

## GENERATING SERIES

The basic idea for which generating series were introduced is to *represent a sequence of numbers by a function*, which on the one hand will be easier to manipulate and on the other hand will allow us to treat the sequence in its entirety. For example, if a sequence of costs is defined by a recurrence equation, the recurrence equation will correspond to a functional equation on the generating series: the latter equation may be solved by algebraic or analytic techniques.

Similarly, generating series will allow us to represent a discrete probability law globally and to handle it more easily: indeed, assuming that  $p_n$  is the probability that event  $n$  occurs, a single generating function  $g$  will represent the whole sequence  $p_n$ ; moreover, the values of  $p_n$  can be recovered from the generating series  $g$ , and techniques for studying the generating series will give properties of the probability distribution (average values, means, etc.).

Generating series were introduced at the end of the eighteenth century in order to study probabilities by the French mathematicians Laplace and de Moivre (the latter took British nationality after the *édit de Nantes* was revoked).

We especially recommend the following handbooks, where many examples of computations on series and applications can be found:

Ronald Graham, Donald Knuth, Oren Patashnik, *Concrete Mathematics*, Addison-Wesley, London (1989).

William Feller, *Probability Theory*, Vol. 1, John Wiley, New York (1968).

Donald Knuth, *The Art of Computer Programming*, Vol. 1, Addison-Wesley, London (1973).

## 8.1 Generalities

### 8.1.1 Intuitions

Let  $u = (u_0, u_1, u_2, \dots, u_p)$  be a sequence of  $p + 1$  numbers; they can be globally represented as a vector, or canonically associated with an element of a fixed vector space; we choose the second option and take the set of polynomials in the variable  $X$  as vector space; the sequence  $u = (u_0, u_1, u_2, \dots, u_p)$  is then represented by the polynomial

$$P(X) = u_0 + u_1X + u_2X^2 + \dots + u_pX^p.$$

If  $u_p \neq 0$ ,  $p$  is said to be the degree of the polynomial  $P(X)$ . The advantage of this second approach is the ability to represent polynomials of an arbitrary degree  $n \in \mathbb{N}$ : a polynomial is simply represented by a sequence  $(u_n)_{n \in \mathbb{N}}$  such that all but a finite number of the  $u_n$ s are equal to zero. A polynomial  $P(X) = u_0 + u_1X + u_2X^2 + \dots + u_pX^p$ , of degree  $p$  is then represented by the sequence  $u = (u_0, u_1, u_2, \dots, u_p, 0, 0, \dots)$ , where  $u_n = 0$  for all  $n > p$ . The  $+$  and  $\times$  operations on sequences correspond to operations on the polynomials.

- The sum  $u + v$  corresponds to the addition of polynomials. The unit for  $+$  is the sequence  $(0, 0, 0, \dots)$ , corresponding to the polynomial function  $Z(x) = 0$  for all  $x$ . In fact, if

$$P(X) = u_0 + u_1X + u_2X^2 + \dots + u_pX^p$$

and

$$Q(X) = v_0 + v_1X + v_2X^2 + \dots + v_qX^q,$$

the polynomial  $P(X) + Q(X)$  is given by

$$P(X) + Q(X) = (u_0 + v_0) + (u_1 + v_1)X + (u_2 + v_2)X^2 + \dots + w_nX^n,$$

where

$$w_nX^n = \begin{cases} u_pX^p & \text{if } p > q, \\ (u_p + v_p)X^p & \text{if } p = q, \\ v_qX^q & \text{if } p < q. \end{cases}$$

- Multiplication is more complex: various problems arise with the definition  $(uv)_n = u_nv_n$ . Firstly, the sequence  $\forall n, u_n = 1$  would be a good candidate for a unit, except for the fact that it counts an infinity of non-zero  $u_n$ s; secondly, as soon as a sequence has a term  $u_n = 0$ , it is not invertible; and finally, the ring of sequences is not an integral domain:  $u \neq 0$ ,  $v \neq 0$  and  $uv = 0$  may occur (in case  $u$  and  $v$  are equal to zero on complementary sets of indices); for this reason the *Hadamard product*  $(uv)_n = u_nv_n$  will no longer be considered in the

sequel. Instead, we will use the *Cauchy product* (or *convolution product*) defined by  $(uv)_n = \sum_{p+q=n} u_p v_q$ , which has the additional advantage of corresponding naturally to the product of polynomials: if the sequence  $u$  is represented by  $P(X) = \sum_0^N u_p X^p$  and the sequence  $v$  is represented by  $Q(X) = \sum_0^M v_q X^q$ , then  $uv$  is represented by  $P(X)Q(X)$ , since the coefficient of  $X^n$  in  $P(X)Q(X)$  is  $(uv)_n = \sum_{p+q=n} u_p v_q$ .

EXAMPLE 8.1 Let  $P(X) = u_0 + u_1 X + u_2 X^2$  and  $Q(X) = v_0 + v_1 X$ .

$$\begin{array}{r} u_0 + u_1 X + u_2 X^2 \\ \times \quad v_0 + v_1 X \\ \hline u_0 v_0 + u_1 v_0 X + u_2 v_0 X^2 \\ + u_0 v_1 X + u_1 v_1 X^2 + u_2 v_1 X^3 \\ \hline u_0 v_0 + (u_1 v_0 + u_0 v_1) X + (u_2 v_0 + u_1 v_1) X^2 + u_2 v_1 X^3 \end{array}$$

If we assume that  $Q(X) = v_0 + v_1 X + v_2 X^2$  with  $v_2 = 0$ , we obtain  $u_2 v_0 + u_1 v_1 = u_2 v_0 + u_1 v_1 + u_0 v_2$ . Similarly,  $u_2 v_1 = u_3 v_0 + u_2 v_1 + u_1 v_2 + u_0 v_3$  with  $u_3 = v_3 = v_2 = 0$ .

EXERCISE 8.1 Find the unit of the convolution product. ◇

We will generalize this approach to sequences  $(u_n)_{n \in \mathbb{N}}$  possibly having an infinite number of non-zero  $u_n$ s, by associating a formal power series  $\mathbf{u} = \sum_{n=0}^{\infty} u_n X^n$  to the sequence  $u = \{u_n / n \in \mathbb{N}\}$ .

Note, first, that it is a *purely formal* extension of the notion of polynomials and that we will not worry about the convergence radius of our series which can be equal to zero. A philosophical remark is called for here (for readers already familiar with series): the generating series can be considered from two different viewpoints:

- firstly, they can be considered as analytic functions of the complex variable  $X$ , and they then inherit all the good (or bad) properties of those functions (convergence, absolute convergence, approximations, etc.) which can be found in all complex analysis handbooks,
- secondly, they can be considered as formal algebraic expressions, generalizing polynomials, where  $X$  is simply a position indicator whose values are irrelevant. We then speak of *formal power series*.

As our goal is understanding the sequence of numbers  $(u_n / n \in \mathbb{N})$ , we will be interested in the second viewpoint. In this viewpoint, all the operations we

perform on the series can be defined and justified in a purely algebraic and formal framework, independently of their convergence.

