Advances in Mathematics 374 (2020) 107387

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

Lucas atoms

Bruce E. Sagan [a,*], Jordan Tirrell [b]

[a] Department of Mathematics, Michigan State University, East Lansing, MI 48824-1027, USA
[b] Department of Mathematics and Computer Science, Washington College, Chestertown, MD 21620, USA

ARTICLE INFO

Article history:
Received 5 September 2019
Received in revised form 16 August 2020
Accepted 17 August 2020
Available online 27 August 2020
Communicated by Petter Brändén

MSC:
primary 11B39
secondary 05A10, 11B65, 11R09

Keywords:
Catalan number
Coxeter group
Cyclotomic polynomial
Gamma expansion
Lucas polynomial
Reduction formula

ABSTRACT

Given two variables s and t, the associated sequence of Lucas polynomials is defined inductively by $\{0\} = 0$, $\{1\} = 1$, and $\{n\} = s\{n-1\} + t\{n-2\}$ for $n \geq 2$. An integer (e.g., a Catalan number) defined by an expression of the form $\prod_i n_i / \prod_j k_j$ has a Lucas analogue obtained by replacing each factor with the corresponding Lucas polynomial. There has been interest in deciding when such expressions, which are a priori only rational functions, are actually polynomials in s, t. The approaches so far have been combinatorial. We introduce a powerful algebraic method for answering this question by factoring $\{n\} = \prod_{d|n} P_d(s,t)$, where we call the polynomials $P_d(s,t)$ Lucas atoms. This permits us to show that the Lucas analogues of the Fuss-Catalan and Fuss-Narayana numbers for all irreducible Coxeter groups are polynomials in s, t. Using gamma expansions, a technique which has recently become popular in combinatorics and geometry, one can show that the Lucas atoms have a close relationship with cyclotomic polynomials $\Phi_d(q)$. Certain results about the $\Phi_d(q)$ can then be lifted to Lucas atoms. In particular, one can prove analogues of theorems of Gauss and Lucas, deduce reduction formulas, and evaluate the $P_d(s,t)$ at various specific values of the variables.

* Corresponding author.
E-mail address: sagan@math.msu.edu (B.E. Sagan).

https://doi.org/10.1016/j.aim.2020.107387
0001-8708/

1. Introduction

We will denote the nonnegative integers by $\mathbb{N}$. Let s, t be variables. Inductively define the nth *Lucas polynomial*, $\{n\} = \{n\}_{s,t}$, by $\{0\} = 0$, $\{1\} = 1$, and

$$\{n\} = s\{n-1\} + t\{n-2\} \tag{1}$$

for $n \geq 2$. These polynomials were introduced and studied by Lucas in [16,18,17]. This sequence has various interesting specializations. For example, $\{n\}_{1,1}$ is the nth Fibonacci number and $\{n\}_{2,-1} = n$. Furthermore, if one considers a third variable q, then a simple induction shows that

$$\{n\}_{1+q,-q} = 1 + q + q^2 + \cdots + q^{n-1}. \tag{2}$$

This summation is usually denoted $[n]_q$ and is important both in the theory of hypergeometric series and in combinatorics. This equation will permit us to make a connection between the Lucas sequence and cyclotomic polynomials.

There has been recent interest in studying Lucas analogues of combinatorial constants. These are connected via (2) with the well-studied q-analogues of such integers. Suppose we are given an integer defined as a quotient of products $\prod_i n_i / \prod_j k_j$ where the n_i and k_j are positive integers. The corresponding *Lucas analogue* is $\prod_i \{n_i\} / \prod_j \{k_j\}$. A priori, this is just a rational function of s and t. But often it is actually a polynomial in these variables with nonnegative integer coefficients. Benjamin and Plott [4] gave a complicated combinatorial interpretation for the Lucas analogue of the binomials coefficients, called Lucanomials. Then Sagan and Savage [21] came up with a simpler one which, unfortunately, appeared to be rigid in that their ideas could not be extended to related constants such as the Catalan numbers. Ekhad [11] found an algebraic argument to show that since the Lucanomials were in $\mathbb{N}[s,t]$, so were the Lucas-Catalans. Bennett, Carrillo, Machacek, and Sagan [6] gave a combinatorial model in the binomial coefficient case which could be extended to the Catalan numbers for all irreducible Coxeter groups, but they were still not able to apply their methods to various other constants. As yet unpublished work has also been done by the Algebraic Combinatorics Seminar at the Fields Institute [1], Garrett and Killpatrick [12], Nenashev [14], and Rao and Suk [19]. Finally, the Lucas atoms were discovered earlier and independently by Levy [15] who showed that they were irreducible over the rationals.

We introduce a new and powerful method for proving that Lucas analogues are polynomials with nonnegative integer coefficients. In particular, we will define a new sequence of polynomials $P_n(s,t)$ which will be called Lucas atoms and satisfy

$$\{n\} = \prod_{d|n} P_d(s,t). \tag{3}$$

The first few Lucas polynomials and Lucas atoms are given in Table 1. Given a product of Lucas polynomials $\prod_i \{n_i\}$ its associated *atomic decomposition* is the product of Lucas

Table 1
The Lucas polynomials and Lucas atoms for $n \leq 6$.

n	$\{n\}$	$P_n(s,t)$
1	1	1
2	s	s
3	s^2+t	s^2+t
4	s^3+2st	s^2+2t
5	$s^4+3s^2t+t^2$	$s^4+3s^2t+t^2$
6	$s^5+4s^3t+3st^2$	s^2+3t

atoms obtained by replacing each $\{n_i\}$ by the corresponding product using (3). One of our principal results shows that atomic decompositions function like prime decompositions of integers. Note that we do not have to consider $P_1(s,t)$ since it is the polynomial 1.

Theorem 1.1. *Suppose $f(s,t) = \prod_i \{n_i\}$ and $g(s,t) = \prod_j \{k_j\}$ for certain $n_i, k_j \in \mathbb{N}$, and write their atomic decompositions as*

$$f(s,t) = \prod_{d \geq 2} P_d(s,t)^{a_d} \quad \text{and} \quad g(s,t) = \prod_{d \geq 2} P_d(s,t)^{b_d}$$

for certain powers $a_d, b_d \in \mathbb{N}$. Then $f(s,t)/g(s,t)$ is a polynomial if and only if $a_d \geq b_d$ for all $d \geq 2$. Furthermore, in this case $f(s,t)/g(s,t)$ has nonnegative integer coefficients.

This result is striking for several reasons. First of all, it gives a condition for polynomiality which is not only sufficient but also necessary. It is also notable that such polynomials must always be in $\mathbb{N}[s,t]$. Thus it is impossible for one of these polynomials to have a coefficient which is $1/2$ or -3.

In the next section, the Lucas atoms are defined and the previous theorem is proved using a connection with cyclotomic polynomials, $\Phi_n(q)$. This correspondence is made through the use of gamma expansions. These expressions are important in geometry because of a conjecture of Gal and in combinatorics because of their usefulness in proving unimodality results. See the recent survey of Athanasiadis [3] for more details. In particular, $P_n(s,t)$ turns out to be the image of $\Phi_n(q)$ under a map which uses the gamma expansion of the latter. It follows that the coefficients of $P_n(s,t)$ are just the absolute values of the gamma coefficients of $\Phi_n(q)$. In Section 3 we use Theorem 1.1 to prove that a host of Lucas analogues are in $\mathbb{N}[s,t]$, including the Fuss-Catalan and Fuss-Narayana numbers for an arbitrary irreducible Coxeter group. It is also natural to ask which theorems about the cyclotomic polynomials have counterparts for the Lucas atoms. Section 4 is devoted to showing that theorems of Gauss and Lucas expressing $\Phi_n(q)$ in terms of two squares can be lifted to the Lucas realm. In Section 5 we prove reduction formulas for Lucas atoms which reduce their computation to knowing $P_p(s,t)$ for a prime p. Section 6 contains various evaluations of $P_n(s,t)$ for specific values of s and t. We end with a section of comments and open questions.

