UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

On the formal series Witt transform

Moree, P.

Published in:
Discrete mathematics

DOI:
10.1016/j.disc.2005.03.004

Link to publication

Citation for published version (APA):
Moree, P. (2005). On the formal series Witt transform. *Discrete mathematics*, *295*(1-3), 143-160. https://doi.org/10.1016/j.disc.2005.03.004

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (http://dare.uva.nl)

Download date: 19 Jan 2021

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 295 (2005) 143–160

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

The formal series Witt transform

Pieter Moree

Max-Planck-Institut, Vivatsgasse 7, D-53111 Bonn, Germany

Received 9 February 2004; received in revised form 14 February 2005; accepted 2 March 2005
Available online 9 April 2005

Abstract

Given a formal power series $f(z) \in \mathbb{C}[\![z]\!]$ we define, for any positive integer r, its rth Witt transform, $\mathscr{W}_f^{(r)}$, by $\mathscr{W}_f^{(r)}(z) = \frac{1}{r}\sum_{d|r} \mu(d) f(z^d)^{r/d}$, where μ denotes the Möbius function. The Witt transform generalizes the necklace polynomials, $M(\alpha; n)$, that occur in the cyclotomic identity

$$\frac{1}{1-\alpha y} = \prod_{n=1}^{\infty} (1-y^n)^{-M(\alpha;n)}.$$

Several properties of $\mathscr{W}_f^{(r)}$ are established. Some examples relevant to number theory are considered.
© 2005 Elsevier B.V. All rights reserved.

MSC: primary 05A19; secondary 11B75; 17B01

Keywords: Cyclotomic identity; Lyndon words

1. Introduction

The polynomial

$$M(\alpha; n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)\alpha^d$$

is called the *necklace polynomial* in [17] and arises naturally in many combinatorial problems. This polynomial is of degree n in α with rational coefficients and takes on integer values

E-mail address: moree@mpim-bonn.mpg.de.

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.03.004

for integer arguments (it is a so-called *integral polynomial*). Taking n to be a prime we infer from this Fermat's little theorem and indeed, in this context the polynomials $M(\alpha; n)$ were first studied (starting with Gauss), see [6, Chapter 11]. If $\alpha \in \mathbb{Z}_{\geqslant 1}$, $n \geqslant 3$ and $n \not\equiv 2 (\mathrm{mod}\, 4)$, then $M(\alpha; n)$ is even [5]. It is not difficult to show [18, Lemma 3] that for $n \geqslant 1$ and $\alpha > 1$, with α real, $M(\alpha; n) > 0$. A sequence $\{a_n\}_{n=1}^{\infty}$ of non-negative integers is said to be *exactly realizable* if there is a set X and a map $T : X \to X$ for which $\#\{x \in X | T^n x = x\} = a_n$ for all $n \geqslant 1$. Puri and Ward [25] proved that a sequence $\{a_n\}_{n=1}^{\infty}$ of non-negative integers is exactly realizable iff $\sum_{d|n} \mu(n/d) a_d$ is non-negative and divisible by n for all $n \geqslant 1$. Taking $X = \mathbb{C}$ and T the map that sends z to z^{α}, we see that the sequence $\{\alpha^n\}_{n=1}^{\infty}$ is exactly realizable for $\alpha \in \mathbb{Z}_{\geqslant 1}$ and hence, by the result of Puri and Ward, that $\{M(\alpha; n)\}_{n=1}^{\infty}$ consists of non-negative integers only.

The necklace polynomial $M(\alpha; n)$ got its name since it can be interpreted as enumerating non-periodic circular strings of n beads that can be strung from beads of at most α distinct colours. It is called the Witt formula when used to count the number of monic irreducible polynomials of degree n over the finite field $\mathbb{F}_q$, with q a prime power. It also gives the dimension of the subspace spanned by the homogeneous elements of degree n in the free Lie algebra over a set of α elements (this is the original context in which Witt [30] discovered his formula). The necklace polynomial also arises in the context of Philip Hall's commutator collecting algorithm, see e.g. [10, Chapter 11]. Golomb [9] showed that the maximum number of words possible in a bounded synchronization delay code with word length n over an alphabet of α elements equals $M(\alpha; n)$. More recently necklace polynomials also arose in the study of multiple zeta series [12]. There are also connections with the theory of formal groups [15].

The cyclotomic identity states, that as formal series we have

$$\frac{1}{1-\alpha y} = \prod_{n=1}^{\infty} \left(\frac{1}{1-y^n} \right)^{M(\alpha;n)}.$$

Using logarithmic differentiation and Möbius inversion the cyclotomic identity is easily established. Metropolis and Rota [17] gave the first natural, i.e. bijective proof of the cyclotomic identity, that is a proof which is entirely set-theoretic, where set-theoretic constructions are made to correspond biuniquely to the algebraic operations on formal power series. They also noted the following properties of the necklace polynomials (where (a, b) denotes the greatest common divisor and $[a, b]$ the least common multiple of the integers a and b).

Theorem 1 (*Metropolis and Rota [17]*).

(1) *We have, for any positive integers α, β and n:*

$$M(\alpha\beta; n) = \sum_{[i,j]=n} (i, j) M(\alpha; i) M(\beta; j),$$

where the sum ranges over all positive integers i and j with $[i, j] = n$.

(2) *We have, for any positive integers* β, r *and* n:

$$M(\beta^r; n) = \sum_{[j,r]=nr} \frac{j}{n} M(\beta; j),$$

where the sum ranges over the integers j with $[r, j] = nr$.

Metropolis and Rota write regarding the above identities: 'We shall be concerned with some remarkable identities satisfied by the polynomials $M(\alpha, n)$, which apparently have not been previously noticed'. However, certainly part 1 of their result was known long before, see e.g. [4], but Metropolis and Rota gave the first combinatorial proof.

In this paper we consider a generalization of the cyclotomic identity and hence also of the necklace polynomial.

Definition 1. For $f(z) \in \mathbb{C}[\![z]\!]$ and $r \geqslant 1$ any integer, let

$$\mathscr{W}_f^{(r)}(z) = \frac{1}{r} \sum_{d|r} \mu(d) f(z^d)^{r/d} = \sum_{j=0}^{\infty} m_f(j, r) z^j.$$

With this definition the cyclotomic identity generalizes as follows:

Theorem 2 (*Moree [19]*). *Suppose that* $f(z) \in \mathbb{Z}[\![z]\!]$. *Then, as formal power series in y and z, we have*

$$\frac{1}{1 - yf(z)} = \prod_{j=0}^{\infty} \prod_{k=1}^{\infty} (1 - z^j y^k)^{-m_f(j,k)}.$$

Note that if we take $f(z) = \alpha$, the cyclotomic identity is obtained and that $\mathscr{W}_f^{(r)}(z) = M(\alpha; r)$.

The following general properties of $\mathscr{W}_f^{(r)}$ will be established in this note. Parts 4 and 5 generalize Theorem 1.

Theorem 3. *Let* $r \geqslant 1$ *be an integer. Let* $f, g \in \mathbb{C}[\![z]\!]$.

