

L2: Advanced Unlabelled Constructions: Multisets, Power Sets and Cycles

Analytic Combinatorics

Yun Kuen Cheung, School of Computing, ANU

Unordered Collections: Multisets and Power Sets

In the previous lecture, we saw that forming a sequence of objects implies an inherent ordering. However, in many combinatorial problems, we form collections where the order of elements does not matter. Such unordered collections come in two flavors, depending on whether objects can be chosen more than once.

Example 1. An *integer partition* of n is an unordered collection of positive integers that sum to n . Unlike compositions where order matters, the partition $\{\{3, 1, 1\}\}$ is considered the same as $\{\{1, 3, 1\}\}$. The other integer partitions of 5 are $\{\{5\}\}$, $\{\{4, 1\}\}$, $\{\{3, 2\}\}$, $\{\{2, 2, 1\}\}$, $\{\{2, 1, 1, 1\}\}$ and $\{\{1, 1, 1, 1, 1\}\}$.

In general, the number of integer partitions of n is the same as the number of non-negative integer solutions (a_1, a_2, \dots, a_n) to $\sum_{i=1}^n ia_i = n$. If we view the integers as our base combinatorial class \mathcal{I} , a partition is a collection of elements from \mathcal{I} where elements can be repeated. This is a *multiset* of integers. If we restrict the collection so that all integers are distinct, we obtain partitions into distinct parts, which form the *power set* of \mathcal{I} .

Definition 2. The **multiset class** of a combinatorial class \mathcal{A} , denoted $\text{MSET}(\mathcal{A})$, is the class of all finite unordered collections of elements from \mathcal{A} , where elements may appear multiple times. The size of a multiset is the sum of the sizes of its elements. For the construction to be admissible, we require that \mathcal{A} contains no elements of size 0, i.e., $a_0 = 0$.

Theorem 3. If $\mathcal{C} = \text{MSET}(\mathcal{A})$ and $a_0 = 0$, the OGF of \mathcal{C} is given by

$$C(z) = \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} A(z^k)\right).$$

Proof: An element of $\text{MSET}(\mathcal{A})$ is uniquely determined by the multiplicity of each object $\alpha \in \mathcal{A}$. Let $m_\alpha \in \{0, 1, 2, \dots\}$ be the number of times α appears in the multiset. The total size is $\sum_{\alpha \in \mathcal{A}} m_\alpha |\alpha|$. Thus, the OGF can be factored as a product over all elements in \mathcal{A} :

$$C(z) = \prod_{\alpha \in \mathcal{A}} \left(\sum_{m=0}^{\infty} z^{m|\alpha|} \right) = \prod_{\alpha \in \mathcal{A}} \frac{1}{1 - z^{|\alpha|}}.$$

Grouping elements by sizes and letting a_n be the number of elements of size n gives:

$$C(z) = \prod_{n=1}^{\infty} \left(\frac{1}{1 - z^n} \right)^{a_n}.$$

To express this solely in terms of $A(z)$, we take the natural logarithm:

$$\log C(z) = \sum_{n=1}^{\infty} -a_n \log(1 - z^n) = \sum_{n=1}^{\infty} a_n \sum_{k=1}^{\infty} \frac{z^{nk}}{k} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{\infty} a_n (z^k)^n = \sum_{k=1}^{\infty} \frac{1}{k} A(z^k).$$

Exponentiating both sides completes the proof. \square

Definition 4. The **power set class** (or **subset class**) of \mathcal{A} , denoted $\text{PSET}(\mathcal{A})$, is the class of all finite unordered collections of distinct elements from \mathcal{A} . Again, we require $a_0 = 0$ for the construction to be admissible.

