Analytic Combinatorics of Unlabeled Objects

Set of exercises IV: responses

1. For each of the following functions $f(z)$, find the radius of convergence and an equivalent (asymptotic) for the coefficients of the power-series expansion $f(z) = \sum a_n z^n$ at $z = 0$.

   (a) $f(z) = \frac{1}{(1-2z)^2} \log\left(\frac{1}{1-z}\right)$.

   (b) $f(z) = \frac{e^{2z}-1}{(1-z)(1-2z)^3}$.

   (c) $f(z) = \frac{1}{2-e^z}$.

Response.

(a) The singularity closest to the origin is $z = 1/2$, as $\log\left(\frac{1}{1-z}\right)$ is analytic on $|z| < 1$. Thus the radius of convergence is $\rho = 1/2$. For the asymptotics, expanding $\log(\frac{1}{1-z})$ around $z = 1/2$, we obtain $f(z) = \frac{1}{(1-2z)^2} \log\left(\frac{1}{1-1/2}\right) + \frac{1}{(1-2z)^2}\left(\frac{1}{1-1/2}\right)(z - 1/2) + \texttt{analytic}$. That is

$$g(z) = f(z) - \left(\tfrac{1}{(1-2z)^2}\log 2 - \tfrac{1}{1-2z}\right)$$

is analytic at $z = 1/2$, and hence analytic on $|z| < 1$. It follows that, for any fixed $\epsilon > 0$, we have $[z^n]g(z) = O((1+\epsilon)^n)$. Thus

$$[z^n]f(z) = [z^n]\tfrac{1}{(1-2z)^2}\log 2 + [z^n]\tfrac{1}{1-2z} + O((1+\epsilon)^n) = (\log 2)\cdot(n+1)\cdot 2^n - 2^n + O((1+\epsilon)^n)\,.$$

We deduce $[z^n]f(z) \sim (\log 2)n2^n$.

(b) The singularity closest to the origin is $z = 1/2$. Thus the radius of convergence is $\rho = 1/2$. In this case, expanding $\frac{e^{2z}-1}{1-z}$ around $z = 1/2$ we obtain

$$f(z) = \frac{2(e-1)}{(1-2z)^3} + \frac{c_1}{(1-2z)^2} + \frac{c_2}{(1-2z)^1} + \text{analytic at } z = 1/2\,.$$

The latter analytic function, being analytic up to $z = 1$, it will not contribute to the dominant asymptotics. Since $[z^n](1 - z/\rho)^{-m} \sim \frac{n^{m-1}}{(m-1)!}\rho^{-n}$ for any positive integer $m \geq 1$,

$$[z^n]f(z) \sim 2(e-1)\frac{n^2}{2}2^n = (e-1)n^2 2^n\,.$$

(c) The singularities satisfy $e^z = 2$, i.e., these are $z = \log 2 + 2\pi i k$ with $k \in \mathbb{Z}$. The closest to the origin is $\log 2$. Thus the radius of convergence is $\rho = \log 2$.
Expand the power series of the denominator around $z = \log 2$,

$$\frac{1}{2-e^z} = \frac{1}{(2-e^z)'_{z=\log 2}(z - \log 2) + \sum_{k\geq 2} c_k (z-\log 2)^k} = \frac{1/2}{\log 2 - z} \times \frac{1}{1 + \sum_{k\geq 1}\hat{c}_k (z - \log 2)^k}\,.$$

The multiplicative inverse $(1+\sum_{k\geq 1}\hat{c}_k(z-\log 2)^k)^{-1}$ is well-defined, since the denominator is not 0 at $z = \log 2$, and $(1 + \sum_{k\geq 1}\hat{c}_k(z - \log 2)^k)^{-1} = 1 + \sum_{k\geq 1} d_k(z - \log 2)^k$ for certain coefficients. Remark, moreover, that this expansion is entire (radius of convergence ∞) as this is the case for $2 - e^z$.