When, moreover, the series happens to converge for some values of  $x$  and, in addition, we know how to compute the corresponding analytic function and we want to study the asymptotic behaviour of the  $u_n$ s, then the usual methods of complex analysis will allow us to find the values of the coefficients of the series, or at least their asymptotic behaviour. In that case, the first approach will be usable.

Note that, conversely, every function which admits a power series expansion having a non-zero convergence radius uniquely determines (because of the uniqueness of the power series expansion) a sequence of numbers consisting of its coefficients.

EXAMPLE 8.2 Consider the example of the Fibonacci numbers denoted by  $F_n$ . We want to determine  $F_n$  given that

$$F_n = F_{n-1} + F_{n-2} \quad \text{and} \quad F_0 = 0 \quad F_1 = 1 .$$

Consider the series  $F(X) = \sum_{n \geq 0} F_n X^n$ . From  $F_n = F_{n-1} + F_{n-2}$  we deduce  $\forall n \geq 2, F_n X^n = F_{n-1} X^n + F_{n-2} X^n = X F_{n-1} X^{n-1} + X^2 F_{n-2} X^{n-2}$ . Summing the equalities  $F_n X^n = X F_{n-1} X^{n-1} + X^2 F_{n-2} X^{n-2}$  for  $n \geq 2$ , and recalling that  $F_0 = 0$  and  $F_1 = 1$ , yields the equation:

$$F(X) = X F(X) + X^2 F(X) + X .$$

Hence:  $(1 - X - X^2)F(X) = X$ . We can thus consider that  $F(X)$  is the power series expansion of the rational function

$$F(X) = \frac{X}{1 - X - X^2} = \frac{X}{(1 - r_1 X)(1 - r_2 X)} = \frac{1}{\sqrt{5}} \left( \frac{1}{1 - r_1 X} - \frac{1}{1 - r_2 X} \right) ,$$

where  $r_1 = \frac{1 + \sqrt{5}}{2}$  and  $r_2 = \frac{1 - \sqrt{5}}{2}$  are the two roots of  $1 - X - X^2 = 0$ . But

$$\frac{1}{1 - Z} = 1 + Z + Z^2 + \dots + Z^n + \dots ,$$

and hence  $F(X) = 1/\sqrt{5}(\sum_{n \geq 0} (r_1^n - r_2^n) X^n)$  and  $F_n = 1/\sqrt{5}(r_1^n - r_2^n)$ .

For the present the formal power series will be denoted by  $\sum_{n=0}^{\infty} u_n X^n$  and the analytic series by  $\sum_{n=0}^{\infty} u_n x^n$ . We will revert to the notation  $\sum_{n=0}^{\infty} u_n x^n$  for all series from Section 8.1.5 onwards. Similarly, for the present, the series will be denoted by boldface letters, in the form  $\mathbf{u} = \sum_{n=0}^{\infty} u_n X^n$  in order to distinguish them from the corresponding sequences  $(u_n)_{n \in \mathbb{N}}$ .

### 8.1.2 Definitions

**Definition 8.3** The power series  $\mathbf{u} = \sum_{n \geq 0} u_n X^n$  is said to be a generating series of coefficients  $u_n$ . The set of power series with coefficients in the set  $\mathbb{C}$  of complex numbers is denoted by  $\mathbb{C}[[X]]$ . The power series  $\mathbf{u}$  is also denoted by  $\mathbf{u}(X)$ .

REMARK 8.4 Similarly, we can consider the set  $\mathbb{N}[[X]]$  (resp.  $\mathbb{R}[[X]]$ ,  $\mathbb{Z}[[X]]$ , ...) of power series with coefficients in  $\mathbb{N}$  (resp.  $\mathbb{R}$ ,  $\mathbb{Z}$ , ...).

**Proposition 8.5** The set of power series, together with

- the addition  $+$  defined by

$$\sum_{n \geq 0} u_n X^n + \sum_{n \geq 0} v_n X^n = \sum_{n \geq 0} (u_n + v_n) X^n \quad \text{and}$$

- the convolution product  $\times$ , defined by

$$\left( \sum_{n \geq 0} u_n X^n \right) \times \left( \sum_{n \geq 0} v_n X^n \right) = \sum_{n \geq 0} \left( \sum_{p+q=n} u_p v_q \right) X^n,$$

is an integral ring (i.e. a ring without zero-divisors).

*Proof.* The unit for addition is the series  $\mathbb{0} = (0)_{n \geq 0}$ ; the unit for the convolution product is the series  $\mathbb{1}$  defined by:  $\mathbb{1}_0 = 1$  and  $\mathbb{1}_n = 0$  for all  $n > 0$ ;  $\mathbb{1}$  will also be denoted by  $1$  from Section 8.1.3 on. The axioms of the ring structure are easily verified (i.e. addition is associative and commutative, product is associative and commutative and distributes over addition).

Finally, recall that  $\mathbf{u} \neq \mathbb{0}$  is a divisor of  $\mathbb{0}$  if  $\mathbf{v}$  exists such that  $\mathbf{v} \neq \mathbb{0}$  and  $\mathbf{u} \times \mathbf{v} = \mathbb{0}$ . If  $\mathbf{u} \times \mathbf{v} = \mathbb{0}$ , and if one of the two series  $\mathbf{u}$  or  $\mathbf{v}$  is different from  $\mathbb{0}$ , then the other one is equal to  $\mathbb{0}$ ; if for instance  $\mathbf{u} \neq \mathbb{0}$ , let  $j = \min\{i / u_i \neq 0\}$ ; one computes the coefficients of  $\mathbf{u} \times \mathbf{v}$  and shows by induction on  $n$  that  $v_n = 0$  for all  $n \geq 0$ .  $\square$

EXERCISE 8.2 Let  $r \geq 0$ . Find a power series  $\mathbf{u}(X)$  whose coefficient of  $X^n$  is  $u_n = \sum_{k=0}^n \binom{r}{k} \binom{r}{n-2k}$ . Hint: it can be noted that  $u_n = 0$  if  $n > 3r$ .  $\diamond$

#### NOTATIONS

1. The convolution product  $\mathbf{u} \times \mathbf{v}$  will be denoted simply by the concatenation  $\mathbf{uv}$  when there is no ambiguity.
2. Let  $i: \mathbb{C} \rightarrow \mathbb{C}[[X]]$  be the mapping defined by  $i(a) = \mathbf{a} = a\mathbb{1} = (a_n)_{n \geq 0}$ , with  $a_0 = a$  and  $a_n = 0$  for all  $n \neq 0$ ;  $i$  is an injection and  $i(0) = \mathbb{0}$ ,  $i(1) = \mathbb{1}$ ; we will denote  $\mathbb{0}$  by  $0$  and  $\mathbb{1}$  by  $1$  from the Section 8.1.3 on.

