Some Factorisation and Divisibility Properties of Catalan Polynomials

A. Frazer Jarvis, Peter J. Larcombe[†]

and

Eric J. Fennessey[‡]

Department of Pure Mathematics
Hicks Building, University of Sheffield, Sheffield S3 7RH, U.K.
{A.F.Jarvis@sheffield.ac.uk}

[†]School of Computing and Mathematics
University of Derby
Kedleston Road, Derby DE22 1GB, U.K.
{P.J.Larcombe@derby.ac.uk}

[‡]BAE Systems Integrated System Technologies
Broad Oak, The Airport, Portsmouth PO3 5PQ, U.K.
{Eric.Fennessey@baesystems.com}

Abstract

We present some factorisation and divisibility properties of Catalan polynomials. Initial results established with *ad hoc* proofs then make way for a more systematic approach and use of the well developed theory of cyclotomic polynomials.

1 Introduction

In [1, Section 5.1, pp.17-25] the essential mathematical properties of the so called Catalan polynomials were given, due in the main to known results on

Dickson and Chebyshev polynomials of the second kind (to which they are related; see Section 2.1 later). Various forms exist for the general $(n+1)$th Catalan polynomial $P_n(x)$: for $n \geq 0$ we have the binomial sum

$$P_n(x) = \sum_{i=0}^{\lfloor \frac{1}{2}n \rfloor} \binom{n-i}{i} (-x)^i \tag{1}$$

with hypergeometric form

$$P_n(x) = {}_2F_1\left(\left. \begin{matrix} -\frac{1}{2}n, -\frac{1}{2}(n-1) \\ -n \end{matrix} \right| 4x \right), \tag{2}$$

and the equivalent matrix forms

$$\begin{aligned} P_n(x) &= (\sqrt{x})^n (1, 1/\sqrt{x}) \begin{pmatrix} 0 & -1 \\ 1 & \frac{1}{\sqrt{x}} \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= (1,0) \begin{pmatrix} 1 & x \\ -1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{aligned} \tag{3}$$

Previous results involving Catalan polynomials may be seen in [1-3]. In terms of work conducted, a summary of their various contexts is given in the Introduction of an accompanying article (to this one) [4]. The first few polynomials are (factored where possible)

$$\begin{aligned} P_0(x) &= 1, \\ P_1(x) &= 1, \\ P_2(x) &= 1-x, \\ P_3(x) &= 1-2x, \\ P_4(x) &= 1-3x+x^2, \\ P_5(x) &= 1-4x+3x^2 = (1-x)(1-3x), \\ P_6(x) &= 1-5x+6x^2-x^3, \\ P_7(x) &= 1-6x+10x^2-4x^3 = (1-2x)(1-4x+2x^2), \\ P_8(x) &= 1-7x+15x^2-10x^3+x^4 = (1-x)(1-6x+9x^2-x^3), \\ P_9(x) &= 1-8x+21x^2-20x^3+5x^4 = (1-3x+x^2)(1-5x+5x^2), \\ P_{10}(x) &= 1-9x+28x^2-35x^3+15x^4-x^5, \\ P_{11}(x) &= 1-10x+36x^2-56x^3+35x^4-6x^5 \\ &= (1-x)(1-2x)(1-3x)(1-4x+x^2), \\ P_{12}(x) &= 1-11x+45x^2-84x^3+70x^4-21x^5+x^6, \\ P_{13}(x) &= 1-12x+55x^2-120x^3+126x^4-56x^5+7x^6 \\ &= (1-5x+6x^2-x^3)(1-7x+14x^2-7x^3), \end{aligned} \tag{4}$$

etc. The basic linear recurrence satisfied by the polynomials is

$$0 = xP_n(x) - P_{n+1}(x) + P_{n+2}(x); \qquad P_0(x) = P_1(x) = 1, \tag{5}$$

from which the closed form

$$P_n(x) = \frac{1}{2^{n+1}} \frac{(1+\sqrt{1-4x})^{n+1} - (1-\sqrt{1-4x})^{n+1}}{\sqrt{1-4x}} \tag{6}$$

follows readily. The bi-variate function

$$\frac{1}{1-t+xt^2} = \sum_{n=0}^{\infty} P_n(x)t^n \tag{7}$$

acts as an ordinary generating function for the polynomials; equations (5)-(7) are taken from [1, resp., (69),(70),(73), pp.17,19].

In this article we examine some factorisation and divisibility aspects of the Catalan polynomials. First, in Section 2, new results are established with *ad hoc* proofs constructed as appropriate. Section 3 then details a more systematic approach to their factorisation over **Z** and an appeal to the well developed theory of cyclotomic polynomials which together allow some interesting insights into the factorisation process; as a consequence, we are motivated to recover earlier results from Section 2. A Summary completes the paper.

2 New Results

Noting that the roots of all Catalan polynomials are real and positive (see the proof of Theorem 4 later), we establish the following result:

Theorem 1 *In seeking rational solutions x of the equation $P_n(x) = 0$ only the arguments $x = 1, \frac{1}{2}, \frac{1}{3}$ need be considered.*

Proof Let $x > \frac{1}{4}$ be rational, and let $\alpha(x) = 4x - 1 > 0$ so that $\sqrt{1-4x} = \sqrt{\alpha(x)}i$. Solving $0 = P_n(x)$ implies, from (6), the solution of

$$0 = (1+\sqrt{\alpha(x)}i)^{n+1} - (1-\sqrt{\alpha(x)}i)^{n+1}, \tag{P1}$$

or

$$1 = \left[\frac{1+\sqrt{\alpha(x)}i}{1-\sqrt{\alpha(x)}i}\right]^{n+1} = z^{n+1}(\alpha), \tag{P2}$$

say, where $z(\alpha) = \frac{1-\alpha}{1+\alpha} + \frac{2\sqrt{\alpha}}{1+\alpha}i$. In the complex plane z lies on the unit disc, and it is straightforward to show that $z(\alpha) = \exp[\theta(\alpha)i]$ with $\mathrm{Re}\{z(\alpha)\} = \cos(\theta(\alpha))$, $\mathrm{Im}\{z(\alpha)\} = \sin(\theta(\alpha))$ where

$$\theta(\alpha) = \cos^{-1}\left(\frac{1-\alpha}{1+\alpha}\right), \tag{P3}$$

so that (P2) reads

$$1 = \exp[(n+1)\theta(\alpha)i]. \tag{P4}$$

Thus, $(n+1)\theta(\alpha) = 2k\pi$ ($k \in \mathbf{Z}$) and we require to solve

$$r(\alpha) = \cos(q\pi) \tag{P5}$$

where $r(\alpha) = \frac{1-\alpha}{1+\alpha}$, $q = 2k/(n+1)$, $r, q \in \mathbf{Q}$. To proceed any further we need to apply the rather useful (and seemingly little known) result which is stated and proven below:

<u>Lemma 1</u> *Let $q, r \in \mathbf{Q}$. If $r = \cos(q\pi)$ then $r \in \{0, \pm\frac{1}{2}, \pm 1\}$.*

<u>Proof</u> We firstly account for a few specific instances of q values to aid the proof. Let $\mathcal{S} = \{0, \pm\frac{1}{2}, \pm 1\}$. Consider (i) $q = 0 \in \mathbf{Q} \Rightarrow r = \cos(0) = 1 \in \mathcal{S}$. Next, suppose $q \in \mathcal{Q} = \{\ldots, -\frac{5}{2}, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots\} = \{k + \frac{1}{2} : k \in \mathbf{Z}\}$. We know that $\cos(\theta\pi) = 0$ iff $\theta \in \mathcal{Q}$, so that (ii) if $q \in \mathcal{Q} \subset \mathbf{Q}$ then $r = \cos(q\pi) = 0 \in \mathcal{S}$.

Now (iii) fix $q \in \mathbf{Q}\backslash\{\mathcal{Q} \cup \{0\}\}$ such that $\cos(q\pi) \in \mathbf{Q}$. We show, noting $\cos(q\pi) \neq 0$ in this instance, that it follows that $\cos(q\pi) = \pm\frac{1}{2}, \pm 1$ to complete the solution set $\mathcal{S}$. To do this we write $q = s/t$ and $2\cos(q\pi) = a/b$, each in its lowest (irreducible) form ($a, b, s, t \in \mathbf{Z}$). The elementary identity $\cos(2x) = 2\cos^2(x) - 1$ gives

$$\begin{aligned} 2\cos(2q\pi) &= 4\cos^2(q\pi) - 2 \\ &= \left(\frac{a}{b}\right)^2 - 2 \\ &= \frac{a^2 - 2b^2}{b^2} \\ &= \frac{u}{v}, \end{aligned} \tag{L1}$$

say. We show the ratio u/v is in its lowest form by assuming the contrary and seeing that this leads to a contradiction. If u/v is reducible there is a prime p which divides both u and v. If $p|v = b^2$ then (a) $p|b$ trivially. Furthermore, if $p|u$ then, mod p, $u = a^2 - 2b^2 \equiv 0$ whence (since $b^2 \equiv$

