

Moscow Journal of Combinatorics and Number Theory

2020
vol. 9 no. 2

On the roots of the Poupard and Kreweras polynomials

Frédéric Chapoton and Guo-Niu Han



On the roots of the Poupard and Kreweras polynomials

Frédéric Chapoton and Guo-Niu Han

The Poupard polynomials are polynomials in one variable with integer coefficients, with some close relationship to Bernoulli and tangent numbers. They also have a combinatorial interpretation. We prove that every Poupard polynomial has all its roots on the unit circle. We also obtain the same property for another sequence of polynomials introduced by Kreweras and related to Genocchi numbers. This is obtained through a general statement about some linear operators acting on palindromic polynomials.

1. Introduction

Let us consider the sequence of polynomials $(F_n)_{n \geq 1}$ in one variable x characterized by the equation

$$(x-1)^2 F_{n+1}(x) = (x^{2n+2} + 1)F_n(1) - 2x^2 F_n(x) \quad \text{for } n \geq 1, \quad (1-1)$$

with the initial condition $F_1 = 1$. When described in this way, their existence is not completely obvious, because the right-hand side must have a double root at $x = 1$ for the recurrence to make sense. The first few terms are given by

$$F_1 = 1,$$

$$F_2 = x^2 + 2x + 1,$$

$$F_3 = 4x^4 + 8x^3 + 10x^2 + 8x + 4,$$

$$F_4 = 34x^6 + 68x^5 + 94x^4 + 104x^3 + 94x^2 + 68x + 34.$$

The polynomial F_n has degree $2n - 2$ and palindromic coefficients.

The coefficients of these polynomials form the Poupard triangle (A8301), first considered by Christiane Poupard [1989] and proved to enumerate some sets of labelled binary trees. It follows from this combinatorial interpretation that all coefficients of F_n are nonnegative integers. For further combinatorial information on these polynomials and their relatives, see [Foata and Han 2013; 2014].

The constant terms of these polynomials form the sequence of *reduced tangent numbers* (A2105), which can be defined for $n \geq 1$ by the formula

$$\frac{2^n (2^{2n} - 1) |B_{2n}|}{n}, \quad (1-2)$$

where B_n are the classical Bernoulli numbers, and starts by

$$1, 1, 4, 34, 496, 11056, 349504, 14873104, 819786496, \dots$$

MSC2010: primary 26C10, 47B39; secondary 11B68, 39A70.

Keywords: palindromic polynomial, unit circle, complex root, linear operator, Bernoulli number.

One can deduce from (1-1) that $F_{n+1}(0) = F_n(1)$, so the reduced tangent numbers also describe the values of the polynomials F_n at $x = 1$.

Our first result is the following unexpected property, which was the experimental starting point of this article.

Theorem 1.1. *For $n \geq 1$, all roots of the polynomial $F_n(x)$ are on the unit circle.*

This is proved in Section 2 in a much more general context, by showing that, for any positive integer D , a linear operator \mathcal{N}_D maps palindromic polynomials with nonnegative coefficients to palindromic polynomials with nonnegative coefficients and all roots on the unit circle.

Whether there is any combinatorial meaning for this theorem, and for the similar theorem below, is rather unclear. Although the coefficients of these polynomials have a combinatorial interpretation, the location of their roots does not tell us anything about the combinatorics. One may speculate about some kind of arithmetic interpretation, maybe in terms of Weil polynomials, given the close relationship to Bernoulli numbers.

As another interesting application, one can consider the sequence of polynomials characterized by

$$(x-1)^2 G_{n+1}(x) = (x^{2n+3} + 1)G_n(1) - 2x^2 G_n(x) \quad \text{for } n \geq 1, \quad (1-3)$$

with initial condition $G_1 = 1 + x$. The first few terms are

$$\begin{aligned} G_1 &= x + 1, \\ G_2 &= 2x^3 + 4x^2 + 4x + 2, \\ G_3 &= 12x^5 + 24x^4 + 32x^3 + 32x^2 + 24x + 12, \\ G_4 &= 136x^7 + 272x^6 + 384x^5 + 448x^4 + 448x^3 + 384x^2 + 272x + 136. \end{aligned}$$

The polynomial G_n has degree $2n - 1$ and palindromic coefficients.