(1) *We have* $\mathscr{W}_{z^k f}^{(r)}(z) = z^{kr} \mathscr{W}_f^{(r)}(z)$.
(2) *We have* $\sum_{d|r} \frac{r}{d} \mathscr{W}_f^{(r/d)}(z^d) = f(z)^r$,
(3) *We have*

$$(-1)^r \mathscr{W}_{-f}^{(r)}(z) = \begin{cases} \mathscr{W}_f^{(r)}(z) + \mathscr{W}_f^{(r/2)}(z^2) & \text{if } r \equiv 2 \pmod 4, \\ \mathscr{W}_f^{(r)}(z) & \text{otherwise}. \end{cases}$$

(4) *We have*

$$\mathscr{W}_{fg}^{(r)}(z) = \sum_{[i,j]=r} (i, j) \mathscr{W}_f^{(i)}(z^{r/i}) \mathscr{W}_g^{(j)}(z^{r/j}),$$

where the sum is over all positive integers i and j with $[i, j] = r$.

(5) *We have*

$$\mathscr{W}^{(r)}_{f^k}(z)=\sum_{[j,k]=rk}\frac{j}{r}\mathscr{W}^{(j)}_f(z^{rk/j}),$$

where the sum is over all positive integers j with $[j,k]=rk$.

(6) *Let* v *and* w *be positive integers. Then*

$$\mathscr{W}^{(r)}_{f^{w/(v,w)}g^{v/(v,w)}}(z)=\sum\frac{(vi,wj)}{(v,w)}\mathscr{W}^{(i)}_f(z^{r/i})\mathscr{W}^{(j)}_g(z^{r/j}),$$

where the sum ranges over the set $\{i,j:\ ij/(vi,wj)=r/(v,w)\}$.

The latter three properties simplify if one puts $\mathscr{C}^{(r)}_f(z)=r\mathscr{W}^{(r)}_f(z)$; the above identities then hold with $\mathscr{W}$ replaced by $\mathscr{C}$ and (i,j) (in part 4), j/r (in part 5) and $(vi,wj)/(v,w)$ (in part 6) left out.

In the following result the coefficients of f are assumed to be integers (recall that a polynomial f is self-reciprocal if $z^{\deg f}f(1/z)=f(z)$).

Theorem 4.

(1) *If* $f(z)\in\mathbb{Z}[z]$ *is self-reciprocal, then so is* $\mathscr{W}^{(r)}_f(z)$.
(2) *If* $f(z)\in\mathbb{Z}[\![z]\!]$, *then* $\mathscr{W}^{(r)}_f(z)\in\mathbb{Z}[\![z]\!]$.
(3) *If* $f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$, *then* $\mathscr{W}^{(r)}_f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$.
(4) *If* $f(z)\in\mathbb{Z}_{\leqslant 0}[\![z]\!]$, *then* $(-1)^r\mathscr{W}^{(r)}_f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$.
(5) *If* $f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$ *and* $g(z)-f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$, *then* $\mathscr{W}^{(r)}_g(z)-\mathscr{W}^{(r)}_f(z)\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$.

The final and (deepest) result is concerned with the monotonicity of the coefficients of $\mathscr{W}^{(r)}_f(z)$.

Theorem 5. *Let* $f(z)=\sum_j a_jz^j\in\mathbb{Z}_{\geqslant 0}[\![z]\!]$. *In parts* 1 *and* 2 *it is assumed that* $a_0>0$. *In the remaining parts it is assumed in addition that* $\{a_j\}_{j=0}^{\infty}$ *is a non-decreasing sequence.*

(1) *Let* $k\geqslant 2$. *The sequence* $\{m_f(k,r)\}_{r=1}^{\infty}$ *is non-decreasing*.
(2) *Let* $k\geqslant 3$. *The sequence* $\{(-1)^r m_{-f}(k,r)\}_{r=1}^{\infty}$ *is non-decreasing*.
(3a) *If* $r\geqslant 1$, *then* $m_f(k,r)\geqslant 1$.
(3b) *If* $r\geqslant 1$, *then the sequence* $\{m_f(k,r)\}_{k=0}^{\infty}$ *is non-decreasing*.
(3c) *If* $r\geqslant 3$, *the sequence* $\{m_f(k,r)\}_{k=2}^{\infty}$ *is strictly increasing*.
(4a) *If* $r\geqslant 1$, *then* $(-1)^r m_{-f}(k,r)\geqslant 1$.
(4b) *If* $r\geqslant 1$, *then the sequence* $\{(-1)^r m_{-f}(k,r)\}_{k=0}^{\infty}$ *is non-decreasing*.
(4c) *If* $r\geqslant 3$, *the sequence* $\{(-1)^r m_{-f}(k,r)\}_{k=2}^{\infty}$ *is strictly increasing*.

The condition that $\{a_j\}_{j=0}^{\infty}$ be non-decreasing for parts 3 and 4 seems to be rather stringent, but actually cannot be dropped.

Note that $m_f(0, r) = M(f(0); r)$. The monotonicity aspects of necklace polynomials are not covered by Theorem 5, but are easily determined using the same methods:

Proposition 1. *Let $\beta(2) = \beta(3) = 2$ and $\beta(k) = 1$ for $k \geqslant 4$. Let $c \geqslant 2$ be an integer. The sequence $\{M(c; r)\}_{r=\beta(c)}^{\infty}$ is strictly increasing. Let $r \geqslant 1$. The sequence $\{M(c; r)\}_{c=1}^{\infty}$ is strictly increasing.*

The remaining part of the paper is concerned with the proof of Theorems 3–5 and the latter proposition. In the next section some lemmas on circular words are established. In the final section some examples are discussed.

2. Circular words and Witt's dimension formula

We will make use of an easy result on cyclic words. A word $a_1 \cdots a_n$ is called *circular* or *cyclic* if a_1 is regarded as following a_n, where $a_1 a_2 \cdots a_n$, $a_2 \cdots a_n a_1$ and all other cyclic shifts (rotations) of $a_1 a_2 \cdots a_n$ are regarded as the same word. A circular word of length n may conceivably be given by repeating a segment of d letters n/d times, with d a divisor of n. Then we say the word is of *period* d. Each word belongs to an unique smallest period; the *minimal period*.

Consider circular words of length n on an alphabet $x_1, \ldots, x_r$ consisting of r letters. The total number of ordinary words such that x_i occurs n_i times equals $\binom{n}{n_1,\ldots,n_r}$, where $n_1 + \cdots + n_r = n$ and

$$\binom{n}{n_1, \ldots, n_r} = \frac{n!}{n_1! \ldots n_r!}.$$

Let $M(n_1, \ldots, n_r)$ denote the number of circular words of length $n_1 + \cdots + n_r = n$ and minimal period n (often called *aperiodic words*) such that the letter x_i appears exactly n_i times. This leads to the formula

$$\binom{n}{n_1, \ldots, n_r} = \sum_{d \mid \gcd(n_1,\ldots,n_r)} \frac{n}{d} M\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d}\right). \tag{1}$$

whence it follows by Möbius inversion that

$$M(n_1, \ldots, n_r) = \frac{1}{n} \sum_{d \mid \gcd(n_1,\ldots,n_r)} \mu(d) \binom{\frac{n}{d}}{\frac{n_1}{d}, \ldots, \frac{n_r}{d}}. \tag{2}$$

Note that $M(n_1, \ldots, n_r)$ is totally symmetric in the variables $n_1, \ldots, n_r$. If $\{n_j\}_{j=1}^{\infty}$ is a sequence such that there is a k for which $n_j = 0$ for every $j \geqslant k+1$, then we define $M(\{n_j\}_{j=1}^{\infty}) = M(n_1, \ldots, n_k)$. Note that

$$\frac{1}{n} \sum_{d \mid n} \mu(d)(z_1^d + \cdots + z_r^d)^{n/d} = \sum_{\substack{n_1+\cdots+n_r=n \\ n_j \geqslant 0}} M(n_1, \ldots, n_r) z_1^{n_1} \ldots z_r^{n_r}. \tag{3}$$

It turns out that the numbers $M(n_1,\ldots,n_r)$ are related to counting so-called basic commutators in group theory [10, Chapter XI]. These numbers also occur in a classical result in Lie theory, namely Witt's formula for the homogeneous subspaces of a finitely generated free Lie algebra L: if H is the subspace of L generated by all homogeneous elements of multidegree $(n_1,\ldots,n_r)$, then $\dim(H)=M(n_1,\ldots,n_r)$, where $n=n_1+\cdots+n_r$. In the Lie algebra context the cyclotomic identity is interpreted as a denominator identity related to the free Lie algebra, see e.g. [13,14]. As the referee pointed out the symmetric polynomials in (3) have been studied in the theory of symmetric functions and have applications to counting permutations with certain properties, for example unimodal permutations, see e.g. Thibon [28], and permutations with prescribed descent set, see e.g. Gessel and Reutenauer [8].