0) $a^2 \equiv 0$ so that (b) $p|a$. Deductions (a),(b) are a contradiction of the assumption that a/b is irreducible. Having established that u/v is in its lowest form, we suppose (for the purpose of the proof in deriving a further contradiction) that $|b| > 1$, allowing us to write

$$\text{den}\{2\cos(2q\pi)\} \;=\; b^2 \;>\; b \;=\; \text{den}\{2\cos(q\pi)\}, \tag{L2}$$

where "den" denotes "denominator". Now, using (L1) above,

$$\begin{aligned} 2\cos(4q\pi) &= [2\cos(2q\pi)]^2 - 2 \\ &= \left(\frac{u}{v}\right)^2 - 2 \\ &= \frac{(a^2 - 2b^2)^2 - 2b^4}{b^4} \end{aligned} \tag{L3}$$

(which, by an argument similar to that just made, is itself irreducible), and we have

$$\text{den}\{2\cos(4q\pi)\} \;=\; b^4 \;>\; b^2 \;=\; \text{den}\{2\cos(2q\pi)\}. \tag{L4}$$

Repeating the process we arrive at the series of inequalities

$$\begin{aligned} b^1 &= \text{den}\{2\cos(2^0 q\pi)\} \\ &< b^2 = \text{den}\{2\cos(2^1 q\pi)\} \\ &< b^4 = \text{den}\{2\cos(2^2 q\pi)\} \\ &< \cdots \\ &< b^{2^n} = \text{den}\{2\cos(2^n q\pi)\}, \end{aligned} \tag{L5}$$

etc., and we have the following: that the sequence $\{\text{den}\{2\cos(2^n q\pi)\}\}_{n=0}^{\infty}$ comprising the denominators of terms (in irreducible form) $2\cos(2^n q\pi)$ is strictly increasing, taking, therefore, an infinite number of distinct values. However, writing $s/t = q = q(t;s) = q(t)$ it is easy to see that $\forall m \in \mathbf{Z}$ the angle $mq(t)\pi$ satisfies the equivalence relation

$$mq(t)\pi \equiv \beta(t) \qquad (\text{mod } 2\pi) \tag{L6}$$

for some element $\beta(t) \in \mathcal{B}(t)$, $\mathcal{B}(t)$ being the finite set $\mathcal{B}(t) = \{(i/t)\pi : i = 0, 1, 2, \ldots, 2t-1\}$.[1] In other words, for a given $m \in \mathbf{Z}$ there exists a rational multiple of π – $\beta(t) \in \mathcal{B}(t)$ – such that $\cos(mq(t)\pi) = \cos(\beta(t))$.

[1]Perhaps an example or two is in order here (congruences are mod 2π): (I) $m = 3$, $q = q(7;1) = q(7) = 1/7$: then $mq(t)\pi = 3\pi/7 \equiv 3\pi/7 = \beta(7) \in \mathcal{B}(7) = \{0, \pi/7, 2\pi/7, \ldots, 13\pi/7\}$. (II) $m = 6$, $q = q(3;2) = q(3) = 2/3$: then $mq(t)\pi = 4\pi \equiv 0 = \beta(3) \in \mathcal{B}(3) = \{0, \pi/3, 2\pi/3, \ldots, 5\pi/3\}$. (III) $m = -4$, $q = q(9;2) = q(9) = 2/9$: then $mq(t)\pi = -8\pi/9 \equiv 10\pi/9 = \beta(9) \in \mathcal{B}(9) = \{0, \pi/9, 2\pi/9, \ldots, 17\pi/9\}$.

Noting that
$\{\cos(2^n q(t)\pi$
$\beta(t) \in \mathcal{B}(t)\}$,
$n = 0, 1, 2, .$
values which
inequalities

The proof is
and in turn
$a = \pm 1, \pm 2,$

The proof o
$r(\alpha) = \frac{1-\alpha}{1+\alpha}$
turn $x(\alpha) =$

Remark 1 In
consider $x \in$
$P_n(0) = 1 \neq$
remaining in
equation
no solutions
mean that

Having show
$1, \frac{1}{2}, \frac{1}{3}$, we s
with these r

These have
sults), and
equations (
polynomials
of this by lis

Noting that the set $\{2^n : n = 0,1,2,\ldots\}$ is a subset of $\mathbf{Z}$, it follows that $\{\cos(2^n q(t)\pi) : n = 0,1,2,\ldots\} \subset \{\cos(mq(t)\pi) : m \in \mathbf{Z}\} = \{\cos(\beta(t)) : \beta(t) \in \mathcal{B}(t)\}$, meaning that the reduced elements of the set $\{\cos(2^n q(t)\pi) : n = 0,1,2,\ldots\}$ (it being a finite one) can only attain a finite number of values which will necessarily contain a maximum value; *this contradicts the inequalities (L5) and the subsequent summary statement.*

The proof is concluded quickly, for since $|b| \not> 1$ we must have $b = \pm 1$, and in turn $\cos(q\pi) = \frac{a}{2b} = \pm\frac{1}{2}a$. The only valid values for $a \in \mathbf{Z}$ are $a = \pm 1, \pm 2$, for which $\cos(q\pi) = \pm\frac{1}{2}, \pm 1$ as required.□

The proof of Theorem 1 is itself now readily completed too, for setting $r(\alpha) = \frac{1-\alpha}{1+\alpha} = 0, \frac{1}{2}, -\frac{1}{2}, 1, -1$ yields just four solutions $\alpha = 1, \frac{1}{3}, 3, 0$, and in turn $x(\alpha) = \frac{1}{4}(\alpha+1) = \frac{1}{2}, \frac{1}{3}, 1, \frac{1}{4}$ (which latter value we discount).□

Remark 1 In the search for rational roots x of $P_n(x)$ we do not need to consider $x \in [0, \frac{1}{4}]$ for the following reasons. Firstly, $x \neq 0, \frac{1}{4}$ since $\forall n \geq 0$ $P_n(0) = 1 \neq 0$ and [1, Remark 2, p.18] $P_n(\frac{1}{4}) = (n+1)2^{-n} \neq 0$. Over the remaining interval $x \in (0, \frac{1}{4})$ then any roots correspond to solutions of the equation $[\frac{1+r(x)}{1-r(x)}]^{n+1} = 1$, where $r(x) = \sqrt{1-4x} > 0$. There are, however, no solutions since the inequalities $1 < 1 + r(x) < 2$ and $0 < 1 - r(x) < 1$ mean that $\frac{1+r(x)}{1-r(x)} > 1$.

Having shown that the only rational roots of the Catalan polynomials are $1, \frac{1}{2}, \frac{1}{3}$, we subsequently find easily those particular polynomials associated with these roots; for $n = 0,1,2,\ldots$,

$$P_{3n+2}(1) \;=\; P_{4n+3}\left(\frac{1}{2}\right) \;=\; P_{6n+5}\left(\frac{1}{3}\right) \;=\; 0. \qquad (8)$$

These have been verified computationally (along with all other main results), and we leave their derivation as a simple reader exercise. The first of equations (8) implies, for instance, that any run of six consecutive Catalan polynomials contains a pair with a common root of 1; we can see examples of this by listing (to 5 d.p.) the root sets for polynomials $P_2(x), \ldots, P_{11}(x)$:

$$\begin{aligned}
P_2(x) &: \{\mathbf{1.0000}\},\\
P_3(x) &: \{0.5000\},\\
P_4(x) &: \{0.3820, 2.6180\},\\
P_5(x) &: \{0.3333, \mathbf{1.0000}\},\\
P_6(x) &: \{0.3080, 0.6431, 5.0489\},\\
P_7(x) &: \{0.2929, 0.5000, 1.7071\},
\end{aligned}$$

$$\begin{aligned}
P_8(x) &: \{0.2831, 0.4260, \mathbf{1.0000}, 8.2909\}, \\
P_9(x) &: \{0.2764, 0.3820, 0.7236, 2.6180\}, \\
P_{10}(x) &: \{0.2716, 0.3533, 0.5830, 1.4487, 12.3435\}, \\
P_{11}(x) &: \{0.2679, 0.3333, 0.5000, \mathbf{1.0000}, 3.7321\}.
\end{aligned} \tag{9}$$

Runs of four or five polynomials may (*e.g.*, $P_8(x), \ldots, P_{11}(x)$ or $P_5(x), \ldots, P_9(x)$) or may not (*e.g.*, $P_3(x), \ldots, P_6(x)$ or $P_6(x), \ldots, P_{10}(x)$) contain such a pair. Runs of three or less won't. Similar statements can be made concerning runs of polynomials possessing (or not) pairs of the other roots $\frac{1}{2}$ and $\frac{1}{3}$.

Theorem 2 *For $n \geq 2$ any consecutive triplet of Catalan polynomials $P_n(x), P_{n+1}(x), P_{n+2}(x)$ has pairwise distinct sets of roots.*

Proof First note once more that all roots of all polynomials are non-zero. Suppose a polynomial pair within any given triplet possesses a common root. We show that this implies two consecutive polynomials have that common root also, which in turn leads to a contradiction.

