuple $(n, m_1, m_2, \ldots, m_s)$ so that $f(\zeta_p)$ can be written

$$f(\zeta_p) = c_0 + c_1\zeta_p + c_2\zeta_p^2 + \ldots c_{p-1}\zeta_p^{p-1} = 0, \quad c_0, c_1, \ldots, c_{p-1} \text{ integers.}$$

The polynomial $\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1} = (X^p - 1)/(X - 1)$ is the minimal polynomial of ζ_p. Then, if c_0 or c_{p-1} is equal to 0, then all the coefficients c_i should be equal to 0 since $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ is a free system over $\mathbb{Z}$. If $c_0 c_{p-1} \neq 0$ then the equalities

$$c_0 = c_1 = c_2 = \ldots = c_{p-1} \quad (\neq 0)$$

should hold since the polynomial $\sum_{j=0}^{p-1} c_j X^j$ vanishes at ζ_p and is of the same degree as $\Phi_p(X)$. The common value can be arbitrarily large. In both cases we have the condition

$$c_0 = c_1 = c_2 = \ldots = c_{p-1}.$$

It means that the distribution of the exponents $n, m_1, m_2, \ldots, m_s$ by class of congruence modulo p should be identical in each class.

Then, if $p \leq n$, the constant term -1 "belongs to" the class "$\equiv 0 \bmod p$", and ζ_p to the class "$\equiv 1 \bmod p$". The term ζ_p^n may belong to another class "$\equiv i \bmod p$" with $i \neq 0, 1$ or to one of the classes "$\equiv 0 \bmod p$" or "$\equiv 1 \bmod p$". If $p > n$ then the term ζ_p^n belongs to another class "$\equiv i \bmod p$" with $i \neq 0, 1$. In both cases we can complete the classes by suitably adding terms "$\zeta_p^{m_i}$". We now chose $s \geq 1$ and m_1, $m_2, \ldots, m_s$ sequentially such that the distribution of the residues modulo p

$$m_1 \bmod p, \; m_2 \bmod p, \; \ldots, \; m_s \bmod p$$

in the respective classes "$\equiv i \bmod p$", with $i = 0, 1, \ldots, p-1$, is equal.

If one solution $(m_1, \ldots, m_s)$ is found, then $\Phi_p(X)$ divides $f(X)$. Another solution $f' \in \mathcal{B}_n$ is now found with $s' = s + p$ and a suitable choice of the exponents $m_{s+1}, \ldots, m_{s+p}$

$$f'(x) = -1 + x + x^n + x^{m_1} + \ldots + x^{m_s} + x^{m_{s+1}} + \ldots x^{m_{s+p}}$$

so that

$$f'(\zeta_p) = c'_0 + c'_1\zeta_p + \ldots + c'_{p-1}\zeta_p^{p-1}$$

where the p residues modulo p of $m_{s+1}, \ldots, m_{s+p}$ are all distinct, satisfying

$$c'_0 = c'_1 = \ldots = c'_{p-1} = c_0 + 1.$$

Then $\Phi_p(X)$ also divides $f'(X)$. Iterating this process we deduce the claim.

5.2 Nonreciprocal parts

Proposition 5 *If $P(z) \in \mathbb{Z}[z]$, $P(1) \neq 0$, is nonreciprocal and irreducible, then $P(z)$ has no root of modulus* 1.

Proof Let $P(z) = a_d z^d + \ldots + a_1 z + a_0$, $a_0 a_d \neq 0$, be irreducible and nonreciprocal. We have $\gcd(a_0, \ldots, a_d) = 1$. If $P(\zeta) = 0$ for some ζ, $|\zeta| = 1$, then $P(\overline{\zeta}) = 0$. But $\overline{\zeta} = 1/\zeta$ and then $P(z)$ would vanish at $1/\zeta$. Hence P would be a multiple of the minimal polynomial P^* of $1/\zeta$. Since $\deg(P) = \deg(P^*)$ there exists $\lambda \neq 0, \lambda \in \mathbb{Q}$, such that $P = \lambda P^*$. In particular, looking at the dominant and constant terms, $a_0 = \lambda a_d$ and $a_d = \lambda a_0$. Hence, $a_0 = \lambda^2 a_0$, implying $\lambda = \pm 1$. Therefore $P^* = \pm P$. Since P is assumed nonreciprocal, $P^* \neq P$, implying $P^* = -P$. Since $P^*(1) = P(1) = -P(1)$, we would have $P(1) = 0$. Contradiction.

For studying the irreducibility of the nonreciprocal parts of the polynomials $f \in \mathcal{B}$, we will follow the method introduced by Ljunggren [L], used by Schinzel [S][S2] and Filaseta [F].