Expanding

$$f(z) = \frac{1/2}{\log 2 - z} + \texttt{analytic at } z = \log 2\,.$$

Since there are no more singularities on $|z| = \log 2$ and the function is meromorphic we deduce that

$$[z^n]f(z) \sim [z^n]\frac{1/2}{\log 2 - z} = [z^n]\frac{1/(2\log 2)}{1 - z/\log 2} = \tfrac{1}{2}(\log 2)^{-(n+1)}\,.$$

2. In this exercise we prove a key inequality in Coding and Information Theory by using the radius of convergence.

   Let $\mathcal{A} = \{a_1, \dots, a_k\}$ and $\mathcal{B} = \{\mathbf{0}, \mathbf{1}\}$. A **binary code** $c\colon \mathcal{A}^\star \to \mathcal{B}^\star$ is a morphism, i.e., $c(xy) = c(x)c(y)$. The code c is *uniquely decodable* iff it is injective.

   (a) Let[1] $A(z) = \sum_{a\in\mathcal{A}} z^{|c(a)|}$. Show $C(z) = \sum_{v\in c(\mathcal{A}^\star)} z^{|v|} = \frac{1}{1-A(z)}$.

   (b) [**Kraft-McMillan inequality**] Prove that if c is uniquely decodable, then

   $$\sum_{a\in\mathcal{A}} 2^{-|c(a)|} \le 1\,.$$

   Hint. Reason by contradiction. Note that power-series are continuous within their radius of convergence.

   (c) [**Shannon bound**] (Optional) Consider a distribution $\mathbf{p} = (p_1, \dots, p_k)$ over $(a_1, \dots, a_k)$. Prove that, for a random symbol X,

   $$H(\mathbf{p}) = \sum_{j=1}^{k} p_j \log_2(1/p_j) \le \sum_{j=1}^{k} p_j |c(a_j)| = \mathbb{E}[c(X)]\,.$$

   Hint. Prove that $\log x \le x - 1$ for all $x \in \mathbb{R}_{>0}$. Use the Kraft-McMillan inequality.

Response.

(a) Since c is a morphism, any element $v \in c(\mathcal{A}^\star)$ can be seen as a *sequence* of elements from $c(\mathcal{A})$, whose OGF is $A(z)$, thus $C(z) = \frac{1}{1-A(z)}$.

(b) Suppose otherwise. Then $A(1/2) = \sum_{a\in\mathcal{A}} 2^{-|c(a)|} > 1$.
– By continuity of $A(z)$ within its radius of convergence, which is infinite since $A(z)$ is actually a polynomial because $\mathcal{A}$ is finite, it follows that there must be $c \in (0, 1/2)$ such that $A(c) = 1$. We suppose that c is the smallest such $c > 0$. Then $A(t) < 1$ for $0 \le t < c$ and $C(z)$ converges there. Observe that increases $C(t) \to \infty$ as $t \to c^-$.
– Being c uniquely decodable, it follows that there must be at most 2^n words of length n in $c(\mathcal{A}^\star)$ for each $n \ge 0$. Hence, for $t \in (0, 1/2)$, we deduce $C(t) \le \sum_{n=0}^{\infty} 2^n t^n = \frac{1}{1-2t}$.This means that $C(t) \le \frac{1}{1-2c} < \infty$ for $0 \le t < c$, a contradiction.

[1]Here $|w|$ is the length of the word, i.e., the number of symbols.

(c) We first prove the inequality $\log x \le x-1$ for all $x>0$. Considering $f(x) = x-1-\log x$, we have $f'(x) = 1-\frac{1}{x}$. Looking at the sign of $f'(x)$, we deduce that $f(x)$ decreases on $(0,1]$ and increases in $[1,\infty)$. Hence the minimum of $f(x)$ is found at $x=1$, $f(x) \ge f(1) = 0$ and the auxiliary inequality is proved.

The inequality we want to prove, $H(\mathbf{p}) \le \mathbb{E}[c(X)]$, is equivalent to

$$\sum_j p_j \log_2(2^{-|c(a_j)|}/p_j) \le 0\,.$$

By using the inequality $\log(x) \le x-1$ we deduce $\log_2(2^{-|c(a_j)|}/p_j) \le \frac{1}{\log 2}\left(2^{-|c(a_j)|}/p_j - 1\right)$, thus

$$\sum_j p_j \log_2(2^{-|c(a_j)|}/p_j) \le \frac{1}{\log 2}\sum_j p_j\left(2^{-|c(a_j)|}/p_j - 1\right) = \frac{1}{\log 2}\left(\sum_j 2^{-|c(a_j)|} - \sum_j p_j\right) = 0\,,$$

where the last equality follows from the Kraft-inequality $\sum_j 2^{-|c(a_j)|} \le 1$ and the equality $\sum_j p_j = 1$. Thus the result is proved.