Let the pair be $P_n(x), P_{n+1}(x)$, or $P_{n+1}(x), P_{n+2}(x)$. Since each pair consists of consecutive polynomials, we are done trivially. If the pair is $P_n(x)$ and $P_{n+2}(x)$, with non-zero common root $x = a$, say, then the linear recurrence (5) reads, at $x = a$, $0 = aP_n(a) - P_{n+1}(a) + P_{n+2}(a) = -P_{n+1}(a)$, so that a is also a root of $P_{n+1}(x)$ and we have that $P_n(x), P_{n+1}(x)$ are a consecutive pair with common root a.[2] With $P_n(a) = P_{n+1}(a) = 0$ then shifting the index of the recurrence (5) via $n \to n-1$ throughout, and evaluating at $x = a$ again, we obtain $0 = aP_{n-1}(a) - P_n(a) + P_{n+1}(a) = aP_{n-1}(a)$, whence a is a root of $P_{n-1}(x)$. Thus, we have established the following: if $P_n(x), P_{n+1}(x)$ are a consecutive polynomial pair with common root $x = a$ then it is also a root of $P_{n-1}(x)$. We can sequentially work this deduction backwards to the point where $P_3(x), P_4(x)$ are a consecutive pair with common root a, so that $P_2(x)$ also has root a. However (5) now yields $0 = aP_1(a) - P_2(a) + P_3(a) = aP_1(a) = a \neq 0$ by assumption, a contradiction.□

Theorem 3 *For $n \geq 0$, $k \geq 2$, the polynomial $P_k(x)$ divides $P_{(k+1)n+k}(x)$.*

Proof Consider the identity

$$P_{r+s}(x) = P_r(x)P_s(x) - xP_{r-1}(x)P_{s-1}(x), \qquad r, s \geq 1, \tag{P6}$$

[2] As indeed are $P_{n+1}(x), P_{n+2}(x)$; the argument which results in the contradiction can, of course, equally be started with this pair.

first given in [1, (82), p.22], which reads

$$\frac{P_{m+k+1}(x)}{P_k(x)} = P_{k+1}(x)\frac{P_m(x)}{P_k(x)} - xP_{m-1}(x) \tag{P7}$$

on setting $r = k+1$, $s = m$ and dividing throughout by $P_k(x) \neq 0$. Suppose $P_k(x)|P_m(x)$ $(k, m \geq 2)$, so that $P_m(x)/P_k(x) \in \mathbf{Z}[x]$. Then evidently, by (P7), $P_{m+k+1}(x)/P_k(x) \in \mathbf{Z}[x]$ and we have that the divisibility of $P_m(x)$ by $P_k(x)$ is sufficient for the divisibility of $P_{m+k+1}(x)$ by $P_k(x)$, which in turn is sufficient for the divisibility of $P_{m+2(k+1)}(x)$ by $P_k(x)$, *etc.* Thus, we see that if $P_k(x)$ divides $P_m(x)$ it follows that $P_k(x)$ divides $P_{m+n(k+1)}(x)$ for $n \geq 0$. Since $P_k(x)$ divides itself we can set $m = k$ and the result is established.□

Remark 2 Theorem 3, with $n = 1$, gives that $P_k(x)$ divides $P_{2k+1}(x)$ for $k \geq 2$, which was noted as part of Properties (c) of [1, p.22; see (85)].

Corollary *For $n \geq 4$, then if $n+1$ is composite $P_n(x)$ is composite.*

Proof By Theorem 3 $P_k(x)$ divides $P_{(k+1)m+k}(x)$ for $m \geq 0$, $k \geq 2$. Consider integers n_1, n_2 such that $n_1 > n_2 \geq 2$, and set $k = n_1 - 1 > 1$, $m = n_2 - 1 \geq 1 \geq 0$, so we have that the polynomial $P_{n_1-1}(x)$ divides $P_{n_1 n_2 - 1}(x)$. However, since the smallest value of $n \geq 4$ for which $n+1$ is composite is $n = 5$ then we can write, provided it is not the square of an odd prime, $n+1$ as the product $n+1 = n_1 n_2$ (≥ 6), whence $P_{n_1-1}(x)$ divides $P_n(x)$; the proof is completed by noting that $P_{n_1-1}(x)$ is a proper polynomial ($n_1 - 1 > 1$, as seen, and $P_2(x) = 1 - x$ is, after the trivial ones $P_0(x) = P_1(x) = 1$, the first proper polynomial which appears in the list (4)), so that $P_n(x)$ has a proper polynomial divisor and is, therefore, composite. The case when, for prime $p \geq 3$, $n+1 = p^2$ is accommodated with the same line of argument with $n_1 = n_2 = p$.□

Theorem 4 *For $n \geq 2$, then if $n+1$ is prime $P_n(x)$ is irreducible.*[3]

Proof We begin with the statement and proof of a lemma:

Lemma 2 *Let α be an algebraic integer of degree n. Then, for $k \in \mathbf{Z}$, $k + \alpha$ is an algebraic integer of degree n.*

Proof Since α is an algebraic integer of degree n there exists a monic polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbf{Z}[x] \setminus \{0\}$, of

[3] Observed empirically in [1, Properties (c), p.22].

minimum degree n, such that $f(\alpha) = 0$. Note that $f(x)$ is monic since $[x^n]\{f(x)\} = 1$. To prove Lemma 2 simply define a degree n polynomial $g(x) = a_0 + a_1(x-k) + a_2(x-k)^2 + \cdots + a_{n-1}(x-k)^{n-1} + (x-k)^n \in \mathbf{Z}[x]\backslash\{0\}$. Since $g(k+\alpha) = f(\alpha) = 0$ then $k+\alpha$ is an algebraic integer of degree at most n. If its degree were (strictly) less than n we could apply the argument again to show that α has degree strictly less than n, which is a contradiction; hence, $k+\alpha$ is an algebraic integer of degree n.□

Noting that we use the terms "degree" and "order" interchangably the proof of Theorem 4 is as follows, for which we need to first introduce some precise terminology. Let $f(x)$ be a non-constant polynomial $\in \mathbf{Z}[x]$ of order $o(f)$, say. We call $f(x)$ *virtually monic* if the highest power of x has a coefficient of magnitude 1, *i.e.*, $[x^{o(f)}]\{f(x)\} = \pm 1$. We call $f(x)$ *virtually monic at both ends* if it is virtually monic and $[x^0]\{f(x)\} = \pm 1$. If a polynomial is virtually monic at both ends then it is virtually monic. A non-constant polynomial $f(x) \in \mathbf{Z}[x]$ of order $o(f)$ has a *dual* $f^*(x)$, of order $o(f)$ similarly (provided $0 \neq [x^0]\{f(x)\}$), defined as $f^*(x) = x^{o(f)} f(\frac{1}{x})$. Clearly, if $f(x)$ is virtually monic at both ends then so is its dual.

We establish the result by contradiction, assuming in the first instance that $P_n(x)$ is reducible. Noting that since n is even ($n+1$ is prime), $o(P_n(x)) = \frac{1}{2}n$ and we write $P_n(x) = T(x)U(x)$, where $T(x), U(x) \in \mathbf{Z}[x]$ are non-constant polynomials with $o(T) + o(U) = \frac{1}{2}n$. Further, from (1) $[x^0]\{P_n(x)\} = 1$, whilst $[x^{o(P_n(x))}]\{P_n(x)\} = [x^{\frac{1}{2}n}]\{P_n(x)\} = (-1)^{\frac{1}{2}n} = \pm 1$, so that $P_n(x)$ is virtually monic at both ends. Hence, both $T(x)$ and $U(x)$ must be virtually monic at both ends, and so each of the duals $T^*(x)$ and $U^*(x)$ are virtually monic at both ends, and so virtually monic. Consider now

$$x^{\frac{1}{2}n} P_n(1/x) = x^{o(T)} T(1/x) \cdot x^{o(U)} U(1/x), \tag{P8}$$

and let ρ be a root of $P_n(x)$ ($\rho \neq 0$; we know from [1] that the roots of $P_n(x)$ are all positive (see (P10) below)). Then using the decomposition (P8) in reverse,

$$\left(\frac{1}{\rho}\right)^{o(T)} T(\rho) \cdot \left(\frac{1}{\rho}\right)^{o(U)} U(\rho) \;=\; \left(\frac{1}{\rho}\right)^{\frac{1}{2}n} P_n(\rho) \;=\; 0. \tag{P9}$$

Thus, $1/\rho$ is a root of either $T^*(x)$ or $U^*(x)$. This means, therefore, that $1/\rho$ is a root of a virtually monic polynomial, and (multiplying throughout (P9) by -1 if necessary) so a root of a monic polynomial of individual degree $< \frac{1}{2}n$. In other words, $1/\rho$ is an algebraic integer of degree $< \frac{1}{2}n$.