2. Defining Lucas atoms

One could define the Lucas atoms $P_n(s,t)$ inductively using (3). But it will be more useful to obtain them from cyclotomic polynomials. First, however, we need some definitions about gamma expansions.

Let $p(q) = \sum_{i\ge 0} a_i q^i$ be a nonzero polynomial in q with coefficients in $\mathbb{C}$, the complex numbers. As usual, the *degree* of $p(q)$, $\deg p(q)$, is the largest index i with $a_i \neq 0$. We will also need the *minimum degree*

$$\operatorname{mdeg} p(q) = \min\{i \mid a_i \neq 0\}$$

and *total degree*

$$\operatorname{totdeg} p(q) = \deg p(q) + \operatorname{mdeg} p(q).$$

For example $p(q) = 2q + 5q^2 + 5q^3 + 2q^4$ has $\operatorname{totdeg} p(q) = 4 + 1 = 5$. If $\operatorname{totdeg} p(q) = d$ then we call $p(q)$ *palindromic* (*symmetric* is also used) if $a_i = a_{d-i}$ for all $0 \le i \le d$. It is easy to see that this is equivalent to the equality

$$q^d p(1/q) = p(q). \tag{4}$$

In this case we call $d/2$ the *center of symmetry* of $p(q)$. Our example polynomial is palindromic with center of symmetry $5/2$. A straight-forward computation shows that the product of palindromic polynomials is palindromic. The same is true of linear combinations of palindromic polynomials with the same center of symmetry, but not in general.

We will need the vector space

$$\mathcal{P}_d(q) = \{p(q) \in \mathbb{C}[q] \mid p(q) \text{ is palindromic with } \operatorname{totdeg} p(q) = d\} \cup \{0\}.$$

The polynomials

$$(1+q)^d,\ q(1+q)^{d-2},\ q^2(1+q)^{d-4},\ \ldots \tag{5}$$

form a basis for $\mathcal{P}_d$ since they all have different degrees and their leading coefficients equal one. So if $p(q) \in \mathcal{P}_d$ then it has *gamma expansion*

$$p(q) = \sum_{j\ge 0} \gamma_j q^j (1+q)^{d-2j} \tag{6}$$

where the scalars $\gamma_0, \gamma_1, \gamma_2, \ldots$ are called the *gamma coefficients* of $p(q)$. Returning to our example

$$2q + 5q^2 + 5q^3 + 2q^4 = 0(1+q)^5 + 2q(1+q)^3 - q^2(1+q)$$

so its gamma coefficients are $0, 2, -1$.

To make the connection with the Lucas sequence, an easy inductive proof shows that

$$\{n\} = \sum_{j\geq 0} a_j s^{n-2j-1} t^j, \tag{7}$$

for certain $a_j \in \mathbb{N}$. Comparison of this expansion with (6) motivates the following definition. Consider

$$\mathcal{P}(q) = \bigcup_{d\geq 0} \mathcal{P}_d(q).$$

Note that the union is disjoint except for the presence of the zero polynomial in all $\mathcal{P}_d$. Define the *Gamma map* $\Gamma : \mathcal{P}(q) \to \mathbb{C}[s, t]$ by taking $p(q)$ of the form (6) to

$$\Gamma(p(q)) = \sum_{j\geq 0} \gamma_j s^{d-2j} (-t)^j. \tag{8}$$

In the next proposition we collect some of the basic properties of this function.

Proposition 2.1. *The map $\Gamma : \mathcal{P}(q) \to \mathbb{C}[s, t]$ has the following properties*

(a) If $p(q), r(q) \in \mathcal{P}(q)$ then

$$\Gamma(p(q)r(q)) = \Gamma(p(q))\Gamma(r(q)).$$

(b) For any d, the restriction of Γ to $\mathcal{P}_d(q)$ is linear.
(c) The map Γ is injective.
(d) If $\Gamma(p(q)) = f(s, t)$ then $f(1 + q, -q) = p(q)$.
(e) If $p(q) \in \mathbb{Z}[q]$ then $\Gamma(p(q)) \in \mathbb{Z}[s, t]$.

Proof. Parts (a) and (b) follow quickly from the remarks after equation (4). Also (c) follows from (d) which defines the inverse map on the image of Γ. For (d) we have, from (6) and (8),

$$f(1 + q, -q) = \sum_{j\geq 0} \gamma_j s^{d-2j} (-t)^j|_{s=1+q,t=-q} = \sum_{j\geq 0} \gamma_j (1 + q)^{d-2j} q^j = p(q).$$

To obtain (e), note that the polynomials in (5) are all monic. So if $p(q) \in \mathbb{Z}[q]$, then its gamma coefficients are all integers. The desired conclusion now follows from the definition of Γ. $\square$

To define the Lucas atoms, we first recall some simple facts about the cyclotomic polynomials. The *nth cyclotomic polynomial* is

$$\Phi_n(q) = \prod_{\zeta}(q - \zeta)$$

where the product is over all primitive nth roots of unity. Since ζ is a primitive nth root if and only if $1/\zeta$ is, and the constant coefficient of $\Phi_n(q)$ is one for $n \geq 2$, it follows from equation (4) that $\Phi_n(q)$ is palindromic for that range of n. So define the *nth Lucas atom* as $P_1(s,t) = 1$ and

$$P_n(s,t) = \Gamma(\Phi_n(q))$$

for $n \geq 2$. The basic properties of $P_n(s,t)$ are as follows.

Proposition 2.2. *For all $n \geq 1$ we have*

(a) $\{n\} = \prod_{d|n} P_d(s,t)$*, and*
(b) $P_n(s,t) \in \mathbb{N}[s,t]$.

Proof. (a) It is well known and easy to prove from the definitions that

$$q^n - 1 = \prod_{d|n} \Phi_d(q). \tag{9}$$

It follows that

$$1 + q + q^2 + \cdots + q^{n-1} = \prod_{\substack{d|n \\ d \geq 2}} \Phi_d(q).$$

So applying Proposition 2.1 (a) and using the fact that $P_1(s,t) = 1$ we have

$$\Gamma(1 + q + q^2 + \cdots + q^{n-1}) = \prod_{d|n} P_d(s,t).$$

But from equation (2) as well as Proposition 2.1 (c) and (d) we have that the left side of the previous equation is $\{n\}$.

(b) Since the leading coefficient of $\{n\}$ is one, an easy induction using part (a) shows that the same is true of the $P_n(s,t)$. A second induction based on (a) now shows that all the coefficients of $P_n(s,t)$ are integers. For nonnegativity, it suffices to show that, for $n \geq 3$, the polynomial $P_n(s,t)$ can be written as a product of factors of the form $s^2 + at$ where $a > 0$. (Nonnegativity for $n \leq 2$ is clear.) Consider any root ζ of $\Phi_n(q)$. Then the complex conjugate $\bar{\zeta}$ is also a root, and $\Phi_n(q)$ has a factor

$$(q - \zeta)(q - \bar{\zeta}) = q^2 - 2bq + 1 = (q+1)^2 - (2b+2)q$$

where b is the real part of ζ. Since $n \geq 3$ we have $a := 2b+2 > 0$. Using Proposition 2.1 (a) shows that

$$\Gamma((q+1)^2 - (2b+2)q) = s^2 + at$$

is a factor of $P_n(s,t)$ as desired. $\square$

We now have all the tools necessary to prove Theorem 1.1.

Proof of Theorem 1.1. Clearly if $a_d \geq b_d$ for all $d \geq 2$ then $f(s,t)/g(s,t)$ is a polynomial. And since the $P_d(s,t)$ all have nonnegative integer coefficients from the previous proposition, the inequalities show that the same is true of the quotient since it is a product of atoms. So it remains to show that $f(s,t)/g(s,t)$ being a polynomial implies that $a_d \geq b_d$ for $d \geq 2$. It is clear that this holds for $d = 2$ since $P_2(s,t) = s$. So suppose $d \geq 3$. Now $f(s,1)/g(s,1)$ is a polynomial in s. And from the proof of Proposition 2.2 (b), we see that the roots of $P_d(s,1)$ are all of the form $\pm\sqrt{-2b-2}$ where b is the real part of a primitive dth root of unity. It follows that no two of these polynomials in s have a common root. So the polynomialty of $f(s,1)/g(s,1)$ implies $a_d \geq b_d$ for all $d \geq 2$. $\square$

3. Lucas analogues

We will now use Theorem 1.1 to show that a large number of Lucas analogues are polynomials with nonnegative integer coefficients. We will start with the binomial coefficients, then consider various types of Fuss-Catalan numbers including those associated with irreducible Coxeter groups, and finally look at Fuss-Narayana numbers.