Theorem 5. If $\mathcal{C} = \text{PSET}(\mathcal{A})$ and $a_0 = 0$, the OGF of \mathcal{C} is

$$C(z) = \exp\left(\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} A(z^k)\right).$$

Proof: By the same reasoning as in Theorem 3, an element of $\text{PSET}(\mathcal{A})$ specifies a multiplicity $m_\alpha \in \{0, 1\}$ for each object $\alpha \in \mathcal{A}$. The OGF is the product

$$C(z) = \prod_{\alpha \in \mathcal{A}} (1 + z^{|\alpha|}) = \prod_{n=1}^{\infty} (1 + z^n)^{a_n}.$$

Taking the logarithm and expanding using $\log(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} x^k$ gives

$$\begin{aligned} \log C(z) &= \sum_{n=1}^{\infty} a_n \log(1 + z^n) = \sum_{n=1}^{\infty} a_n \sum_{k=1}^{\infty} \frac{(-1)^{k-1} z^{nk}}{k} \\ &= \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \sum_{n=1}^{\infty} a_n (z^k)^n = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} A(z^k). \end{aligned}$$

Exponentiating both sides completes the proof. □

Example 6. Let \mathcal{P} be the class of all integer partitions. An integer partition is a multiset of positive integers, so $\mathcal{P} = \text{MSET}(\mathcal{I})$, where $\mathcal{I} = \mathcal{Z}_1 + \mathcal{Z}_2 + \dots$ is the class of positive integers introduced in Lecture 1. The OGF of \mathcal{I} is $I(z) = \frac{z}{1-z}$. Using the product formula from the proof of Theorem 3, the OGF is

$$P(z) = \prod_{n=1}^{\infty} \frac{1}{1 - z^n}.$$

This is Euler's famous generating function for integer partitions. Similarly, the class of partitions into distinct parts is $\mathcal{D} = \text{PSET}(\mathcal{I})$, which yields

$$D(z) = \prod_{n=1}^{\infty} (1 + z^n).$$

Exercise 7. Let \mathcal{O} be the class of partitions whose parts are odd integers. Let \mathcal{D} be the class of partitions whose parts are distinct integers. Write down the infinite product generating functions $O(z)$ and $D(z)$ for these two classes. By algebraically manipulating the products, prove that the number of partitions of n into odd parts equals the number of partitions of n into distinct parts.

Exercise 8. Let \mathcal{A} be a combinatorial class with $a_0 = 0$. Let $M_i(z)$ be the OGF of $\text{MSET}_i(\mathcal{A})$, the class of multisets with exactly i objects from \mathcal{A} , counted with multiplicity. Let $P_i(z)$ be the OGF of $\text{PSET}_i(\mathcal{A})$, the class of subsets containing exactly i distinct objects from \mathcal{A} . Show the following identities:

$$M_2(z) = \frac{A(z)^2 + A(z^2)}{2}, \quad M_3(z) = \frac{A(z)^3 + 3A(z)A(z^2) + 2A(z^3)}{6},$$

$$P_2(z) = \frac{A(z)^2 - A(z^2)}{2}, \quad P_3(z) = \frac{A(z)^3 - 3A(z)A(z^2) + 2A(z^3)}{6}.$$

Example 9. In Lecture 1, complete binary trees were *ordered*: the left and right subtrees of an internal node were distinguished. We now consider the unordered version. An *unordered complete binary tree* is either a leaf or an internal node attached to two unordered complete binary subtrees. Two such trees are considered the same if one can be transformed into the other by a sequence of left-right swaps at internal nodes.

Let \mathcal{T} be the class of unordered complete binary trees, where the size is the number of internal nodes. A leaf contributes the neutral class \mathcal{E} . An internal node contributes one atom \mathcal{Z} , together with an unordered multiset of exactly two subtrees from \mathcal{T} . Hence

$$\mathcal{T} = \mathcal{E} + \mathcal{Z} \times \text{MSET}_2(\mathcal{T}).$$

By Exercise 8, its OGF satisfies

$$T(z) = 1 + \frac{z}{2} (T(z)^2 + T(z^2)).$$

Writing $T(z) = \sum_{n=0}^{\infty} t_n z^n$ and comparing coefficients gives $t_0 = 1$ and, for $n \geq 1$,

$$t_n = \frac{1}{2} \left(\sum_{i=0}^{n-1} t_i t_{n-1-i} + \begin{cases} t_{(n-1)/2}, & n \text{ odd,} \\ 0, & n \text{ even.} \end{cases} \right).$$

Using this recurrence for $n \leq 12$ gives

$$T(z) = 1 + z + z^2 + 2z^3 + 3z^4 + 6z^5 + 11z^6 + 23z^7 + 46z^8 + 98z^9 + 207z^{10} + 451z^{11} + 983z^{12} + \mathcal{O}(z^{13}).$$