Using (1) one infers (on taking the logarithm of either side and expanding it as a formal series) that

$$\frac{1}{1-z_1-\cdots-z_r}=\prod_{n_1,\ldots,n_r=0}^{\infty}(1-z_1^{n_1}\cdots z_r^{n_r})^{-M(n_1,\ldots,n_r)},$$

where $(n_1,\ldots,n_r)=(0,\ldots,0)$ is excluded in the product. It is a consequence of the latter identity, that if $a_j\in\mathbb{Z}_{\geqslant 0}$ for $1\leqslant j\leqslant n$, then as formal series we have $1-a_1t-\cdots-a_nt^n=\prod_{k\geqslant 1}(1-t^k)^{e_k}$, with $e_k\in\mathbb{Z}_{\geqslant 0}$. This was proved earlier in [18, Lemma 4] using zeta functions of finite automata.

2.1. A sign twisted variation of $M(n_1,\ldots,n_r)$

In our considerations a sign twisted variation of (2) comes up.

Lemma 1. *Let k and r be positive integers with $k\leqslant r$ and n_j non-negative integers and put $t_k=n_1+\cdots+n_k$ and $n=n_1+\cdots+n_r$. Put*

$$V_k(n_1,\ldots,n_r)=\frac{(-1)^{t_k}}{n}\sum_{d\mid \gcd(n_1,\ldots,n_r)}\mu(d)(-1)^{t_k/d}\begin{pmatrix}\frac{n}{d}\\ \frac{n_1}{d},\ldots,\frac{n_r}{d}\end{pmatrix}.$$

Then

$$V_k(n_1,\ldots,n_r)=\begin{cases}M(n_1,\ldots,n_r)+M\left(\frac{n_1}{2},\ldots,\frac{n_r}{2}\right) & \text{if } t_k\equiv 2 \pmod 4 \text{ and } 2\mid \gcd(n_1,\ldots,n_r),\\ M(n_1,\ldots,n_r) & \text{otherwise}.\end{cases}$$

Proof. The only not immediately obvious case is when $t_k\equiv 2 \pmod 4$ and $2\mid\gcd(n_1,\ldots,n_r)$. So assume we are in this case. Note that then at least one of the n_j is congruent to $2 \pmod 4$. Write $M(n_1,\ldots,n_r)$ as $S_{\text{odd}}+S_{\text{even}}$, where in S_{odd} all terms with d odd are collected. Thus $M(n_1,\ldots,n_r)=S_{\text{odd}}+S_{\text{even}}$. We have

$$V_k(n_1,\ldots,n_r)=S_{\text{odd}}-S_{\text{even}}=M(n_1,\ldots,n_r)-2S_{\text{even}}.$$

Using that at least one of the n_j satisfies $n_j\equiv 2 \pmod 4$, we infer that $2S_{\text{even}}=-M(n_1/2,\ldots,n_r/2)$. $\square$

Note that

$$\frac{1}{n}\sum_{d|n}\mu(d)(-z_1^d-\cdots-z_k^d+z_{k+1}^d+\cdots+z_r^d)^{n/d}$$
$$=\sum_{\substack{n_1+\cdots+n_r=n\\ n_j\geqslant 0}}(-1)^{n_1+\cdots+n_k}V_k(n_1,\ldots,n_r)z_1^{n_1}\cdots z_r^{n_r}. \quad (4)$$

Remark 1. The numbers $M(k,m-k)$ and $V_1(k,m-k)$ were already studied in a different guise around 1900 by Daublebsky von Sterneck (see e.g. [1, Volume II, pp. 222–264]). Daublebsky von Sterneck showed that the number of ways of selecting k parts, respectively k distinct parts, from $0,1,\ldots,m-1$ so that their sum is congruent to $1(\mathrm{mod}\, m)$ equals $M(k,m-k)$, respectively $V_1(k,m-k)$. Simple proofs of Daublebsky von Sterneck's results were later given by Ramanathan [26], see also [2,7]. Ramanathan uses properties of Ramanujan sums and in [2,7] the authors make use of Gauss polynomials. Let φ denote Euler's totient function. The function $\Phi(k,n)=\varphi(n)\mu(n/(k,n))/\varphi(n/(k,n))$ (called von Sterneck function by some authors) was introduced by Daublebsky von Sterneck in this context. He proved several of its properties. The von Sterneck function, however, is equal to the Ramanujan sum $c_n(k)$, which was introduced later by Ramanujan.

Remark 2. The numbers $M(n_1,\ldots,n_r)$ were interpreted as dimensions by Witt (see the previous section). The numbers $V_k(n_1,\ldots,n_r)$ can also be interpreted as dimensions (in the context of free Lie superalgebras), see [23].

Remark 3. By setting $V_0(n_1,\ldots,n_r,m)=M(n_1,\ldots,n_r)$ it is possible to deal with $M(n_1,\ldots,n_r)$ and $V_k(n_1,\ldots,n_r)$ in a more uniform way. For reasons of exposition this route has not been chosen.

2.2. Lyndon words

If w is a circular word counted by $M(n_1,\ldots,n_r,m)$ we can choose amongst the rotations of w one which is lowest with respect to a given lexicographical order (since we work with numbers as letters it is most natural to say that $i<j$ if $i<j$ as natural numbers). This is the idea of Lyndon words, which we now describe more precisely.

If $\mathscr{A}$ is an alphabet (assumed to be finite for simplicity of description), let $\mathscr{A}^*$ be the set of words with letters from $\mathscr{A}$ and $\mathscr{A}^+$ the set of non-empty words. Suppose we have a total order on $\mathscr{A}$. We extend the total ordering to $\mathscr{A}^+$ in the following way: For any $u,v\in\mathscr{A}^+$, $u<v$ iff either $v\in u\mathscr{A}^+$ or $u=ras$, $v=rbt$, with $a<b$; $a,b\in\mathscr{A}$; $r,s,t\in\mathscr{A}^*$. By definition a *Lyndon word* is an aperiodic word that is minimal amongst all the rotations of it. E.g. for $\mathscr{A}=\{a,b\}$ and $a<b$, the list of first Lyndon words is $\{a,b,ab,aab,abb,aaab,aabb,\ldots\}$. Let L denote the set of Lyndon words. The following proposition is quite useful.

Proposition 2. *A word $w\in\mathscr{A}^+$ is a Lyndon word iff $w\in\mathscr{A}$ or $w=lm$ with $l,m\in L$, $l<m$.*

Proof. Cf. the proof of Proposition 5.1.3 of [16]. □

The above proposition shows that given a Lyndon word w, the word wz is also Lyndon (unless $w = z$), where z is the letter which is highest in the total order on $\mathscr{A}$. We call this procedure *Lyndon extension*.