We first need to consider the Lucas factorization of the *Lucatorial*

$$\{n\}! = \{1\}\{2\}\cdots\{n\}.$$

To describe the factorization we will need the *floor* or *round-down function* $\lfloor r \rfloor$ which is the largest integer less than or equal to the rational number r. Given a product $f(s,t)$ of Lucas polynomials, let

$$\log_d f(s,t) = \text{the power of } P_d(s,t) \text{ in its Lucas factorization.}$$

The subscript will be omitted if d is clear from context or is generic and fixed.

Lemma 3.1. *For $d \geq 2$ we have*

$$\log_d \{n\}! = \lfloor n/d \rfloor.$$

Furthermore, for integers m, n, d

$$\left\lfloor \frac{m}{d} \right\rfloor + \left\lfloor \frac{n}{d} \right\rfloor \leq \left\lfloor \frac{m+n}{d} \right\rfloor.$$

Proof. We have that P_d is a factor of $\{j\}$ if and only if $d|j$. So the number of such factors in $\{n\}!$ is $\lfloor n/d \rfloor$. The inequality is well known so we omit the proof. $\square$

Now for $0 \leq k \leq n$, we define the *Lucanomial*

$$\left\{ {n \atop k} \right\} = \frac{\{n\}!}{\{k\}!\{n-k\}!}.$$

Theorem 3.2. *For* $0 \leq k \leq n$ *we have* $\left\{ {n \atop k} \right\} \in \mathbb{N}[s,t]$.

Proof. Applying the previous lemma gives, for any $d \geq 2$,

$$\log_d(\{k\}!\{n-k\}!) = \left\lfloor \frac{k}{d} \right\rfloor + \left\lfloor \frac{n-k}{d} \right\rfloor \leq \left\lfloor \frac{n}{d} \right\rfloor = \log_d\{n\}!.$$

So we are done by Theorem 1.1. $\square$

We will now consider various types of Catalan numbers. Given positive integers a, b with $\gcd(a,b) = 1$ the corresponding *rational Catalan number* is

$$\mathrm{Cat}(a,b) = \frac{1}{a+b}\binom{a+b}{a}.$$

One obtains the usual Catalan numbers by letting $a = n$ and $b = n+1$. The corresponding Lucas analogue is

$$\mathrm{Cat}\{a,b\} = \frac{1}{\{a+b\}}\left\{ {a+b \atop a} \right\}.$$

The Algebraic Combinatorics Seminar at the Fields Institute [1] was the first to prove that the q-Fibonacci analogue of $\mathrm{Cat}(a,b)$ is a polynomial in q and their method works as well for the Lucas analogue. This proof is also algebraic and is presented in [6]. A combinatorial proof has yet to be found.

Theorem 3.3. *If* $\gcd(a,b) = 1$ *then* $\mathrm{Cat}\{a,b\} \in \mathbb{N}[s,t]$.

Proof. There are two cases. If d does not divide $a+b$ then $\log\{a+b\} = 0$ and so the result follows from the previous theorem. If d divides $a+b$ then d divides neither a nor b since $\gcd(a,b) = 1$. It follows that $\lfloor a/d \rfloor = \lfloor (a-1)/d \rfloor$ and $\lfloor b/d \rfloor = \lfloor (b-1)/d \rfloor$. So

$$\log(\{a+b\}\{a\}!\{b\}!) \leq 1 + \left\lfloor \frac{a+b-1}{d} \right\rfloor = \left\lfloor \frac{a+b}{d} \right\rfloor = \log\{a+b\}!$$

by Lemma 3.1. Theorem 1.1 completes the proof. $\square$

Table 2
The finite irreducible Coxeter groups and their degrees.

W	$d_1, \ldots, d_n$
A_n	$2, 3, 4, \ldots, n+1$
B_n	$2, 4, 6, \ldots, 2n$
D_n	$2, 4, 6, \ldots, 2n-2, n$
E_6	$2, 5, 6, 8, 9, 12$
E_7	$2, 6, 8, 10, 12, 14, 18$
E_8	$2, 8, 12, 14, 18, 20, 24, 30$
F_4	$2, 6, 8, 12$
H_3	$2, 6, 10$
H_4	$2, 12, 20, 30$
$I_2(m)$	$2, m$

Let W be a finite irreducible Coxeter group with degrees $d_1 < \cdots < d_n$. A list of these groups and their degrees is given in Table 2 where the degrees for D_n are not listed in increasing order. If k is a positive integer then W has corresponding *Fuss-Catalan number*

$$\operatorname{Cat}^{(k)} W = \prod_{j=1}^{n} \frac{d_j + kd_n}{d_j}.$$

The study of these constants and related ideas has come to be known as "Coxeter-Catalan combinatorics." See the memoir of Armstrong [2] for more information. The corresponding Lucas analogue is

$$\operatorname{Cat}^{(k)}\{W\} = \prod_{j=1}^{n} \frac{\{d_j + kd_n\}}{\{d_j\}}.$$

When referring to a specific W, we put the curly brackets around the subscript giving the rank, e.g., $\operatorname{Cat}^{(k)} B_{\{n\}}$.

Theorem 3.4. *For all finite irreducible Coxeter groups W and all positive integers k we have $\operatorname{Cat}^{(k)}\{W\} \in \mathbb{N}[s,t]$.*

Proof. We note that for the classical types A_n, B_n, D_n Bennett et al. [6] were able to prove this result by combinatorial arguments. It remains open to do the same for the exceptional groups. We will proceed group by group.

Type A_{n-1}. In this case we can express the Fuss-Catalan analogue in terms of the rational Catalan analogue since

$$\operatorname{Cat}^{(k)} A_{\{n-1\}} = \frac{\{(k+1)n\}!}{\{n\}!\{kn+1\}!} = \operatorname{Cat}\{n, kn+1\}.$$

So the result follows from the previous theorem.

Type B_n. In type B_n one can cancel powers of two from the numerator and denominator and so express $\operatorname{Cat}^{(k)} B_n$ as a binomial coefficient. But one can no longer do this when each factor is replaced by the corresponding Lucas polynomial. Instead we will consider a generalization of $\operatorname{Cat}^{(k)} B_{\{n\}}$. Given an integer $m \geq 1$ we let

$$\{n : m\}! = \{m\}\{2m\} \cdots \{nm\}$$

and define an *m-divisible Lucanomial* to be

$$\left\{ \begin{matrix} n : m \\ k : m \end{matrix} \right\} = \frac{\{n : m\}!}{\{k : m\}!\{n-k : m\}!}. \tag{10}$$

So we have the special case

$$\operatorname{Cat}^{(k)} B_{\{n\}} = \left\{ \begin{matrix} (k+1)n : 2 \\ n : 2 \end{matrix} \right\}.$$

To show that (10) is in $\mathbb{N}[s,t]$, note that P_d divides terms at intervals of length $d/\gcd(d,m)$ in $\{n : m\}!$. The rest of the proof is much the same as for the Lucanomials and so is omitted.

Type D_n. We have

$$\begin{aligned} \operatorname{Cat}^{(k)} D_{\{n\}} &= \frac{\{n+2(n-1)k\}}{\{n\}} \left\{ \begin{matrix} (k+1)(n-1) : 2 \\ n-1 : 2 \end{matrix} \right\} \\ &= \frac{\{n+2(n-1)k\}}{\{n\}} \\ &\quad \cdot \frac{\{2+2(n-1)k\}\{4+2(n-1)k\} \cdots \ \{2(k+1)(n-1)\}}{\{n-1 : 2\}!}. \end{aligned}$$

Given $d \geq 2$ there are two cases. If d does not divide n then the factors of P_d in the denominator all occur inside the 2-divisible Lucanomial and so cancel out as for type B_n.

