THE CYCLE CONSTRUCTION

Philippe Flajolet and Michèle Soria†
INRIA, Rocquencourt
78153–Le Chesnay (France)

Abstract. We give a direct generating function construction for cycles of combinatorial structures.

Let $\mathcal{A}$ be a class of combinatorial structures, with $A(z)$ its corresponding *ordinary generating function*: $A(z) = \sum_{\alpha\in\mathcal{A}} z^{|\alpha|}$. We use corresponding letters for classes and generating functions. Consider the class $\mathcal{C}$ whose elements are cycles of elements of $\mathcal{A}$. The following result is classical [6], [1]:

$$C(z) = \sum_{k\geq 1} \frac{\phi(k)}{k} \log \frac{1}{1-A(z^k)}\,, \tag{0}$$

where $\phi(k)$ is the Euler totient function. This result is proved by Read [6] using Pólya theory [5] and a classical computation of the *Zyklenzeichner* of the cyclic group. De Bruijn and Klarner [1] have another derivation, which amounts to the Lyndon factorization of free monoids [4, p. 64]. Our purpose in this note is to show that equality (0) follows directly from basic principles of combinatorial analysis [3], using elementary concepts of combinatorics on words from Lothaire [4].

Principle 1. *Every non-empty word over $\mathcal{A}$ has a unique root which is a primitive word.*

For instance with $\alpha, \beta \in \mathcal{A}$, word $\alpha\beta\alpha\beta\beta\alpha\beta\alpha\beta\beta\alpha\beta\alpha\beta\beta$ decomposes into $\alpha\beta\alpha\beta\beta|\alpha\beta\alpha\beta\beta|\alpha\beta\alpha\beta\beta$ and its root is the primitive (also called aperiodic) word $\alpha\beta\alpha\beta\beta$. Let $\mathcal{S} = \mathcal{A}^+$ be the set of non-empty words formed with elements of $\mathcal{A}$, and $\mathcal{PS}$ the set of primitive words. From Principle 1, we have‡

$$S(z,u) \equiv \frac{uA(z)}{1-uA(z)} = \sum_{k\geq 1} PS(z^k, u^k)\,. \tag{1a}$$

From Moebius inversion applied to (1a), we get an explicit form for $PS(z,u)$:

$$PS(z,u) = \sum_{k\geq 1} \mu(k) S(z^k, u^k) = \sum_{k\geq 1} \mu(k) \frac{u^k A(z^k)}{1-u^k A(z^k)}\,. \tag{1b}$$

Principle 2. *Every primitive k-cycle has k distinct primitive word representations.*

A cycle is said to be primitive iff any associated word is primitive. We use the notation $[\ldots]$ to denote a cycle. Then, for instance, the 5-cycle $[ababb] = [babba] = \ldots = [babab]$ is primitive, while the 6-cycle $[abbabb]$ is not. We let $\mathcal{PC}$ denote the class of primitive cycles. Principle 2 permits to express the bivariate generating function $PC(z,u)$ via the transformation $u^k \mapsto u^k/k$ applied to $PS(z,u)$:

$$PC(z,u) = \int_0^u PS(z,t)\,\frac{dt}{t}\,. \tag{2a}$$

Integrating with respect to u, we derive

$$PC(z,u) = \sum_{k\geq 1} \frac{\mu(k)}{k} \log \frac{1}{1-u^k A(z^k)}\,. \tag{2b}$$

---

† also at LRI Université Paris-Sud 91405–Orsay.

‡ We introduce bivariate generating functions, and make a consistent use of variable u to mark the number of letters (called length) in a sequence (word) or a cycle: The coefficient of $[u^\ell z^n]$ in a generating function $f(z,u)$ of $\mathcal{F}$ represents the number of structures in $\mathcal{F}$ of total size n having length ℓ.

Principle 3. *Every cycle has a root which is a primitive cycle*
A cycle like $[\alpha\beta\alpha\beta\beta\alpha\beta\alpha\beta\beta\alpha\beta\alpha\beta\beta]$ has a unique root defined up to cyclic order that is here $[\alpha\beta\alpha\beta\beta] \equiv [\beta\alpha\beta\beta\alpha] \equiv \ldots$. For generating functions, this entails the relation

$$C(z,u) = \sum_{k\geq 1} PC(z^k, u^k) \qquad \text{and} \qquad C(z) = \sum_{k\geq 1} PC(z^k, 1). \tag{3a}$$

Using the relation $\sum_{p|k} \mu(p)/p = \phi(k)/k$ in summation (3a), we obtain

$$C(z,u) = \sum_{k\geq 1} \frac{\phi(k)}{k} \log \frac{1}{1-u^k A(z^k)}. \tag{3b}$$

Specializing (3b) with $u = 1$ establishes Equation (0). ∎

Thus the generating function for ℓ–cycles, which is obtained by extracting the coefficient of $[u^\ell]$ in (3b), is found to be

$$\frac{1}{\ell}\sum_{k|\ell} \phi(k) A(z^k)^{\ell/k}.$$

Other results from [1] can also be derived from (3a). The multiset construction $\mathcal{F} = \mathcal{M}(\mathcal{G})$ ($\mathcal{F}$ is the class of all finite multisets of elements of $\mathcal{G}$) is known [5] to translate into

$$F(z) = \exp \sum_k \frac{1}{k} G(z^k).$$

Using identities $\sum_{d/n} \mu(d) = \delta_{n,1}$ and $\sum_{d/n} \phi(d) = n$, the generating functions for multisets of primitive cycles and multisets of cycles (with u again marking length) are found to be

$$\frac{1}{1-uA(z)} \qquad \text{and} \qquad \prod_{k\geq 1} \frac{1}{1-u^k A(z^k)}.$$

By considering singularities of corresponding generating functions [5], it is easy to derive asymptotic results. Assume for instance that the radius of convergence ρ of $A(z)$ satisfies $\rho < 1$ and that $A(\rho) = +\infty$. Then, we have:

- The number of $\mathcal{A}$–cycles of size n and length ℓ is asymptotically $\frac{1}{\ell}$ times the number of $\mathcal{A}$–sequences having size n and length ℓ .
- The number of $\mathcal{A}$–cycles of size n is asymptotically $1/n$ times the number of $\mathcal{A}$–sequences of size n.
- The length of a random $\mathcal{A}$–cycle of length n is asymptotically Gaussian with mean and variance that are $O(n)$. (See [2] for similar results).

These results can be extended to the case when $\rho = 1$ and $A(z)$ has only a pole at $z = 1$ on its circle of convergence.

References

[1] N. G. De Bruijn and D. A. Klarner: "Multisets of aperiodic cycles", *Siam J. Alg. Disc. Meth.* **3**, 1982, 359-368

[2] P. Flajolet and M. Soria: "Normal Limiting Distributions for the Number of Components in Combinatorial Structures", *J. of Combinatorial Theory* Ser. A, to appear (1989).

[3] I. Goulden and D. Jackson: *Combinatorial Enumerations.* Wiley, New York, 1983.

[4] M. Lothaire: *Combinatorics on Words,* Encyclopedia of Mathematics and Its Applications, Vol 17, Academic Press (1983).

[5] G. Pólya: "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen", *Acta Mathematica* **68**, 1937, 145–254. Translated in: G. Pólya and R. C. Read, *Cominatorial Enumeration of Groups, Graphs and Chemical Componds*, Springer, New-York, 1987.

[6] R. C. Read: "A note on the number of functional digraphs", *Math. Ann.* **143**, 1961, 109-110.