The Cyclotomic Identity via Lyndon Words

DAVID CALLAN
Department of Statistics
University of Wisconsin-Madison
1210 W. Dayton St
Madison, WI 53706-1693
callan@stat.wisc.edu

1. Introduction. The identity of the title is

$$\frac{1}{1-az} = \prod_{n\geq 1} \frac{1}{(1-z^n)^{M(a,n)}} \tag{1}$$

where $M(a,n) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})a^d$.

Here μ is the classical Möbius function, and (1) is a formal power series identity in z. When a is a positive integer, the exponent $M(a,n)$ is also a positive integer and counts the number of circular arrangements of n letters taken from an alphabet of a letters. This suggests the possibility of a combinatorial proof. The present note shows how a straightforward search for such a proof leads almost directly to the Unique Factorization Theorem for the so-called Lyndon words that arise in the theory of Combinatorics on Words. The Lyndon word proof does not seem to be well known. It is only vaguely referred to in Rota and Metropolis's 1983/84 papers [1, 2], where a "natural" bijective proof is given. Nor is it mentioned in several subsequent proofs and generalizations [3, 4, 5, 6, 7].

2. Notation and Terminology. Let $\mathcal{A} = \{A, B, C, \ldots\}$ denote a fixed alphabet of a distinct letters. A *word* (on alphabet $\mathcal{A}$) is any finite sequence of these letters. The *length* of a word is the number of letters in its sequence. There is one word of length 0: the empty word. Let $\mathcal{W}(a,n)$ denote the set of a^n words of length n on $\mathcal{A}$ and let $\mathcal{W}(a) = \bigcup_{n=0}^{\infty} \mathcal{W}(a,n)$ denote the set of all words on $\mathcal{A}$. In fact, $\mathcal{W}(a)$ is a monoid with the product of two words given by juxtaposition and the empty word as identity. Let $\mathcal{W}(a)^+$ denote the set of nonempty words in $\mathcal{W}(a)$.

$\mathcal{W}(a)^+$ is partitioned into equivalence classes, called *necklaces*, by the following equivalence relation: $w_1 \sim w_2$ iff w_2 can be obtained from w_1 by cyclic rotation of its letters. Thus $\{ABA, AAB, BAA\}$ is a necklace, as is $\{ABAB, BABA\}$. A word $w \in \mathcal{W}(a)^+$ is *primitive* if it cannot be expressed as a power of a shorter word. Let $<$ denote lex (dictionary) order on $\mathcal{W}(a)^+$. Thus $A < AA < AB < B$. A word $w \in \mathcal{W}(a)^+$ is called a *Lyndon* word if it is (i) primitive, and (ii) minimal in its necklace equivalence class (relative to lex order). Thus A and AAB are Lyndon words unlike $ABAB$ (not primitive) and ABA (not minimal).

3. Combinatorial Interpretation of Coefficients. The number of Lyndon words of length n on an alphabet of a letters can be counted by Möbius inversion and is given by the expression $M(a,n)$ above [8, §5.1, p. 65]. So let us visualize a listing $\{p_{ij}\}_{j=1}^{M(a,i)}$ of the Lyndon

words of length i for each i, arranged vertically, and a corresponding listing of the (expanded) factors on the right side of the cyclotomic identity (1) as in Figure 1 below.

$$\begin{array}{cc}
p_{11} & (1+z+z^2+\cdots+z^k+\ldots) \\
\vdots & \vdots \\
\vdots & \vdots \\
p_{i1} & (1+z^i+z^{2i}+\cdots+z^{ki}+\ldots) \\
\vdots & \vdots \\
p_{i,M(a,i)} & (1+z^i+z^{2i}+\cdots+z^{ki}+\ldots) \\
p_{i+1,1} & (1+z^{i+1}+z^{2(i+1)}+\cdots+z^{k(i+1)}+\ldots) \\
\vdots & \vdots \\
\vdots & \vdots
\end{array}$$