Now suppose $d|n$. In any product of the form $\{2l\}\{2l+2\} \cdots \{2m\}$, the Lucas atom P_d will divide terms at intervals of length $d' = d/\gcd(d,2)$. Since $d|n$ we have that P_d will appears in exactly $n/d' - 1$ factors in $\{n-1 : 2\}!$, giving a total of n/d' times in the denominator of the Fuss-Catalan analogue. If d does not divide $2(n-1)k$ then P_d will divide n/d' terms in the numerator of the last fraction of the above displayed equation and we will be done. If $d|2(n-1)k$ then P_d will only divide $n/d' - 1$ terms in that product, but will also divide $\{n+2(n-1)k\}$ in the numerator, giving the required number of n/d' copies.

Type $I_2(m)$. We have

$$\operatorname{Cat}^{(k)} I_{\{2\}}(m) = \frac{\{km+2\}\{(k+1)m\}}{\{2\}\{m\}}.$$

If P_d appears as a factor in the denominator for $d \geq 3$ then we must have $d|m$. It follows that $d|(k+1)m$ and so is canceled by the corresponding factor in the numerator. If $d = 2$ then there are two cases. If m is even then similar consideration show that P_2^2 appears in both the denominator and the numerator. If m is odd then the denominator only has one P_2. In the numerator, that factor will appear in $\{km+2\}$ if k is even or $\{(k+1)m\}$ if k is odd.

The exceptional types. For the exceptional W, we do not need to consider an infinite number of values of k. This is because whether a given P_d divides a factor $\{a+bk\}$ in the numerator depends only on the congruence class of k modulo d. And the number of choices for d is limited by the factors in the denominator. But those factors do not depend on k and so there are only finitely many choices. In fact, these demonstrations are so straightforward that they can easily be done by hand. So we will only illustrate the procedure in a particular example. Consider

$$\operatorname{Cat}^{(k)} H_{\{4\}} = \frac{\{2+30k\}\{12+30k\}\{20+30k\}\{30+30k\}}{\{2\}\{12\}\{20\}\{30\}}.$$

Now P_4 is in the factorization of $\{12\}$ and $\{20\}$ in the denominator, so we must show it is also appears in the expansion of two of the factors in the numerator regardless of k. Reducing modulo 4, we see that it suffices to look at P_4 factors of

$$\{2+2k\} \cdot \{2k\} \cdot \{2k\} \cdot \{2+2k\} = \{2k\}^2 \cdot \{2(k+1)\}^2.$$

So if k is even, then P_4^2 appears in $\{2k\}^2$, while if k is odd then it divides $\{2(k+1)\}^2$. $\square$

Let W be a finite irreducible Coxeter group of rank n, and let k, i be integers with k positive and $0 \leq i \leq n$. The corresponding *Fuss-Narayana numbers* are $\operatorname{Nar}^{(k)}(W, i)$ which count the number of k-multichains in the noncrossing partition poset of W whose bottom element has rank i. It can be proved that these are always polynomials in k [2, Theorem 3.5.5]. However, there does not seem to be a simple product formula for them which holds for all W, k, i. However, when $i = 1$ we have

$$\operatorname{Nar}^{(k)} W := \operatorname{Nar}^{(k)}(W, 1) = n \prod_{j=1}^{n-1} \frac{kd_n - d_j + 2}{d_j}. \tag{11}$$

Also, for all i,

$$\operatorname{Nar}^{(k)}(A_{n-1}, i) = \frac{1}{n}\binom{n}{i}\binom{kn}{n-i-1},$$

$$\operatorname{Nar}^{(k)}(B_n, i) = \binom{n}{i}\binom{kn}{n-i},$$

$$\mathrm{Nar}^{(k)}(D_n, i) = \binom{n}{i}\binom{k(n-1)}{n-i} + \binom{n-2}{i}\binom{k(n-1)+1}{n-i}.$$

We denote the Lucas analogues by replacing W with $\{W\}$ for a general Coxeter group, and replacing a subscript n by $\{n\}$ in types A, B, and D. We note that Garrett and Killpatrick used a recursion to show that $\mathrm{Nar}^{(1)}(A_{\{n-1\}}, i)$ is an integer when $s = t = 1$. More recently, Nenashev [14] has discovered a combinatorial interpretation for the polynomials $\mathrm{Nar}^{(1)}(A_{\{n-1\}}, i)$.

Theorem 3.5. *For all finite irreducible Coexter groups and all positive integers k we have $\mathrm{Nar}^{(k)}\{W\} \in \mathbb{N}[s,t]$. This is also true of $\mathrm{Nar}^{(k)}(A_{\{n-1\}}, i)$, $\mathrm{Nar}^{(k)}(B_{\{n\}}, i)$, and $\mathrm{Nar}^{(k)}(D_{\{n\}}, i)$ for all i.*

Proof. The $\mathrm{Nar}^{(k)}\{W\}$ are taken care of in much the same way as the Fuss-Catalan analogues for the exceptional groups. And in type B and D the analogues are just sums and products of Lucanomials. So we will only give details for

$$\mathrm{Nar}^{(k)}(A_{\{n-1\}}, i) = \frac{1}{\{n\}}\left\{ {n \atop i} \right\}\left\{ {kn \atop n-i-1} \right\}.$$

If d does not divide n then P_d can only appear in the denominators of the Lucanomials and so the inequality in Theorem 1.1 holds for these d by Theorem 3.2. If $d|n$ then it can not divide both i and $n-i-1$. The demonstration is now completed as in the proof of Theorem 3.3. $\square$

4. Two square theorems

In this section we will find Lucas analogues of theorems of Gauss and Lucas which express (appropriately modified) cyclotomic polynomials in terms of squares of two other polynomials. This will turn out to be easy to do by applying the function Γ defined by (8).

The result of Lucas [20, pp. 309–315, p. 443] is as follows. In it, $\phi(n)$ denotes the Euler totient function.

Theorem 4.1 *(Lucas' formula). If $n \geq 5$ is odd and square-free, then there are polynomials $C_n(q)$ and $D_n(q)$ such that*

$$\Phi_n\left((-1)^{(n-1)/2} q\right) = C_n^2(q) - nqD_n^2(q).$$

If $n \geq 4$ is even and square-free then there are polynomials $C_n(q)$ and $D_n(q)$ such that

$$\Phi_{2n}(q) = C_n^2(q) - nqD_n^2(q).$$

In both cases

1. $C_n(q), D_n(q) \in \mathbb{Z}[q]$,
2. $\deg C_n(q) = \phi(n)/2$ *and* $\deg D_n = \phi(n)/2 - 1$,
3. $C_n(q)$ *and* $D_n(q)$ *are both palindromic.*

To state the analogous result for Lucas atoms we define, for $f(s,t) \in \mathbb{C}[s,t]$,

$$\operatorname{sdeg} f(s,t) = \text{largest power of } s \text{ in } f(s,t).$$

Theorem 4.2. *If $n \geq 5$ is square-free and satisfies $n \equiv 1 \pmod 4$, then there are polynomials $G_n(s,t)$ and $H_n(s,t)$ such that*

$$P_n(s,t) = G_n^2(s,t) + ntH_n^2(s,t). \tag{12}$$

If $n \geq 4$ is even and square-free, then there are polynomials $G_n(s,t)$ and $H_n(s,t)$ such that

$$P_{2n}(s,t) = G_n^2(s,t) + ntH_n^2(s,t).$$

In both cases

1. $G_n(s,t), H_n(s,t) \in \mathbb{Z}[s,t]$,
2. $\operatorname{sdeg} G_n(s,t) = \phi(n)/2$ *and* $\operatorname{sdeg} H_n(s,t) = \phi(n)/2 - 1$. □