Lemma 4 (Ljunggren) *Let $P(x) \in \mathbb{Z}[x]$, $\deg(P) \geq 2$, $P(0) \neq 0$. The nonreciprocal part of $P(x)$ is reducible if and only if there exists $w(x) \in \mathbb{Z}[x]$ different from $\pm P(x)$ and $\pm P^*(x)$ such that $w(x)\, w^*(x) = P(x)\, P^*(x)$.*

Proof Let us assume that the nonreciprocal part of $P(x)$ is reducible. Then there exists two nonreciprocal polynomials $u(x)$ and $v(x)$ such that $P(x) = u(x)v(x)$. Let $w(x) = u(x)v^*(x)$. We have:

$$w(x)\, w^*(x) = u(x)v^*(x)u^*(x)v(x) = P(x)\, P^*(x).$$

Conversely, let us assume that the nonreciprocal part $c(x)$ of $P(x)$ is irreducible and that there exists $w(x)$ different of $\pm P(x)$ and $\pm P^*(x)$ such that $w(x)\, w^*(x) = P(x)\, P^*(x)$. Let $P(x) = a(x)c(x)$ be the factorization of P where every irreducible factor in a is reciprocal. Then

$$P(x)\, P^*(x) = a^2(x)\, c(x)\, c^*(x) = w(x)\, w^*(x).$$

We deduce $w(x) = \pm\, a(x)\, c(x) = \pm\, P(x)$ or $w(x) = \pm\, a(x)\, c^*(x) = \pm\, P^*(x)$. Contradiction.

Proposition 6 *For any $f \in \mathcal{B}_n$, $n \geq 3$, denote by*

$$f(x) = A(x)B(x)C(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

where $s \geq 1$, $m_1 - n \geq n - 1$, $m_{j+1} - m_j \geq n - 1$ for $1 \leq j < s$, the factorization of f where A is the cyclotomic component, B the reciprocal noncyclotomic component, C the nonreciprocal part. Then C is irreducible.

Proof Let us assume that C is reducible, and apply Lemma 4. Then there should exist $w(x)$ different of $\pm f(x)$ and $\pm f^*(x)$ such that $w(x)\,w^*(x) = f(x)\,f^*(x)$. For short, we write

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j} \qquad \text{and} \quad w(x) = \sum_{j=0}^{q} b_j x^{k_j}$$

where the coefficients a_j and the exponents d_j are given, and the b_j's and the k_j's are unkown integers, with $|b_j| \geq 1$, $0 \leq j \leq q$,

$$a_0 = -1,\ a_1 = a_2 = \ldots = a_r = 1,$$

$$0 = d_0 < d_1 = 1 < d_2 = n < d_3 = m_1 < \ldots < d_{r-1} = m_{s-1} < d_r = m_s,$$

$$0 = k_0 < k_1 < k_2 < \ldots < k_{q-1} < k_q.$$

The relation $w(x)\,w^*(x) = f(x)\,f^*(x)$ implies the equality: $2k_q = 2d_r$; expanding it and considering the terms of degree $k_q = d_r$, we deduce $\|f\|^2 = \|w\|^2 = r+1$ which is equal to $s+3$. Since $f^*(1) = f(1)$ and that $w^*(1) = w(1)$, it also implies $f(1)^2 = w(1)^2$ and $b_0 b_q = -1$. Then we have two equations

$$r-1 = \sum_{j=1}^{q-1} b_j^2, \qquad\qquad (r-1)^2 = (\sum_{j=1}^{q-1} b_j)^2.$$

We will show that they admit no solution except the solution $w(x) = \pm f(x)$ or $= \pm f^*(x)$.

Since all $|b_j|$'s are ≥ 1, the inequality $q \leq r$ necessarily holds. If $q = r$, then the b_j's should all be equal to -1 or $+1$, what corresponds to $\pm f(x)$ or to $\pm f^*(x)$. If $2 \leq q < r$, the maximal value taken by a coefficient b_j^2 is equal to the largest square less than or equal to $r-q+1$, so that $|b_j| \leq \sqrt{r-q+1}$. Therefore there is no solution for the cases "$q = r-1$" and "$q = r-2$". If $q = r-3$ all b_j^2's are equal to 1 except one equal to 4, and

$$r-1 = \sum_{j=1}^{r-4} b_j^2, \qquad\qquad (r-1)^2 > (\sum_{j=1}^{r-4} b_j)^2.$$

This means that the case "$q = r-3$" is impossible. The two cases "$q = r-4$" and "$q = r-5$" are impossible since, for $m = 5$ and 6, $\sum_{j=1}^{r-m} b_j^2$ cannot be equal to $r-1$. This is general. For $q \leq r-3$ at least one of the $|b_j|$'s is equal to 2; in this case we would have

$$r-1 = \pm \sum_{j=1}^{q-1} b_j \leq \sum_{j=1}^{q-1} |b_j| < \sum_{j=1}^{q-1} b_j^2 = r-1.$$

Contradiction.