Theorem 1.2. *For $n \geq 1$, all roots of the polynomial $G_n(x)$ are on the unit circle.*

Because the polynomials G_n have odd degree, they are all divisible by $x + 1$. One can also show by induction that the polynomial G_n is divisible by 2^{n-1} . The quotient polynomials $2^{1-n} G_n / (x + 1)$ have appeared in [Kreweras 1997], dealing with refined enumeration of some sets of permutations. Their constant terms are the Genocchi numbers (A1469), given by the formula

$$2(2^{2n} - 1)|B_{2n}|, \quad (1-4)$$

where B_n are again the Bernoulli numbers.

Both theorems above are proved in Section 2 using a family of operators \mathcal{N}_D acting on palindromic polynomials. Section 3 describes explicit simple eigenvectors of the operator \mathcal{N}_1 . In Section 4, some evidence is given for the general asymptotic behaviour of the iteration of the operators \mathcal{N}_D for $D > 1$. Section 5 contains various statements and conjectures on values of the operators \mathcal{N}_D on specific palindromic polynomials.

Let us note as a side remark that another family of polynomials, also related to Bernoulli numbers, has been proved in [Lalín and Smyth 2013] to have only roots on the unit circle, by different methods.

2. Operators \mathcal{N}_D and roots on the unit circle

Let us consider a polynomial $P(x) = \sum_{j=0}^d p_j x^j$ with rational coefficients. Let us say that the polynomial P is *palindromic of index d* if $p_j = p_{d-j}$ for all j . Note that the index can also be described as the sum of the degree and the valuation. For example, the index of the polynomial $x = 0 + x + 0x^2$ is 2. For any $d \geq 0$, let V_d be the vector space spanned by palindromic polynomials of index d .

For every nonnegative integer D , let us introduce a linear operator \mathcal{N}_D from V_d to V_{d+2D-2} . This operator is characterized by the formula

$$(x - 1)^2 \mathcal{N}_D(P)(x) = (x^{d+2D} + 1)P(1) - 2x^D P(x). \tag{2-1}$$

The definition requires that the right-hand side is divisible by $(x - 1)^2$. By the linearity of (2-1), it is enough to check this property for the basis elements $x^i + x^{d-i}$ with $0 \leq i \leq d$, where one finds

$$\mathcal{N}_D(x^i + x^{d-i}) = 2 \frac{(1 - x^{i+D})(1 - x^{d+D-i})}{(1 - x)^2}, \tag{2-2}$$

which is a polynomial with nonnegative integer coefficients. Note that when $d = 2i$, one can divide (2-2) by 2.

The definition of \mathcal{N}_D and formula (2-2) imply immediately the following lemma.

Lemma 2.1. *Let P be a nonzero palindromic polynomial of index d with nonnegative integer coefficients. If $d \leq 1$, assume moreover that $D > 0$. Then $\mathcal{N}_D(P)$ is a nonzero palindromic polynomial of index $d + 2D - 2$ with positive integer coefficients.*

Let us record the following useful statement as a lemma.

Lemma 2.2. *When iterating i times \mathcal{N}_D on a palindromic polynomial P of odd index with integer coefficients, the integer 2^i divides $\mathcal{N}_D^i P$.*

Proof. If the index of a palindromic polynomial P is odd, then it is divisible by $x + 1$. When P has integer coefficients, (2-1) then implies that $\mathcal{N}_D(P)$ has one further factor 2. The lemma follows by induction. \square

Recall that a palindromic polynomial $P = \sum_{j=0}^d p_j x^j$ is called *unimodal* if the sequence of coefficients is increasing up to the middle coefficient(s), then decreasing. A polynomial P is called *concave* if the piecewise linear function that maps j to p_j is a concave function. A concave polynomial P is called *strictly concave* if every point (j, p_j) is moreover an extremal point in the graph of this piecewise linear function.

Lemma 2.3. *Let P be a nonzero palindromic polynomial of index d with nonnegative integer coefficients. If $d \leq 1$, assume moreover that $D > 0$. Then $\mathcal{N}_D(P)$ is unimodal and concave. If P has no zero coefficient, then $\mathcal{N}_D(P)$ is strictly concave.*

Proof. By (2-2), the polynomial $\mathcal{N}_D(P)$ is a nonnegative linear combination of unimodal and concave polynomials, and hence is itself unimodal and concave. Each term in (2-2) gives two extremal points, or just one extremal point when $i = d - i$. When P has no zero coefficient, this implies that there is an extremal point above every integer between 1 and $d + 1$. \square

Let us now recall a beautiful criterion obtained in [Lakatos and Losoncz 2004].