Proof. We will only prove the statement about odd n as the one for even values is obtained similarly. Since $n \equiv 1 \pmod 4$ we have from Theorem 4.1 that

$$\Phi_n(q) = \Phi_n\left((-1)^{(n-1)/2}q\right) = C_n^2(q) - nqD_n^2(q). \tag{13}$$

Since $n \geq 5$ we know that $\Phi_n(q)$ is palindromic with $\operatorname{sdeg} P_n(s,t) = \deg \Phi_n(q) = \phi(n)$. From the given facts about $C_n(q)$ and $D_n(q)$ we see that $C_n^2(q)$ and $qD_n^2(q)$ are both palindromic of total degree $\phi(n)$. So, from Proposition 2.1 (a) and (b), we can apply Γ to both sides of (13) and obtain (12). The fact that the polynomials G and H have integer coefficients is a consequence of Proposition 2.1 (e). And the statement about their degrees follows directly from the definition of Γ. □

One might wonder if it is possible to get an analogue of Lucas' formula when n is square-free and congruent to 3 modulo 4. However, one does not seem to exist. For example, we have

$$P_7(s,t) = s^6 + 5s^4t + 6s^2t^2 + t^3$$

If the desired $G_7(s,t)$ and $H_7(s,t)$ did exist, then the term t^3 in $P_7(s,t)$ could not come from G_7^2 because of the odd power of t. But t^3 could also not arise from $7tH_7^2$ since $H_7 \in \mathbb{Z}[s,t]$ and so every term in the product has coefficient divisible by 7.

We will now consider the formula of Gauss [13, Articles 356–357]. To state it, we define a polynomial $p(q) = \sum_i a_i q^i$ with $\operatorname{totdeg} p(q) = d$ to be *anti-palindromic* if $a_i = -a_{d-i}$ for all $0 \le i \le d$.

Theorem 4.3 *(Gauss' formula). If $n \ge 5$ is odd and square-free, then there are polynomials $A_n(q)$ and $B_n(q)$, such that*

$$4\Phi_n(q) = A_n^2(q) - (-1)^{(n-1)/2} n q^2 B_n^2(q)$$

where

1. *$A_n(q), B_n(q) \in \mathbb{Z}[q]$,*
2. *$\deg A_n(q) = \phi(n)/2$ and $\deg B_n = \phi(n)/2 - 2$,*
3. *If $n \equiv 1 \pmod 4$ then $A_n(q)$ and $B_n(q)$ are palindromic.*
4. *If $n \equiv 3 \pmod 4$ then $A_n(q)$ is antipalindromic and B_n is palindromic if n is prime, or vice-versa if n is composite.*

Again, only the case when $n \equiv 1 \pmod 4$ seems to have a Lucas analogue. The proof of the next result is close enough to that of Theorem 4.2 that we leave it to the reader.

Theorem 4.4. *If $n \ge 5$ is square-free and satisfies $n \equiv 1 \pmod 4$, then there are polynomials $E_n(s,t)$ and $F_n(s,t)$, such that*

$$4P_n(s,t) = E_n^2(s,t) - nt^2 F_n^2(s,t)$$

where

1. *$E_n(s,t), F_n(s,t) \in \mathbb{Z}[s,t]$,*
2. *$\operatorname{sdeg} E_n(s,t) = \phi(n)/2$ and $\operatorname{sdeg} F_n(s,t) = \phi(n)/2 - 2$.* □

5. Reduction formulas

The reduction formulas permit the calculation of $\Phi_n(q)$ in terms of $\Phi_m(q)$ for $m < n$. And these computations are done over the integers rather than the complex numbers. The following reductions are all easy to prove directly from the definition of $\Phi_n(q)$ and properties of primitive roots of unity.

Theorem 5.1 *(Reduction formulas). Let n be a positive integer and p be a prime not dividing n.*

(a) We have

$$\Phi_p(q) = [p]_q = 1 + q + q^2 + \cdots + q^{p-1}.$$

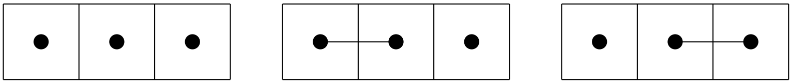

Fig. 1. The tilings in $\mathcal{T}(3)$.

(b) If $m \geq 2$ then

$$\Phi_{p^m n}(q) = \Phi_{pn}(q^{p^{m-1}}).$$

(c) For all p we have

$$\Phi_{pn}(q) = \frac{\Phi_n(q^p)}{\Phi_n(q)}.$$

And for $p = 2$ we also have

$$\Phi_{2n}(q) = \Phi_n(-q). \quad \square$$

So given any n, we can use part (b) to reduce the calculation of $\Phi_n(q)$ to that of the radical (square-free part) of n. Then part (c) turns computation for the radical into knowing $\Phi_p(q)$ for primes p. And for these we have an explicit formula in part (a).

It does not seem as if one can find analogues for these formulas merely by applying Γ. The problem is that the necessary substitutions do not appear to behave well with respect to this map. Instead, we will need a number of lemmas. For some of them, it will be convenient to use a combinatorial description of $\{n\}$ in terms of tilings. For more information about this approach, see the book of Benjamin and Quinn [5]. Consider a row of n boxes. A *tiling*, T, of this row is a covering of the boxes with disjoint tiles where each tile covers two boxes (called a *domino*) or one box (called a *monomino*). Let $\mathcal{T}(n)$ denote the set of such tilings. The set $\mathcal{T}(3)$ is displayed in Fig. 1. Give a single tiling T the weight

$$\operatorname{wt} T = s^{\text{number of monominos in } T} t^{\text{number of dominos in } T}.$$

Also weight any set $\mathcal{T}$ of tilings by

$$\operatorname{wt} \mathcal{T} = \sum_{T \in \mathcal{T}} \operatorname{wt} T.$$

Returning to Fig. 1 we see that $\operatorname{wt}(\mathcal{T}(3)) = s^3 + 2st = \{4\}$. This illustrates a general result which is easy to prove by induction and gives a combinatorial explanation for equation (7).

Lemma 5.2. *For all $n \geq 1$ we have*

$$\{n\} = \mathrm{wt}(\mathcal{T}(n-1)). \quad \square$$

From this result, we get our Lucas analogue of Theorem 5.1 (a). If f is a polynomial in s, t then let $[s^i t^j]f$ be the coefficient of $s^i t^j$ in f.

Corollary 5.3. *For $n \geq 1$ we have*

$$\{n\} = \sum_{k \geq 0} \binom{n-k-1}{k} s^{n-2k-1} t^k.$$

So if p is prime then

$$P_p(s,t) = \sum_{k \geq 0} \binom{p-k-1}{k} s^{p-2k-1} t^k.$$

Proof. The second statement follows from the first and the fact that for a prime p we have $\{p\} = P_1 P_p = P_p$. To prove the first, from the previous lemma, $[s^{n-2k-1}t^k]\{n\}$ is the number of tilings of $\mathcal{T}(n-1)$ with k dominoes and $n-2k-1$ monominoes. But the number of ways to do this is the number of ways of choosing k dominoes from a total of $n-k-1$ tiles, giving the desired binomial coefficient. $\square$

The odd primes and 2 will take different roles in our investigation. So we will need the following result.