5.3 Thickness of the annular neighbourhoods of $|z|=1$ containing the nonlenticular roots

Let $n \geq 3$, and δ_n be a real number >0, smaller than 1. Let

$$\mathcal{D}_{n,\delta_n} := \{z \mid |z|<1, \delta_n < |G_n(z)|\}.$$

We now characterize the geometry of the zeroes, in $\mathcal{D}_{n,\delta_n}$, of a given

$$f(x) := -1+x+x^n+x^{m_1}+x^{m_2}+\ldots+x^{m_s} \quad \in \mathcal{B}_n$$

where $s>0$, $m_1-n \geq n-1$, $m_{q+1}-m_q \geq n-1$ for $1 \leq q < s$. Obviously a zero $x \in \mathcal{D}_{n,\delta_n}$ of f is $\neq 0$ and is not a zero of the trinomial $-1+x+x^n$. Moreover

$$\delta_n < |-1+x+x^n| = |x^{m_1}+x^{m_2}+\ldots+x^{m_s}| < |x|^{m_1}+|x|^{m_2}+\ldots+|x|^{m_s}. \quad (10)$$

This inequality implies that $1-|x|$ is necessarily small. Indeed the function $Y : u \to \sum_{j=1}^{s} u^{m_j}$ is increasing, with increasing derivative, on $(0,1]$, so that the unique real value $0<r<1$ which satisfies $Y(r)=\delta_n$ admits the upper bound $e_{sup}<1$ given by $s-\delta_n = Y'(1)(1-e_{sup}) = (\sum_{j=1}^{s} m_j)(1-e_{sup})$; so that

$$r < e_{sup} = 1 - \frac{s-\delta_n}{\sum_{j=1}^{s} m_j}.$$

Let us now give a lower bound e_{inf} of r, as a function of n, s, δ_n and m_s. If $s=1$, using $m_1 \geq n+(n-1)$, the inequality $\delta_n \leq |x|^{m_1} \leq |x|^{2n-1}$ implies:

$$e_{inf} = \delta_n^{1/(2n-1)} \leq r.$$

As soon as the assumption $\limsup_{n\to\infty}(\operatorname{Log}\delta_n)/n = 0$ is satisfied, then e_{inf} tends to 1 as n tends to infinity. This assumption means that the domain $\mathcal{D}_{n,\delta_n}$ should avoid small disks centered at the lenticular roots of G_n.

If $s \geq 2$, using the inequalities $m_{q+1}-m_q \geq n-1$, $1 \leq q < s$, we deduce, from (10),

$$\delta_n < |x|^{m_1}+|x|^{m_2}+\ldots+|x|^{m_s} \leq |x|^{2n-1}\Big(\frac{1-|x|^{(n-1)(s-1)}}{1-|x|^{n-1}}\Big)+|x|^{m_s}.$$

Putting $H=|x|^{n-1}$, we are now bound to solve the following equation in H

$$\delta_n = H^2\Big(\frac{1-H^{s-1}}{1-H}\Big)+H^{m_s-1}$$

to find e_{inf}, for $H<1$ close to one, of the form $1-\epsilon$. It is easy to check that the expression of ϵ, at the first-order, is

$$\epsilon \;=\; 2\frac{ns-\delta_n n+\delta_n-s}{ns^2+ns-s^2+2m_s-2n-s},$$

leading to

$$e_{inf} = \left(1-2\frac{ns-\delta_n n+\delta_n-s}{ns^2+ns-s^2+2m_s-2n-s}\right)^{1/(n-1)}$$

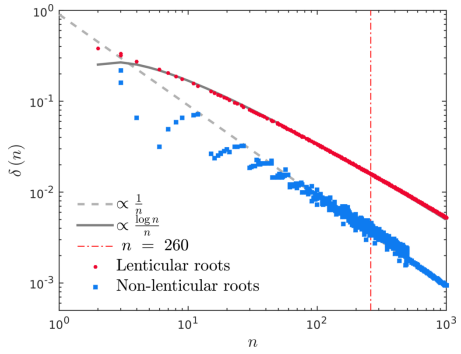

Fig. 7 Thickness $\delta(n)$, proportional to $1/n$ at the first-order, of the annular neighbourhood of the unit circle which contains the nonlenticular roots (of modulus < 1), represented as a function of the dynamical degree n, for the almost Newman polynomials f of the class $\mathcal{B}$. The curve "lenticular roots" represents the distance between 1 and the positive real zero (summit) of the lenticulus of $f \in \mathcal{B}$; this distance is $\mathrm{Log}\, n/n$ at the first-order. The method of random picking in $\mathcal{B}_n$ is used, for n less than 1000.

For n, δ_n and s fixed, the function $m_s \to \epsilon$ is decreasing and then $m_s \to e_{inf}$ is increasing. This means that the thickness of the annular neighbourhood of $|z| = 1$ containing the nonlenticular roots of f diminishes as the degree m_s of f tends to infinity, for a fixed number of monomials $s+3$ and a fixed dynamical degree n.