Figure 1

The coefficient of z^n on the right side of the cyclotomic identity (1) is the number of ways to select one power of z from each row in Fig. 1 such that their exponents sum to n. Letting the term z^{ki} in the row labelled p_{ij} correspond to k copies of the Lyndon word p_{ij}, we see that this coefficient is equal to the number of sets (multisets really) of Lyndon words (on a letters) whose lengths sum to n. Let $\mathcal{C}(a,n)$ denote the collection of such multisets. For example, $\mathcal{C}(2,3)$ consists of 8 multisets: $(1)\{A,A,A\}$ $(2)\{AAB\}$ $(3)\{AB,A\}$ $(4)\{ABB\}$ $(5)B,AA\}$ $(6)\{B,AB\}$ $(7)\{BB,A\}$ $(8)\{B,B,B\}$. Now recall $\mathcal{W}(a,n)$ is the set of all n-letter words on our a-letter alphabet; thus $\mathcal{W}(2,3) = \{AAA,$ $AAB,$ $ABA,$ $ABB,$ $BAA,$ $BAB,$ $BBA,$ $BBB\}$. Clearly the coefficient of z^n on the left side of (1) is $a^n = |\mathcal{W}(a,n)|$.

4. A Bijection. So far we have identified corresponding coefficients in (1) with the cardinalities of all words of length n on $\mathcal{A}$—$\mathcal{W}(a,n)$, and all multisets of Lyndon words on $\mathcal{A}$ whose lengths sum to n—$\mathcal{C}(a,n)$. All that's missing is a bijection $\mathcal{W}(a,n) \longleftrightarrow \mathcal{C}(a,n)$. To go from $\mathcal{C}(a,n)$ to $\mathcal{W}(a,n)$, surely the most obvious thing to do is to erase the commas. For $\mathcal{C}(2,3)$ above, this works!

It will work in general provided we arrange the Lyndon words comprising a multiset in an appropriate order, and reverse lex ($\geq$) will do. Let this be done (as it quietly was for $\mathcal{C}(2,3)$ above) giving a canonical representation of each element of $\mathcal{C}(a,n)$. Now let $\psi : \mathcal{C}(a,n) \to \mathcal{W}(a,n)$ denote the "erase the commas" map. For ψ to be a bijection the following theorem must be true (it is).

Theorem 1 *Any word $w \in \mathcal{W}(a,n)$ can be uniquely factored as a weakly decreasing product of Lyndon words w_i:*

$$w = w_1 w_2 \cdots w_r \qquad w_1 \geq w_2 \geq \cdots \geq w_r$$

This is sometimes called the Chen-Fox-Lyndon factorization and an exposition can be found in [8, p. 67]. Algorithms for effecting the factorization are also discussed there and implemented in the *Mathematica*^{TM} package CombinatoricsOnWords available from **http://www.stat.wisc.edu/~callan/**

References

[1] N. Metropolis and G. C. Rota, Witt vectors and the algebra of necklaces, *Advances in Math.* 50 (1983), 95–125.

[2] N. Metropolis and G. C. Rota, The cyclotomic identity, AMS *Contemporary Mathematics* 34 (1984), 19–27.

[3] K. Varadarajan and K. Wehrhahn, Aperiodic rings, necklace rings, and Witt vectors, *Advances in Math.* 81 (1990), 1–29.

[4] D. E. Taylor, A natural proof of the cyclotomic identity, *Bull. Austral. Math. Soc.* 42 (1990), 185–189.

[5] Adrian M. Nelson, A generalized cyclotomic identity, *Advances in Math.* 83 (1990), 1–29.

[6] H. L. Buchanan, A. Knopfmacher, M. E. Mays, On the cyclotomic identity and related product expansions *Australasian J. of Comb.* 8 (1993), 233-245.

[7] V. Domocos and W. R. Schmitt, An application of linear species, *Discrete Math.* 132 (1994), 377–381.

[8] M. Lothaire, Combinatorics on Words, Cambridge University Press, NY, 1997.