Lemma 2.4. Let $P(x) = \sum_{j=0}^d p_j x^j$ be a palindromic polynomial of index d . If

$$|p_d| \geq \frac{1}{2} \sum_{j=1}^{d-1} |p_j|, \quad (2-3)$$

then all roots of P are on the unit circle.

The criterion above has been generalized recently in [Vieira 2017], which gives a sufficient condition for having a given number of roots on the unit circle.

From the criterion of Lemma 2.4, one deduces:

Theorem 2.5. Let $P(x) = \sum_{j=0}^d p_j x^j$ be a palindromic polynomial of index d . If

$$2p_j \geq p_{j-1} + p_{j+1} \quad \text{for all } 0 \leq j \leq d, \quad (2-4)$$

with the convention that $p_{-1} = p_{d+1} = 0$, then all roots of P are on the unit circle.

Proof. Let $Q(x) = (1-x)^2 P(x)$. Then $Q(x) = \sum_{j=0}^{d+2} q_j x^j$, where

$$\begin{aligned} q_0 &= p_0, \\ q_{j+1} &= p_{j+1} + p_{j-1} - 2p_j \quad (0 \leq j \leq d), \\ q_{d+2} &= p_d. \end{aligned}$$

Note that Q is also palindromic of index $d+2$.

By the hypothesis (2-4), all $q_j \leq 0$ for $1 \leq j \leq d+1$. Since $Q(1) = 0$, we have

$$\sum_{j=1}^{d+1} |q_j| = - \sum_{j=1}^{d+1} q_j = q_0 + q_{d+2} = 2q_{d+2}.$$

Note that therefore $q_0 \geq 0$.

Since $Q(x)$ is palindromic, and

$$|q_{d+2}| = \frac{1}{2} \sum_{j=1}^{d+1} |q_j|,$$

one can therefore apply Lemma 2.4 to $Q(x)$ and conclude that $Q(x)$ has all its roots on the unit circle. This implies the same property for $P(x)$. \square

Theorem 2.6. Let P be a nonzero palindromic polynomial of index d with nonnegative integer coefficients. If $d \leq 1$, assume moreover that $D > 0$. Then $\mathcal{N}_D(P)$ is a nonzero palindromic polynomial of index $d + 2D - 2$ with nonnegative integer coefficients, and all roots of $\mathcal{N}_D(P)$ are on the unit circle.

Proof. This is an application of Theorem 2.5. The definition of \mathcal{N}_D and the hypothesis that P has nonnegative coefficients imply immediately the condition (2-4). \square

Let us now apply Theorem 2.6 to the proofs of Theorems 1.1 and 1.2. The defining recurrence (1-1) for the polynomials F_n can be written as $F_{n+1} = \mathcal{N}_D(F_n)$ with the initial condition $F_1 = 1$. The property follows by induction. The same proof works for G_n with the initial polynomial $1+x$.

Let us now state two useful lemmas.

Lemma 2.7. For all $d \geq 0$, the polynomial $x^d + 1$ is in the kernel of \mathcal{N}_0 .

Proof. This is a direct consequence of (2-2). □

Lemma 2.8. Let $d \geq 2$ be an integer. Then

$$\mathcal{N}_0(1 + x + \dots + x^d) = \sum_{i=0}^{d-2} (d-1-i)(i+1)x^i. \tag{2-5}$$

Proof. From the definition of \mathcal{N}_0 by (2-2), and by the previous lemma, this is equal to

$$\sum_{j=1}^{d-1} \frac{1-x^j}{1-x} \frac{1-x^{d-j}}{1-x}.$$

Expanding, one finds that the coefficient of x^i is the cardinality of

$$\{(j, k) \mid 0 \leq k \leq j-1 \text{ and } 0 \leq i-k \leq d-j-1\}.$$

But this is the same as the set

$$\{(j, k) \mid 1 \leq j-k \leq d-i-1 \text{ and } 0 \leq k \leq i\},$$

whose cardinality is $(d-1-i)(i+1)$. □

3. Sinus polynomials as eigenvectors

As can be seen in Figure 1, right, the roots of the Poupard polynomials $F_n(x)$ are very close to some of the roots of $x^{2n} + 1$, with two missing roots on the right. Moreover the plot of the coefficients of $F_n(x)$ seems to approximate a concave continuous function, as in Figure 1, left.