Therefore all the zeroes of f which lie in $\mathcal{D}_{n,\delta_n}$ belong to

$$\{z \mid e_{inf} < z < 1\}.$$

An example of dependency of e_{inf} with m_s is given by Figure 2 b) and Figure 3 b): for fixed $n = 12$ and $s = 5$, and varying m_s from 35 to 385.

5.4 Proof of Theorem 3

(i) By Proposition 2 the nonreciprocal part C is nontrivial. By Proposition 6 the nonreciprocal part C is irreducible. By Proposition 5 the irreducible factor C never vanishes on the unit circle.
(ii) For $n \geq 3$ the Rényi β-expansion of 1 in base $\theta_n^{-1} > 1$ is the sequence of digits of the coefficient vector of $G_n(x)+1$ (Lothaire [Lo], Chap. 7); the digits lie in the alphabet $\{0,1\}$. We have

$$d_{\theta_n^{-1}}(1) = 0.10^{n-2}1.$$

Similarly $d_{\theta_{n-1}^{-1}}(1) = 0.10^{n-3}1$, where the sequence of digits comes from the coefficient vector of $G_{n-1}(x)+1$. Let $\beta > 1$ denote the real algebraic integer such that the Rényi β-expansion of 1 in base β is exactly the sequence of digits of the coefficient vector of $f(x)+1$. We have:

$$d_\beta(1) = 0.10^{n-2}10^{m_1-n-1}10^{m_2-m_1-1}1 \ldots 10^{m_s-m_{s-1}-1}1.$$

Since the two following lexicographical conditions are satisfied:

$$d_{\theta_n^{-1}}(1) = 0.10^{n-2}1 \preccurlyeq_{lex} d_\beta(1) \preccurlyeq_{lex} d_{\theta_{n-1}^{-1}}(1) = 0.10^{n-3}1$$

Lemma 5.1 (ii) in Flatto, Lagarias and Poonen [FLP] implies:

$$\theta_n^{-1} < \beta < \theta_{n-1}^{-1} \quad \Longleftrightarrow \quad \theta_{n-1} < 1/\beta < \theta_n.$$

Since $-C^*$ is nontrivial, monic, irreducible, nonreciprocal, and vanishes at β, it is the minimal polynomial of β, and β is nonreciprocal.

6 Heuristics on the irreducibility of the polynomials of $\mathcal{B}$

The Monte-Carlo method is used for testing the Odlyzko Poonen Conjecture ("OP Conjecture") on the Newman polynomials, the variant Conjecture ("variant OP Conjecture") on the almost Newman polynomials and for estimating the proportion of irreducible polynomials in the class $\mathcal{B}$. The Conjectures "OP" and "variant OP" state that the proportion of irreducible polynomials in the class of Newman polynomials, resp. almost Newman polynomials, is one. This value of one is reasonable in the context of the general Conjectures on random polynomials [BBBSWW].

The probability of $f \in \mathcal{B}$ to be an irreducible polynomial can be defined asymptotically as follows. Let $s \geq 1, n \geq 2$ and $N \geq n$. Let $\mathcal{B}_n^{(N,s)}$ denote the set of the polynomials $f \in \mathcal{B}_n$ having $s+3$ monomials such that $\deg(f) \leq N$. Denote

$$\mathcal{B}^{(N,s)} := \bigcup_{2 \leq n \leq N} \mathcal{B}_n^{(N,s)}, \qquad \mathcal{B}^{(N)} := \bigcup_{s \geq 1} \mathcal{B}^{(N,s)}.$$

Then $\mathcal{B} = \cup_{N \geq 2} \mathcal{B}^{(N)}$. For $s \geq 1$, let $\mathcal{B}^{[s]} = \cup_{N \geq 2} \mathcal{B}^{(N,s)}$. For every $s \geq 1$ though the two adherence values

$$\liminf_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N,s)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N,s)}\}} \leq \limsup_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N,s)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N,s)}\}}, \tag{11}$$

exist, and, in a similar way,

$$\liminf_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N)}\}} \leq \limsup_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N)}\}}, \tag{12}$$

exist, without being a priori equal, we find that, for $s = 1$ and $s = 2$, and for arbitrary values of $s \geq 1$, there is a numerical evidence that the limits exist in both (11) and (12) (i.e. $\liminf = \limsup$). Table 1 reports the proportion of irreducible quadrinomials ($s = 1$), resp. irreducible pentanomials ($s = 2$), in the class $\mathcal{B}$, with the 90%-confidence interval under the assumption that the limit exists in each case. We find that the proportion of irreducible polynomials in $\mathcal{B}$ is

$$\lim_{N \to \infty} \frac{\#\{f \in \mathcal{B}^{(N)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(N)}\}} = 0.756 \pm 0.02235.$$