Lemma 5.4. *If p is an odd prime then*

$$P_{2p}(s,t) = \sum_{k \geq 0} \left[\binom{p-k}{k} + \binom{p-k-1}{k-1} \right] s^{p-2k-1} t^k, \tag{14}$$

and

$$sP_{2p}(s,t) = \{p+1\} + t\{p-1\}. \tag{15}$$

Proof. The second equation follows from the first the previous corollary. We now prove the first. By Proposition 2.2 (a), it suffices to let Q_{2p} be the right-hand side of (14) and show that

$$\{2p\} = P_1 P_2 P_p Q_{2p}$$

But, again using the previous corollary,

$$P_1P_2P_pQ_{2p} = s\left(\sum_{i\geq 0}\binom{p-i-1}{i}s^{p-2i-1}t^i\right) \\ \times\left(\sum_{j\geq 0}\left[\binom{p-j}{j}+\binom{p-j-1}{j-1}\right]s^{p-2j-1}t^j\right)$$

So

$$[s^{2p-2k-1}t^k]P_1P_2P_pQ_{2p} = \sum_{i+j=k}\binom{p-i-1}{i}\binom{p-j}{j} \\ +\sum_{i+j=k-1}\binom{p-i-1}{i}\binom{p-j-2}{j}. \tag{16}$$

Using Corollary 5.3 yet again

$$[s^{2p-2k-1}t^k]\{2p\} = \binom{2p-k-1}{k}.$$

To show equality of the right-hand sides of the previous two equations note that the single binomial coefficient is the number of tilings of $2p-1$ squares with k dominoes. These tilings are of two types: those with no domino between the $(p-1)$st and pth squares and those where these two squares contain a domino. The first sum in (16) counts the first set of tilings because they can be formed by concatenating a tiling of $p-1$ squares having i dominoes with a tiling of p squares have j dominoes where $i+j=k$. Similarly, the second sum enumerates the second set of tilings since after the given domino is removed then one is left with a tiling of $p-2$ squares and a tiling of $p-1$ squares with a total of $k-1$ dominoes. □

Our goal now is to prove an analogue of Theorem 5.1 (c) for Lucas atoms. We still need several lemmas. The next result is simple to prove using an argument like that in the last paragraph of the previous demonstration. So we omit the proof.

Lemma 5.5. *For $m,n\geq 0$ we have*

$$\{m+n\} = \{m+1\}\{n\}+t\{m\}\{n-1\}. \quad \square$$

We use the notation M or D for a monomino or domino tile, respectively. Also, ST will denote the concatenation of tilings S and T and we will use multiplicity notation such as T^2 for the concatenation of T with itself. We also let $\{n\}=0$ if $n\leq 0$. Define the *sign* of an integer m to be

$$\epsilon(m) = \begin{cases} -1 & \text{if } m \text{ is even,} \\ +1 & \text{if } m \text{ is odd.} \end{cases}$$

Lemma 5.6. *For $m \geq 1$ we have*

$$\{m\}^2 = \{m-1\}\{m+1\} + \epsilon(m)t^{m-1}$$

Proof. We will give a proof when m is odd as the other case is similar. Let $n = m-1$. It suffices to find a weight-preserving bijection

$$f : [\mathcal{T}(n) \times \mathcal{T}(n)]^- \to \mathcal{T}(n-1) \times \mathcal{T}(n+1)$$

where $[\mathcal{T}(n) \times \mathcal{T}(n)]^-$ is $\mathcal{T}(n) \times \mathcal{T}(n)$ with the pair $(D^{n/2}, D^{n/2})$ removed. Label the n squares left to right from 1 to n. Given a pair (S,T) in the domain, consider the largest index $i \geq 0$ such that only dominoes cover squares of index less than or equal to i in both S and T. So i is even and write $S = D^{i/2}S'$ and $T = D^{i/2}T'$. Since $(S,T) \neq (D^{n/2}, D^{n/2})$ the tilings S', T' are nonempty. If $S' = MS''$ for some S'' then let $f(S,T) = (D^{i/2}S'', D^{i/2}MT')$. If $S' = DS''$ then, by maximality of i, we must have $T' = MT''$ for some T''. In this case let $f(S,T) = (D^{i/2}MS'', D^{i/2}DT'')$. Clearly this map preserves weight. And its inverse is easy to construct, so it is bijective. $\square$

The next lemma can be thought of as a combination of the previous two.

Lemma 5.7. *If $n \geq 2m$ then*

$$\{n\} = (\{m+1\} + t\{m-1\})\{n-m\} + \epsilon(m)t^m\{n-2m\}.$$

Proof. We induct on n, assuming m is odd as the even case is similar. For the base cases, first consider $n = 2m$. So we wish to prove

$$\{2m\} = \{m+1\}\{m\} + t\{m-1\}\{m\}$$

which follows by letting $m = n$ in Lemma 5.5. For the other base case, suppose $n = 2m+1$ and compute the right-hand side of the equality using Lemma 5.6 and then Lemma 5.5

$$\{m+1\}^2 + t\{m-1\}\{m+1\} + t^m = \{m+1\}^2 + t(\{m\}^2 - t^{m-1}) + t^m = \{2m+1\}.$$

For the induction step, we use the defining recursion for the Lucas sequence several times on the right-hand side of the desired equation, letting $A = \{m+1\} + t\{m-1\}$ for readability,

$$\begin{aligned}
&A\{n-m\} + t^m\{n-2m\} \\
&\qquad = A(\{n-m-1\} + t\{n-m-2\}) + t^m(\{n-2m-1\} + t\{n-2m-2\}) \\
&\qquad = (A\{n-m-1\} + t^m\{n-2m-1\}) + t(A\{n-m-2\} + t^m\{n-2m-2\}) \\
&\qquad = \{n-1\} + t\{n-2\} \\
&\qquad = \{n\}
\end{aligned}$$

which is what we wished to show. $\square$

We have one last identity to prove before demonstrating our first main theorem of this section. Note that we can unify the two cases in the following results by using the fact that for p prime we have, by equation (15),

$$\{p+1\} + t\{p-1\} = \begin{cases} s^2 + 2t & \text{if } p = 2, \\ sP_{2p} & \text{if } p \geq 3. \end{cases} \tag{17}$$

But because of the subscripts, it is easier to read these results in the format we present.

Lemma 5.8. *If p is prime then for all $n \geq 0$ we have*

$$\{pn\} = \begin{cases} \{p\} \cdot \{n\}_{s^2+2t,-t^2} & \text{if } p = 2, \\ \{p\} \cdot \{n\}_{sP_{2p},t^p} & \text{if } p \geq 3. \end{cases}$$

Proof. We will do the case for odd primes as $p = 2$ is similar. Induct on n. The identity is easy to check when $n = 0, 1$. For $n \geq 2$ we use in turn the recursion defining the Lucas sequence, induction, equation (17), and Lemma 5.7 (with n replaced by pn and m replaced by p) to obtain

$$\begin{aligned} \{p\} \cdot \{n\}_{sP_{2p},t^p} &= \{p\} \left(sP_{2p} \cdot \{n-1\}_{sP_{2p},t^p} + t^p \cdot \{n-2\}_{sP_{2p},t^p} \right) \\ &= sP_{2p} \cdot \{pn-p\} + t^p \cdot \{pn-2p\} \\ &= (\{p+1\} + t\{p-1\}) \cdot \{pn-p\} + t^p \cdot \{pn-2p\} \\ &= \{pn\} \end{aligned}$$

as desired. $\square$

We can finally prove our analogue of Theorem 5.1 (c).

Theorem 5.9. *If $n \geq 2$ is a positive integer and p is a prime not dividing n, then*

$$P_{pn}(s,t) = \begin{cases} \dfrac{P_n(s^2+2t,-t^2)}{P_n(s,t)} & \text{if } p = 2, \\ \dfrac{P_n(sP_{2p},t^p)}{P_n(s,t)} & \text{if } p \geq 3. \end{cases}$$

Proof. We assume p is odd as $p = 2$ is similar. We also continue to use P_n as an abbreviation for $P_n(s,t)$, but not for any other set of variables. Induct on n. For $n = 2$, we use the previous lemma and Proposition 2.2 (a) to write

$$\{p\}\{2\}_{sP_{2p},t^p} = \{2p\} = P_2 P_p P_{2p}.$$

Solving for P_{2p} and using the fact that $\{p\} = P_p$ completes the base case.