Shift operations can be defined on series:

- Let  $u = (u_n)_{n \geq 0}$  and  $a \in \mathbb{C}$ , then,  $\mathbf{u}_{a,r} = \mathbf{u}X + \mathbf{a}$  is the series verifying  $(u_{a,r})_0 = a$ , and for  $n > 0$ ,  $(u_{a,r})_n = u_{n-1}$ . This operation consists of translating all the coefficients of  $\mathbf{u}$  one position to the right, and adding an  $a$  at the beginning.
- Let  $u = (u_n)_{n \geq 0}$ , then  $\mathbf{u}_l = \frac{\mathbf{u} - \mathbf{u}_0}{X}$  is the series defined by  $\forall n \geq 0$ ,  $(u_l)_n = u_{n+1}$ . This operation consists of suppressing  $u_0$  and translating the other coefficients of  $\mathbf{u}$  one position to the left.

EXERCISE 8.3 Define a series  $\mathbf{v}$  such that  $\mathbf{u}_{a,r} = \mathbf{u} \times \mathbf{v} + \mathbf{a}$  and  $\mathbf{u} - \mathbf{u}_0 = \mathbf{u}_l \times \mathbf{v}$ .  $\diamond$

We will characterize invertible series, which, in the sequel, will yield a convenient tool for computing terms of the form  $1/f(x)$ , where  $f(x)$  is a function represented by a series.

**Lemma 8.6** Let  $\mathbf{u} \neq \mathbf{0}$ ,  $\mathbf{v}$  and  $\mathbf{v}'$  be power series. Then

$$\mathbf{u}\mathbf{v} = \mathbf{u}\mathbf{v}' \implies \mathbf{v} = \mathbf{v}'.$$

*Proof.* If  $\mathbf{v} \neq \mathbf{v}'$ , there exists a  $k$  such that  $v_k \neq v'_k$ . Let  $m$  be the least such  $k$ , and let  $n$  be the least integer such that  $u_n \neq 0$ . Then:

$$\begin{aligned} (\mathbf{u}\mathbf{v})_{n+m} &= \sum_{p=0}^{n+m} u_p v_{n+m-p} \\ &= \sum_{p=n}^{n+m} u_p v_{m+n-p} \quad (\text{because } u_p = 0 \text{ if } p < n) \\ &= \sum_{p=0}^m u_{n+p} v_{m-p} \\ &= \sum_{p=0}^m u_{n+m-p} v_p. \end{aligned}$$

Similarly,

$$(\mathbf{u}\mathbf{v}')_{n+m} = \sum_{p=0}^m u_{n+m-p} v'_p;$$

hence,

$$\begin{aligned} (\mathbf{u}\mathbf{v} - \mathbf{u}\mathbf{v}')_{n+m} &= \sum_{p=0}^m u_{n+m-p} (v_p - v'_p) \\ &= u_n (v_m - v'_m) \quad (\text{because } v_p = v'_p \text{ if } p < m). \end{aligned}$$

Because  $u_n \neq 0$  and  $v_m \neq v'_m$ ,  $(\mathbf{u}\mathbf{v} - \mathbf{u}\mathbf{v}')_{n+m} \neq 0$ , and that contradicts  $\mathbf{u}\mathbf{v} = \mathbf{u}\mathbf{v}'$ .  $\square$

**Definition 8.7**

1. Let  $\mathbf{u}, \mathbf{v} \neq \mathbb{0}$  be power series. Then  $\mathbf{v}$  is said to divide  $\mathbf{u}$  if and only if there exists a (necessarily unique) power series  $\mathbf{w}$  such that  $\mathbf{u} = \mathbf{v}\mathbf{w}$ . The unique  $\mathbf{w}$  such that  $\mathbf{u} = \mathbf{v}\mathbf{w}$  is denoted by  $\mathbf{u}/\mathbf{v}$ .
2. A series  $\mathbf{u}$  is said to be invertible if and only if there exists a series  $\mathbf{v}$  such that  $\mathbf{u}\mathbf{v} = \mathbb{1}$ .  $\mathbf{v}$  is called the inverse of  $\mathbf{u}$ .

**Lemma 8.8** Let  $\mathbf{u} \neq \mathbb{0}, \mathbf{v} \neq \mathbb{0}$  be power series. Let  $n$  (resp.  $m$ ) be the least integer such that  $u_n \neq 0$  (resp.  $v_m \neq 0$ ). Then  $\mathbf{v}$  divides  $\mathbf{u}$  if and only if  $m \leq n$ .

*Proof.* Assume, first, that  $\mathbf{u} = \mathbf{v}\mathbf{w}$ . Then  $u_q = (\mathbf{v}\mathbf{w})_q = \sum_{p=0}^q v_p w_{q-p}$ . If  $q < m$  then  $\sum_{p=0}^q v_p w_{q-p} = 0 = u_q$ , hence  $q < n$ , and thus  $m \leq n$ .

Assume now that  $m \leq n$ . The sequence  $(w_p)_{p \geq 0}$  is inductively defined by:

$$(B) \quad w_p = \begin{cases} 0 & \text{if } p < n - m, \\ u_n/v_m & \text{if } p = n - m. \end{cases}$$

$$(I) \quad w_{n+m+i+1} = (u_{n+i+1} - \sum_{p=0}^{n-m+i} v_{n+i+1-p} w_p) / v_m, \text{ for } i \geq 0.$$

Let  $\mathbf{w} = \sum w_p X^p$ . Let us compute  $\mathbf{v}\mathbf{w}$ :  $(\mathbf{v}\mathbf{w})_q = \sum_{p=0}^q w_p v_{q-p}$ :

- If  $q < n - m$ ,  $(\mathbf{v}\mathbf{w})_q = 0 = u_q$ .
- If  $q \geq n - m$ , then  $(\mathbf{v}\mathbf{w})_q = \sum_{p=n-m}^q w_p v_{q-p} = \sum_{p=0}^{q-n+m} w_{p+n-m} v_{q-n+m-p}$ .
  - If  $n - m < q < n$ , the sum  $\sum_{p=0}^{q-n+m} w_{p+n-m} v_{q-n+m-p}$  is null and is equal to  $u_q$ .
  - If  $q = n$ , we have  $(\mathbf{v}\mathbf{w})_q = \sum_{p=0}^m w_{p+n-m} v_{m-p} = \sum_{p=0}^m w_{n-p} v_p = w_{n-m} v_m = u_n$ .
  - If  $q > n$ , let  $q = n + i + 1$ , then

$$\begin{aligned} (\mathbf{v}\mathbf{w})_q &= \sum_{p=0}^{n+i+1} w_{n+i+1-p} v_p = \sum_{p=m}^{n+i+1} w_{n+i+1-p} v_p \\ &= \sum_{p=0}^{n-m+i+1} w_{n-m+i+1-p} v_{p+m} = \sum_{p=0}^{n-m+i+1} w_p v_{n+i+1-p} \\ &= \sum_{p=0}^{n-m+i} w_p v_{n+i+1-p} + w_{n-m+i+1} v_m \\ &= u_{n+i+1} = u_q. \end{aligned} \quad \square$$

**Corollary 8.9** A series  $\mathbf{u} = u_0 + u_1X + \cdots + u_nX^n + \cdots$  in  $\mathbb{C}[[X]]$  is invertible if and only if  $u_0 \neq 0$ .