Table 1 Asymptotic proportion of irreducible polynomials in various classes: Newman polynomials, almost Newman polynomials, $\mathcal{B}$ and the subclasses $\mathcal{B}^{[0]}$, $\mathcal{B}^{[1]}$, $\mathcal{B}^{[2]}$ of $\mathcal{B}$ (Maximal polynomial degree: 3000, number of Monte-Carlo runs: 4000)

polynomials (class)	proportion	90%-confidence interval (estimated)	expected
OP (Newman)	0.967	0.00930	1 (Conjectured)
variant OP (almost Newman)	0.968	0.00916	1 (Conjectured)
class $\mathcal{B}$	0.756	0.02235	3/4 (Conjectured)
trinomials (s=0)	$5/6 = 0.833\ldots$	-	5/6 exact (Selmer)
quadrinomials (s=1)	0.575	0.02573	unkown
pentanomials (s=2)	0.826	0.01601	unkwon

This value justifies the statement of the Asymptotic Reducibility Conjecture. The reason of this residual reducibility finds its origin in Proposition 4 where cyclotomic polynomials are asymptotically present in the factorizations, though the authors have no proof of it. By Monte-Carlo methods, polynomials of degrees N up to 3000 are tested (Figure 8), and the number of monomials $s+3$ in each $f \in \mathcal{B}_n^{(N)}$ is random in the range of values of s.

In the case "$s=0$", $\cup_{n\geq 2}\mathcal{B}^{(N=n,s=0)}$ denotes the set of trinomials of the type $-1+x+x^n$, $n \geq 2$, whose factorization was studied by Selmer [Sr]; the proportion of irreducible trinomials is exact:

$$\lim_{n\to\infty} \frac{\#\{f \in \mathcal{B}^{(n,s=0)} \mid f \text{ irreducible}\}}{\#\{f \in \mathcal{B}^{(n,s=0)}\}} \;=\; 5/6 = 0.833\ldots \tag{13}$$

7 Lenticular roots on continuous curves steming from $z=1$ and boundary of Solomyak's fractal

In this paragraph we first recall the constructions of Solomyak [Sk] on the sets of zeroes of the family $\mathcal{W}$ of power series having real coefficients in the interval $[0,1]$, in the interior of the unit disk, and Solomyak's Theorem 11. Then we will recall how the polynomials of the class $\mathcal{B}$ are related to elements of $\mathcal{W}$.

Let

$$\mathcal{W} := \{h(z) = 1 + \sum_{j=1}^{\infty} a_j z^j \mid a_j \in [0,1]\}$$

be the class of power series defined on $|z|<1$ equipped with the topology of uniform convergence on compacts sets of $|z|<1$. The subclass $\mathcal{W}_{0,1}$ of $\mathcal{W}$ denotes functions whose coefficients are all zeros or ones. The space $\mathcal{W}$ is compact and convex. Let

$$\mathcal{G} := \{\lambda \mid |\lambda|<1, \exists\, h(z) \in \mathcal{B} \text{ such that } h(\lambda)=0\} \quad \subset \{z \mid |z|<1\}$$

be the set of zeroes of the power series belonging to $\mathcal{W}$. The elements of $\mathcal{G}$ lie within the unit circle and curves in $|z|<1$ given in polar coordinates, close to

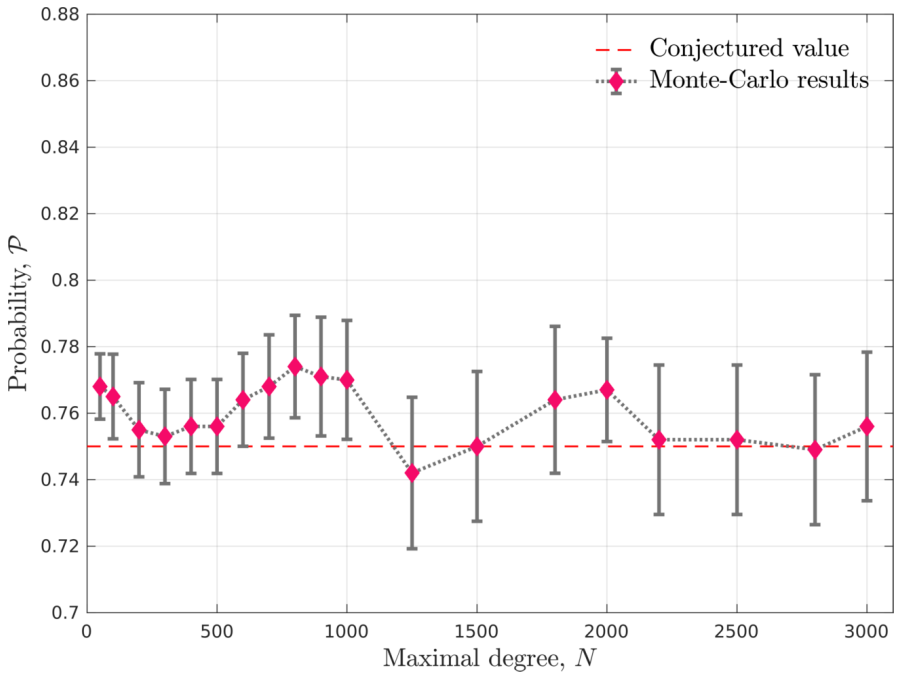

Fig. 8 Probability to be irreducible for a polynomial of the class $\mathcal{B}$ having degree less than N. The estimated 90% confidence intervals are represented. A limit value, as N tends to infinity, is conjectured to exist and its value is conjectured to be the rational number 3/4.

the unit circle, by [VG2]. The domain $D(0,1)\setminus\mathcal{G}$ is star-convex due to the fact that: $h(z)\in\mathcal{W}\Longrightarrow h(z/r)\in\mathcal{W}$, for any $r>1$ ([Sk], §3).