One expects that, up to a global multiplicative factor, the polynomials obtained when iterating n times the operator \mathcal{N}_D (for some fixed $D > 1$) are always becoming, when n is large, very close to the polynomials described in this section. Some kind of justification will be given in the next section.

Let us consider the polynomial $S_{m,n}(x)$ defined for $n \geq 2$ and odd $m \geq 1$ by

$$S_{m,n}(x) = \frac{x^{mn} + 1}{x^2 - 2x \cos \frac{\pi}{n} + 1}, \tag{3-1}$$

whose roots are the roots of $x^{mn} + 1$ except $\exp(i\pi/n)$ and its conjugate.

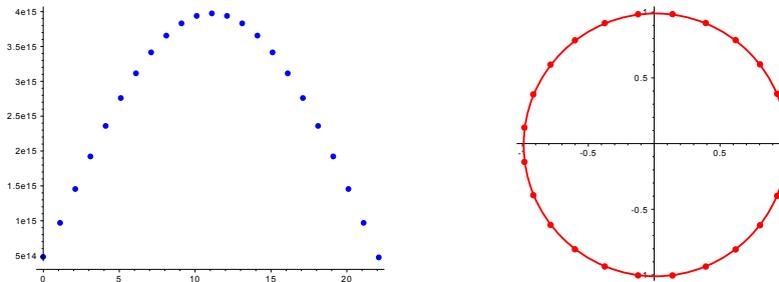


Figure 1. Coefficients and roots of the Poupard polynomial F_{12} .

Let us first give an alternative expression for $S_{m,n}$.

Lemma 3.1. *The polynomial $S_{m,n}$ has the explicit expression*

$$S_{m,n}(x) = \frac{1}{\sin \frac{\pi}{n}} \sum_{k=0}^{mn-2} \sin\left(\frac{(k+1)\pi}{n}\right) x^k. \quad (3-2)$$

Proof. The proof is a simple computation, expanding both sides as polynomials in x and $\zeta = \exp(i\pi/n)$, also using that m is odd. \square

This implies that the plot of the coefficients of $S_{1,n}$ looks very much like a sinus curve, like Figure 1, left.

Proposition 3.2. *For every $n \geq 2$ and odd $m \geq 1$, the polynomial $S_{m,n}$ is an eigenvector of the operator \mathcal{N}_1 acting on V_{mn-2} for the eigenvalue $1/(1 - \cos(\pi/n))$.*

Proof. The proof is another explicit computation using the definition of $S_{m,n}$ in (3-1) and the definition of the operator \mathcal{N}_1 in (2-1). \square

Note that the eigenvalue is also the value $S_{m,n}(1)$.

In general, the Galois conjugates of the polynomial $S_{1,n}$ do not provide a complete set of eigenvectors for the operator \mathcal{N}_1 acting on V_{n-2} . The other eigenvectors are $S_{m,n/m}$ for odd divisors m of n , and their Galois conjugates.

The family of operators \mathcal{N}_1 acting on the spaces V_{n-2} of palindromic polynomials looks very much like discrete versions of the Laplacian operator ∂_x^2 acting on the space of functions f on the real interval $[0, 1]$ such that $f(1-x) = f(x)$ for all x and $f(0) = f(1) = 0$.

4. Asymptotic behaviour from recurrence

Our next point is to justify in a heuristic way that iterating an operator \mathcal{N}_D for some $D > 1$ produces a sequence of polynomials that gets closer and closer to the sinus polynomials $S_{1,n}$. We have not tried to make these computations rigorous.

Let us consider a family of polynomials H_n of index n defined by iterating \mathcal{N}_D , starting from an arbitrary palindromic polynomial H_m with nonnegative coefficients and index m . Throughout this section, the index n belongs to an arithmetic progression of step $\delta = 2D - 2$ starting at m . Let us write

$$H_n(x) = \sum_{k=0}^n H_{n,k} x^k. \quad (4-1)$$

We will assume the following asymptotic ansatz for the constant terms:

$$H_n(0) \simeq AB^n C n^{En} \quad (4-2)$$

for some constants A, B, C, E , with A, B, E positive. This ansatz is motivated by the known case of the tangent numbers, where $B = 2/(e\pi)$, $E = 1$ and $C = -\frac{1}{2}$. This ansatz implies

$$H_{n+\delta}(0)/H_n(0) \simeq B^\delta e^{\delta E} n^{\delta E}. \quad (4-3)$$

We will also assume that there exists a smooth function Ψ which is a probability distribution function on the real interval $[0, 1]$ vanishing at 0 and 1, with $\Psi(1 - x) = \Psi(x)$ on this interval and such that

$$H_{n,k} \simeq \frac{\alpha_n}{n} \Psi\left(\frac{k}{n}\right) + H_{n,0} \tag{4-4}$$

is a good asymptotic approximation when n is large, for some sequence α_n to be determined.