In [16, Section 5.3] the connection of Lyndon words with free Lie algebras is discussed, cf. [29].

2.3. Monotonicity

In this section monotonicity properties of $M(n_1, \dots, n_r)$ and $V_k(n_1, \dots, n_r)$ are being considered.

Proposition 3.
(1) *Suppose that* $n_2 \geqslant 1$, *then* $M(0, n_2, \dots, n_r) \leqslant M(1, n_2 - 1, n_3, \dots, n_r)$.
(2) *If* $n_2 \geqslant 2$, *then* $M(0, n_2, \dots, n_r) < M(1, n_2 - 1, n_3, \dots, n_r)$.
Let $1 \leqslant k \leqslant r$.
(3) *Suppose that* $n_2 \geqslant 1$, *then* $V_k(0, n_2, \dots, n_r) \leqslant V_k(1, n_2 - 1, n_3, \dots, n_r)$.
(4) *If* $n_2 \geqslant 2$ *and* $n_2 + \cdots + n_r \geqslant 3$, *then* $V_k(0, n_2, \dots, n_r) < V_k(1, n_2 - 1, n_3, \dots, n_r)$.

Proof. (1) Let w be a Lyndon word counted by $M(0, n_2, \dots, n_r)$. It starts with a 2 and does not contain a 1. Replace this 2 by a 1. This yields a Lyndon word counted by $M(1, n_2 - 1, n_3, \dots, n_r)$. Since this procedure is injective it follows that $M(0, n_2, \dots, n_r) \leqslant M(1, n_2 - 1, n_3, \dots, n_r)$.

(2) Since by assumption $n_2 \geqslant 2$, the set $M(1, n_2 - 1, n_3, \dots, n_r)$ counts at least one Lyndon word of the form $1z2$. Since $2z2$ is not a Lyndon word, the claimed inequality follows.

(3) This follows from part 1, together with Lemma 1 except for the case where $t_k \equiv 2 \pmod 4$ and $2 \mid \gcd(n_1, \dots, n_r)$, in which case we have to show that

$$M(0, n_2, \dots, n_r) + M\left(0, \frac{n_2}{2}, \dots, \frac{n_r}{2}\right) \leqslant M(1, n_2 - 1, n_3, \dots, n_r).$$

In case the second quantity in the latter inequality equals zero, we are done by part 1, so assume that $M(0, n_1/2, \dots, n_r/2) \geqslant 1$. The Lyndon words counted by $M(0, n_2, \dots, n_r)$ we deal with as before. If $2w$ is a Lyndon word counted by $M(0, n_1/2, \dots, n_r/2)$, we consider the word $1w2w$. Since w does not contain a 1, it is a Lyndon word. It is counted by $M(1, n_2 - 1, n_3, \dots, n_r)$ and $2w2w$ is not counted by $M(0, n_2, \dots, n_r)$.

(4) This follows on using part 2 and noting in addition that $1w2w$ does not end in a 2. $\square$

The idea of using Lyndon extension to prove the next result was kindly communicated to the author by Prof. F. Ruskey. Profs. Bryant [3] and Petrogradsky [24] proved part 1 of the next proposition using Lie algebraic methods (Hall basis, respectively Lyndon–Shirshov basis of a free Lie algebra).

Proposition 4. *Let* $1 \leqslant k \leqslant r + 1$.

(1) *Suppose that* $n_1 + \cdots + n_r \geqslant 1$. *Then* $\{M(n_1, \dots, n_r, m)\}_{m=0}^{\infty}$ *is a non-decreasing sequence. We have* $\{M(m, 0, \dots, 0)\}_{m=1}^{\infty} = \{1, 0, 0, \dots\}$ *in the remaining case* (*i.e. the case* $n_1 + \cdots + n_r = 0$).

(2) *Suppose that* $n_1 + \cdots + n_r \geqslant 1$. *Then* $\{V_k(n_1, \ldots, n_r, m)\}_{m=0}^{\infty}$ *is a non-decreasing sequence. In the remaining case one has* $\{V_k(m, 0, \ldots, 0)\}_{m=1}^{\infty} = \{1, 1, 0, \ldots\}$.

Proof. (1) First proof. This follows at once from Lyndon extension. Choose the Lyndon words as representatives of the circular words counted by $M(n_1, \ldots, n_r, m)$. Now concatenate each such word with the letter $r+1$. By Proposition 2 this yields another Lyndon word which is counted by $M(n_1, \ldots, n_r, m+1)$. Since the concatenation is injective, it follows that $M(n_1, \ldots, n_r, m) \leqslant M(n_1, \ldots, n_r, m+1)$. Second proof (by Dion Gijswijt). If $M(n_1, \ldots, n_r, m) = 0$, there is nothing to prove, so assume that $M(n_1, \ldots, n_r, m) \geqslant 1$. If we have a circular word counted by $M(n_1, \ldots, n_r, m)$ do the following: if $m = 0$ insert the letter $r+1$ anywhere in the sequence. This yields an aperiodic circular word that is counted by $M(n_1, \ldots, n_r, m+1)$. If $m \geqslant 1$ look for a longest consecutive string of letters $r+1$ in a circular word counted by $M(n_1, \ldots, n_r, m)$ and insert another letter $r+1$ after it. This clearly yields an aperiodic word counted by $M(n_1, \ldots, n_r, m+1)$. Since this extension procedure is injective, the result follows.

(2) This follows from part 1, together with Lemma 1 except for the case where $t_k \equiv 2 \pmod 4$ and $2 \mid \gcd(n_1, \ldots, n_r, m)$, in which case we have to show that

$$M(n_1, \ldots, n_r, m) + M\left(\frac{n_1}{2}, \ldots, \frac{n_r}{2}, \frac{m}{2}\right) \leqslant M(n_1, \ldots, n_r, m+1). \tag{5}$$

In case the second quantity in the latter inequality equals zero, we are done by part 1, so assume that $M(n_1/2, \ldots, n_r/2, m/2) \geqslant 1$. The Lyndon words counted by $M(n_1, \ldots, n_r, m)$ we extend as before. Let W be the set of words thus produced. If w is a Lyndon word counted by $M(n_1/2, \ldots, n_r/2, m/2)$, we consider the word wwz, where z stands for the letter $r+1$. By Proposition 2 it follows that wwz is a Lyndon word (note that $w \neq z$). This word is counted by $M(n_1, \ldots, n_r, w)$ and is not in W.

For the final part of the assertion we use the easy observation that

$$\frac{(-1)^m}{m} \sum_{d \mid m} (-1)^{m/d} \mu(d) = \begin{cases} 1 & \text{if } m \leqslant 2, \\ 0 & \text{otherwise.} \end{cases}$$

This concludes the proof. □

The following result sharpens Proposition 4.

Theorem 6. *Let* $r \geqslant 1$ *and* $n_1, \ldots, n_r$ *be non-negative numbers.*

(1) *The sequence* $\{M(n_1, \ldots, n_r, m)\}_{m=0}^{\infty}$ *is strictly increasing if* $n_1 + \cdots + n_r \geqslant 3$ *or* $r = 2$ *and* $n_1 = n_2 = 1$.

(2) *The sequence* $\{V_k(n_1, \ldots, n_r, m)\}_{m=0}^{\infty}$ *is strictly increasing if* $n_1 + \cdots + n_r \geqslant 3$ *or* $r = 2$ *and* $n_1 = n_2 = 1$, *when* $1 \leqslant k \leqslant r+1$.

In the proof we make use of the following trivial result.