3. (a) Prove the following classical lemma:

Daffodil Lemma. Let $f(z)$ be analytic on $|z|<\rho$, with non-negative coefficients at $z=0$. If the expansion does not reduce to a single monomial and, for some $w \ne 0$, $|w|<\rho$, we have $f(|w|) = |f(w)|$, then

(a.1) we must have $w = Re^{i\theta}$ with $\theta/(2\pi) = \frac{r}{p}$ a rational, $\gcd(r,p)=1$, $p>0$,

(a.2) the non-zero coefficients $a_n = [z^n]f(z)$ occur at positions n all belonging to $a + p\mathbb{Z}_{\ge 0}$ for some fixed a.

(b) [The statement has been corrected] Consider the class $\mathcal{C}$ of binary words without K consecutive ones, with $K \in \mathbb{Z}_{\ge 2}$ fixed.

(b.1) Prove that $C(z) = \frac{1-z^K}{1-z} + \frac{1}{1-z\frac{1-z^K}{1-z}}$.

(b.2) Give a polynomial equation characterizing the radius of convergence $z=\rho_C$. Prove that ρ_C is a simple pole of $C(z)$.

(b.3) Prove that there are no other singularities on $|z| = \rho_C$.

(b.4) Conclude that $[z^n]C(z) \sim c\cdot \rho_C^{-n}$ and give an expression for c in terms of ρ_C and K.

Note. The Fibonacci numbers correspond to the case $K=2$, then $[z^n]C(z) = f_{n+1}$ and $\rho_C = 1/\phi$, $\phi = (1+\sqrt{5})/2$.

Responses.

(a.1) Notice that $|f(w)| \le f(|w|)$ holds always, due to the triangle inequality. For there to be equality, all terms of the sum in $f(w)$ must "point" in the same direction seen as vectors in the complex plane.

Write $f(z) = \sum a_n z^n$. By hypothesis the coefficients $a_n \ge 0$, and there are at least two $a_{n_1} > 0$ and $a_{n_2} > 0$ with $n_1 < n_2$. By the previous argument we must have that $\arg(a_{n_1}w^{n_1}) = \arg(a_{n_2}w^{n_2})$, the angle is the same. Since the coefficients are positive, this is equivalent to $\arg(w^{n_1}) = \arg(w^{n_2})$. Thus, if $w = Re^{i\theta}$, then $\theta n_1 \equiv \theta n_2 (\mathrm{mod} 2\pi)$. Thus $\theta(n_2-n_1) = 2\pi m$ for some $m\in\mathbb{Z}$ and we deduce $\theta = 2\pi\frac{m}{n_2-n_1}$.

(a.2) Here $p > 0$ is the denominator of the reduced fraction $\theta/(2\pi) = r/p$. Let $k = a$ be the smallest index[2] such that $a_k > 0$. Any index n with $a_n > 0$ must satisfy, due to part (a) that $\theta(n-a) \in 2\pi\mathbb{Z}$. Using the equation for θ, we have $\frac{r}{p}(n-a) \in \mathbb{Z}$, but then p must divide $n-a$, because $\gcd(r,p) = 1$. Thus $n \in a + p\mathbb{Z}_{\geq 0}$.

(b.1) The class can be specified as $\mathcal{C} = \texttt{Seq}_{<K}(\mathbf{1}) + \texttt{Seq}_{\geq 1}(\texttt{Seq}_{<K}(\mathbf{1}) \cdot \mathbf{0})$, where the subscript of the sequences denote a restriction to the involved lengths. This is explained as follows: either there are no $\mathbf{0}$s, and in this case we have to most $K-1$ $\mathbf{1}$s, or we have a sequence of at least one $\mathbf{0}$, which may be preceded by a sequence of at most $K-1$ $\mathbf{1}$s.

Thus it follows that the ordinary generating function is

$$C(z) = 1 + z + \ldots + z^{K-1} + \frac{1}{1 - z \times (1 + z + \ldots + z^{K-1})} = \frac{1-z^K}{1-z} + \frac{1}{1 - z\frac{1-z^K}{1-z}},$$

where we have used $1 + z + \ldots + z^{K-1} = \frac{1-z^K}{1-z}$.