Taking the sum of (4-4) over k ranging from 0 to n and using the hypothesis on Ψ , one gets

$$H_{n+\delta,0} = H_n(1) \simeq \alpha_n + (n + 1)H_{n,0}.$$

Assuming that $nH_{n,0}$ is negligible compared to $H_{n+\delta,0}$, one obtains that a correct choice for α_n is

$$\alpha_n = H_{n+\delta,0}.$$

From (2-1), one deduces that the action of \mathcal{N}_D at the level of coefficients is given by

$$H_{n+\delta,k+D} - 2H_{n+\delta,k+D-1} + H_{n+\delta,k+D-2} = -2H_{n,k}, \tag{4-5}$$

except for $k = 0$ and $k = n$.

Replacing in (4-5) the coefficients by the expression from (4-4), one obtains

$$\frac{\alpha_{n+\delta}}{n + \delta} \left(\Psi\left(\frac{k + D}{n + \delta}\right) - 2\Psi\left(\frac{k + D - 1}{n + \delta}\right) + \Psi\left(\frac{k + D - 2}{n + \delta}\right) \right) \simeq -2 \left(\frac{\alpha_n}{n} \Psi\left(\frac{k}{n}\right) + H_{n,0} \right). \tag{4-6}$$

Using now the growth ansatz, one can get rid of $H_{n,0}$ in the rightmost term and obtain

$$\Psi\left(\frac{k + D}{n + \delta}\right) - 2\Psi\left(\frac{k + D - 1}{n + \delta}\right) + \Psi\left(\frac{k + D - 2}{n + \delta}\right) \simeq -2 \frac{\alpha_n}{\alpha_{n+\delta}} \Psi\left(\frac{k}{n}\right). \tag{4-7}$$

The left-hand side is an approximation of the second derivative of Ψ , so one obtains

$$\frac{1}{2(n + \delta)^2} \Psi''\left(\frac{k}{n + \delta}\right) \simeq -2 \frac{\alpha_n}{\alpha_{n+\delta}} \Psi\left(\frac{k}{n}\right). \tag{4-8}$$

If $\delta E = 2$, one therefore reaches the differential equation

$$\Psi'' = -F\Psi, \tag{4-9}$$

where $F = 4/(B^\delta e^2)$. Because Ψ vanishes at 0, it must be a multiple of $\sin(\sqrt{F}x)$. Because Ψ vanishes at 1 and is positive on the interval $[0, 1]$, necessarily $F = \pi^2$ and therefore $B^\delta = (2/(e\pi))^2$. Because Ψ is a probability distribution, one must have $\Psi = \frac{\pi}{2} \sin(\pi x)$.

One can therefore conclude that, under several plausible but unproven assumptions, the asymptotic shape of the coefficients of the polynomials H_n is approximating that of the polynomials $S_{1,n+2}$.

5. Various remarks

5.1. Action of the operator \mathcal{N}_0 . Applying the operator \mathcal{N}_0 decreases the index by 2, so that iterating this operator on any initial polynomial P of index d always vanishes after a finite number of steps. Let \mathcal{N}_0^{\max} be the last nonidentically zero iterate of \mathcal{N}_0 acting on V_d . Let us denote by ρ the linear map that maps P to the constant term of $\mathcal{N}_0^{\max}(P)$.

For example, here is a sequence of iterates of \mathcal{N}_0 :

$$x^4 + x^3 + x^2 + x + 1, \quad 3x^2 + 4x + 3, \quad 4.$$

In this case, $\rho(x^4 + x^3 + x^2 + x + 1) = 4$.

Let us present some special cases of initial choices where the value of ρ is interesting.

For $n \geq 0$, consider the polynomial

$$Q_n(t) = \sum_{i=0}^{2n+1} \rho\left(\frac{x^i - x^{2n+1-i}}{x-1}\right) t^i, \quad (5-1)$$

recording this sequence of final values. By the antisymmetry of the argument of ρ , the polynomial Q_n vanishes at $t = 1$. Let $P_n(t)$ be the quotient $Q_n(t)/(t-1)$, which is clearly a palindromic polynomial.