More About Integer Partitions and Compositions

Example 10. A *strictly increasing composition* of an integer n is a sequence of positive integers (p_1, p_2, \dots, p_k) such that $p_1 + p_2 + \dots + p_k = n$ and $p_1 < p_2 < \dots < p_k$. Although compositions are sequences where order matters, the strict monotonicity condition completely determines the ordering. Since every subset of positive integers can be sorted into exactly one strictly increasing sequence, there is a natural one-to-one correspondence between strictly increasing compositions and integer partitions into distinct parts. We can consider two cases depending on the allowed values of k :

1. Exactly K parts: If $k = K$ is a fixed positive integer, a strictly increasing composition is equivalent to an integer partition into exactly K distinct parts. By subtracting i from each part p_i , we obtain a weakly increasing sequence $0 \leq p_1 - 1 \leq p_2 - 2 \leq \dots \leq p_K - K$, which corresponds to a

partition into at most K parts. The sum of the subtracted terms is $\frac{K(K+1)}{2}$, so the OGF is

$$\frac{z^{K(K+1)/2}}{(1-z)(1-z^2)\cdots(1-z^K)}.$$

2. Any number of parts: If the number of parts is arbitrary, the class of strictly increasing compositions is isomorphic to the class of partitions into distinct parts, whose OGF is $\prod_{n=1}^{\infty}(1+z^n)$ as shown in Example 6.

Example 11. Let $P_{K,L}(z)$ be the OGF for the class of integer partitions with at most K parts and each part at most L . A partition of this type can be represented by a Ferrers diagram that fits entirely inside a bounding box of K rows and L columns. We can divide these valid Ferrers diagrams into two disjoint sets:

1. Diagrams with fewer than K parts: These diagrams fit inside a $(K-1) \times L$ box, and their generating function is simply $P_{K-1,L}(z)$.
2. Diagrams with exactly K parts: These diagrams must have a full first column of length K . Removing this first column yields a valid Ferrers diagram fitting inside a $K \times (L-1)$ box. Since removing the first column removes exactly K boxes (reducing the total size by K), the generating function for this case is $z^K P_{K,L-1}(z)$.

Combining these two cases yields the recurrence relation for $K, L \geq 1$:

$$P_{K,L}(z) = P_{K-1,L}(z) + z^K P_{K,L-1}(z),$$

with the boundary conditions $P_{0,L}(z) = 1$ and $P_{K,0}(z) = 1$ for any $K, L \geq 0$. Solving this recurrence relation (which we leave as an exercise to the reader) leads to the closed-form rational expression known as the q -binomial coefficient or *Gaussian polynomial*:

$$P_{K,L}(z) = \binom{K+L}{K}_z = \frac{(1-z^{K+L})(1-z^{K+L-1})\cdots(1-z^{L+1})}{(1-z^K)(1-z^{K-1})\cdots(1-z)}.$$

Unlike unbounded integer partitions which admit a clean symbolic construction via $\text{MSET}(\mathcal{I})$, this restricted case does not easily yield to a direct translation using the standard symbolic operators (MSET , PSET or SEQ). Adding simultaneous bounds on the number of parts and their maximum size breaks the structural independence required by these operators, making the recurrence relation on Ferrers diagrams the most natural combinatorial approach.

Exercise 12. Let a_n be the number of integer solutions to $x_1 + x_2 + x_3 = n$ subject to $x_1 \geq 1$, $x_2 \geq 2x_1 + 1$ and $x_3 \geq 3x_2 + 2$. By introducing slack variables $y_1 = x_1 - 1$, $y_2 = x_2 - 2x_1 - 1$ and $y_3 = x_3 - 3x_2 - 2$, show that the OGF is

$$A(z) = \frac{z^{15}}{(1-z^9)(1-z^4)(1-z)}.$$

Exercise 13.

(a) By considering the conjugate of a Ferrers diagram (transposing its rows and columns), explain why the number of partitions of n into exactly K parts equals the number of partitions of n whose largest part is exactly K .