The roots of $P_n(x)$ are given generally by [1, (97), p.25]

$$x_{\lambda(n)} = \frac{1}{2}\frac{1}{1+\cos(\theta(\lambda))}, \tag{P10}$$

where $\theta(\lambda) = 2\pi\lambda/(n+1)$ and λ takes values $\lambda = 1, 2, \ldots, n$ (excluding any value for which $2\lambda = n+1$). At least one value of $\lambda(n)$ must describe a root $x_{\lambda(n)}$ which corresponds to ρ, whence

$$2 + 2\cos\left(\frac{2\pi\lambda}{n+1}\right) = \frac{1}{\rho} \tag{P11}$$

is an algebraic integer of degree $< \frac{1}{2}n$, a deduction for which we now provide an immediate contradiction. Since $n+1$ is prime each ratio $\lambda/(n+1)$ is in its simplest form, and by a result due to Lehmer [5, Theorem 1, p.165] $2\cos[2\pi\lambda/(n+1)]$ is an algebraic integer of degree $\frac{1}{2}\phi(n+1)$, where $\phi(n)$ is Euler's so called totient function which enumerates the number of integers $d \in [1, n]$ that are coprime to n ($d = 1$ is regarded as coprime to all $n \geq 1$). With $n+1$ prime here, $\phi(n+1) = n$ trivially and we have that $2\cos[2\pi\lambda/(n+1)]$ is an algebraic integer of degree $\frac{1}{2}n$, which is also the degree of the algebraic integer $2 + 2\cos[2\pi\lambda/(n+1)]$ by Lemma 2, yielding the required contradiction on the assumed reducibility of $P_n(x)$.□

2.1 Catalan and Chebyshev/Dickson Polynomials: Some Remarks

It was noted in [1, (71),(72), p.18] that the general Chebyshev polynomial of the second kind

$$U_n(x) = \frac{1}{2}\frac{(x+\sqrt{x^2-1})^{n+1} - (x-\sqrt{x^2-1})^{n+1}}{\sqrt{x^2-1}} \tag{10}$$

(which is, in turn, the instance $E_n(2x, 1)$ of the general two parameter Dickson polynomial (of the second kind) $E_n(x,a) = \sum_{i=0}^{\lfloor \frac{1}{2}n \rfloor} \binom{n-i}{i}(-a)^i x^{n-2i}$) is, for $n \geq 0$, related to the corresponding Catalan polynomial according to

$$P_n(x) = (\sqrt{x})^n U_n\left(\frac{1}{2\sqrt{x}}\right). \tag{11}$$

Existing results for Chebyshev/Dickson polynomials can, therefore, be translated in principle directly to statements for Catalan polynomials.[4] Property 3 of [7, p.1234], for instance, states that if $l \geq 1$ is integer s.t. $m =$

[4] It is known, for example, that the degree n integral polynomial $U_n(x)$ has roots which are real, distinct, symmetric about $x = 0$ and of the form $\cos[k\pi/(n+1)]$ ($k = 1, \ldots, n$), from which those of $P_n(x)$ follow readily; other properties were listed in [1, Sections 5.1.3 and 5.1.5, pp.18-20,21-25] based on stand alone arguments, and results taken from [6].

$(n+1)l-1$, then $U_n(x)|U_m(x)$; setting $m=(p+1)k+p$, $n=k$, and replacing $U_k(x)$ by $P_k(x)$, then for $p=0,1,2,\ldots$, this reads as our Theorem 3. The proof, however, relies on a mixed recurrence involving Chebyshev polynomials of both first and second kind (in contrast to our proof), and other work in [7] on Chebyshev polynomials is not re-interpreted here in the context of Catalan polynomials.[5] Instead, in what follows next we will leave our results and *ad hoc* proofs as they are and rather than appealing to work elsewhere on Chebyshev (or Dickson) polynomials bring to bear on the question of factorisation of Catalan polynomials a more formalised approach and an application of the theory of cyclotomic polynomials underpinned by the properties of ordinary and primitive roots of unity; in doing so, we find we are also able to recover Theorems 2,3 and 4.

3 Cyclotomic Polynomials: Theory and Application

3.1 Fundamental Features

We begin by giving a quick reminder of the essential features of cyclotomic polynomials (see also Footnote 10 later) before we apply them to the task in hand, providing illustrative examples.

We recall that an (ordinary) nth root of unity r, say, is a so called *primitive* nth root if, for $k=1,\ldots,n$, $k=n$ is the smallest value of k for which $r^k=1$. Thus, we see trivially that 1 is the primitive first root of unity, whilst -1 is the primitive square root of unity. In addition, $\omega_{a,b}=\frac{1}{2}(-1\pm\sqrt{3}\,i)$ are each primitive cube roots of unity. The primitive fourth roots of unity are immediate as $\pm i$, whilst there are 4 primitive fifth roots of unity, being those complex ordinary fifth roots (writing these as $\rho_1,\ldots,\rho_4$ for the moment, they are given explicitly in Section 3.3). The 6 ordinary roots of unity are seen to be $\pm 1, \pm\omega_{a,b}$, delivering just $-\omega_{a,b}$ as the two primitive sixth roots; the process continues. For nth roots of unity $\xi_1,\ldots,\xi_n$, say, the nth cyclotomic polynomial $\Phi_n(x)$ is, for $n\geq 1$, defined as

$$\Phi_n(x)=\prod_{\substack{\text{primitive } \xi_k \\ k=1}}^{n}(x-\xi_k), \tag{12}$$

[5] See Theorem 4 therein (p.1235) which gives a result on the greatest common divisor between two Chebyshev polynomials $U_n(x), U_m(x)$, and the subsequent section on modular factorisation which—as a topic of potential interest in the context of Catalan polynomials—lies beyond the scope of this paper. Chapter 5 of the book by Rivlin [8] is another obvious source of (potentially transferable) results on Chebyshev polynomials.

and we now list $\Phi_1(x), \ldots, \Phi_6(x)$ as examples. Denoting by ω either one of the primitive cube roots $\omega_{a,b}$, we write

$$\begin{aligned}
\Phi_1(x) &= x-1, \\
\Phi_2(x) &= x-(-1) \;=\; x+1 \;=\; (x^2-1)/(x-1), \\
\Phi_3(x) &= (x-\omega_a)(x-\omega_b) \\
&= (x-\omega)(x-\omega^2) \;=\; x^2+x+1 \;=\; (x^3-1)/(x-1), \\
\Phi_4(x) &= (x-i)(x-(-i)) \;=\; x^2+1, \\
\Phi_5(x) &= (x-\rho_1)(x-\rho_2)(x-\rho_3)(x-\rho_4) \\
&= x^4+x^3+x^2+x+1 \;=\; (x^5-1)/(x-1), \\
\Phi_6(x) &= (x-(-\omega_a))(x-(-\omega_b)) \\
&= (x+\omega)(x+\omega^2) \;=\; x^2-x+1, \qquad (13)
\end{aligned}$$

where we have taken advantage of the fact that $\omega_{a,b}^2 = \omega_{b,a}$ and $\omega_{a,b}^2 + \omega_{a,b} = -1$. Note that $\Phi_p(x) = (x^p-1)/(x-1) = x^{p-1} + x^{p-2} + \cdots + x + 1$ for p prime since observing that it holds when $p = 2$ – in every other case (*i.e.*, p odd) then aside from unity itself all other $p-1$ ordinary complex roots of unity are themselves primitive pth roots.

In general, an nth root of unity $\exp(2m\pi i/n)$ is a primitive nth root whenever $m = 0, \ldots, n-1$ and n are coprime. Thus, the number $\phi(n)$ of primitive nth roots of unity is given by the cardinality of the set $\{m \in [0, n-1] : m, n \text{ are coprime}\}$, from which it follows that $\deg\{\Phi_n(x)\} = \phi(n)$. More interestingly, it can be shown that $n = \sum_{d|n\,(1 \le d \le n)} \phi(d)$ (for example, $12 = 1+1+2+2+2+4 = \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = \sum_{d|12} \phi(d)$), along with the result[6]

$$x^n - 1 = \prod_{d|n\,(1 \le d \le n)} \Phi_d(x), \qquad n \ge 1, \qquad (14)$$

which (given $\Phi_1(x)$) allows an inductive computation of cyclotomic polynomials through the re-arrangement

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n\,(d \ne n)} \Phi_d(x)}, \qquad n \ge 2. \qquad (15)$$

It is easy to check, for instance, that $x^3 - 1 = \Phi_1(x)\Phi_3(x)$ and $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$. Equation (14), then, tells us that for $n \ge 2$ the n roots of unity are simply those roots of the polynomial $\prod_{d|n} \Phi_d(x)$ which

[6] The proof of (14) is simple; an nth root of unity will be a primitive dth root for some $d|n$, whilst, conversely, if $d|n$ then a primitive dth root of unity is an nth root of unity.

contains, as factors, cyclotomic polynomials formed from primitive roots of unity. In other words, any nth root of unity co-incides with a primitive dth root of unity for some divisor d of n. Note that all cyclotomic polynomials are monic with integer coefficients (this is straightforward to establish) and, further, that since $\Phi_n(x)$ is irreducible in the polynomial ring $\mathbf{Q}[x]$ ($\forall n \geq 1$; see Eisenstein's Irreducibility Criterion) then it is the minimal polynomial of any primitive nth root of unity.

3.2 Connecting Cyclotomic and Catalan Polynomials

Consider $\zeta = \zeta(x)$ defined as

$$\zeta(x) = \frac{1 + \sqrt{1-4x}}{1 - \sqrt{1-4x}}. \tag{16}$$

With a little algebra we find, from (16), the reverse relation

$$x(\zeta) = \frac{\zeta}{(\zeta+1)^2}. \tag{17}$$

By (6) it is clear that solving the equation $P_n(x) = 0$ is equivalent to solving $\zeta^{n+1}(x) = 1$. Now, whilst $\zeta = 1$ is an $(n+1)$th root of unity, we discount this value since it corresponds to $x(1) = \frac{1}{4}$ which is never a Catalan polynomial root (it is known (see Remark 1 earlier) that $P_n(\frac{1}{4}) = (n+1)/2^n \neq 0$). In addition, for n odd then $\zeta = -1$ is an $(n+1)$th root of unity but this too is discounted since the value corresponds to $x(-1) = -\infty$. Thus *we conclude that $\zeta = \zeta(x) \neq \pm 1$ is a root of the polynomial $\zeta^{n+1} - 1 = \prod_{d|n+1} \Phi_d(x)$ iff $x = x(\zeta)$ is a root of the Catalan polynomial $P_n(x)$*, an observation that we can now apply.