EXERCISE 8.4 Prove that a series  $\mathbf{u} = a_0 + a_1X + \cdots + a_nX^n + \cdots$  with coefficients in a ring is invertible if and only if  $a_0$  is invertible.  $\diamond$

### 8.1.3 Operations on series

From the present section on, we will cease using the boldface notation when denoting series.

Operations on series naturally correspond to the operations on sequences introduced in Section 7.4.1. We recall these in the list given below: the first column contains the operation on sequences, and the second column the corresponding operation on series. For instance, the first line of the list should be read as: if  $v = (Eu)_n = u_{n-1}$ , then the operation corresponding to  $E$  on the series is the mapping  $u \mapsto Xu = v$ . Indeed, it can be verified that if  $u = \sum_{n \geq 0} u_n X^n$ , then  $Xu = \sum_{n \geq 1} u_{n-1} X^n$ .

Lines 6 and 7 of the list given below can be used for *defining* the differentiation and integration operations on power series; it can then be proved that, when the convergence radii of the corresponding series are not equal to zero, the operations thus defined coincide with the usual differentiation and integration operations on analytic functions: for instance, if we *define the derivative* of the power series  $u = (u_n)_{n \geq 0}$  as being the power series  $v = ((n + 1)u_{n+1})_{n \geq 0}$  (1st column of line 7), and if, moreover,  $u$  and  $v$ , considered as analytic series, have non-zero convergence radii and define the analytic functions  $u(x)$  and  $v(x)$ , then we have:  $u'(x) = v(x)$ .

sequences	series
1. $v_n = (Eu)_n = u_{n-1}, v_0 = 0$	$v = Xu = uX + 0 = u_{0,r}$
2. $v_n = (\Delta u)_n = ((\mathbb{1} - E)u)_n = u_n - u_{n-1}$ $v_0 = u_0$	$v = (1 - X)u$
3. $v_n = \left( \sum u \right)_n = u_0 + \cdots + u_n$	$v = \frac{u}{1 - X}$
4. $w_n = u_n + v_n$	$w = u + v$
5. $w_n = \sum_{p+q=n} u_p v_q$	$w = uv$
6. $v_n = (n + 1)u_{n+1}$	$v = u'$
7. $v_n = \frac{u_{n-1}}{n}, v_0 = 0$	$v = \int_0^x u(t)dt$

EXERCISE 8.5 Verify lines 2–7 of the list given above.  $\diamond$



EXAMPLE 8.10 Recall that the derivative of  $\frac{1}{1-x}$  is  $\frac{1}{(1-x)^2}$ ; hence, by (6),

$$\frac{1}{(1-x)^2} = \sum_{n \geq 0} (n+1)x^n.$$

Similarly, taking the integral of  $\frac{1}{1-x}$  and applying line 7, we obtain

$$\log \frac{1}{1-x} = \sum_{n \geq 1} \frac{x^n}{n}.$$

Multiplying this last equality by  $\frac{1}{1-x}$  and using line 3, we obtain

$$\frac{1}{1-x} \log \frac{1}{1-x} = \sum_{n \geq 1} H_n x^n,$$

where

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Taking derivatives again:

$$\frac{1}{(1-x)^2} \log \frac{1}{1-x} + \frac{1}{(1-x)^2} = \sum_{n \geq 0} (n+1)H_{n+1}x^n;$$

hence

$$\frac{1}{1-x} \left[ \sum_{n \geq 1} H_n x^n + \sum_{n \geq 0} x^n \right] = \sum_{n \geq 0} (n+1)H_{n+1}x^n.$$

Applying 3 once more:

$$\sum_{n \geq 0} \left[ \left( \sum_{i=1}^n H_i \right) + \left( \sum_{i=0}^n 1 \right) \right] x^n = \sum_{n \geq 0} (n+1)H_{n+1}x^n,$$

and also  $\sum_{i=1}^n H_i = (n+1)(H_{n+1} - 1)$ .

### 8.1.4 Exponential generating series

We have associated a power series with a sequence; this power series can be said to be polynomial; we can also associate an *exponential generating series* with each sequence as follows. To the sequence  $u = u_0, u_1, \dots, u_n, \dots$  we will associate the series:

$$\hat{u} = u_0 + u_1X + \dots + u_n \frac{X^n}{n!} + \dots .$$

The exponential terminology originates from the fact that we associate with the sequence  $u_n = 1, \forall n$ , the series  $\sum_{n \geq 0} \frac{x^n}{n!}$ , which is the expansion of the function  $e^x$  into a power series. As in the case of ordinary generating series, operations on the corresponding exponential generating series are associated with the operations on sequences. We give a short list below.

sequences	series
$w_n = u_n + v_n$	$(\hat{u}, \hat{v}) \mapsto \hat{w} = \hat{u} + \hat{v}$
$v_n = u_{n+1}$	$\hat{u} \mapsto \hat{v} = \hat{u}'$
$v_n = u_{n-1}$	$\hat{u} \mapsto \hat{v} = \int_0^X \hat{u}(t) dt$
$w_n = \sum_{p=0}^n \binom{n}{p} u_p v_{n-p}$	$(\hat{u}, \hat{v}) \mapsto \hat{w} = \hat{u}\hat{v}$

**EXERCISE 8.6**

1. Show that:  $\int_0^\infty t^n e^{-t} dt = n!$ .
2. Conclude from 1 that:  $\int_0^\infty \hat{u}(xt)e^{-t} dt = u(x)$  provided that the series is convergent and that the integral exists. ◇

### 8.1.5 Partial fraction expansion of rational functions

We will now study a computation method which is very useful for obtaining the coefficients of a generating series in a simple way (this method is also used in probability theory).

**Proposition 8.11** *Let  $g(x) = \sum_{n \geq 0} u_n x^n$  be a generating series which is the power series expansion of a rational function of the form  $g(x) = \frac{U(x)}{V(x)}$ , where  $U$  and  $V$  are two polynomials having no common root and such that  $\deg(U) < \deg(V) = m$ . Let us assume, moreover, that  $V(x)$  has  $m$  distinct roots  $r_1, \dots, r_m$ , i.e.  $V(x) = (x - r_1) \cdots (x - r_m)$ . Then, constants  $a_1, \dots, a_m$  exist such that:*

$$g(x) = \frac{a_1}{x - r_1} + \dots + \frac{a_m}{x - r_m} . \tag{8.1}$$

To find  $a_i$ , let us multiply the equation (8.1) by  $x - r_i$ ; we have

$$g_i(x) = \frac{a_1(x - r_i)}{x - r_1} + \dots + \frac{a_{i-1}(x - r_i)}{x - r_{i-1}} + a_i + \frac{a_{i+1}(x - r_i)}{x - r_{i+1}} + \dots + \frac{a_m(x - r_i)}{x - r_m} .$$