(b) An *increasing composition* of n into exactly K parts is a sequence of positive integers (p_1, p_2, \dots, p_K) such that $p_1 + p_2 + \dots + p_K = n$ and $p_1 \leq p_2 \leq \dots \leq p_K$. Using part (a), show that the OGF for the class of such increasing compositions is

$$P_K(z) = \frac{z^K}{(1-z)(1-z^2)\cdots(1-z^K)}.$$

Inverse of Multiset and Power Set Constructions

The multiset construction relates the OGF of a class $\mathcal{C} = \text{MSET}(\mathcal{A})$ to the OGF of the underlying class \mathcal{A} via the formula $C(z) = \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} A(z^k)\right)$. In some combinatorial problems, we are given the generating function $C(z)$ of the composite class and wish to determine the generating function $A(z)$ of the building blocks. We can invert the multiset construction using the *Möbius inversion formula*.

Theorem 14. If $\mathcal{C} = \text{MSET}(\mathcal{A})$ and $a_0 = 0$, then

$$A(z) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log C(z^k),$$

where μ is the Möbius function.

Proof: Taking the logarithm of the multiset generating function yields

$$\log C(z) = \sum_{k=1}^{\infty} \frac{1}{k} A(z^k).$$

We substitute z with z^m , multiply by $\mu(m)/m$, and sum over all $m \geq 1$:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{m} \log C(z^m) = \sum_{m=1}^{\infty} \frac{\mu(m)}{m} \sum_{k=1}^{\infty} \frac{1}{k} A(z^{mk}).$$

Let $j = mk$. Rearranging the sums by grouping terms for a fixed j gives

$$\sum_{j=1}^{\infty} A(z^j) \sum_{m|j} \frac{\mu(m)}{m \cdot (j/m)} = \sum_{j=1}^{\infty} \frac{A(z^j)}{j} \sum_{m|j} \mu(m).$$

Recall the fundamental property of the Möbius function: $\sum_{m|j} \mu(m)$ equals 1 if $j = 1$, and equals 0 for $j > 1$. Thus, all terms on the right-hand side vanish except for $j = 1$, leaving exactly $A(z)$. \square

This inversion formula is particularly useful when the composite objects are easily enumerated, but the fundamental “irreducible” components are intricate.

Example 15. Consider the problem of counting the number of *monic irreducible polynomials* of degree n over a finite field with q elements, denoted \mathbb{F}_q . Let \mathcal{I} be the class of all monic irreducible polynomials over \mathbb{F}_q , where the size of a polynomial is its degree.

Let \mathcal{M} be the class of all monic polynomials over \mathbb{F}_q . Since a monic polynomial of degree n is uniquely determined by its n lower-degree coefficients, and there are q choices for each coefficient, the number of monic polynomials of degree n is exactly q^n . Thus, the OGF of \mathcal{M} is

$$M(z) = \sum_{n=0}^{\infty} q^n z^n = \frac{1}{1 - qz}.$$

On the other hand, by unique factorization, every monic polynomial over \mathbb{F}_q can be factored uniquely into a product of monic irreducible polynomials. Therefore, $\mathcal{M} = \text{MSET}(\mathcal{I})$. Applying Theorem 14 and the equality $\log \frac{1}{1-x} = \sum_{m=1}^{\infty} \frac{x^m}{m}$, the OGF of the monic irreducible polynomials is

$$I(z) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log M(z^k) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log \frac{1}{1 - qz^k} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \sum_{m=1}^{\infty} \frac{q^m}{m} z^{km}.$$

The coefficient of z^n is found by collecting the terms for which $km = n$. Thus, $m = n/k$, and we sum over all divisors k of n :

$$i_n = \sum_{k|n} \frac{\mu(k)}{k} \frac{q^{n/k}}{n/k} = \frac{1}{n} \sum_{k|n} \mu(k) q^{n/k}.$$

Asymptotically, the dominant term in the sum corresponds to $k = 1$, giving $i_n \sim \frac{q^n}{n}$ as $n \rightarrow \infty$.