For the induction step we use in turn Proposition 2.2 (a), the hypotheses on p and n, induction, and Lemma 5.8 to obtain

$$\begin{aligned}
\{pn\} &= \prod_{d|pn} P_d \\
&= \prod_{d|n} P_d P_{pd} \\
&= P_p P_n P_{pn} \prod_{\substack{d|n \\ d\neq 1,n}} P_d \cdot P_d(sP_{2p}, t^p)/P_d \\
&= \frac{P_p P_n P_{pn} \{n\}_{sP_{2p},t^p}}{P_n(sP_{2p}, t^p)} \\
&= \frac{P_n P_{pn} \{pn\}}{P_n(sP_{2p}, t^p)}
\end{aligned}$$

Solving for P_{pn} finishes the proof. $\square$

We can use this theorem to give a new relation between cyclotomic polynomials. Note that setting $s = q + 1$ and $t = -q$ in the left-hand side of (17) we get, using (2),

$$\{p + 1\} + t\{p - 1\} = [p + 1]_q - q[p - 1]_q = q^p + 1.$$

Using this substitution, we have the following immediate corollary of Theorem 5.9.

Corollary 5.10. *If $n \geq 2$ is a positive integer and p is prime not dividing n, then*

$$\Phi_{pn}(q)\Phi_n(q) = P_n(q^p + 1, \epsilon(p)q^p). \quad \square$$

We also have a Lucas analogue of Theorem 5.1 (b).

Theorem 5.11. *If n is a positive integer, p is a prime not dividing n, and $m \geq 2$ then*

$$P_{p^m n}(s, t) = \begin{cases} P_{p^{m-1}n}(s^2 + 2t, -t^2) & \text{if } p = 2, \\ P_{p^{m-1}n}(sP_{2p}, t^p) & \text{if } p \geq 3. \end{cases}$$

Proof. We induct on m, where the base case is similar enough to the induction step that we will only provide details for the latter. And we will also just consider odd primes for similar reasons. Given m, we induct on n. For $n = 1$, by Lemma 5.8 we have

$$\{p^m\} = \{p\}\{p^{m-1}\}_{sP_{2p},t^p}$$

Now expand both sides, using Proposition 2.2 (a) and use the fact that $\{p\} = P_p$, to get

$$P_p P_{p^2} \cdots P_{p^m} = P_p \cdot P_p(sP_{2p}, t^p) \cdot P_{p^2}(sP_{2p}, t^p) \cdot \ \cdots \ \cdot P_{p^{m-1}}(sP_{2p}, t^p).$$

Using the induction hypothesis on m to cancel all but one factor on each side gives the desired equality. To deal with $n \geq 2$, expand $\{p^m n\}$ in a similar fashion to what was done for $\{pn\}$ in Theorem 5.9. After cancellation of terms, which uses the induction hypotheses on both m and n, one obtains $P_{p^m n}/P_{p^{m-1}n}(sP_{2p}, t^p) = 1$ which is what we wish to prove. $\square$

Again, we can get a relation between cyclotomic polynomials and Lucas atoms by specialization.

Corollary 5.12. *If n is a positive integer, p is prime not dividing n, and $m \geq 2$ then*

$$\Phi_{p^m n}(q) = P_{p^{m-1}n}(q^p + 1, \epsilon(p)q^p). \quad \square$$

6. Evaluations

There are a number of interesting evaluations of the cyclotomic polynomials at various integers. For example, suppose $b > 1$ is an integer relatively prime to the prime p, and n is the multiplicative order of b modulo p. Then it follows quickly from (9) that $p | \Phi_n(b)$. For a more substantive example, there is the following conjecture which is implied by a conjecture of Bouniakowsky [7].

Conjecture 6.1. *For every positive integer n there are infinitely many positive integers b such that $\Phi_n(b)$ is prime.*

We will prove some facts about the Lucas atoms modulo two and three. The proofs will provide an application of the reduction formulas from Section 5. They will also permit us to say something about the divisibility of the cyclotomic polynomials themselves. We first need some information about the coefficients of $P_n(s, t)$.

Lemma 6.2. *For $n \geq 3$ we have*

$$P_n = \sum_{k=0}^{\phi(n)/2} c_k s^{\phi(n)-2k} t^k$$

for certain constants c_k, where $c_0 = 1$ and

$$c_{\phi(n)/2} = \begin{cases} p & \text{if } n = 2 \cdot p^m \text{ for a prime } p \geq 2 \text{ and } m \geq 1, \\ 1 & \text{else.} \end{cases}$$

Proof. All of these statements about P_n are proved similarly, so we will just present a demonstration for the value of $c_{\phi(n)/2}$. We induct on n, where the case $n = 3$ is easy to check. From Lemma 5.2 we can write

$$\{n\} = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} a_j s^{n-2j-1} t^j \tag{18}$$

where the largest power of t has coefficient

$$a_{\lfloor (n-1)/2 \rfloor} = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases} \tag{19}$$

Now using Proposition 2.2 (a), induction, and the fact that $\sum_{d|n} \phi(d) = n$, we get from (18) that the degree of P_n as a polynomial in t is $\phi(n)/2$. Using the same line of reasoning with (19) we see that $c_{\phi(n)/2} = 1$ for n odd. To complete the proof, we now repeat this argument in turn for the cases of $n = 2 \cdot p^m$ where p is prime, and of $n = 2^l \cdot k$ where k is odd and either $l \geq 2$ or k has at least two prime factors. The details are left to the reader. $\square$

We can now determine the behavior of $P_n(s,t)$ when s, t are taken modulo 2.

Theorem 6.3. *Suppose $n \geq 2$. Then*

(a) $P_n(0,0) = 0$,
(b) $P_n(1,0) = 1$,
(c) $2|P_n(0,1)$ *if and only if* $n = 2^m$ *for some* $m \geq 1$,
(d) $2|P_n(1,1)$ *if and only if* $n = 3 \cdot 2^m$ *for some* $m \geq 0$.

Proof. The first three statements follow easily from the previous lemma. So consider $P_n(1,1)$. Suppose first that 3 does not divide n. Let the nth Fibonacci number be denoted F_n and recall that $F_n = \{n\}_{1,1}$. It is well known and simple to prove that $2|F_n$ if and only if $3|n$. So if 3 is not a divisor of n then $\{n\}_{1,1}$ is odd. Thus the same must be true of its factor $P_n(1,1)$.

Since $P_3(1,1) = 2$, we will now consider $n = 3k$ where $k \geq 2$ is not divisible by 3. From Theorem 5.9 we see that $P_{3k}(1,1) \equiv P_k(0,1)/P_k(1,1) \pmod 2$ since, as we have just proved, the denominator is not divisible by 2. By part (c), $P_k(0,1)$ is even precisely when $k \geq 2$ is a power of 2, which finishes this case.

Finally, suppose $n = 3^m k$ where $m \geq 2$ and k is not divisible by 3. By Theorem 5.11 and the fact that $P_6(1,1)$ is even we have $P_{3^m k}(1,1) \equiv P_{3^{m-1}k}(0,1) \pmod 2$. But $3^{m-1}k$ is never a power of two since $m \geq 2$. So, by part (c) again, we have that $P_{3^{m-1}k}(0,1)$, and thus $P_{3^m k}(1,1)$, is odd as announced in the statement of the theorem. $\square$

We can use the previous result to find the highest power of two which divides an evaluation of a cyclotomic polynomial. For any prime p and integer n we let $\nu_p(n)$ be the highest power of p dividing n.

Corollary 6.4. *If b is an integer and $n \geq 3$. Then*

$$\nu_2(\Phi_n(b)) = \begin{cases} 1 & \text{if } n = 2^m \text{ for some } m \geq 2 \text{ and } b \text{ is odd,} \\ 0 & \text{else.} \end{cases}$$

Proof. We have $\Phi_n(b) = P_n(b+1, -b)$. So we are only interested in the case where the two arguments in P_n are of different parity. But by Theorem 6.3, the only time $P_n(b+1, -b)$ for can be even for $n \geq 3$ is when $n = 2^m$ for some $m \geq 2$. So we need to investigate what happens when $\Phi_{2^m}(b) = b^{2^{m-1}} + 1$. Clearly if b is even then this is not divisible by 2. And it is also easy to check that if b is odd then, since 2^{m-1} is even, we have $\Phi_{2^m}(b) \equiv 2 \pmod 4$ which completes the proof. □

The proofs of the next two results are similar enough to those of Theorem 6.3 and Corollary 6.4 that we will omit them. However, as a labor-saving device, we note that because the powers of s in $P_n(s,t)$ are all even for $n \geq 3$, we always have $P_n(a,b) = P_n(-a,b)$.