Proposition 5.1. *For every $n \geq 0$, the polynomial P_n is the Poupard polynomial F_{n+1} .*

Proof. For $n = 0$, one can check that $P_n(t) = 1$. Assume $n > 0$. For $0 \leq i \leq 2n$, the coefficient $c_{n,i}$ of t^i in $P_n(t)$ can be written as

$$-\rho\left(\sum_{0 \leq k \leq i} \frac{x^k - x^{2n+1-k}}{x-1}\right) = \rho\left(\frac{x^{i+1} - 1}{x-1} \frac{x^{2n+1-i} - 1}{x-1}\right). \quad (5-2)$$

Let us now compute $c_{n,i+2} - 2c_{n,i+1} + c_{n,i}$ for $0 \leq i \leq 2n-2$. Starting from the left-hand side of (5-2), this is given by

$$\rho(x^{i+1} + x^{2n-i-1}).$$

Using now (2-2) for \mathcal{N}_0 and the definition of ρ as the final value for the iteration of \mathcal{N}_0 , this becomes

$$2\rho\left(\frac{x^{i+1} - 1}{x-1} \frac{x^{2n-i-1} - 1}{x-1}\right),$$

in which one can recognize $-2c_{n-1,i}$ using the right-hand side of (5-2).

Moreover, $c_{n,1} - 2c_{n,0} = \rho(1 + x^{2n}) = 0$ because $1 + x^{2n}$ is in the kernel of \mathcal{N}_0 by Lemma 2.7.

Let us now check that $c_{n,0} = \sum_{i=0}^{2n-2} c_{n-1,i}$. First, by (5-2), the left-hand side is the image by ρ of $\mathcal{N}_0(1 + x + \dots + x^{2n})$, given by Lemma 2.8. The right-hand side is the image by ρ of

$$\sum_{i=0}^{2n-2} \sum_{0 \leq k \leq i} \sum_{k \leq j \leq 2n-2-k} x^j = \sum_{j=0}^{2n-2} (2n-1-j)(j+1)x^j, \quad (5-3)$$

which is the exact same expression.

All these properties of the coefficients $c_{n,i}$ imply exactly that the polynomial $P_n(t)$ is the image of $P_{n-1}(t)$ by \mathcal{N}_1 , acting on the variable t . \square

For $n \geq 0$, consider the polynomial

$$Q'_n(t) = \sum_{i=0}^{2n} \rho\left(\frac{x^i - x^{2n-i}}{x-1}\right) t^i, \quad (5-4)$$

recording this sequence of final values. By the antisymmetry of the argument of ρ , the polynomial Q'_n vanishes at $t = 1$. Let $P'_n(t)$ be the quotient $Q'_n(t)/(t-1)$, which is clearly a palindromic polynomial of odd index.

Proposition 5.2. *For every $n \geq 1$, the polynomial Q'_n is the Kreweras polynomial G_n .*

Proof. The proof is very similar to the previous one. One first check that Q'_1 is $1 + x$. Then one checks by looking at coefficients that Q'_{n+1} is $\mathcal{N}_1(Q'_n)$. □

Let us now describe some similar conjectural properties. For the starting sequence $(2^{-j}(1+x)^{2j})_{j \geq 0}$, one gets the following values of ρ :

$$1, 1, 5, 61, 1385, 50521, 2702765, 199360981, 19391512145, \dots,$$

which seem to be the Euler numbers (A364). Similarly, for the starting sequence $(2^{-j}(1+x)^{2j+1})_{j \geq 0}$, one gets

$$1, 3, 25, 427, 12465, 555731, 35135945, \dots$$

This seems to be the closely related sequence (A9843).

As a final conjectural remark, let us consider the following extension of the two previous cases.

Conjecture 5.3. *For every i, j , the number $\rho(x^i(1+x)^j)$ is divisible by $2^{\lfloor j/2 \rfloor}$.*

This property is clear if j is odd by Lemma 2.2, but not at all if j is even.

Assuming this conjecture, one can define, for every integer n , the square matrix M_n whose coefficient $M_n(i, j)$, for $0 \leq i \leq n$ and $0 \leq j \leq n$, is $\rho(x^i(1+x)^j)2^{-\lfloor j/2 \rfloor}$.