3.3 Application

We are now in a position to apply the above in search of Catalan polynomial factors, and we illustrate this with some examples- initially low level ones.

<u>Case $n = 1$</u> Here $n + 1 = 2$, and the solutions of $1 = \zeta^2$ are $\zeta = \pm 1$, both of which we discount. The Catalan polynomial $P_1(x)$ has, therefore, no roots/factors, which is correct since $P_1(x) = 1$.

<u>Case $n = 2$</u> Here $n + 1 = 3$, and the solutions of $1 = \zeta^3$ are $\zeta = 1$ (discounted) and $\zeta = \omega_{a,b} = \frac{1}{2}(-1 \pm \sqrt{3}i)$ given earlier. Both values are

dealt with simultaneously by observing that $(1+\zeta)^2 = (1+\omega_{a,b})^2 = (1+\omega_{a,b}+\omega_{a,b}^2)+\omega_{a,b} = 0+\omega_{a,b} = \omega_{a,b} = \zeta$, so that $x(\zeta) = \zeta/(1+\zeta)^2 = 1$ which confirms that the Catalan polynomial $P_2(x) = 1-x$ has but a single root of 1.

<u>Case $n = 3$</u> This case is similar to the previous one in that the solutions $\zeta = \pm i$ of $1 = \zeta^4$ (discounting the other two solutions $\zeta = \pm 1$) each have the property that $(1+\zeta)^2 = 2\zeta$, giving $x(\zeta) = \zeta/(1+\zeta)^2 = \frac{1}{2}$ as the correct sole root of $P_3(x) = 1-2x$.

<u>Case $n = 4$</u> We solve $1 = \zeta^5$, discounting the root $\zeta = 1$. The complex pairs $\rho_{1,2} = \frac{1}{4}[(\sqrt{5}-1) \pm \sqrt{10+2\sqrt{5}}\,i]$ and $\rho_{3,4} = \frac{1}{4}[(-\sqrt{5}-1) \pm \sqrt{10-2\sqrt{5}}\,i]$ complete the root set. It is found, with a little work, that setting $\zeta = \rho_{1,2}$ yields one root of $P_4(x)$ as $x(\zeta) = \zeta/(1+\zeta)^2 = 2/(3+\sqrt{5})$, whilst setting $\zeta = \rho_{3,4}$ produces the other root $x(\zeta) = 2/(3-\sqrt{5})$. Thus, $P_4(x)$ may be constructed as $P_4(x) = (x - \frac{2}{3+\sqrt{5}})(x - \frac{2}{3-\sqrt{5}}) = 1 - 3x + x^2$.

<u>Case $n = 5$</u> The solutions of $1 = \zeta^6$ are, from earlier, known to be ± 1 (discounted) together with $\pm\omega_{a,b}$. With $\zeta = \omega_{a,b}$ then $x(\zeta) = 1$ (by the Case $n = 2$), whilst putting $\zeta = -\omega_{a,b}$ gives $(1+\zeta)^2 = (1-\omega_{a,b})^2 = (1+\omega_{a,b}+\omega_{a,b}^2) - 3\omega_{a,b} = 0 - 3\omega_{a,b} = -3\omega_{a,b} = 3\zeta$, so that $x(\zeta) = \frac{1}{3}$. These two roots of $P_5(x) = (1-x)(1-3x)$ are indeed correct.

<u>Case $n = 6$</u> We discount the unity solution of $1 = \zeta^7$, with factors generated by the conjugate pairs $\zeta = \gamma_{1,2} = \cos(2\pi/7) \pm i\sin(2\pi/7)$, $\zeta = \gamma_{3,4} = -\cos(3\pi/7) \pm i\sin(3\pi/7)$ and $\zeta = \gamma_{5,6} = -\cos(\pi/7) \pm i\sin(\pi/7)$. These pairs result in values $x(\gamma_{1,2}) = [1+\cos(2\pi/7)]/[3+4\cos(2\pi/7) - \cos(3\pi/7)] = 0.307979$, $x(\gamma_{3,4}) = [1-\cos(3\pi/7)]/[3-4\cos(3\pi/7) - \cos(\pi/7)] = 0.643104$, and $x(\gamma_{5,6}) = 1/2[1-\cos(\pi/7)] = 5.048917$, with (subject to roundoff error) $(0.307979 - x)(x - 0.643104)(x - 5.048917) = 1 - 5x + 6x^2 - x^3 = P_6(x)$. The values given here were determined by use of Maple.

<u>Case $n = 7$</u> Discounting the solutions ± 1 of $1 = \zeta^8$, the solution pair $\pm i$ generates the factor $1 - 2x$ of $P_7(x)$ (see Case $n = 3$). The remaining two conjugate pairs are $\zeta = (1 \pm i)/\sqrt{2}$ and $\zeta = (-1 \pm i)/\sqrt{2}$ which pairwise yield values $x(\zeta) = 1/(2 \pm \sqrt{2})$ and, in turn (up to a multiplicative constant), the quadratic factor $1 - 4x + 2x^2$; we have, therefore, the factorisation $P_7(x) = (1-2x)(1-4x+2x^2)$.

<u>Remark 3</u> It is of course known that if, for $m \in [0, n-1]$, $\zeta = \exp(2m\pi i/n)$ is an nth root of unity, then so is $1/\zeta$. The reason why—as seen in the examples above—conjugate pairs of roots of unity correspond to the *same*

Catalan polynomial root value is simply because in this instance, by (17), $x(\zeta) = x(\frac{1}{\zeta})$.

Remark 4 It is clear that for odd $n \geq 1$ the (even) $n+1$ associated roots of unity contain ± 1 which, when discounted, leaves $\frac{1}{2}(n-1)$ complex conjugate pairs of solutions, each pair giving a root of the polynomial $P_n(x)$ whose degree is $\frac{1}{2}(n-1)$. For even $n \geq 2$ the (odd) $n+1$ associated roots of unity contain 1 (discounted), leaving $\frac{1}{2}n$ complex conjugate solution pairs to each yield a root of the polynomial $P_n(x)$ of degree $\frac{1}{2}n$. This confirms the order of $P_n(x)$, as dependent on the parity of n, which is clear from (1).

Thus far we have not utilised the connection between Catalan and cyclotomic polynomials through the notion of a primitive root of unity. In considering Catalan polynomial factorisation the following examples show how this can be done, moving from what with increasing n would otherwise be an evermore burdensome route —reliant strongly on numerical approximations of roots of unity— to a more manageable algebraic one which appeals to the theory of cyclotomic polynomials in general, and also to the observation in particular that, from (16),

$$\begin{aligned}\zeta(x) + \frac{1}{\zeta(x)} &= \frac{1+\sqrt{1-4x}}{1-\sqrt{1-4x}} + \frac{1-\sqrt{1-4x}}{1+\sqrt{1-4x}} \\ &= \frac{1}{x} - 2, \end{aligned} \tag{18}$$

so that, in addition to (17), we have $x(\zeta) = (\zeta + \frac{1}{\zeta} + 2)^{-1}$.

Case $n = 11$ Consider the equation

$$\begin{aligned} 0 \;=\; \zeta^{12} - 1 &= \prod_{d|12} \Phi_d(\zeta) \\ &\Phi_1(\zeta)\Phi_2(\zeta)\Phi_3(\zeta)\Phi_4(\zeta)\Phi_6(\zeta)\Phi_{12}(\zeta). \end{aligned} \tag{19}$$

Now the roots of $\Phi_1(\zeta), \Phi_2(\zeta)$, being $\zeta = \pm 1$, are discounted, whilst the roots of $\Phi_3(\zeta)$, $\Phi_4(\zeta)$ and $\Phi_6(\zeta)$ (resp., $\omega_{a,b}, \pm i$ and $-\omega_{a,b}$) correspond, from earlier cases seen, to the linear factors $1-x$, $1-2x$ and $1-3x$.

We focus, therefore, on $0 = \Phi_{12}(\zeta) = \zeta^4 - \zeta^2 + 1$. The roots of $\Phi_{12}(\zeta)$ are the 4 primitive twelfth roots of unity $e^{\pi i/6}, e^{5\pi i/6}, e^{7\pi i/6}, e^{11\pi i/6}$ (obtained as $e^{2m\pi i/12} = e^{m\pi i/6}$, where $m \in \{k \in [0,11] : k, 12 \text{ are coprime}\} = \{1,5,7,11\}$), however we do not actually need to identify these explicitly. Dividing throughout by $\zeta^2 \neq 0$ this reads $0 = \zeta^2 - 1 + \frac{1}{\zeta^2} = (\zeta + \frac{1}{\zeta})^2 - 3 =$

$I(\zeta)$, say. With reference to (18), then setting $\zeta(x)+\frac{1}{\zeta(x)}=x^*-2$, the required factor will be forthcoming from $I(x^*)=(x^*-2)^2-3=1-4x^*+x^{*2}$, with the *actual* factor delivered by $I(\frac{1}{x})$, *i.e.*, $1-4x+x^2$ (in this case the same expression). Thus we have identified the remaining quadratic factor, with $P_{11}(x)=(1-x)(1-2x)(1-3x)(1-4x+x^2)$ as seen in (4).