The same factorization viewpoint also counts square-free polynomials. Let \mathcal{S} be the class of monic square-free polynomials over the same finite field, again with degree as size. A monic polynomial is square-free exactly when each monic irreducible factor appears with multiplicity either 0 or 1. Thus, $\mathcal{S} = \text{PSET}(\mathcal{I})$, and hence

$$S(z) = \prod_{n=1}^{\infty} (1 + z^n)^{i_n}.$$

Using $1 + x = (1 - x^2)/(1 - x)$ and the identity $M(z) = \prod_{n=1}^{\infty} (1 - z^n)^{-i_n}$ for all monic polynomials, we obtain

$$S(z) = \prod_{n=1}^{\infty} \left(\frac{1 - z^{2n}}{1 - z^n} \right)^{i_n} = \frac{M(z)}{M(z^2)} = \frac{1 - qz^2}{1 - qz}.$$

By extracting coefficients, there are $s_n = q^n - q^{n-1}$ monic square-free polynomials for all $n \geq 2$.

Exercise 16. Write $k = 2^m \ell$, where ℓ is odd, and define

$$\gamma(k) = \begin{cases} \mu(\ell), & m = 0, \\ 2^{m-1} \mu(\ell), & m \geq 1. \end{cases}$$

(a) Prove that if $\mathcal{C} = \text{PSET}(\mathcal{A})$ and $a_0 = 0$, then

$$A(z) = \sum_{k=1}^{\infty} \frac{\gamma(k)}{k} \log C(z^k).$$

(b) Let \mathcal{C} be the class with exactly one object of each non-negative size, so that $C(z) = 1/(1-z)$. Suppose \mathcal{A} is a class such that $\mathcal{C} = \text{PSET}(\mathcal{A})$. Use part (a) to show that

$$A(z) = \sum_{j=0}^{\infty} z^{2^j}.$$

Interpret the result in terms of binary representations of non-negative integers.

Cycles

We now consider collections of objects arranged circularly, where configurations differing only by a cyclic shift are considered identical. Take necklaces as an example. Consider forming a necklace of length n using beads of different colors. If we use beads $\{R, G, B\}$, the sequence (R, G, R, B) is the same necklace as (G, R, B, R) , (R, B, R, G) and (B, R, G, R) because rotating the necklace yields the same configuration. However, it is distinct from (R, R, G, B) . On the other hand, (R, G, B, R, G, B) is the same necklace only as (G, B, R, G, B, R) and (B, R, G, B, R, G) .

Definition 17. The **cycle class** of \mathcal{A} , denoted $\text{CYC}(\mathcal{A})$, is the class of directed cycles of elements from \mathcal{A} . We require $a_0 = 0$.

Theorem 18. If $\mathcal{C} = \text{CYC}(\mathcal{A})$ and $a_0 = 0$, the OGF of \mathcal{C} is

$$C(z) = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log \frac{1}{1 - A(z^k)},$$

where φ is Euler's totient function.

The proof of Theorem 18 is deferred to the appendix at the end of this lecture note.

Example 19. Consider the problem of enumerating necklaces made of beads in 3 colors, say red, green and blue. We first define the class of a single bead, $\mathcal{A} = \mathcal{Z}_R + \mathcal{Z}_G + \mathcal{Z}_B$. Its OGF is $A(z) = 3z$. The class of all such necklaces is $\mathcal{N} = \text{CYC}(\mathcal{A})$. By Theorem 18, its generating function is:

$$N(z) = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log \frac{1}{1 - 3z^k}.$$

Using $\log \frac{1}{1-x} = \sum_{m=1}^{\infty} \frac{x^m}{m}$, we have:

$$[z^n]N(z) = [z^n] \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \sum_{m=1}^{\infty} \frac{(3z^k)^m}{m} = [z^n] \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{\varphi(k)}{km} 3^m z^{km}.$$

The coefficient of z^n is collected from all terms for which $km = n$. Thus, $m = n/k$, and we sum over all divisors k of n :

$$[z^n]N(z) = \sum_{k|n} \frac{\varphi(k)}{n} 3^{n/k} = \frac{1}{n} \sum_{k|n} \varphi(k) 3^{n/k}.$$

Example 20. Consider the class of cycles where each component (“bead”) has size either 1 or 2. Let $\mathcal{A} = \mathcal{Z}_1 + \mathcal{Z}_2$ be the class of a single component. Its OGF is $A(z) = z + z^2$. The class of such cycles is $\mathcal{C} = \text{CYC}(\mathcal{A})$. By Theorem 18, its OGF is:

$$C(z) = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log \frac{1}{1 - A(z^k)} = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log \frac{1}{1 - z^k - z^{2k}}.$$