For every $\phi\in(0,2\pi)$, there exists $\lambda=re^{i\phi}\in\mathcal{G}$; the point of minimal modulus with argument ϕ is denoted $\lambda_\phi=\rho_\phi e^{i\phi}\in\mathcal{G}$, $\rho_\phi<1$. A function $h\in\mathcal{W}$ is called ϕ-optimal if $h(\lambda_\phi)=0$. Denote by $\mathcal{K}$ the subset of $(0,\pi)$ for which there exists a ϕ-optimal function belonging to $\mathcal{W}_{0,1}$. Denote by $\partial\mathcal{G}_S$ the "spike": $[-1,\frac{1}{2}(1-\sqrt{5})]$ on the negative real axis.

Theorem 11 (Solomyak) *(i) The union $\mathcal{G}\cup\mathbb{T}\cup\partial\mathcal{G}_S$ is closed, symmetrical with respect to the real axis, has a cusp at $z=1$ with logarithmic tangency (cf Figure 1 in* [Sk]*),*

(ii) the boundary $\partial\mathcal{G}$ is a continuous curve, given by $\phi\to|\lambda_\phi|$ on $[0,\pi)$, taking its values in $[\frac{\sqrt{5}-1}{2},1)$, with $|\lambda_\phi|=1$ if and only if $\phi=0$. It admits a left-limit at π^-, $1>\lim_{\phi\to\pi^-}|\lambda_\phi|>|\lambda_\pi|=\frac{1}{2}(-1+\sqrt{5})$, the left-discontinuity at π corresponding to the extremity of $\partial\mathcal{G}_S$.

(iii) at all points $\rho_\phi e^{i\phi}\in\mathcal{G}$ such that ϕ/π is rational in an open dense subset of $(0,2)$, $\partial\mathcal{G}$ is non-smooth,

(iv) there exists a nonempty subset of transcendental numbers L_{tr}, of Hausdorff dimension zero, such that $\phi\in(0,\pi)$ and $\phi\notin\mathcal{K}\cup\pi\mathbb{Q}\cup\pi L_{tr}$ implies that the boundary curve $\partial\mathcal{G}$ has a tangent at $\rho_\phi e^{i\phi}$ (smooth point).

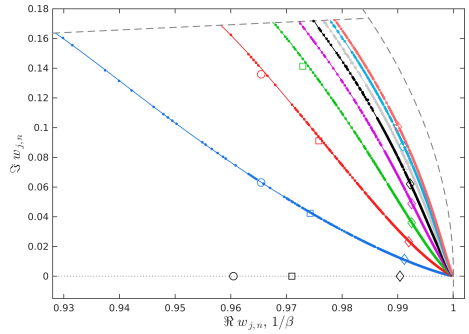

Fig. 9 Curves stemming from 1 which constitute the lenticular zero locus of all the polynomials of the class $\mathcal{B}$. These (universal) curves are continuous. The first one above the real axis, corresponding to the zero locus of the first lenticular roots, lies inside the boundary of Solomyak's fractal [Sk]. The lenticular roots of the polynomials f in the examples of the Figures 4, 5 and 6 are represented by the respective symbols o, $\Box$, $\diamond$. The dashed lines represent the unit circle and the top boundary of the angular sector $|\arg z| < \pi/18$. The complete set of curves, i.e. the locus of lenticuli, is obtained by symmetrization with respect to the real axis.

Proof [Sk], § 3 and § 4.

Let $\beta > 1$ be a real number and $T_\beta : [0,1] \to [0,1], x \to \beta x - \lfloor \beta x \rfloor = \{\beta x\}$ be the β-transformation. The i-iterate of T_β is denoted by T_β^i. The orbit $(T_\beta^i(1))_{i\geq 1}$ of 1 in the interval $[0,1]$ defines the sequence (t_i) of digits $t_i := \lfloor \beta T_\beta^{i-1}(1) \rfloor$ which belong to the alphabet $\{0,1\}$ and satisfy the conditions of Parry (Lothaire [Lo], Chap. 7). The Parry Upper function $f_\beta(z)$ at β is defined as the power series having coefficient vector: "$-1 \quad t_1 \quad t_2 \quad t_3 \quad \ldots$". When the Parry Upper function $f_\beta(z)$ at β is a polynomial, by Lemma 5.1 (ii) in [FLP], and