Case $n=13$. We write $\zeta^{14}-1=\Phi_1(\zeta)\Phi_2(\zeta)\Phi_7(\zeta)\Phi_{14}(\zeta)$, with factors generated from $\Phi_7(\zeta)$ and $\Phi_{14}(\zeta)$ only. Consider first, then,

$$\begin{aligned} 0 &= \Phi_7(\zeta) = \zeta^6+\zeta^5+\zeta^4+\zeta^3+\zeta^2+\zeta+1 \\ &= \left(\zeta+\frac{1}{\zeta}\right)^3+\left(\zeta+\frac{1}{\zeta}\right)^2-2\left(\zeta+\frac{1}{\zeta}\right)-1 \\ &= I(\zeta), \end{aligned} \tag{20}$$

after dividing through by ζ^3 and re-arranging. Hence, $I(x^*)=(x^*-2)^3+(x^*-2)^2-2(x^*-2)-1=x^{*3}-5x^{*2}+6x^*-1$, with the associated factor given by $I(\frac{1}{x})$ as $1-5x+6x^2-x^3$. The other factor is found from consideration of

$$0 = \Phi_{14}(\zeta) = \zeta^6-\zeta^5+\zeta^4-\zeta^3+\zeta^2-\zeta+1, \tag{21}$$

that is,

$$0 = \left(\zeta+\frac{1}{\zeta}\right)^3-\left(\zeta+\frac{1}{\zeta}\right)^2-2\left(\zeta+\frac{1}{\zeta}\right)+1 = I(\zeta). \tag{22}$$

With $I(x^*)=(x^*-2)^3-(x^*-2)^2-2(x^*-2)+1=x^{*3}-7x^{*2}+14x^*-7$, we have $1-7x+14x^2-7x^3$ as the other factor immediate from $I(\frac{1}{x})$; hence (and in agreement with (4)), $P_{13}(x)=(1-5x+6x^2-x^3)(1-7x+14x^2-7x^3)$.

We consider one further example to illustrate the mechanics of factorisation. If we look at $P_{59}(x)$, then we must first write down all the divisors $d=1,2,3,4,5,6,10,12,15,20,30,60$ of $n+1=60$. Excluding $d=1,2$ (which lead to no factors), we find that the factors of $P_{59}(x)$ are of respective order $\frac{1}{2}\phi(3),\frac{1}{2}\phi(4),\frac{1}{2}\phi(5),\frac{1}{2}\phi(6),\ldots,\frac{1}{2}\phi(30),\frac{1}{2}\phi(60)=1,1,2,1,2,2,4,4,4,8$, so that there are three linear, quadratic and quartic factors each, together with a single factor of order 8; this concurs with the actual decomposition[7] $P_{59}(x)=(1-x)(1-2x)(1-3x)(1-3x+x^2)(1-4x+x^2)(1-5x+5x^2)(1-8x+19x^2-12x^3+x^4)(1-7x+14x^2-8x^3+x^4)(1-9x+26x^2-24x^3+x^4)(1-16x+105x^2-364x^3+714x^4-784x^5+440x^6-96x^7+x^8)$, and

[7] The precise factors are found algebraically as in the manner detailed for $P_{11}(x)$ and $P_{13}(x)$.

we conclude that *for $n \geq 2$ $P_n(x)$ is factorisable as a product of irreducible polynomials of degree $\frac{1}{2}\phi(d)$ for all divisors $d > 2$ of $n+1$.* As a corollary, it is immediate that should $n+1$ be prime then the only factor of $P_n(x)$ is itself, which is, therefore, irreducible (and of degree $\frac{1}{2}\phi(n+1) = \frac{1}{2}n$); *this is Theorem 4.*

Based on the work of this section we can now proceed to re-prove Theorems 2 and 3, both proofs heavily reliant on an important bijection established at the start of the first one.

Theorem 2 (New Proof) Let $\mathbf{R}_+ = \mathbf{R} \cap (0, \infty)$ be the set of positive reals, and $\mathbf{N}_+ = \mathbf{N}\backslash\{0\}$ the positive integers. We define, for $n \in \mathbf{N}_+$, sets $\mathcal{U}_n = \{\zeta \in \mathbf{C} : \zeta^{n+1} = 1 \text{ and } \mathrm{Im}(\zeta) > 0\}$, $\mathcal{R}_n = \{x \in \mathbf{R}_+ : P_n(x) = 0\}$ (being, resp., the set of all $(n+1)$th roots of unity lying in the top half of the complex plane, and the set of all (positive real) roots of $P_n(x)$), and the mapping $\tau : \mathbf{C}\backslash\{-1\} \to \mathbf{C}$ defined as $\tau(\zeta) = \frac{\zeta}{(1+\zeta)^2}$. If τ_n is the restriction of τ to $\mathcal{U}_n$ then it is a relatively straightforward matter to show that *τ_n is a bijection*[8] between $\mathcal{U}_n$ and $\mathcal{R}_n$ which permits a rather elegant argument to be formed.

To prove Theorem 2 we argue by contradiction, supposing at the outset that the statement is false and that some pair of the triplet of polynomials $P_n(x), P_{n+1}(x), P_{n+2}(x)$ possess a common root. Thus, this root is a common element between two of the sets $\mathcal{R}_n, \mathcal{R}_{n+1}, \mathcal{R}_{n+2}$ and, by bijection, its value mapped by τ (via the restrictions $\tau_n, \tau_{n+1}, \tau_{n+2}$) occurs in two of the sets $\mathcal{U}_n, \mathcal{U}_{n+1}, \mathcal{U}_{n+2}$. Now the set $\mathcal{U}_n$ can be written instead as $\mathcal{U}_n = \{\exp[2k\pi i/(n+1)] : k = 1, \ldots, \lfloor \frac{1}{2}n \rfloor\}$ which means, writing $\mathcal{B}_n = \{k/(n+1) : k = 1, \ldots, \lfloor \frac{1}{2}n \rfloor\}$, that this common element is shared between two of the sets $\mathcal{B}_n, \mathcal{B}_{n+1}, \mathcal{B}_{n+2}$. W.l.o.g., therefore, we suppose this root lies in $\mathcal{B}_n$, and is repeated in $\mathcal{B}_{n+s}$ (where $s = 1$ or 2), whereupon there exists integers $k_1 \in [1, \lfloor n/2 \rfloor]$, $k_2 \in [1, \lfloor (n+s)/2 \rfloor]$ such that

$$\frac{k_1}{n+1} = \frac{k_2}{n+s+1}. \tag{P12}$$

Clearly $k_2 > k_1$ for equality, and since both are integer then we must have $k_2 = k_1 + \delta_k$ for some integer $\delta_k \geq 1$. Hence,

$$\frac{k_1}{n+1} = \frac{k_1 + \delta_k}{n+s+1}, \tag{P13}$$

i.e.,

$$\delta_k = k_1 s/(n+1). \tag{P14}$$

[8] We leave the precise details of the proof of this bijection to the interested reader as it largely uses ideas seen earlier in the section.

However, $1 \le s \le 2$ and $1 \le k_1 \le \lfloor \frac{1}{2}n \rfloor \le \frac{1}{2}n$, whence follows the contradiction

$$1 \;\le\; \delta_k \;=\; \frac{k_1 s}{n+1} \;\le\; \frac{\frac{1}{2}n \cdot 2}{n+1} \;=\; \frac{n}{n+1} \;<\; 1, \qquad \text{(P15)}$$

as required.□

Theorem 3 (New Proof) Let $k \ge 2$ be integer. The Catalan polynomial

$$P_k(x) \;=\; \sum_{i=0}^{\lfloor \frac{1}{2}k \rfloor} \binom{k-i}{i} (-x)^i \;=\; \alpha_k \prod_{i=1}^{\lfloor \frac{1}{2}k \rfloor} (x - \rho_i), \qquad \text{(P16)}$$

has roots $\rho_1, \rho_2, \ldots, \rho_{\lfloor \frac{1}{2}k \rfloor}$, say, with

$$\alpha_k \;=\; [x^{\lfloor \frac{1}{2}k \rfloor}]\{P_k(x)\} \;=\; (-1)^{\lfloor \frac{1}{2}k \rfloor} \binom{k - \lfloor \frac{1}{2}k \rfloor}{\lfloor \frac{1}{2}k \rfloor} \;\in\; \mathbf{Z}. \qquad \text{(P17)}$$