Lemma 2. *We have*

$$M(0, m) = \begin{cases} 1 & \textit{if } m = 1, \\ 0 & \textit{if } m > 1, \end{cases} \quad \textit{and } M(1, m) = 1 \textit{ for } m \geqslant 1.$$

Let $m \geqslant 0$. *We have*

$$M(2, m) = \begin{cases} m/2 & \text{if } m \text{ is even}, \\ (m+1)/2 & \text{otherwise}. \end{cases}$$

If $\gcd(n_1, \ldots, n_r) = 1$ *we have*

$$M(n_1, \ldots, n_r, m+1) = \frac{(n_1 + \cdots + n_r + m)}{m+1} M(n_1, \ldots, n_r, m).$$

Proof of Theorem 6. (1) If $n_1, n_2 \geqslant 1$, then $1^{n_1} \cdots r^{n_r}$ is a Lyndon word and hence

$$M(n_1, \ldots, n_r) \geqslant 1 \text{ if } r \geqslant 2 \text{ and } n_1, n_2 \geqslant 1. \tag{6}$$

Case 1. $r = 1$ and $n_1 \geqslant 3$. We have $M(n_1, 0) = 0$ and $M(n_1, 1) = 1$, so we may assume that $m = 1$. The word $1^{n_1-1}2^m12$ is counted by $M(n_1, m+1)$, but not counted by the $M(n_1, m)$ words amongst the $M(n_1, m+1)$ that come from Lyndon extension (since $1^{n_1-1}2^m1$ is not a Lyndon word). It follows that $M(n_1, m+1) > M(n_1, m)$.

Case 2. $r \geqslant 2$, $n_1, n_2 \geqslant 1$. Consider a Lyndon word counted by $M(n_1, n_2 - 1, n_3, \ldots, n_r, m+1)$ (such a word exists by (6)) and extend it with a 2. Since a Lyndon word counted by $M(n_1, n_2 - 1, n_3, \ldots, n_r, m+1)$ starts with a 1, this will yield, by Proposition 2, again a Lyndon word (counted by $M(n_1, \ldots, n_r, m+1)$). This word is not amongst those coming from Lyndon extension (they all end with a number $\geqslant 3$).

On combining these results with Lemma 2 the proof of part 1 is easily completed.

(2) The argument of Case 1 applies here as well. In addition we have to check now that none of the words after extension is of the form wwz (so as to avoid that they are being counted as well under the $M(n_1/2, \ldots, n_r/2, m/2)$ words that were injected into $M(n_1, \ldots, n_r, m+1)$ in the proof of Proposition 4. A Lyndon word that is being extended is clearly not of the form ww. The only non-Lyndon word used in the previous argument, $1^{n_1-1}2^m12$ (with $m \geqslant 2$), is also not of this form. □

3. The proof of Theorem 3

Recall that if f and g are arithmetic functions, the classical Möbius inversion formula states that $g(n) = \sum_{d|n} f(d)$ iff $f(n) = \sum_{d|n} \mu(d) g(n/d)$. Lemma 3 is an analogue of this result for sequences of formal series. By writing $A^{(r)}(x) = \sum a_{j,r} x^j$ and $B^{(r)}(x) = \sum b_{j,r} x^j$, a known Möbius inversion formula for arithmetic functions in two variables is obtained (see e.g. [11]). Lemma 3 is the main ingredient in the proof of Theorem 3.

Lemma 3. *Let* $\{A^{(r)}(z)\}_{r=1}^{\infty}$ *and* $\{B^{(r)}(z)\}_{r=1}^{\infty}$ *be two sequences of formal series. Then*

$$A^{(r)}(z) = \sum_{d|r} B^{(r/d)}(z^d) \text{ iff } B^{(r)}(z) = \sum_{d|r} \mu(d) A^{(r/d)}(z^d).$$

Proof. We have

$$\begin{aligned}\sum_{d|r}\mu(d)A^{(r/d)}(z^d) &= \sum_{d|r}\mu(d)\sum_{e|\frac{r}{d}}B^{(r/de)}(z^{de})\\ &= \sum_{m|r}\left(\sum_{d|m}\mu(d)\right)B^{(r/m)}(z^m)\\ &= B^{(r)}(z).\end{aligned}$$

Conversely,

$$\begin{aligned}\sum_{d|r}B^{(r/d)}(z^d) &= \sum_{d|r}\sum_{e|\frac{r}{d}}\mu(e)A^{(r/de)}(z^{de})\\ &= \sum_{m|r}\left(\sum_{e|m}\mu(e)\right)A^{(r/m)}(z^m)\\ &= A^{(r)}(z).\end{aligned}$$

In both strings of identities we used that $\sum_{d|m}\mu(d)=0$ if $m>1$. □

Proof of Theorem 3.

(1) Trivial.
(2) Immediate from Lemma 3 and the definition of $\mathscr{W}_f^{(r)}$.
(3) Similar to the proof of Lemma 1.
(4) By Lemma 3 it is enough to show that

$$\sum_{d|r}\frac{r}{d}\mathscr{W}_{fg}^{(r/d)}(z^d)=\sum_{d|r}\frac{r}{d}\sum_{[i,j]=\frac{r}{d}}(i,j)\mathscr{W}_f^{(i)}(z^{r/i})\mathscr{W}_g^{(j)}(z^{r/j}).$$

By part 2 the left-hand side of this purported identity equals $f(z)^r g(z)^r$. The summation conditions on the right are equivalent to $i|r$ and $j|r$, that is, i and j independently range over the divisors of r. Thus, noting that $[i,j](i,j)=ij$, we obtain, for the right-hand side,

$$\sum_{i|r} i\mathscr{W}_f^{(i)}(z^{r/i})\sum_{j|r} j\mathscr{W}_g^{(j)}(z^{r/j})=f(z)^r g(z)^r,$$

where part 2 was used again.

(5) By Lemma 3 it is enough to show that

$$\sum_{d|r}\frac{r}{d}\mathscr{W}_{f^k}^{(r/d)}(z^d)=\sum_{d|r}\frac{r}{d}\sum_{[j,k]=\frac{rk}{d}}\frac{jd}{r}\mathscr{W}_f^{(j)}(z^{rk/j}).$$

The left-hand side is seen to equal $f(z)^{kr}$, the right-hand side simplifies to $\sum_{j|rk} j\mathscr{W}_f^{(j)}(z^{rk/j})=f(z)^{rk}$.

(6) Combine the identities of part 5 and part 6 (cf. the proof of Theorems 5 and 6 of [17]). □

4. The proof of Theorems 4 and 5

We now have the necessary ingredients to prove Theorem 4.

Proof of Theorem 4.

(1) Trivial.

(2) Very similar to that of part 3: instead of (3) use (4). An alternative proof is discussed in the next section.

(3) Write $f(z)=\sum_j a_j z^j$. Let $k \geqslant 0$ be an arbitrary integer. In order to prove that the coefficient of z^k in $\mathscr{W}_f^{(r)}(z)$ is non-negative it is enough to prove this with $f(z)$ replaced by $f_k(z)=\sum_{j=0}^k a_j z^j$. Let $r=f_k(1)$. We apply Eq. (3) with $z_1,\ldots,z_{a_1}=1, z_{a_1+1},\ldots,z_{a_1+a_2}=z$ etc. Thus for example we write $2+z+z^2$ as $z_1+z_2+z_3+z_4$ with $z_1=1$, $z_2=1$, $z_3=z$ and $z_4=z^2$. Since every number of the form $M(m_1,\ldots,m_r)$ is an integer, the result then follows from (3).