(b.2) Clearly the singularity comes from the term $\frac{1}{1-z\times(1+z+\ldots+z^{K-1})} = \frac{1}{1-z\frac{1-z^K}{1-z}}$, as the other is a polynomial (in the quotient form there is a removable singularity). As long as $|z \times (1 + z + \ldots + z^{K-1})| < 1$ the function $C(z)$ is analytic. By Pringsheim's Theorem, the radius of convergence of a power series with positive coefficients is itself a dominant singularity. Thus it is enough to look at the positive axes to determine ρ_C.

The singularity comes when $\rho_C \times (1 + \rho_C + \ldots + \rho_C^{K-1}) = 1$ We note that $\rho_C < 1$ as $1 \times (1 + 1 + \ldots + 1^{K-1}) = K > 1$. We give a simpler equation for ρ_C. We simplify $\frac{1}{1-z\frac{1-z^K}{1-z}} = \frac{1-z}{1-2z+z^{K+1}}$. Since $\rho_C \neq 1$, to have a singularity it follows that

$$1 - 2\rho_C + \rho_C^{K+1} = 0\,.$$

The polynomial $p(x) = 1 - 2x + x^{K+1}$ has a derivative $p'(x) = -2 + (K+1)x^K$. If ρ_C were a double root, then $p'(\rho_C) = 0$ and so $\rho_C^K = \frac{2}{K+1}$. Since $0 = 1 - 2\rho_C + \rho_C^{K+1}$, we deduce $0 = 1 - 2\rho_C + \rho_C\frac{2}{K+1} = 1 - 2\rho_C(1 - 1/(K+1))$, i.e., $\rho_C = (K+1)/(2K)$.

But $2/(K+1) = \rho_C^K$ yields $(K+1)^{K+1} = 2^{K+1}K^K$. Since $\gcd(K, K+1) = 1$ and $(K+1)^{K+1}$ divides $2^{K+1}K^K$, $(K+1)^{K+1}$ must divide 2^{K+1}. However $K+1 \geq 3$ and so $(K+1)^{K+1} > 2^{K+1}$, an absurd. Thus ρ_C is a simple root and the pole is simple.

(b.3) We apply the Daffodil Lemma. Suppose $w = \rho_C e^{i\theta}$ were a dominant singularity. Then again we must have $w \times (1+w+\ldots+w^{K-1}) = 1$. Let $f(z) = w \times (1+w+\ldots+w^{K-1})$. We have $|f(w)| = 1 = f(\rho_C) = f(|w|)$. Thus we are ready to apply the Lemma: $\theta = 2\pi \cdot r/p$ for some reduced fraction with $\gcd(r,p) = 1$ and $p > 0$. But $(a.2)$ implies that, then, all non-zero coefficients of $f(z)$ belong to $a + p\mathbb{Z}_{\geq 0}$ for some a. Looking at $f(z)$, this is only possible for $p = 1$, and it follows that $\theta \in 2\pi\mathbb{Z}$ and $w = \rho_C$. Thus there are no other dominant singularities.

(b.4) The generating function $C(z)$ is rational and $\rho_C > 0$ is the only dominant singularity. We proved that the pole at $z = \rho_C$ is simple, and then $C(z) \sim \frac{c}{1-z/\rho_C}$ for some $c \neq 0$, as $z \to \rho_C$. By the principle of asymptotics of rational functions (see Section 3.2 of the notes), or the Transfer Theorm (a bit overkill, but true), $[z^n]C(z) \sim c \cdot \rho_C^{-c}$.

[2] Sorry for the choice of the letter a...

The constant c must equal

$$\lim_{z\to\rho_C}(1-z/\rho_C)C(z) = -\tfrac{1}{\rho_C}\lim_{z\to\rho_C}(z-\rho_C)\frac{1-z}{p(z)} = -\frac{1-\rho_C}{\rho_C}\frac{1}{p'(\rho_C)} = \frac{1-\rho_C}{\rho_C}\frac{1}{2-(K+1)\rho_C^K}.$$

Extra. Since $c > 0$ by combinatorial considerations, and $\rho_C < 1$, we deduce that $2 > (K+1)\rho_C^K$, i.e., $\sqrt[K]{2/(K+1)} > \rho_C$.