We first note that for k even then, trivially, $\lfloor \frac{1}{2}k \rfloor = \frac{1}{2}k$ and $\alpha_k = (-1)^{\frac{1}{2}k} = \pm 1$, whilst for k odd $\lfloor \frac{1}{2}k \rfloor = \frac{1}{2}(k-1)$ and we find that $\alpha_k = (-1)^{\frac{1}{2}(k-1)} \cdot \frac{1}{2}(k+1) = \pm \frac{1}{2}(k+1)$. If we consider further the polynomial

$$P_{(k+1)n+k}(x) \;=\; \beta_{k,n} \prod_{i=1}^{\lfloor \frac{1}{2}[(k+1)n+k] \rfloor} (x - \omega_i), \qquad \text{(P18)}$$

with roots $\omega_1, \omega_2, \ldots, \omega_{\lfloor \frac{1}{2}[(k+1)n+k] \rfloor}$ $(n \ge 0)$, then (noting that $\beta_{k,n} \in \mathbf{Z}$) we now look at the ratio $\beta_{k,n}/\alpha_k$ for both k even/odd cases. For k even the ratio $\beta_{k,n}/\alpha_k = \pm\beta_{k,n} \in \mathbf{Z}$. For k odd we note that $(k+1)n + k$ is odd so we can write down immediately

$$\begin{aligned} \beta_{k,n} &= [x^{\lfloor \frac{1}{2}[(k+1)n+k] \rfloor}]\{P_{(k+1)n+k}(x)\} \\ &= (-1)^{\frac{1}{2}[(k+1)n+k-1]} \cdot \frac{1}{2}(k+1)(n+1), \end{aligned} \qquad \text{(P19)}$$

whence

$$\begin{aligned} \frac{\beta_{k,n}}{\alpha_k} &= \frac{(-1)^{\frac{1}{2}[(k+1)n+k-1]} \cdot \frac{1}{2}(k+1)(n+1)}{(-1)^{\frac{1}{2}(k-1)} \cdot \frac{1}{2}(k+1)} \\ &= (-1)^{\frac{1}{2}(k+1)n}(n+1) \\ &\in \mathbf{Z}. \end{aligned} \qquad \text{(P20)}$$

In other words, we have shown that $\beta_{k,n}/\alpha_k \in \mathbf{Z}$ for all k, n. Suppose now that $x = \rho \in \mathcal{R}_k$ is one of the roots of $P_k(x)$. Then, by the previous bijection, this corresponds to a particular $(k+1)$th root of unity $\zeta_\rho = \zeta(\rho) \in \mathcal{U}_k$. Since $(\zeta_\rho)^{(k+1)(n-1)} = [(\zeta_\rho)^{k+1}]^{n+1} = [1]^{n+1} = 1$, ζ_ρ is also a $(k+1)(n+1)$th root of unity in $\mathcal{U}_{(k+1)n+k}$, mapping bijectively to the *same* root $x = \rho$ of $P_{(k+1)n+k}(x)$. It follows, therefore, that every root of $P_k(x)$ is contained in $P_{(k+1)n+k}(x)$ and (ordering the roots of $P_{(k+1)n+k}(x)$ as $\rho_1, \rho_2, \ldots, \rho_{\lfloor\frac{1}{2}k\rfloor}, \omega_{\lfloor\frac{1}{2}k\rfloor+1}, \ldots, \omega_{\lfloor\frac{1}{2}[(k+1)n+k]\rfloor}$) we have the relation

$$P_{(k+1)n+k}(x) = P_k(x)R(x), \tag{P21}$$

with

$$R(x) \;=\; R(x;k,n) \;=\; \gamma_{k,n} \prod_{i=\lfloor\frac{1}{2}k\rfloor+1}^{\lfloor\frac{1}{2}[(k+1)n+k]\rfloor} (x-\omega_i) \tag{P22}$$

denoting the quotient polynomial and, by necessity, $\gamma_{k,n} = \beta_{k,n}/\alpha_k \subset \mathbf{Z}$. To complete the proof we need to show that the polynomial $R(x) \in \mathbf{Q}[x]$, and we argue by contradiction, assuming that it is not and so possesses at least one coefficient which is irrational. Let h be the highest power of x in $R(x)$ which has an irrational coefficient $r = r(k,n)$, say, and consider the term in $x^{\lfloor\frac{1}{2}k\rfloor+h}$ in $P_k(x)R(x)$, with (irrational) coefficient $a_k r$, given by the product of the $x^{\lfloor\frac{1}{2}k\rfloor}$ term in $P_k(x)$ with the x^h term in $R(x)$. Within the polynomial $P_k(x)R(x)$ other possible terms in $x^{\lfloor\frac{1}{2}k\rfloor+h}$ are found by products of terms of type $x^{\lfloor\frac{1}{2}k\rfloor-1}\cdot x^{h+1}$, $x^{\lfloor\frac{1}{2}k\rfloor-2}\cdot x^{h+2}$, and so on, with terms in $x^{\lfloor\frac{1}{2}k\rfloor-1}, x^{\lfloor\frac{1}{2}k\rfloor-2}, \ldots$, lying in $P_k(x) \in \mathbf{Z}[x]$, whilst terms in $x^{h+1}, x^{h+2}, \ldots$ (whose coefficients are rational since each power $h+1, h+2$, *etc.*, is greater than h), are drawn from $R(x)$. In other words (by (P21)),[9]

$$\begin{aligned}[x^{\lfloor\frac{1}{2}k\rfloor+h}]\{P_{(k+1)n+k}(x)\} &= [x^{\lfloor\frac{1}{2}k\rfloor+h}]\{P_k(x)R(x)\} \\ &= a_k r + c_1 s_1 + c_2 s_2 + \cdots \end{aligned} \tag{P23}$$

($c_1, c_2, \ldots, \in \mathbf{Z}$, $s_1, s_2, \ldots, \in \mathbf{Q}$), which, being irrational, is a contradiction since $P_{(k+1)n+k}(x) \in \mathbf{Z}[x]$. Hence, $R(x) \in \mathbf{Q}[x]$ and so $P_k(x)R(x) = P_{(k+1)n+k}(x)$ is factorisable over $\mathbf{Q}[x]$, and in turn over $\mathbf{Z}[x]$ (by Gauss' Lemma, a standard result), whence we have $P_{(k+1)n+k}(x)/P_k(x) \in \mathbf{Z}[x]$. □

4 Summary

In this article we have, for the first time in any detail, attempted to analyse factorisation and divisibility of Catalan polynomials. Some initial stand alone results are established, and subsequently recovered by applying known

[9] Evidently, the number of terms in the r.h.s. of (P23) is dependent on the position of the postulated x^h term in the degree $\lfloor\frac{1}{2}[(k+1)n+k]\rfloor - \lfloor\frac{1}{2}k\rfloor$ polynomial $R(x)$.

properties of roots of unity and cyclotomic polynomials[10] which also allow the factorisation process to be understood more clearly. No existing results on Chebyshev or Dickson polynomials— to which Catalan polynomials are connected—are used here, indeed we leave the question of how to interpret our results (in conjunction with cyclotomic polynomial theory) to form corresponding ones in the context of Chebyshev polynomials as offering a future potential piece of work.

Finally, we note that the Catalan polynomials are in fact but one family of a much larger class of polynomials, each of which is associated with an integer sequence whose ordinary generating function is governed by a quadratic equation with functional coefficients in $\mathbf{Z}[x]$ (such as that for the Catalan sequence through which the Catalan polynomials are defined; others studied previously are the (Large) Schröder and Motzkin polynomials, so named after their namesake sequences[11]). It remains a possibility that some of the results presented here might well be carried over, and appear in a similar form, in other such polynomial family cases; this, too, defines an open problem at present.

5 Acknowledgement

This paper is a revised and extended form of the version submitted for publication some while ago. At that time the referee— to whom we are very grateful made a number of constructive critisisms and comments which have assisted the authors in re-shaping, and developing the remit of, the article.

References

[1] Clapperton, J.A., Larcombe, P.J. and Fennessey, E.J. (2008). On iterated generating functions for integer sequences, and Catalan polynomials, *Util. Math.*, **77**, pp.3-33.

[10]Whilst the general theory of these polynomials appears regularly in texts as standard material, it is perhaps worth mentioning for completeness that in 1975 Apostol brought together in an extended bibliography [9] a useful reference listing of work published on cyclotomic polynomials since 1919; it would appear [T.M. Apostol, *Priv. Comm.*] that the list has not been updated.

[11]See [10], for example (where the Appendix gives a description of the basic characteristics of both the (Large) Schröder and Motzkin polynomials $S_n(x)$ and $M_n(x)$), or a previous publication [11]. These polynomials—together with the Catalan polynomials—have been chosen to be studied as they possess the common feature that their derivative sequences each have a well established combinatorial interpretation in the context of 2D lattice paths, and in that sense they form a natural grouping.

[2] Clapperton, J.A., Larcombe, P.J., Fennessey, E.J. and Levrie, P. (2008). A class of auto-identities for Catalan polynomials, and Padé approximation, *Cong. Num.*, **189**, pp.77-95.

[3] Clapperton, J.A., Larcombe, P.J. and Fennessey, E.J. (2009). Some new identities for Catalan polynomials, *Util. Math.*, **80**, pp.3-10.

[4] Clapperton, J.A., Larcombe, P.J. and Fennessey, E.J. (2014). Generalised Catalan polynomials and their properties, *Bull. I.C.A.*, to appear (this issue).

[5] Lehmer, D.H. (1933). A note on trigonometric algebraic numbers, *Amer. Math. Month.*, **40**, pp.165-166.

[6] Lidl, R., Mullen, G.L. and Turnwald, G. (1993). Dickson polynomials (Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 65), Longman, London, U.K.