$$1 < \beta < \theta_2^{-1} = \frac{1+\sqrt{5}}{2},$$

the Conditions of Parry are exactly expressed by the defining conditions

$$n \geq 3,\ s \geq 0,\ m_1 - n \geq n-1,\ m_{q+1} - m_q \geq n-1 \text{ for } 1 \leq q < s$$

of the polynomial f of the class $\mathcal{B}$ in (1), with $f(x) = -1 + t_1 x + t_2 x^2 + t_3 x^3 + \ldots$. The polynomials f of the class $\mathcal{B}$ can be viewed as all the polynomial sections of all the Parry Upper functions $f_\beta(z)$ at β for all $1 < \beta < \theta_2^{-1}$. The correspondance $\beta \leftrightarrow f_\beta(z)$ is one-to-one [VG].

Now the identity $\lfloor \beta T_\beta^{i-1}(1) \rfloor = \beta T_\beta^{i-1}(1) - T_\beta^i(1), i \geq 2$, implies the factorization

$$-1 + t_1 x + t_2 x^2 + t_3 x^3 + \ldots = -(1-\beta x)(1 + \sum_{j\geq 1} T_\beta^i(1) x^i)$$

for which the second factor belongs to $\mathcal{W}$. Hence, except the collection of the real zeroes $(1/\beta)$ which are those of the polynomials $f \in \mathcal{B}$ in $[0,1]$, all the zeroes

of the polynomials $f \in \mathcal{B}$, of modulus < 1, lie within Solomyak's fractal domain $\mathcal{G}$, having boundary described by Theorem 11. By construction the zero locus of the first roots in Figure 9 is included in this boundary. Therefore it has logarithmic tangency at $z = 1$. The zero loci of the second roots, third roots, etc, closer to $|z| = 1$, in Figure 9, lie within $\mathcal{G}$. In Figure 9 are represented these (universal) curves on which the zeroes of preceding examples are reported. A complete study of these curves will be reported somewhere else.

References

[BBBSWW] C. Borst, E. Boyd, C. Brekken, S. Solberg, M.M. Wood and P.M. Wood, *Irreducibility of Random Polynomials*, preprint (2017).

[D] E. Dobrowolski, *On a Question of Lehmer and the Number of Irreducible Factors of a Polynomial*, Acta Arith. **34** (1979), 391–401.

[F] M. Filaseta, *On the Factorization of Polynomials with Small Euclidean Norm*, in Number Theory in Progress (Zakopane–Kościelisko, 1997), Vol. 1, de Gruyter, Berlin (1999), 143–163.

[FFN] M. Filaseta, C. Finch and C. Nicol, *On Three Questions Concerning* 0,1-*Polynomials*, J. Théorie Nombres Bordeaux **18** (2006), 357–370.

[FFK] M. Filaseta, K. Ford and S. Konyagin, *On an Irreducibility Theorem of A. Schinzel Associated with Coverings of the Integers*, Illinois J. Math. **44** (2000), 633–643.

[FM] M. Filaseta and M. Matthews, *On the Irreducibility of* 0,1-*Polynomials of the Form* $f(x)x^n + g(x)$, Coll. Math. **99** (2004), 1–5.

[FhJ] C. Finch and L. Jones, *On the Irreducibility of* $\{-1,0,1\}$– *Quadrinomials*, Integers **6** (2006), #A16.

[FLP] L. Flatto, J.C. Lagarias and B. Poonen, *The Zeta Function of the beta Transformation*, Ergod. Th & Dynam. Sys. **14** (1994), 237–266.

[K] S.V. Konyagin, *On the Number of Irreducible Polynomials with* 0,1 *Coefficients*, Acta Arith. **88** (4) (1999), 333–350.

[L] W. Ljunggren, *On the Irreducibility of Certain Trinomials and Quadrinomials*, Math. Scand. **8** (1960), 65–70.

[Lo] M. Lothaire, *Algebraic Combinatorics on Words*, in Encylopedia of Mathematics and its Applications, Vol. **90**, Cambridge University Press, Cambridge (2002).

[MS] M. Mignotte and D. Ştefănescu, *On the Roots of Lacunary Polynomials*, Mathematical Inequalities & Applications **2** (1) (1999), 1–13.

[Ms] W.H. Mills, *The Factorization of Certain Quadrinomials*, Math. Scand. **57** (1985), 44–50.

[OP] A.M. Odlyzko and B. Poonen, *Zeros of Polynomials with* 0,1 *Coefficients*, Enseign. Math. **39** (1993), 317–348.

[S] A. Schinzel, *Reducibility of Lacunary Polynomials I.*, Acta Arith. **16** (1969/70), 123–159.

[S2] A. Schinzel, *Reducibility of Lacunary Polynomials III.*, Acta Arith. **34** (1978), 227–266.

[S3] A. Schinzel, *On the Number of Irreducible Factors of a Polynomial*, Colloq. Math. Soc. János Bolyai **13** (1976), 305–314.