Letting  $x = r_i$ , we obtain  $g_i(r_i) = a_i$ . Moreover,

$$g_i(x) = \frac{U(x)}{(x - r_1) \cdots (x - r_{i-1})(x - r_{i+1}) \cdots (x - r_m)}$$

and, for  $x = r_i$ ,

$$(r_i - r_1) \cdots (r_i - r_{i-1})(r_i - r_{i+1}) \cdots (r_i - r_m) = V'(r_i),$$

hence

$$a_i = g_i(r_i) = \frac{U(r_i)}{V'(r_i)}.$$

**Proposition 8.12** (Computation of  $u_n$  – asymptotic value) *Let  $U$  and  $V$  satisfy the hypotheses of Proposition 8.11. Let  $r_1$  be a simple root of  $V(x)$ , such that, for all other roots  $r_j$ ,  $|r_1| < |r_j|$ ; then when  $n \rightarrow \infty$ ,  $u_n \sim \frac{-a_1}{r_1^{n+1}}$ .*

*Proof.* The power series expansion of  $\frac{1}{x - r_i}$  is known:

$$\frac{1}{x - r_i} = -\frac{1}{r_i} \left( \frac{1}{1 - \frac{x}{r_i}} \right) = -\frac{1}{r_i} \left( 1 + \frac{x}{r_i} + \frac{x^2}{r_i^2} + \cdots + \frac{x^n}{r_i^n} + \cdots \right).$$

By (8.1), we have

$$g(x) = \sum_{n \geq 0} \left( \sum_{i=1}^m \frac{-a_i}{r_i^{n+1}} \right) x^n. \quad (8.2)$$

Identifying with  $g(x) = \sum_{n \geq 0} u_n x^n$ , we obtain  $u_n = \sum_{i=1}^m \frac{-a_i}{r_i^{n+1}}$ , whence  $r_1^{n+1} u_n = -a_1 + \sum_{i=2}^m (-a_i) \left( \frac{r_1}{r_i} \right)^{n+1}$ . If, moreover,  $|r_1| < |r_j|$  for all the other roots  $r_j$ , then  $\sum_{i=2}^m (-a_i) \left( \frac{r_1}{r_i} \right)^{n+1}$  tends to 0 as  $n$  tends to infinity, and thus  $r_1^{n+1} u_n$  tends to  $-a_1$ ; hence  $u_n \sim \frac{-a_1}{r_1^{n+1}}$ .  $\square$

**EXERCISE 8.7** Can you eliminate some of the restrictions assumed for obtaining the partial fraction expansion?  $\diamond$

We state without proof the general form of Proposition 8.11.

**Proposition 8.13** Let  $g(x) = \sum_{n \geq 0} u_n x^n$  be a generating series which is the power series expansion of a rational function of the form  $g(x) = \frac{U(x)}{V(x)}$ , where  $U$  and  $V$  are two polynomials having no common root and such that  $\deg(U) < \deg(V) = m$ . Let us assume, moreover, that  $V(x)$  has the  $m$  roots  $r_1, \dots, r_m$ , and that  $V(x) = c(x - r_1)^{d_1} \cdots (x - r_m)^{d_m}$ . In this case, we have

$$g(x) = \sum_{n \geq 0} \left( \sum_{i=1}^m \frac{P_i(n)}{r_i^n} \right) x^n, \tag{8.3}$$

where, for  $i = 1, \dots, m$ ,  $P_i(n)$  is a polynomial in the variable  $n$  of degree  $d_i - 1$ , whose coefficient  $a_i$  of  $n^{d_i-1}$  is given, if  $V^{(d_i)}$  denotes the  $d_i$ th derivative of  $V$ , by

$$\begin{aligned} a_i &= \frac{d_i U(r_i)}{(-r_i)^{d_i} c V^{(d_i)}(r_i)} \\ &= \frac{U(r_i)}{(-r_i)^{d_i} (d_i - 1)! c \prod_{j \neq i} (r_i - r_j)^{d_j}}. \end{aligned}$$

The proof is by induction on  $\max(d_1, \dots, d_m)$ , by showing that

$$g(x) - \sum_{i=1}^m \frac{a_i (d_i - 1)!}{(1 - x/r_i)^{d_i}}$$

is a rational fraction whose denominator is divisible by none among the  $(x - r_i)^{d_i}$ s.

**EXAMPLE 8.14** Let the sequence  $u_n$  be defined by  $u_0 = 1$ , and

$$u_n = qu_{n-1} + p(1 - u_{n-1}),$$

where  $p + q = 1$  and  $q \neq 1$ .  $u_n$  represents the probability of obtaining an even number of ‘tails’ after  $n$  successive tosses of a coin. Let  $g(x) = \sum_{n \geq 0} u_n x^n$ . Let us multiply equation  $u_n = qu_{n-1} + p(1 - u_{n-1})$  by  $x^n$  for each  $n > 0$  in  $\mathbb{N}$ , and add the equalities thus obtained:

$$\begin{aligned} & \vdots \\ u_n x^n &= xqu_{n-1}x^{n-1} + xp(1 - u_{n-1})x^{n-1} \\ & \vdots \\ u_1 x &= xqu_0 + xp(1 - u_0). \end{aligned}$$

We obtain

$$\begin{aligned} g(x) - 1 &= qx \sum_{n \geq 0} u_n x^n + px \sum_{n \geq 0} x^n - px \sum_{n \geq 0} u_n x^n \\ &= qxg(x) + px \frac{1}{1-x} - pxg(x), \end{aligned}$$

or

$$g(x)(1 - (q-p)x) = 1 + px \frac{1}{1-x} = \frac{1 - x(1-p)}{1-x} = \frac{1 - qx}{1-x},$$

hence

$$g(x) = \frac{1 - qx}{(1-x)(1 - (q-p)x)} = \frac{a_1}{1-x} + \frac{a_2}{1 - (q-p)x};$$

and, after computing  $a_1$  and  $a_2$ , which yield

$$a_1 = a_2 = \frac{1-q}{1-(q-p)} = \frac{p}{2p} = \frac{1}{2},$$

$$\begin{aligned} g(x) &= \frac{1}{2} \left( \frac{1}{1-x} + \frac{1}{1-(q-p)x} \right) \\ &= \frac{1}{2} \left( \sum_{n \geq 0} x^n + \sum_{n \geq 0} (q-p)^n x^n \right) = \frac{1}{2} \sum_{n \geq 0} (1 + (q-p)^n) x^n, \end{aligned}$$

hence

$$u_n = \frac{1}{2}(1 + (q-p)^n).$$

We deduce (see Chapter 12) the formula

$$\frac{1}{2}(1 + (q-p)^n) = \sum_{k=0}^{n/2} \binom{n}{2k} p^{2k} q^{n-2k};$$

indeed,  $\binom{n}{2k} p^{2k} q^{n-2k}$  represents the probability of obtaining  $2k$  ‘tails’ in a sequence of  $n$  successive tosses of a coin (in technical terms in a sequence of  $n$  Bernoulli trials).

#### EXERCISE 8.8

1. Prove that

$$\sum_{k=0}^{\infty} \frac{x^{2^k}}{1 - x^{2^{k+1}}} = \frac{x}{1-x}.$$

2. Deduce the following identity, where the  $F_n$ s are the Fibonacci numbers:

$$\sum_{k=0}^{\infty} \frac{1}{F^{2^k}} = \frac{7 - \sqrt{5}}{2}.$$

This equality is called the Millin identity, and was proved by Dale Miller. (His name was misprinted in the first paper stating the result.)  $\diamond$

## 8.2 Applications of generating series to recurrences

### 8.2.1 Linear recurrences with constant coefficients

Let the sequence  $u_n$  be defined by the recurrence equation (7.9)

$$\forall n \geq k, \quad u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k} \quad (7.9)$$

and let  $u(z) = \sum_{n \geq 0} u_n z^n$  be the associated generating series. We will compute the generating series, and deduce the  $u_n$ s.