(4) Follows on combining part 3 above with part 3 of Theorem 3.

(5) From (3) and the definition of $M(n_1,\ldots,n_r)$ (given in (2)), we deduce that

$$\frac{1}{n}\sum_{d|n}\mu(d)(z_1^d+\cdots+z_r^d)^{n/d}=\frac{1}{n}\sum_{d|n}\mu(d)(z_1^d+\cdots+z_{r-1}^d)^{n/d} + \sum_{\substack{n_1+\cdots+n_r=n\\ n_j\geqslant 0,\ n_r\geqslant 1}} M(n_1,\ldots,n_r)z_1^{n_1}\cdots z_r^{n_r}.$$

The remainder of the argument should be obvious to the reader (cf. the proof of part 3). □

Remark 4. Part 2 can also be proved using the theory of formal groups [27].

We now come to the proof of Theorem 5.

Proof of Theorem 5. (1) Write $f(z)=\sum_j a_j z^j$. Put $w_1=\cdots=w_{a_0}=0$, $w_{a_0+1}=\cdots=w_{a_0+a_1}=1$, $w_{a_0+a_1+1}=\cdots=w_{a_0+a_1+a_2}=2$, etc. On applying (3), cf. the proof of part 5, we see that the coefficient of z^k in $\mathscr{W}_f^{(r)}(z)$ equals

$$m_f(k,r)=\sum_{\substack{\sum_j n_j w_j=k,\ \sum_j n_j=r\\ n_j\geqslant 0}} M(\{n_j\}_{j=1}^\infty). \tag{7}$$

The assumption $a_0>0$ implies that $w_1=0$. With each solution of the system $\sum_j n_j w_j=k$ and $\sum_j n_j=r$ we associate $\{n'_j\}_{j=1}^\infty$ with $n'_j=n_j$ for all $j\geqslant 2$ and with $n'_1=n_1+1$. Note that $\sum_j n'_j w_j=k$ and $\sum_j n'_j=r+1$. Note that the assignment $\{n_j\}_{j=1}^\infty \to \{n'_j\}_{j=1}^\infty$ is injective. Using part 1 of Proposition 4 we infer that $M(\{n_j\}_{j=1}^\infty)\leqslant M(\{n'_j\}_{j=1}^\infty)$. This, in combination with (7) and the injectivity, yields that

$$m_f(k,r)\leqslant \sum_{\substack{\sum_j n'_j w_j=k\\ \sum_j n'_j=r+1\\ n'_j\geqslant 0}} M(\{n'_j\}_{j=1}^\infty)\leqslant \sum_{\substack{\sum_j m_j w_j=k\\ \sum_j m_j=r+1\\ m_j\geqslant 0}} M(\{m_j\}_{j=1}^\infty)=m_f(k,r+1).$$

(2) The analogue of (3) reads

$$\frac{(-1)^n}{n}\sum_{d|n}\mu(d)(-z_1^d-\cdots-z_r^d)^{n/d}=\sum_{\substack{n_1+\cdots+n_r=n\\ n_j\geqslant 0}}V_r(n_1,\ldots,n_r)z_1^{n_1}\cdots z_r^{n_r},$$

whence, cf. the proof of part 1,

$$(-1)^r m_{-f}(k,r)=\sum_{\substack{\sum_j n_jw_j=k,\ \sum_j n_j=r\\ n_j\geqslant 0}}V_\infty(\{n_j\}_{j=1}^\infty),$$

where, if t is such that $n_k=0$ for every $k\geqslant t+1$, $V_\infty(\{n_j\}_{j=1}^\infty)$ is defined as $V_t(n_1,\ldots,n_t)$. The remainder of the proof is quite similar to that of part 1.

(3) Let $r\geqslant 1$. Suppose that $\sum_j n_jw_j=k$ and $\sum_j n_j=r$ with $n_j\geqslant 0$. Let t be the (unique) integer such that $n_t\geqslant 1$ and $n_{t+j}=0$ for every $j\geqslant 1$. Let $t_1=t+a_{w_t}$. Since $a_{w_t}\leqslant a_{w_t+1}$ (by assumption), it follows that $w_{t_1}=w_t+1$. To this solution $\{n_j\}_{j=1}^\infty$ we associate $\{n'_j\}_{j=1}^\infty$ with $n'_t=n_t-1$, $n'_{t_1}=1$ and $n'_j=n_j$ for $j\neq t,t_1$. Note that $\sum_j n'_jw_j=k+1$ and $\sum_j n'_j=r$.

(3a) Let t_2 be such that $w_{t_2}=k$ (by assumption $f(z)\in\mathbb{Z}_{\geqslant 1}[\![z]\!]$ and hence $\{w_1,w_2,\ldots\}=\mathbb{Z}_{\geqslant 0}$ and such a t_2 exists). Since $k\geqslant 1$ (by assumption), $t_2\geqslant 2$. Let $n_1=r-1$ and $n_{t_2}=1$ and set $n_j=0$ for $j\neq 1,t_2$. Then $M(\{n_j\}_{j=1}^\infty)\geqslant 1$ (by (6) and $M(0,1)=1$). The result now follows by (7).

(3b) From part 1 of Proposition 4 and the fact that $M(n_1,\ldots,n_r)$ is totally symmetric in $n_1,\ldots,n_r$, we infer that $M(\{n_j\}_{j=1}^\infty)\leqslant M(\{n'_j\}_{j=1}^\infty)$. Using this, (7), and the injectivity of the assignment $\{n_j\}\to\{n'_j\}$, we then obtain

$$m_f(k,r)\leqslant\sum_{\substack{\sum_j n'_jw_j=k+1\\ \sum_j n'_j=r\\ n'_j\geqslant 0}}M(\{n'_j\}_{j=1}^\infty)\leqslant\sum_{\substack{\sum_j m_jw_j=k+1\\ \sum_j m_j=r\\ m_j\geqslant 0}}M(\{m_j\}_{j=1}^\infty)=m_f(k+1,r).\tag{8}$$

(3c) If $r\geqslant 3$ and $k\geqslant 2$ one checks that the system of equations $\sum_j n_jw_j=k$ and $\sum_j n_j=r$ has a solution in non-negative integers n_j such that $n_t\geqslant 2$. For such a solution we have, by part 2 of Proposition 4, $M(\{n_j\}_{j=1}^\infty)<M(\{n'_j\}_{j=1}^\infty)$. This ensures that the first inequality in (8) becomes strict.

(4) A variation of the proof of part 3 that is left to the reader. □

Proof of Proposition 1. Using (7) one finds that, for $c\geqslant 1$,

$$M(c;r)=\sum_{\substack{n_1+\cdots+n_c=r\\ n_j\geqslant 0}}M(n_1,\ldots,n_c).$$

On invoking Proposition 4 and Theorem 6 the result then follows after some calculation. □

5. An alternative proof of part 2 of Theorem 4

An alternative proof of part 2 of Theorem 4 is obtained on combining Theorem 2 with Lemma 4. Both the proof of Theorem 2 and Lemma 4 are taken from [19] and repeated here for the convenience of the reader.