[S4] A. Schinzel, *On the Number of Irreducible Factors of a Polynomial II.*, Ann. Polon. Math. **42** (1983), 309–320.

[Sr] E.S. Selmer, *On the Irreducibility of Certain Trinomials*, Math. Scand. **4** (1956), 287–302.

[Sk] B. Solomyak, *Conjugates of beta-Numbers and the Zero-Free Domain for a Class of Analytic Functions*, Proc. London Math. Soc. **68** (1994), 477–498.

[VG] J.-L. Verger-Gaugry, *Uniform Distribution of the Galois Conjugates and Beta-Conjugates of a Parry Number Near the Unit Circle and Dichotomy of Perron Numbers*, Uniform Distribution Theory J. **3** (2008), 157–190.

[VG2] J.-L. Verger-Gaugry, *On the Conjecture of Lehmer, Limit Mahler Measure of Trinomials and Asymptotic Expansions*, Uniform Distribution Theory J. **11** (2016), 79–139.

[VG3] J.-L. Verger-Gaugry, *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus*, preprint (2017), arXiv:1709.03771; v2 version (2018).

[WO] A.N. Willson Jr. and H.J Orchard, *An Efficient Resultant for Determining Reciprocal Zeros in Polynomials*, Linear Alg. Applic. **411** (2005), 309–327.

Appendix

The coding of the Monte-Carlo algorithm and the PARI/GP program used in the present study is as follows:

Algorithm 1 *Pseudo-code of the PARI/GP program used to estimate the probability to find an irreducible polynomial in the class* $\mathcal{B}_{N_{\max}} = \cup_{k=1}^{N_{\max}} \mathcal{B}_k$.

Require: $N_{\max} \in \mathbb{N}$ ▷ *Maximal polynomial degree*
Require: $M \in \mathbb{N}$ ▷ *Number of Monte-Carlo drawings*
  Irreducible[1:M] $\leftarrow 0$
  for $k = 1$ *to* M ***do***
    $N \leftarrow$ *Random* $(2 \dots N_{\max})$
    $n \leftarrow$ *Random* $(2 \dots N)$
    $p(x) = -1 + x + x^n$ ▷ *We initialize with this trinomial*
    $m \leftarrow 2n - 1$ ▷ $m_1 - n \geqslant n - 1$
    while $m \leqslant N$ ***do***
      $\Delta m \leftarrow$ *Random* $(0 \dots N - m)$
      $p(x) \leftarrow p(x) + x^{m+\Delta m}$
      $m \leftarrow m + \Delta m + n - 1$ ▷ $m_{s+1} - m_s \geqslant n - 1$
    end while
    if *IrreducibilityTest* $\big(p(x)\big) \equiv$ ***True then***
      Irreducible [k] $\leftarrow 1$
    end if
  end for
  $\mathbb{P} \approx \frac{1}{M} \sum_{k=1}^{M}$ *Irreducible [k]* ▷ *Approximate probability by frequency*

```
This script estimates the probability of finding a sparse irreducible
polynomial with coefficients in {-1, 0, 1} in the class B.

/* First, we increase the stack size: */
default(parisize, 1073741824); /* 1 Gb */

/* Search horizon in polynomial degree: */
Nmax = 3000;

/* Number of Monte-Carlo runs */
M = 1000;

/* The vector, where we stock the results of the irreducibility test: */
Irred = vector(M);

printf("Some information about computation:\n");
printf("  ->  Maximal polynomial degree: %d\n", Nmax);
printf("  -> Number of Monte-Carlo runs: %d\n\n", M);
printf("Computations started. Please, wait...");

ts = getabstime(); /* Record start time */
/* The main loop over realizations!: */
for (i = 1, M, {
  printf("iter = %d\n", i);
  N = 2 + random(Nmax - 1);
  n = 2 + random(N - 1);
  /* print(n); */
  /* P is the vector of coefficients */
  P = concat(concat(1, vector(n-2)), [1, -1]);
  p = length(P); /* we shall need it below */
  m = 2*n - 1; /* the next term has the degree >= m */
  while (m <= N,
   s = m + random(N - m + 1);
   P = concat(concat(1, vector(s - p)), P);
   p = length(P);
   m = s + n - 1;
  );
  pp = Pol(P, x); /* Convert vector to the polynomial: */
  /* print(pp); */
  if (polisirreducible(pp), /* if polynomial is irreducible, we note it */
   Irred[i] = 1;
  );
});
```

```
te = getabstime(); /* Simulation end time */
printf("Done. Execution time = %.3f s.\n", (te-ts)/1000);

/* Let's do some statistical analysis of obtained data */
Mean = vecsum(Irred)/M;
Var  = 0.0;
for (i = 1, M, {
  Var += (Irred[i] - Mean)$^2$;
});
Var = sqrt(Var/(M - 1));
Err = 1.645*Var/sqrt(M);

printf("Estimated probability: %1.3f\n", Mean);
printf("Estimated 90%%-confidence interval  : %
```