Multiplying (7.9) by  $z^n$  we obtain

$$\forall n \geq k, \quad u_n z^n = a_1 z u_{n-1} z^{n-1} + a_2 z^2 u_{n-2} z^{n-2} + \cdots + a_k z^k u_{n-k} z^{n-k}$$

and summing up all these equalities for  $n \geq k$ ,

$$\begin{aligned} u_k z^k &= a_1 z u_{k-1} z^{k-1} + a_2 z^2 u_{k-2} z^{k-2} + \cdots + a_k z^k u_0 \\ u_{k+1} z^{k+1} &= a_1 z u_k z^k + a_2 z^2 u_{k-1} z^{k-1} + \cdots + a_k z^k u_1 z \\ &\vdots \\ u_n z^n &= a_1 z u_{n-1} z^{n-1} + a_2 z^2 u_{n-2} z^{n-2} + \cdots + a_k z^k u_{n-k} z^{n-k}, \\ &\vdots \end{aligned}$$

we obtain

$$\sum_{n \geq k} u_n z^n = a_1 z \sum_{n \geq k-1} u_n z^n + a_2 z^2 \sum_{n \geq k-2} u_n z^n + \cdots + a_k z^k \sum_{n \geq 0} u_n z^n.$$

For  $0 \leq i \leq k-1$ , let  $P_i(z) = u_0 + u_1 z + \cdots + u_i z^i$ , so that

$$u(z) = P_{i-1}(z) + \sum_{n \geq i} u_n z^n;$$

hence

$$\begin{aligned} u(z) - P_{k-1}(z) &= a_1 z (u(z) - P_{k-2}(z)) + \cdots \\ &\quad + a_{k-1} z^{k-1} (u(z) - P_0(z)) + a_k z^k u(z). \end{aligned}$$

And thus

$$\begin{aligned} u(z) &= \frac{P_{k-1}(z) - a_1 z P_{k-2}(z) - \cdots - a_{k-1} z^{k-1} P_0(z)}{1 - a_1 z - a_2 z^2 - \cdots - a_k z^k} \\ &= \frac{P(z)}{1 - a_1 z - a_2 z^2 - \cdots - a_k z^k}, \end{aligned}$$

where  $P(z)$  is a polynomial in  $z$  of degree less than or equal to  $k-1$ ; the rational fraction defining  $u(z)$  has a power series expansion which can be obtained by standard techniques (see Section 8.1.5), and this allows one to find the coefficients of the series  $u(z)$ , i.e. the sequence  $u_n$ .

REMARK 8.15 Note that  $r_i$  is a multiple root of multiplicity  $d_i$  of the characteristic polynomial if and only if  $\rho_i = 1/r_i$  is a multiple root of the same multiplicity  $d_i$  of  $V(z) = 1 - a_1z - a_2z^2 - \cdots - a_kz^k$ . The same phenomenon will occur for non-homogeneous linear recurrences with constant coefficients.

Summing up, the above general method can be split into three steps:

1. Multiply the recurrence equation by  $z^n$  and sum on  $n$ ; to the left of the '=' sign is the generating series  $u(z)$  where the  $k$  first terms have been deleted, i.e. the expression  $u(z) - P_{k-1}(z)$ , and to the right of the '=' sign is an expression of the form  $u(z)P(z) + Q(z)$ , where  $P$  and  $Q$  are polynomials in  $z$ .
2. Solve the equation in  $u(z)$  thus obtained; we obtain a rational function;
3. Find the power series expansion of the rational function giving the coefficients of  $u(z)$ , namely the  $u_n$ s, for  $n \geq k$ . This last step is usually the step demanding most effort and computations.

Note, finally, that the methods using generating series are very suitable for some manipulations on sequences: for instance if the generating series  $u(z)$  of the sequence  $u_n$  is known, and if we are interested in the subsequence  $v_n = u_{2n}$  of even index terms, it is enough to remark that the sequence  $v_n$  is determined by

$$\frac{u(z) + u(-z)}{2} = \sum_{n \geq 0} u_{2n} z^{2n}.$$

Similarly, the subsequence  $v_n = u_{2n+1}$  of odd index terms is determined by

$$\frac{u(z) - u(-z)}{2} = \sum_{n \geq 0} u_{2n+1} z^{2n+1}.$$

EXERCISE 8.9 The Fibonacci numbers are defined by  $F_0 = 0$ ,  $F_1 = 1$  and, for  $n \geq 2$ ,  $F_n = F_{n-1} + F_{n-2}$ . Determine the generating series of the sequence  $F_{2n}$  of Fibonacci numbers of even index.  $\diamond$

EXERCISE 8.10 Solve the following recurrence equations by the generating series method.

1.  $\forall n \geq 2, 2u_n = 3u_{n-1} - u_{n-2}$ .
2.  $\forall n \geq 2, u_n = 4u_{n-1} - 4u_{n-2}$ .  $\diamond$

### 8.2.2 Non-homogeneous linear recurrences with constant coefficients

The preceding method can easily be applied and is illustrated in this example. Consider the recurrence equation

$$u_n = u_{n-1} + 2u_{n-2} + (-1)^n, \quad n \geq 2,$$

with  $u_0 = u_1 = 1$ , and let  $u(z) = \sum_{n \geq 0} u_n z^n$  be the associated generating series.

Writing

$$\begin{aligned} u_0 &= 1 \\ u_1 z &= z = z u_0 \\ u_2 z^2 &= z u_1 z + 2z^2 u_0 + (-1)^2 z^2 \\ &\vdots \\ u_n z^n &= z u_{n-1} z^{n-1} + 2z^2 u_{n-2} z^{n-2} + (-1)^n z^n \\ &\vdots \end{aligned}$$

we deduce, by summing up the above equalities and adding the corrective term  $(-1)^1 z$  on each side of the thus obtained equality, that

$$u(z) - z = z u(z) + 2z^2 u(z) + \frac{1}{1+z};$$

hence

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

By Proposition 8.13, we have

$$u_n = a2^n + (bn+c)(-1)^n,$$

with  $a = 7/9$  and  $b = 1/3$ . Substituting these values and letting  $n = 0$  in the preceding equation, we obtain  $c = 2/9$ .