Proof of Theorem 2. Using part 2 of Theorem 3 we deduce that

$$f(z)^r = \sum_{d|r} \frac{r}{d} \mathscr{W}_f^{(r/d)}(z^d) = \sum_{d|r} \frac{r}{d} \sum_{j=0}^{\infty} m_f\left(j, \frac{r}{d}\right) z^{jd},$$

from which it is inferred that

$$\sum_{r=1}^{\infty} y^r f(z)^r = \sum_{j=0}^{\infty} \sum_{k=1}^{\infty} m_f(j,k)k \sum_{d=1}^{\infty} z^{jd} y^{kd}.$$

The latter identity with both sides divided out by y can be rewritten as

$$\frac{f(z)}{1 - yf(z)} = \sum_{j=0}^{\infty} \sum_{k=1}^{\infty} \frac{m_f(j,k)kz^j y^{k-1}}{1 - z^j y^k}.$$

Formal integration of both sides with respect to y gives

$$-\log(1 - yf(z)) = -\sum_{j=0}^{\infty} \sum_{k=1}^{\infty} m_f(j,k) \log(1 - z^j y^k),$$

whence the result follows. □

An *unital series* is, by definition, a series whose constant term is the identity.

Proposition 5 (*Metropolis and Rota [17, Proposition 1]*). *If $f \in \mathbb{Z}[\![x]\!]$ is unital, then it has an unique expansion of the form $f(z) = \prod_{n=1}^{\infty} (1 - z^n)^{-e_n}$, where the e_n are integers.*

The following result generalizes this to two variables.

Lemma 4 (*Moree [19]*). *Suppose that $f(z, y) = \sum_{j,k} \alpha(j,k) z^j y^k$ where the $\alpha(j,k)$ are integers and $f(0,0) = 0$. Then there are unique integers $e(j,k)$ such that, as formal series, we have*

$$1 + f(z,y) = \prod_{j=0}^{\infty} \prod_{\substack{k=0 \\ (j,k)\neq(0,0)}}^{\infty} (1 - z^j y^k)^{e(j,k)}.$$

Proof. We say that $z^{j_1} y^{k_1}$ is of lower weight than $z^{j_2} y^{k_2}$ if $k_1 < k_2$ or $k_1 = k_2$ and $j_1 < j_2$. Suppose that $z^j y^k$ is the term of lowest weight appearing in $f(z, y)$. Then consider $(1 + f(z,y))(1 - z^j y^k)^{\alpha(j,k)}$. This can be rewritten as $1 + g(z, y)$ where all the coefficients of

$g(z, y)$ are integers and the term of lowest weight in $g(z, y)$ has strictly larger weight than the term of lowest weight in $f(z, y)$. Now iterate.

It is not obvious from this argument that if we start with a different weight ordering of the terms $X^j Y^k$ we end up with the same integers $e(j, k)$. Suppose that $h(X)$ has integer coefficients, then the coefficients $e(n)$ in $1 + h(X) = \prod_{n=1}^{\infty} (1 - X^n)^{e(n)}$ are unique by Proposition 5. Hence, by setting $X=0$, respectively $Y=0$, we obtain that $e(0, k)$, respectively $e(j, 0)$ are uniquely determined. Setting $Y = X^m$ we obtain that $1 + f(X, X^m) = \prod_{n=1}^{\infty} (1 - X^n)^{f(n)}$, where $f(n)$ is uniquely determined and $f(2m) = e(2m, 0) + e(m, 1) + e(0, 2)$. The uniqueness of $e(0, 2)$, $e(2m, 0)$ and $f(2m)$ then implies the uniqueness of $e(m, 1)$. We will complete the proof by using induction. So suppose we have established that $e(j, k)$ with $k \leqslant r$ for some $r \geqslant 1$ are uniquely determined. Using that $f((r+2)m) = \sum_{k=0}^{r+2} e((r+2-k)m, k)$, we infer by the induction hypothesis and using that $e(0, r+2)$ and $f((r+2)m)$ are uniquely determined, that $e(m, r + 1)$ is uniquely determined. $\square$

6. Examples

Example 1. It turns out that the coefficients of the Möbius transform in case $f(z) = 1 + z$ have several interesting properties. Note that, with $f(z) = 1 + z$, we have

$$\mathscr{W}_f^{(r)}(z) = \frac{1}{r} \sum_{d|r} \mu(d)(1 + z^d)^{r/d} = \sum_{j=0}^{r} m_f(j, r) z^j, \tag{9}$$

where

$$m_f(j, r) = \frac{1}{r} \sum_{d \,|\, \gcd(j,r)} \mu(d) \begin{pmatrix} \frac{r}{d} \\ \frac{j}{d}, \frac{r-j}{d} \end{pmatrix} = M(j, r - j) \in \mathbb{Z}_{\geqslant 0}.$$

The numbers $M(j, r - j)$ also arise in the theory of relative partitions, see Remark 1. Witt's work [30] yields the following result (where the formulation from Proposition 2.10 of [14] with $r = 1$ is being used).

Proposition 6. *Let $V = \bigoplus_{i,j=1}^{\infty} V_{(i,j)}$ be a $(\mathbb{Z}_{>0} \times \mathbb{Z}_{>0})$-graded vector space over $\mathbb{C}$ with $\dim V_{(i,j)} = 1 \in \mathbb{Z}_{>0}$ for all $i, j \geqslant 1$, and let $L = \bigoplus_{m,n=1}^{\infty} L_{(m,n)}$ be the free Lie algebra generated by V. We have*

$$\frac{1}{n} \sum_{d|n} \mu(d)(1 + z^d)^{n/d} = \sum_{j=0}^{n} \dim(L_{(j,n-j)}) z^j = \sum_{j=0}^{n} m_f(j, n) z^j.$$

Since $1 + z$ is self-reciprocal, so is $\mathscr{W}_f^{(r)}(z)$ by part 1 of Theorem 4. It follows that $\dim(L_{(j,n-j)}) = \dim(L_{(n-j,j)})$.

Example 2. Many constants in number theory have the form $\prod_{p > p_m} h(1/p)$, where h is a rational function and $h(z) = 1 + \mathrm{O}(z^2)$ (as z tends to zero) and the product is over all primes $p > p_m$, with p_m the mth prime. Examples are the twin prime constant T and A the Artin constant (defined in (13)). We have the formal identity $h(z) = \prod_{n=2}^{\infty}(1-z^n)^{-e_n}$, with the e_n uniquely determined integers (by Proposition 5). This identity can be used to expand $\prod_{p>p_m} h(1/p)$ in terms of the partial zeta function $\zeta_m(s) = \prod_{p \leqslant p_m}(1-p^{-s})\zeta(s)$, where $\zeta(s)$ denotes the Riemann zeta function. Formally we have

$$\prod_{p>p_m} h\left(\frac{1}{p}\right) = \prod_{p>p_m}\prod_{n=2}^{\infty}(1-p^{-n})^{-e_n} = \prod_{n=2}^{\infty}\prod_{p>p_m}(1-p^{-n})^{-e_n} = \prod_{n=2}^{\infty}\zeta_m(n)^{e_n}. \tag{10}$$

For m large enough it can be shown that such an identity always holds, see Theorem 1 of [18]. These identities can be used to evaluate constants of this format with high numerical accuracy.

To conclude we give a result concerning a class of more complicated constants in which the Witt transform arises. These are the constants arising in the left hand side of (12), where χ is any Dirichlet character.

Theorem 7 (*Moree [19]*). *Suppose that $f(z) = \sum_{j\geqslant 1} a(j)z^j \in \mathbb{Z}[\![z]\!]$. Let $j_0 \geqslant 1$ denote the smallest integer such that $a(j_0) \neq 0$. Let $g(z) = \sum_{j\geqslant 1}|a(j)|z^j$. Let $m_f(j,r)$ be defined as in Definition* 1. *Then, as formal power series in y and z, one has*

$$1 - yf(z) = \prod_{k=1}^{\infty}\prod_{j=kj_0}^{\infty}(1-z^j y^k)^{m_f(j,k)}. \tag{11}$$

Moreover, the numbers $m_f(j,k)$ are integers.