[7] Rayes, M.O., Trevisan, V. and Wang, P.S. (2005). Factorization properties of Chebyshev polynomials, *Comp. Math. Appl.*, **50**, pp.1231-1240.

[8] Rivlin, T.J. (1990). Chebyshev polynomials: from approximation theory to algebra and number theory (2nd Ed.), Wiley, New York, U.S.A.

[9] Apostol, T.M. (1975). The resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$, *Math. Comp.*, **29**, pp.1-6.

[10] Clapperton, J.A., Larcombe, P.J. and Fennessey, E.J. (2011). Two new identities for polynomial families, *Bull. I.C.A.*, **62**, pp.25-32.

[11] Clapperton, J.A., Larcombe, P.J. and Fennessey, E.J. (2010). New theory and results from an algebraic application of Householder root finding schemes, *Util. Math.*, **83**, pp.3-36.

Lobb Numbe

We present two
$0 \le m \le n$. Th
Catalan's parent
triangle C, obta
$(K_{n,m})$ in a spe

In 1838, the Belgian
investigated the well-
correctly parenthesiz
right parentheses. It
where $n \ge 0$ [**1, 5, 6**,
integer.

The parenthesiza
ways. Two of them

- Find the numb
0s and 1s such
or equal to the
- Find the numb
positive ones
negative.

Although Catala
cover them. The grea
found them in his s

BULLETIN of the INSTITUTE of COMBINATORICS and its APPLICATIONS

ISSN
1183-1278

Edited by:

B.L. Hartnell

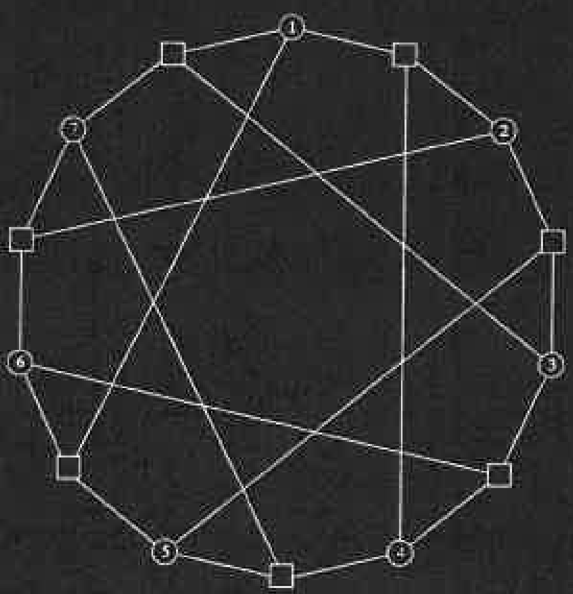
W.L. Kocay

Mirka Miller

E.A. Ruet d'Auteuil

Anne Penfold Street

G.H.J. van Rees



Bulletin of the ICA, Volume 71, May, 2014
Table of Contents

Commemorating 200 Years Since the Birth of Eugène Charles Catalan

Guest Editor
Peter J. Larcombe

Dedication

This Special May 2014 Bulletin Issue is Dedicated to the Memory of
David R. French ('Frenchy')
1943—2014

The Catalan sequence has an almost unparalleled ubiquity in discrete mathematics, arising as, or in, the solution of a wide variety of apparently disparate and unconnected counting problems. Throughout the major part of the 19th century the accepted version of its discovery linked the initial identification of the sequence to Leonhard Euler, who in 1751 wrote of its elements as providing solutions to the so called ***triangulated decompositions of polygons***—a problem which is today well known and through which the Catalan sequence was to eventually bear the name of Catalan himself, seemingly after a flurry of activity (by Catalan and some contemporaries) during the 1830s and 1840s. This false attribution (and others) continued until 1988 when a Chinese historian, J. Luo, detailed a new context as evidence of an even earlier awareness of the Catalan sequence by the scholar Antu Ming (who during the first half of the 1700s examined, via geometrical considerations, a certain type of infinite series containing Catalan numbers).

From such beginnings well over 250 years ago, the Catalan sequence has continued to make regular appearances in the literature—sometimes in surprising ways—whilst the Catalan numbers have interesting mathematical properties in their own right which link with other integer sequences. My own personal interest in the Catalan sequence took off when it arose in an enumeration problem on which I was working with an undergraduate final year student in the mid 1990s (strangely, it took many years for this work to be disseminated), and—after the assimilation and translation of the relevant material—I wrote, and co-wrote, a series of short pieces on the origins of the Catalan sequence in an attempt to clarify that part of its history. Since then both Catalan and the Catalan numbers have at times figured in my work, most recently through the so called Catalan polynomials which I discovered with a Ph.D. student (James Clapperton) and great friend Dr. Eric Fennessey (in our study of iterated generating functions) and which form the basis of my joint contributions to this Special Issue. I am, of course, not alone in my Catalan-related pursuits. Professor Richard P. Stanley, for instance, has aptly termed an extreme enthusiasm for all matters Catalan as "Catalania" ("Catalan mania"), a 'condition' whose 'sufferers' will undoubtedly recognise! Richard himself keeps a wonderful Catalan Addendum to Volume 2 of his well known book *Enumerative Combinatorics* active as an up-to-date resource for researchers in which he details new interpretations and problems, and Professor Thomas Koshy has been moved to write a stand alone undergraduate text *Catalan Numbers with Applications* for a less specialised readership (see overleaf for more details on these books). Each, in its own particular way, serves the mathematical community well, along with the numerous articles which have, over the years, formed a substantial body of work on the Catalan sequence and secured its place at the forefront of the world of integer sequences.

One wonders what Catalan—who as well as being politically active was quite eclectic in his mathematical endeavours—would have made of the way the sequence has captivated academics eager to understand its fundamental nature and application; certainly, it is testimony to the importance of the Catalan numbers that so many people, at all academic levels, continue to develop and often retain an interest in them, and there is no sign of this ending. It is, therefore, a great pleasure to write this Foreword in my capacity as Guest Editor, as the I.C.A. formally celebrates both the significant and longstanding impact of the Catalan sequence within discrete mathematics. The invited contributions on offer here are as varied as they are interesting, forming a timely and fitting tribute to Catalan and the Catalan sequence.

Enjoy !

Peter J. Larcombe
Professor of Discrete and Applied Mathematics
Office E319 (Gateway to 'Cataland')
School of Computing and Mathematics
University of Derby
Kedleston Road
Derby DE22 1GB
England, U.K.
[P.J.Larcombe@derby.ac.uk]

Major Contributions to the Literature on Catalan Numbers by Stanley and Koshy

R.P. Stanley (1999). "Enumerative Combinatorics", Volume 2 (Cambridge Studies in Advanced Mathematics No. 62), Cambridge University Press, Cambridge, U.K.
Some useful background information on the Catalan numbers (with references) appears in the *Notes* section at the end of Chapter 6 of this advanced level book, with the subsequent Exercises 6.19 offering a number of combinatorial illustrations. Stanley continues to update the original presentation in the textbook with an "EC2 Supplement" (available from his M.I.T. homepage) which contains errata, updates a nd new material. In addition, a "Catalan Addendum" offers new problems related to Catalan numbers, with solutions, reflecting his deep and enduring interest in them and a determination to see them disseminated; Catalan interpretations in the Addendum currently stand at over 200 in number, the collation of which is a commendable achievement on the part of Stanley.

T. Koshy (2009). "Catalan Numbers with Applications", Oxford University Press, New York, U.S.A.
Koshy's text is aimed at a broad readership (of mathematical amateurs, high school students/teachers, and both undergraduate and postgraduate level students), in which he pulls together and catalogues many different aspects of the Catalan sequence and its numerous contexts. The book—as the author rightly states—is the first to collect and present an orderly treatise on the various occurrences, applications and properties of the Catalan numbers, and Koshy draws on a multitude of reference material to create a very useful resource.

Some Other Works of Note on Catalan

In 1996 the Société Belge des Professeurs de Mathématique d'Expression Française (Mons, Belgium) published "Eugène Catalan: Géomètre sans Patrie, Républicain sans République", a 200+ page book by F. Jongmans on the life and work of Catalan. [Prior to this, and as a precursor, the author had contributed a chapter (Chapter 3, pp.23-41) with the same title in a publication "Regards Sur 175 Ans de Science à l'Université de Liège 1817-1992" (Ed. A.-C. Bernès) which was produced in 1992 under the auspices of the University's Centre d'Histoire des Sciences et des Techniques to mark this period of general scientific activity at the university.]

Other works of note are the articles "Eugène Catalan and the Rise of Russian Science" (*Acad. Roy. Belg. Bull. Class. Sci.*, **2** (1991), pp.59-90) by P.L. Butzer and F. Jongmans, "Les Relations Épistolaires Entre Eugène Catalan et Ernesto Cesàro" (*ibid.*, **10** (1999), pp.223-271) by Butzer *et al.*, and "Quelques Pièces Choisies dans la Correspondance d'Eugène Catalan" (*Bull. Soc. Roy. Sci. Liège*, **50** (1981), pp.287-309) by Jongmans. All bar the final reference are predated by about a century by P. Mansion's "Notice sur les Travaux Mathématiques de Eugène-Charles Catalan" which appeared in *Ann. l'Acad. Roy. Sci. Lett. Beaux-Arts Belg.* in 1896 (**62**, pp.115-172).