To extract the coefficients, we notice that $1 - z - z^2$ factors as $(1 - \phi z)(1 - \bar{\phi} z)$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. Thus, we can split the logarithm:

$$\log \frac{1}{1 - z^k - z^{2k}} = \log \frac{1}{1 - \phi z^k} + \log \frac{1}{1 - \bar{\phi} z^k} = \sum_{m=1}^{\infty} \frac{\phi^m + \bar{\phi}^m}{m} z^{km}.$$

Substituting this back into $C(z)$, we get:

$$C(z) = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \sum_{m=1}^{\infty} \frac{\phi^m + \bar{\phi}^m}{m} z^{km}.$$

To find the number of such cycles of size n , we extract the coefficient of z^n by collecting terms for which $km = n$, so $m = n/k$. Summing over all divisors k of n , we obtain the exact formula:

$$[z^n]C(z) = \frac{1}{n} \sum_{k|n} \varphi(k) (\phi^{n/k} + \bar{\phi}^{n/k}).$$

As $n \rightarrow \infty$, the dominant term in the sum corresponds to $k = 1$, and since $|\bar{\phi}| < 1 < \phi$, the coefficient is exponentially dominated by ϕ^n . Thus, we obtain the asymptotic approximation $[z^n]C(z) \sim \frac{\phi^n}{n}$.

Exercise 21. A *cycle composition* of an integer n is a cyclic arrangement of positive integers whose sum is n .

- (a) Express the class of cycle compositions symbolically, and write down its OGF $C(z)$.
(b) Using the logarithmic expansion $\log \frac{1-x}{1-2x} = \sum_{m=1}^{\infty} \frac{2^m-1}{m} x^m$, extract the coefficients of $C(z)$ to derive an exact formula for the number of cycle compositions of n .

Summary of Unlabelled Constructions

Construction	Combinatorial Class	Ordinary Generating Function
Disjoint Union	$\mathcal{A} + \mathcal{B}$	$A(z) + B(z)$
Cartesian Product	$\mathcal{A} \times \mathcal{B}$	$A(z)B(z)$
Sequence	$\text{SEQ}(\mathcal{A})$	$\frac{1}{1-A(z)}$
Multiset	$\text{MSET}(\mathcal{A})$	$\exp\left(\sum_{k=1}^{\infty} \frac{1}{k} A(z^k)\right)$
Power Set	$\text{PSET}(\mathcal{A})$	$\exp\left(\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} A(z^k)\right)$
Inverse of Multiset	\mathcal{A} s.t. $\mathcal{C} = \text{MSET}(\mathcal{A})$	$\sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log C(z^k)$
Inverse of Power Set	\mathcal{A} s.t. $\mathcal{C} = \text{PSET}(\mathcal{A})$	$\sum_{k=1}^{\infty} \frac{\gamma(k)}{k} \log C(z^k)$
Cycle	$\text{CYC}(\mathcal{A})$	$\sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log \frac{1}{1-A(z^k)}$

Appendix: Proof of Theorem 18

The proof relies on bivariate generating functions and Möbius inversion.

Lemma 22. Möbius Inversion Formula for Bivariate Generating Functions. Let $F(z, u)$ and $G(z, u)$ be formal power series without constant terms. If

$$F(z, u) = \sum_{k \geq 1} G(z^k, u^k),$$

then

$$G(z, u) = \sum_{k \geq 1} \mu(k) F(z^k, u^k),$$

where μ is the Möbius function.

Proof: Let $F(z, u) = \sum_{n,j} f_{n,j} z^n u^j$ and $G(z, u) = \sum_{n,j} g_{n,j} z^n u^j$. Let a, b be two relatively prime non-negative integers; if one of them is 0, then the other must be 1. Observe that

$$f_{ta, tb} = \sum_{k|t} g_{\frac{ta}{k}, \frac{tb}{k}} = \sum_{k|t} g_{ka, kb}.$$

Let $\hat{f}(t) = f_{ta, tb}$ and $\hat{g}(k) = g_{ka, kb}$. Then $\hat{f}(t) = \sum_{k|t} \hat{g}(k)$. By the standard Möbius inversion formula,

$$g_{ta, tb} = \hat{g}(t) = \sum_{k|t} \mu(k) \hat{f}\left(\frac{t}{k}\right) = \sum_{k|t} \mu(k) f_{\frac{ta}{k}, \frac{tb}{k}}.$$