Let $\varepsilon > 0$ be fixed. Identity (11) *holds for all complex numbers y and z with $g(|z|)y < 1-\varepsilon$ and $|z| < \rho_c$, where ρ_c is the radius of convergence of the Taylor series of g around $z = 0$. If, moreover, $\rho_c > \frac{1}{2}$, $g(\frac{1}{2}) < 1$ and $\sum_p g(1/p)$ converges, then*

$$\prod_p \left(1 - \chi(p) f\left(\frac{1}{p}\right)\right) = \prod_{k=1}^{\infty}\prod_{j=kj_0}^{\infty} L(j,\chi^k)^{-m_f(j,k)}. \tag{12}$$

In the latter sum and product p runs over all primes.

Recall that the Dirichlet L-series for χ^k, $L(s,\chi^k)$, is defined, for $\mathrm{Re}(s) > 1$, by $\sum_{n=1}^{\infty}\chi^k(n)n^{-s}$. Since Dirichlet L-series in integer values are very easily evaluated with high decimal precision, this result allows one to evaluate with high decimal precision the constant appearing on the left hand side of (12). In the case of the constants

$$B_\chi = \prod_p \left(1 + \frac{[\chi(p)-1]p}{[p^2-\chi(p)](p-1)}\right),$$

arising in the study of some problems involving the multiplicative order, e.g. [19,20,22], one obtains from Theorem 7 the following proposition:

Proposition 7 (*Moree [19]*). *Let $f(z) = -(1-z-z^2)^{-1}$. We have*

$$B_\chi = A\,\frac{L(2,\chi)L(3,\chi)}{L(6,\chi^2)} \prod_{r=1}^{\infty} \prod_{j=3r+1}^{\infty} L(j,\chi^r)^{-m_f(j-3r,r)},$$

where

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots \tag{13}$$

denotes the Artin constant and $(-1)^{r-1}e(j,r) = -m_f(j-3r,r)$.

As a formal series we have $1/(1-z-z^2) = \sum_{j\geqslant 0} F_{j+1}z^j$, with F_j the jth Fibonacci number. The Taylor coefficients of $(1-z-z^2)^{-r}$ are known as *convolved Fibonacci numbers*. Thus the numbers $e(j,r)$ are closely related to convolved Fibonacci numbers. Numerical computation suggests that actually $e(j,r) \geqslant 1$ and, moreover, that these numbers enjoy certain monotonocity properties in both the j and r direction. On using Theorem 4 various of these numerical observations can be actually proved, see [21] for details.

Acknowledgements

There are too many mathematicians to thank here for their kind E-mail comments on my questions. I would like to especially mention Profs. Bryant, Fulman, Haukkanen, Jibladze, Petrogradsky, Reiner, Ruskey, Stanton and Stienstra. Prof. Ruskey's suggestion of using Lyndon words turned out to be very useful. Profs. Feingold, Kang and Mays kindly sent me some reprints. I thank Dr. Christa Binder for sending me some biographical material concerning the Austrian mathematician R. Daublebsky von Sterneck (1871–1928) and several of his illustrous relatives.

References

[1] P. Bachmann, Niedere Zahlentheorie, Erster Teil, Zweiter Teil: Additive Zahlentheorie, Chelsea Publishing Co., New York, 1968.
[2] M. Beck, A.J. Feingold, M.D. Weiner, Arithmetic partition sums and orbits of $\mathbb{Z}_n^k$ under the symmetric group S_k, unpublished manuscript.
[3] R.M. Bryant, e-mail to the author, September 30th, 2003.
[4] L. Carlitz, An arithmetic function, Bull. Amer. Math. Soc. 43 (1937) 271–276.
[5] L.J. Cummings, M.E. Mays, On the parity of the Witt formula, Congr. Numer. 80 (1991) 49–56.
[6] L.E. Dickson, History of the Theory of Numbers I: Divisibility and Primality, Chelsea Publishing Co., New York, 1966.
[7] A. Elashvili, M. Jibladze, D. Pataraia, Combinatorics of necklaces and "Hermite reciprocity", J. Algebraic Combin. 10 (1999) 173–188.

[8] I.M. Gessel, C. Reutenauer, Counting permutations with given cycle structure and descent set, J. Combin. Theory Ser. A 64 (1993) 189–215.
[9] S.W. Golomb, Irreducible polynomials, synchronization codes, primitive necklaces, and the cyclotomic algebra, Combinatorial Mathematics and its Applications, Proceedings of Conference of University of North Carolina, Chapel Hill, NC, 1967, 1969, pp. 358–370.
[10] M. Hall Jr., The Theory of Groups, The Macmillan Co., New York, 1959.
[11] P. Haukkanen, An abstract Möbius inversion formula with number-theoretic applications, Discrete Math. 142 (1995) 87–96.
[12] M.E. Hoffman, The algebra of multiple harmonic series, J. Algebra 194 (1997) 477–495.
[13] S.-J. Kang, M.-H. Kim, Free Lie algebras, generalized Witt formula, and the denominator identity, J. Algebra 183 (1996) 560–594.
[14] S.-J. Kang, M.-H. Kim, Dimension formula for graded Lie algebras and its applications, Trans. Amer. Math. Soc. 351 (1999) 4281–4336.
[15] C. Lenart, Formal group-theoretic generalizations of the necklace algebra, including a q-deformation, J. Algebra 199 (1998) 703–732.
[16] M. Lothaire, Combinatorics on Words, Cambridge University Press, Cambridge, 1997.
[17] N. Metropolis, G.-C. Rota, Witt vectors and the algebra of necklaces, Adv. Math. 50 (1983) 95–125.
[18] P. Moree, Approximation of singular series and automata, Manuscripta Math. 101 (2000) 385–399.
[19] P. Moree, On the average number of elements in a finite field with order or index in a prescribed residue class, Finite Fields Appl. 10 (2004) 438–463.
[20] P. Moree, On the distribution of the order and index of $g(\mathrm{mod}\ p)$ over residue classes I, J. Number Theory, to appear, but already electronically available.
[21] P. Moree, Convoluted convolved Fibonacci numbers, J. Integer Seq. 7 (2004), Article 04.2.2., pp. 14 (electronic).
[22] F. Pappalardi, On Hooley's theorem with weights. Number theory, II (Rome, 1995), Rend. Sem. Mat. Univ. Politec. Torino 53 (1995) 375–388.
[23] V.M. Petrogradsky, Witt's formula for restricted Lie algebras, Adv. Appl. Math. 30 (2003) 219–227.
[24] V.M. Petrogradsky, e-mail to the author, October 29th, 2003.
[25] Y. Puri, T. Ward, Arithmetic and growth of periodic orbits, J. Integer Seq. 4 (2001), Article 01.2.1, 18 pp. .
[26] K.G. Ramanathan, Some applications of Ramanujan's trigonometrical sum $C_m(n)$, Proc. Indian Acad. Sci., Sect. A 20 (1944) 62–69.
[27] J. Stienstra, e-mail to the author, November 14th, 2003.
[28] J.-Y. Thibon, The cycle enumerator of unimodal permutations, Ann. Combin. 5 (2001) 493–500.
[29] G. Viennot, Algèbres de Lie libres et monoïdes libres, Lecture Notes in Mathematics, vol. 691, Springer, Berlin, 1978.
[30] E. Witt, Treue Darstellung Liescher Ringe, J. Reine Angew. Math. 177 (1937) 152–160.