**EXERCISE 8.11** Solve the following recurrence equation:

$$\forall n \geq 2, \quad u_n = 4u_{n-1} - 4u_{n-2} + n - 1, \quad \text{with } u_0 = 1 \text{ and } u_1 = 1. \quad \diamond$$

**EXERCISE 8.12** Solve the simultaneous recurrence equations

$$\begin{aligned} u_n &= 2v_{n-1} + u_{n-2}, & \text{with } u_0 = 1 \text{ and } u_1 = 0, \\ v_n &= u_{n-1} + v_{n-2}, & \text{with } v_0 = 0 \text{ and } v_1 = 1. \end{aligned} \quad \diamond$$

**EXERCISE 8.13** Solve the recurrence equation

$$\forall n \geq 2, \quad u_n = 3u_{n-1} - 2u_{n-2} + n/2^n, \quad \text{with } u_0 = 1 \text{ and } u_1 = 0. \quad \diamond$$



### 8.2.3 Partitioning integers

The problem is that of finding the number of vectors of integers  $v = (n_1, \dots, n_p)$  which are solutions of  $a_1 n_1 + \dots + a_p n_p = n$ , with fixed  $a_1, \dots, a_p \in \mathbb{N}$ . We illustrate this type of problem with an example. How many ways are there to change a \$100 bill for \$1 and \$5 bills? It boils down to finding the number of solutions of the equation:  $p + 5q = 100$ . Let the series

$$\begin{aligned} u(x) &= 1 + x + x^2 + \dots + x^p + \dots \\ w(x) &= 1 + x^5 + x^{10} + \dots + x^{5q} + \dots \end{aligned}$$

We have

$$(uw)(x) = \sum_{n \geq 0} \left( \sum_{p+5q=n} x^p x^{5q} \right).$$

Consequently, the number of solutions of  $p + 5q = n$  is the coefficient of  $x^n$  in the series  $v(x) = u(x)w(x)$ . But

$$u(x) = \frac{1}{1-x}, \quad w(x) = \frac{1}{1-x^5},$$

and hence

$$v(x) = (uw)(x) = \frac{1}{(1-x)(1-x^5)}.$$

The standard method consists of computing the partial fraction expansion of  $uw$ , and deducing therefrom the coefficient of  $x^{100}$  in  $uw$ . Here this partial fraction expansion would have the form:

$$v(x) = \frac{a}{(1-x)^2} + \frac{b}{1-x} + \frac{c}{1-e^{i\alpha}x} + \frac{\bar{c}}{1-e^{-i\alpha}x} + \frac{d}{1-e^{2i\alpha}x} + \frac{\bar{d}}{1-e^{-2i\alpha}x},$$

where  $e^{i\alpha}, e^{-i\alpha}, e^{2i\alpha}, e^{-2i\alpha}$  are the complex roots of  $x^5 = 1$ . Here we can, however, perform a simpler and more astute computation: noting that  $1-x^5 = (1-x)(1+x+x^2+x^3+x^4)$ , we can deduce

$$\begin{aligned} v(x) &= \frac{1+x+x^2+x^3+x^4}{(1-x^5)^2} \\ &= (1+x+x^2+x^3+x^4) \sum_{n \geq 0} (n+1)x^{5n}. \end{aligned}$$

The number of ways to change  $n$  dollars for \$1 and \$5 bills is thus the coefficient of  $x^n$  in  $v(x)$ . Any arbitrary  $n$  can be uniquely written in the form  $n = 5k + r$  with  $0 \leq r \leq 4$ , and the coefficient of  $x^{5k+r}$  in  $v(x)$  is then  $k+1$ . For instance, there are  $v_{20} = 21$  ways to change \$100 for \$1 and \$5 bills.

EXERCISE 8.14 Find the number of ways of bringing up a total of  $n$  with tokens of value 2 and 3.  $\diamond$

EXERCISE 8.15 Assuming that in Morse code a dot takes two time units, and a dash takes three time units, find the number of words taking  $n$  time units in the Morse code.  $\diamond$

EXERCISE 8.16 How can you find the number of ways of changing \$100 for \$1, \$2 and \$5 bills?  $\diamond$

### 8.2.4 Finite linear recurrence equations with non-constant coefficients

The method consists of associating with the recurrence equation defining the sequence  $u_n$  a functional or differential equation on the generating series  $u(x)$  corresponding to  $u_n$ . This method can be applied in the case of linear recurrence equations with constant or non-constant coefficients.

- In the case of recurrence equations with constant coefficients, the functional equation will be of the form  $u(x) = \frac{U(x)}{V(x)}$ , where  $U$  and  $V$  are polynomials in  $x$ . More precisely, if the recurrence equation is of the form:  $u_n = a_1u_{n-1} + \dots + a_ku_{n-k}$ , with initial values  $u_0, \dots, u_{k-1}$ , and if  $u(x) = \sum_{n \geq 0} u_n x^n$ , then (see Section 8.2.1)  $u(x) = \frac{U(x)}{V(x)}$ , with

$$V(x) = 1 - a_1x - a_2x^2 - \dots - a_kx^k,$$

and  $U(x)$  a polynomial of degree  $\leq k - 1$ . It is then sufficient to find the partial fraction expansion of the rational function  $\frac{U}{V}$  by the methods described in Section 8.1.5, Proposition 8.11 and Proposition 8.13 in order to obtain the  $u_n$ s. See Example 8.14.

- In the case of recurrence equations with non-constant coefficients, we will in general obtain a differential equation involving the derivatives of  $u(x)$  of order 1, 2, etc. The problem will hence be more complex. We will illustrate the method with a simple example.

EXAMPLE 8.16 Let the sequence  $u_n$ , for  $n \geq 2$ , be defined by

$$nu_n + (n - 2)u_{n-1} - u_{n-2} = 0, \quad \text{with } u_0 = u_1 = 1.$$

Multiplying the recurrence equation by  $x^{n-1}$  and summing for  $n \geq 2$ , we obtain

$$\sum_{n \geq 2} nu_n x^{n-1} + \sum_{n \geq 2} (n - 2)u_{n-1} x^{n-1} - \sum_{n \geq 2} u_{n-2} x^{n-1} = 0, \quad (8.4)$$

i.e.

$$\sum_{n \geq 2} nu_n x^{n-1} + x \sum_{n \geq 2} (n-1)u_{n-1} x^{n-2} - \sum_{n \geq 2} u_{n-1} x^{n-1} - x \sum_{n \geq 2} u_{n-2} x^{n-2} = 0.$$

Hence,  $u(x) = \sum_{n \geq 0} u_n x^n$ ; then

$$u'(x) = \sum_{n \geq 0} (n+1)u_{n+1} x^n = \sum_{n \geq 1} nu_n x^{n-1},$$

so that  $u'(x) = u_1 + \sum_{n \geq 2} nu_n x^{n-1}$ . Equation (8.4) can be written

$$(u'(x) - u_1) + xu'(x) - u(x) + u_0 - xu(x) = 0$$

or

$$(u'(x) - 1) + x(u'(x) - u(x)) - u(x) + 1 = 0$$

and, then,

$$(u'(x) - u(x))(1+x) = 0;$$

hence  $u(x) = u'(x)$ , and  $u(x) = \lambda e^x$ , with  $\lambda = 1$  since  $u(0) = 1$ . Finally,

$$u(x) = \sum_{n \geq 0} \frac{x^n}{n!} \quad \text{and} \quad u_n = \frac{1}{n!}.$$

EXERCISE 8.17 Solve the recurrence equation

$$\forall n \geq 1, \quad 2nu_n = u_{n-1} + \frac{1}{(n-1)!},$$

with  $u_0 = 2$ , and the convention  $0! = 1$ . ◇

### 8.2.5 Complete recurrence equations

The method of Section 8.2.1 can still be applied; of course the computation of the series can no longer be reduced to the power series expansion of a rational function because the functional equation defining the series may be more complex. Let us study an example.