Conjecture 5.4. *For all $n \geq 0$, the determinant d_n of the matrix M_n is given by the formula*

$$d_n = (n-1)!^{\varepsilon(1)}(n-2)!^{\varepsilon(2)}(n-3)!^{\varepsilon(3)} \dots 1!^{\varepsilon(n-1)}, \tag{5-5}$$

where

$$\varepsilon(k) = \begin{cases} 2 & \text{if } k \text{ is odd,} \\ 4 & \text{if } k \text{ is even.} \end{cases}$$

For example, M_6 is equal to

$$\begin{pmatrix} 1 & 1 & 1 & 3 & 5 & 25 \\ 1 & 2 & 3 & 14 & 33 & 226 \\ 2 & 8 & 18 & 120 & 378 & 3336 \\ 10 & 64 & 198 & 1728 & 6858 & 74304 \\ 104 & 896 & 3528 & 38016 & 182088 & 2339712 \\ 1816 & 19456 & 92808 & 1188864 & 6668568 & 99118080 \end{pmatrix}, \tag{5-6}$$

whose determinant is indeed $5!^2 4!^4 3!^2 2!^4 1!^2$.

This matrix contains entries with large prime factors, for example $92808 = 2^3 3^2 1289$, but the determinant has only small prime factors.

5.2. Action of the operator \mathcal{N}_1 . Applying the operator \mathcal{N}_1 does not change the index, so iterating this operator on any initial choice gives an infinite sequence of palindromic polynomials of the same index.

For example, starting with x gives a sequence of polynomials

$$x, \quad x^2 + 2x + 1, \quad 4x^2 + 6x + 4, \quad 14x^2 + 20x + 14, \quad 48x^2 + 68x + 48, \quad 164x^2 + 232x + 164, \quad \dots,$$

whose constant terms and middle coefficients are given by A7070 and by A6012. Indeed, the action of \mathcal{N}_1 on reciprocal polynomials of index 2 is given in the basis $\{1 + x^2, x\}$ by the matrix

$$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$$

so that both sequences satisfy the recurrence $a_n = 4a_{n-1} - 2a_{n-2}$ with appropriate initial conditions.

5.3. Action of the operator \mathcal{N}_2 . Applying the operator \mathcal{N}_2 increases the index by 2, so iterating this operator gives an infinite sequence of polynomials for every initial choice. In each such sequence, the sequence of constant terms is, up to a shift of indices by 1, the same as the sequence of values at $x = 1$. Some examples were presented in the introduction, related to reduced tangent numbers and Genocchi numbers. Let us record one more family of examples.

Using the polynomials $x^i(x+1)$ for $i \geq 0$ as starting points, one gets a table of constant terms:

$$\begin{pmatrix} 1 & 1 & 3 & 17 & 155 & 2073 \\ 0 & 1 & 6 & 55 & 736 & 13573 \\ 0 & 1 & 10 & 135 & 2492 & 60605 \\ 0 & 1 & 15 & 280 & 6818 & 211419 \\ 0 & 1 & 21 & 518 & 16086 & 619455 \\ 0 & 1 & 28 & 882 & 34020 & 1592811 \end{pmatrix}.$$

Here i is the row index and in each row the term of index j is the constant term divided by 2^j . This table seems to be essentially the Salié triangle (A65547).

References

- [Foata and Han 2013] D. Foata and G.-N. Han, “Finite difference calculus for alternating permutations”, *J. Difference Equ. Appl.* **19**:12 (2013), 1952–1966. MR Zbl
- [Foata and Han 2014] D. Foata and G.-N. Han, “Tree calculus for bivariate difference equations”, *J. Difference Equ. Appl.* **20**:11 (2014), 1453–1488. MR Zbl
- [Kreweras 1997] G. Kreweras, “Sur les permutations comptées par les nombres de Genocchi de 1-ière et 2-ième espèce”, *European J. Combin.* **18**:1 (1997), 49–58. MR Zbl
- [Lakatos and Losoncz 2004] P. Lakatos and L. Losoncz, “Self-inversive polynomials whose zeros are on the unit circle”, *Publ. Math. Debrecen* **65**:3-4 (2004), 409–420. MR Zbl
- [Lalín and Smyth 2013] M. N. Lalín and C. J. Smyth, “Unimodularity of zeros of self-inversive polynomials”, *Acta Math. Hungar.* **138**:1-2 (2013), 85–101. Addendum in **147**:1 (2015), 255–257. MR Zbl
- [Poupard 1989] C. Poupard, “Deux propriétés des arbres binaires ordonnés stricts”, *European J. Combin.* **10**:4 (1989), 369–374. MR Zbl
- [Vieira 2017] R. S. Vieira, “On the number of roots of self-inversive polynomials on the complex unit circle”, *Ramanujan J.* **42**:2 (2017), 363–369. MR Zbl

Received 16 Jan 2020. Revised 15 May 2020.