Thus, for any $(n, j) \neq (0, 0)$, we have $g_{n,j} = \sum_{k|\gcd(n,j)} \mu(k) f_{n/k, j/k}$. Substituting this into the series for $G(z, u)$ gives:

$$G(z, u) = \sum_{(n,j) \neq (0,0)} g_{n,j} z^n u^j = \sum_{(n,j) \neq (0,0)} \left(\sum_{k|\gcd(n,j)} \mu(k) f_{\frac{n}{k}, \frac{j}{k}} \right) z^n u^j.$$

Let $n = kn'$ and $j = kj'$. As the pair (n, j) ranges over all pairs except $(0, 0)$ and k ranges over their common divisors, the variables (n', j') implicitly range over all pairs except $(0, 0)$, while k ranges independently over all positive integers. Reordering the summation over the triples (k, n', j') yields:

$$G(z, u) = \sum_{k=1}^{\infty} \mu(k) \sum_{(n', j') \neq (0,0)} f_{n', j'} z^{kn'} u^{kj'} = \sum_{k=1}^{\infty} \mu(k) F(z^k, u^k). \quad \square$$

Definition 23. A sequence $\sigma \in \text{SEQ}_{\geq 1}(\mathcal{A})$ is **primitive** (or **aperiodic**) if it is not the repetition of a shorter sequence. That is, σ cannot be written as τ^k for any $k > 1$.

Since cyclic configurations are defined by factoring out cyclic shifts, it is crucial to track the number of components in a sequence rigorously. We therefore introduce a bivariate generating function $S(z, u)$ for non-empty sequences, where z marks the total size and u marks the number of components:

$$S(z, u) = \sum_{n=1}^{\infty} u^n A(z)^n.$$

Let $P(z, u)$ be the corresponding bivariate generating function for primitive sequences. Since every sequence σ has a unique primitive root τ such that $\sigma = \tau^k$, a primitive sequence of size s with n components repeated k times yields a sequence of size ks with kn components. Thus, we have the relation:

$$S(z, u) = \sum_{k=1}^{\infty} P(z^k, u^k).$$

By Lemma 22,

$$P(z, u) = \sum_{k=1}^{\infty} \mu(k) S(z^k, u^k) = \sum_{k=1}^{\infty} \mu(k) \sum_{n=1}^{\infty} u^{kn} A(z^k)^n.$$

A cycle is primitive if its linear representations (sequences) are primitive. There is an exact n -to-1 correspondence between primitive sequences of n components and primitive cycles of n components, because all n cyclic shifts of a primitive sequence are distinct. Thus, the bivariate generating function for primitive cycles, $PC(z, u)$, is obtained by dividing the term for sequences of n components by n . This corresponds to integrating with respect to u :

$$PC(z, u) = \int_0^u \frac{P(z, t)}{t} dt = \sum_{k=1}^{\infty} \mu(k) \sum_{n=1}^{\infty} \int_0^u t^{kn-1} A(z^k)^n dt = \sum_{k=1}^{\infty} \mu(k) \sum_{n=1}^{\infty} \frac{u^{kn}}{kn} A(z^k)^n.$$

By the Maclaurin series $\sum_{n=1}^{\infty} \frac{x^n}{n} = \log \frac{1}{1-x}$, we get:

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

Setting $u = 1$ gives the univariate OGF for primitive cycles:

$$PC(z) = PC(z, 1) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log \frac{1}{1 - A(z^k)}.$$

Finally, every cycle is uniquely formed by repeating a primitive cycle m times, for some positive integer m . Hence, the OGF for $\mathcal{C} = \text{CYC}(\mathcal{A})$ is

$$C(z) = \sum_{m=1}^{\infty} PC(z^m) = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log \frac{1}{1 - A(z^{mk})}.$$

Let $j = mk$. We can rearrange the double sum by grouping terms with the same j :

$$C(z) = \sum_{j=1}^{\infty} \left(\sum_{k|j} \frac{\mu(k)}{k} \right) \log \frac{1}{1 - A(z^j)}.$$

Applying the arithmetic identity $\sum_{k|j} \frac{\mu(k)}{k} = \frac{\varphi(j)}{j}$, we complete the proof.