Theorem 6.5. *Suppose $n \geq 3$. Then*

1. $P_n(0,0) = 0$,
2. $P_n(\pm 1, 0) = 1$,
3. $3|P_n(0, \pm 1)$ *if and only if* $n = 2 \cdot 3^m$ *for some* $m \geq 1$,
4. $3|P_n(\pm 1, 1)$ *if and only if* $n = 4 \cdot 3^m$ *for some* $m \geq 0$,
5. $3|P_n(\pm 1, -1)$ *if and only if* $n = 3 \cdot 3^m$ *for some* $m \geq 0$. □

Corollary 6.6. *If b is an integer and $n \geq 3$. Then*

$$\nu_3(\Phi_n(b)) = \begin{cases} 1 & \text{if } n = 3^m \text{ for some } m \geq 1 \text{ and } b \equiv 1 \pmod 3, \\ 0 & \text{else.} \end{cases} \qquad \square$$

We note that, as opposed to the situation in Corollaries 6.4 and 6.6, one can have $\nu_p(\Phi_n(b)) \geq 2$ for primes other than 2 and 3. For example $\Phi_4(7) = 50 = 2 \cdot 5^2$. We also remark that extending Theorems 6.3 and 6.5 to arbitrary primes is almost certainly hard. One of the crucial tools in their proofs is the knowledge of the period of the Fibonacci sequence modulo 2 and modulo 3. Although it is easy to see that this sequence is periodic modulo any integer, finding a formula for the period is a famous unsolved problem.

7. Comments and open problems

We will now present some avenues for future research hoping that the reader will be interested in exploring them.

(1) Combinatorial interpretations. Since the Lucas atoms have nonnegative integer coefficients, one would hope that they count something. But we have been unable to come up with a simple combinatorial interpretation for these polynomials, despite the fact that there are various well-known interpretations for the Lucas polynomials themselves. By using the reduction formulas, we have determined a complicated way of describing $P_n(s,t)$ when n is a power of a prime in terms of certain colored tilings. But it seems unlikely that this will extend to all n. Once an interpretation is in place, it would be nice to take that as the *definition* of the Lucas atoms and then derive properties such as the decomposition (3) combinatorially.

(2) Alternating gamma vectors. One of the reasons for interest in gamma expansions is because of their connection with unimodality. Call a polynomial $p(q) = \sum_{j\geq 0} a_j q^j$ with real coefficients *unimodal* if

$$a_0 \leq a_1 \leq \ldots \leq a_m \geq a_{m+1} \geq \ldots$$

for some index m. Unimodal sequences abound in algebra, combinatorics, and geometry. See the survey articles of Stanley [22] and Brenti [9] and Brändén [8] for more information. Now suppose that $p(q)$ is palindromic. If its gamma coefficients are all nonnegative, then $p(q)$ must be unimodal since all the polynomials involved in its expansion are unimodal with the same center of symmetry. However, the definition of the map Γ in (8) suggests that it might also be interesting to look at gamma expansions where the coefficients alternate in sign. For example, this is true of the gamma expansions of the cyclotomic polynomials and their products. Very little work has been done in this direction and we are only aware of a single paper of Brittenham, Carroll, Petersen, and Thomas [10] on this topic.

(3) Coxeter groups. There are several ways in which the proofs of Theorems 3.4 and 3.5 could be improved. First, it would be nice to have uniform proofs for all finite irreducible W rather than having to go case-by-case. It would also be desirable to find combinatorial proofs, especially in the cases where one is not already known. And the best scenario would be to have these proofs rely on the combinatorics of the groups themselves. In particular, it would be very interesting if these Lucas analogues are the generating functions for some statistics on the poset of noncrossing partitions $NC(W)$ which would reduce to the original counts when $s = 2$ and $t = -1$.

Acknowledgments

We wish to thank Richard Stanley who originally had the idea of factoring the Lucas polynomials into Lucas atoms. Without his seminal insight, this paper could not have been written. We also thank Clifford Smyth for pointing out the reference to the paper of Levy.

References

[1] F. Aliniaeifard, N. Bergeron, C. Ceballos, T. Denton, S. Li Xiao, Algebraic Combinatorics Seminar, Fields Institute, 2013–2015, http://garsia.math.yorku.ca/fieldseminar/.
[2] D. Armstrong, Generalized noncrossing partitions and combinatorics of Coxeter groups, Mem. Am. Math. Soc. 202 (949) (2009) x+159.
[3] C.A. Athanasiadis, Gamma-positivity in combinatorics and geometry, preprint, arXiv:1711.05983.
[4] A.T. Benjamin, S.S. Plott, A combinatorial approach to Fibonomial coefficients, Fibonacci Q. 46/47 (1) (2008/09) 7–9.
[5] A.T. Benjamin, J.J. Quinn, Proofs That Really Count, The Dolciani Mathematical Expositions, vol. 27, Mathematical Association of America, Washington, DC, 2003.
[6] C. Bennet, J. Carrillo, J. Machacek, B. Sagan, Combinatorial interpretations of lucas analogues of binomial coefficients and catalan numbers, preprint, arXiv:1809.09036.
[7] V. Bouniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, Mém. Acad. Imp. Sci. St.-Pétersbg. 6 (1857) 305–329.
[8] P. Brändén, Unimodality, log-concavity, real-rootedness and beyond, in: Handbook of Enumerative Combinatorics, in: Discrete Math. Appl. (Boca Raton), CRC Press, Boca Raton, FL, 2015, pp. 437–483.
[9] F. Brenti, Log-concave and unimodal sequences in algebra, combinatorics, and geometry: an update, in: Jerusalem Combinatorics '93, in: Contemp. Math., vol. 178, Amer. Math. Soc., Providence, RI, 1994, pp. 71–89.
[10] C. Brittenham, A.T. Carroll, T. Kyle Petersen, C. Thomas, Unimodality via alternating gamma vectors, Electron. J. Comb. 23 (2) (2016) 2.40, 22.
[11] S.B. Ekhad, The Sagan-Savage Lucas-Catalan polynomials have positive coefficients, preprint, arXiv:1101.4060, 2011.
[12] K. Garrett, K. Killpatrick, A recursion for the FiboNarayana numbers and the generalized Narayana numbers, preprint, arXiv:1910.08855, 2019.
[13] C.F. Gauss, Disquisitiones Arithmeticae, Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, revised by William C. Waterhouse, Cornelius Greither and A.W. Grootendorst and with a preface by Waterhouse.
[14] Gleb Nenashev, personal communication.
[15] D. Levy, The irreducible factorization of Fibonacci polynomials over $\mathbf{Q}$, Fibonacci Q. 39 (4) (2001) 309–319.
[16] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques, Am. J. Math. 1 (2) (1878) 184–196.
[17] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques, Am. J. Math. 1 (4) (1878) 289–321.
[18] E. Lucas, Theorie des fonctions numeriques simplement periodiques [continued], Am. J. Math. 1 (3) (1878) 197–240.
[19] S. Rao, J. Suk, Diheadral sieving phenomena, preprint, arXiv:1710.06517, 2017.
[20] H. Riesel, Prime Numbers and Computer Methods for Factorization, second edition, Progress in Mathematics, vol. 126, Birkhäuser Boston, Inc., Boston, MA, 1994.
[21] B.E. Sagan, C.D. Savage, Combinatorial interpretations of binomial coefficient analogues related to Lucas sequences, Integers 10 (A52) (2010) 697–703.
[22] R.P. Stanley, Log-concave and unimodal sequences in algebra, combinatorics, and geometry, in: Graph Theory and Its Applications: East and West, Jinan, 1986, in: Ann. New York Acad. Sci., vol. 576, New York Acad. Sci., New York, 1989, pp. 500–535.