FRÉDÉRIC CHAPOTON:

chapoton@unistra.fr

Institut de Recherche Mathématique Avancée, UMR 7501, Université de Strasbourg et CNRS, Strasbourg, France

GUO-NIU HAN:

guoniu.han@unistra.fr

Institut de Recherche Mathématique Avancée, UMR 7501, Université de Strasbourg et CNRS, Strasbourg, France

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

EDITORS-IN-CHIEF

- Yann Bugeaud Université de Strasbourg (France)
bugaud@math.unistra.fr
- Nikolay Moshchevitin Lomonosov Moscow State University (Russia)
moshchevitin@gmail.com
- Andrei Raigorodskii Moscow Institute of Physics and Technology (Russia)
mraigor@yandex.ru
- Ilya D. Shkredov Steklov Mathematical Institute (Russia)
ilya.shkredov@gmail.com

EDITORIAL BOARD

- Iskander Aliev Cardiff University (United Kingdom)
- Vladimir Dolnikov Moscow Institute of Physics and Technology (Russia)
- Nikolay Dolbilin Steklov Mathematical Institute (Russia)
- Oleg German Moscow Lomonosov State University (Russia)
- Michael Hoffman United States Naval Academy
- Grigory Kabatiansky Russian Academy of Sciences (Russia)
- Roman Karasev Moscow Institute of Physics and Technology (Russia)
- Gyula O. H. Katona Hungarian Academy of Sciences (Hungary)
- Alex V. Kontorovich Rutgers University (United States)
- Maxim Korolev Steklov Mathematical Institute (Russia)
- Christian Krattenthaler Universität Wien (Austria)
- Antanas Laurinčikas Vilnius University (Lithuania)
- Vsevolod Lev University of Haifa at Oranim (Israel)
- János Pach EPFL Lausanne (Switzerland) and Rényi Institute (Hungary)
- Rom Pinchasi Israel Institute of Technology – Technion (Israel)
- Alexander Razborov Institut de Mathématiques de Luminy (France)
- Joël Rivat Université d'Aix-Marseille (France)
- Tanguy Rivoal Institut Fourier, CNRS (France)
- Damien Roy University of Ottawa (Canada)
- Vladislav Salikhov Bryansk State Technical University (Russia)
- Tom Sanders University of Oxford (United Kingdom)
- Alexander A. Sapozhenko Lomonosov Moscow State University (Russia)
- József Solymosi University of British Columbia (Canada)
- Andreas Strömbergsson Uppsala University (Sweden)
- Benjamin Sudakov University of California, Los Angeles (United States)
- Jörg Thuswaldner University of Leoben (Austria)
- Kai-Man Tsang Hong Kong University (China)
- Maryna Viazovska EPFL Lausanne (Switzerland)
- Barak Weiss Tel Aviv University (Israel)

PRODUCTION

- Silvio Levy (Scientific Editor)
production@msp.org

Cover design: Blake Knoll, Alex Scorpan and Silvio Levy

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2020 is US \$310/year for the electronic version, and \$365/year (+\$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
 **mathematical sciences publishers**
nonprofit scientific publishing
<http://msp.org/>
© 2020 Mathematical Sciences Publishers

A dynamical Borel–Cantelli lemma via improvements to Dirichlet’s theorem	101
DMITRY KLEINBOCK and SHUCHENG YU	
Algebraic cryptanalysis and new security enhancements	123
VITALIĬ ROMAN’KOV	
On the behavior of power series with positive completely multiplicative coefficients	147
OLEG A. PETRUSHOV	
On the roots of the Poupard and Kreweras polynomials	163
FRÉDÉRIC CHAPOTON and GUO-NIU HAN	
Generalized colored circular palindromic compositions	173
PETROS HADJICOSTAS	
Square-full primitive roots in arithmetic progressions	187
VICHIAN LAOHAKOSOL, TEERAPAT SRICHAN and PINTHIRA TANGSUPPHATHAWAT	