Recall (Example 7.1) that the number of binary trees with  $n$  nodes is given by the recurrence equation  $b_n = \sum_{k=0}^{n-1} b_k b_{n-k-1}$  for  $n \geq 1$ , and  $b_0 = 1$ . Let  $b(x) = \sum_{n \geq 0} b_n x^n$  be the associated generating series; substituting for  $b_n$  in the generating series  $b(x)$  the value of  $b_n$ , which is given by the recurrence equation, we have

$$b(x) = 1 + \sum_{n \geq 1} \left( \sum_{k=0}^{n-1} b_k b_{n-k-1} \right) x^n = 1 + x \sum_{n \geq 1} \left( \sum_{p+q=n-1} b_p b_q x^{n-1} \right),$$

that is

$$b(x) = 1 + x(b(x))^2.$$

$b(x)$  is thus the solution of the equation in  $b$ :  $xb^2 - b + 1 = 0$ , whose roots are  $\frac{1 \pm \sqrt{1-4x}}{2x}$ . Since  $b(0) = b_0 = 1$ , the numerator should be divisible by  $2x$ , and this allows a single possible solution  $\frac{1 - \sqrt{1-4x}}{2x}$  (the other solution being undefined for  $x = 0$ ). Now, let us recall the power series expansion of  $(1+u)^\alpha$ , valid for  $\alpha \in \mathbb{R}$ ,

$$(1+u)^\alpha = 1 + \alpha u + \dots + \binom{\alpha}{k} u^k + \dots,$$

where, by convention,

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}.$$

Here we obtain

$$\begin{aligned} \sqrt{1-4x} &= \sum_{k \geq 0} \binom{1/2}{k} (-4x)^k = \sum_{k \geq 0} \frac{1/2(-1/2)(-3/2)\dots(3-2k)/2}{k!} (-4x)^k \\ &= 1 + \sum_{k \geq 1} (-1)^{k-1} \frac{(2k-2)!(-4)^k x^k}{k! 2^k 2^{k-1} (k-1)!} \\ &= 1 + \sum_{k \geq 1} -\frac{(2k-2)! 2}{k!(k-1)!} x^k. \end{aligned}$$

Hence,

$$b(x) = \sum_{n \geq 1} \frac{(2(n-1))!}{n!(n-1)!} x^{n-1} = \sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} x^n$$

and

$$\forall n \geq 0, \quad b_n = \frac{1}{n+1} \binom{2n}{n} = \frac{1}{n+1} \frac{(2n)!}{n!n!}.$$

The number  $b_n = \frac{1}{n+1} \binom{2n}{n}$  is the  $n$ th *Catalan number*. The Catalan numbers are useful in combinatorics.

EXERCISE 8.18 Let  $A = \{ (, ) \}$  be the alphabet consisting of two parentheses (left and right). The set of strings of balanced parentheses, also called the Dyck language, is the subset  $D \subseteq A^*$  defined by

- (B)  $\varepsilon \in D$ ,  
 (I) if  $x$  and  $y$  are in  $D$ , then  $(x)y$  is also in  $D$ .

1. Verify that this definition coincides with the one given in Example 3.9 and that all the strings of balanced parentheses are words of even length.
2. Let  $u_n$  be the number of strings of balanced parentheses of length  $2n$ ; find a recurrence equation defining  $u_n$  in terms of the  $u_i$ s, for  $i < n$ . Deduce  $u_n$ .
3. How can you generalize this result to the Dyck language on an alphabet  $A_k = \{a_1, \dots, a_k, \bar{a}_1, \dots, \bar{a}_k\} = B_k \cup \bar{B}_k$  (assuming there are  $k$  different types of parentheses), defined by

- (B)  $\varepsilon \in D$ ,  
 (I) if  $x$  and  $y$  are in  $D$ , then  $a_i x \bar{a}_i y$  is also in  $D$ , for all  $i = 1, \dots, k$ .  $\diamond$

EXERCISE 8.19 Solve the recurrence equation

$$\forall n \geq 1, \quad u_n = u_{n-1} + 2u_{n-2} + \dots + nu_0, \quad \text{with } u_0 = 1. \quad \diamond$$

EXERCISE 8.20 Solve the recurrence equation

$$\forall n > 1, \quad u_n = -2nu_{n-1} + \sum_{k=0}^n \binom{n}{k} u_k u_{n-k},$$

with  $u_0 = 0$  and  $u_1 = 1$ , using exponential generating series.  $\diamond$

### 8.2.6 Average complexity of algorithms

Generally speaking, the generating series can be applied to the analysis of the average complexity of algorithms. Let  $A$  be an algorithm computing on data  $D$ , and let  $D_n$  be the set of data of size  $n$ , assumed to be all equally probable. Let  $c(d)$  be the time complexity of algorithm  $A$  on data  $d$ . Then, the average time complexity of  $A$  on  $D_n$  is

$$m_n = \frac{1}{|D_n|} \sum_{d \in D_n} c(d),$$

where  $|D_n|$  is the cardinality of  $D_n$ . Let us denote by  $|d|$  the size of  $d$  and let  $c(x) = \sum_{n \geq 0} c_n x^n$ , where  $c_n = \sum_{d \in D_n} c(d)$ .

We can define the generating series of the enumeration of the  $D$ s similarly:

$$d(x) = \sum_{n \geq 0} |D_n| x^n = \sum_{n \geq 0} d_n x^n.$$

We then have  $m_n = \frac{c_n}{d_n}$ .

REMARK 8.17 We can adopt the notation  $\sum_{d \in D} c(d)x^{|d|}$ , directly introducing the object  $d$  in the definition of the generating series of the enumeration. This method enables us to directly find the equation satisfied by the generating series in many cases of combinatorial enumeration problems without considering the associated recurrence equation.

EXERCISE 8.21 Let  $A = \{\text{blue, red, green}\}$  a set of colours. During a Master-mind game, one forms size  $n$  sequences with these three colours. Let  $a_i$  be the  $i$ th colour of the current solution.

1. Let  $t_n$  be the number of solutions of length  $n$ , such that, for  $i$  in  $\{1, \dots, n-2\}$ ,  $a_i \neq a_{i+2}$ .
  - (a) Compute  $t_1, t_2$  and  $t_3$ .
  - (b) Find a recurrence equation for  $t_n$ .
  - (c) Deduce  $t_n$ .
2. Let  $s_n$  be the number of size  $n$  solutions, such that either  $a_i \neq a_{i+2}$  or  $a_i = a_{i+1} = a_{i+2}$ , for  $i = 1, \dots, n-2$ .
  - (a) Compute  $s_1, s_2, s_3$  and  $s_4$ .
  - (b) Find a recurrence equation for  $s_n$ .
  - (c) Compute  $\sum_{n=1}^{\infty} s_n z^n$  and deduce  $s_n$ . ◇

EXERCISE 8.22 After giving a dictation to his pupils, a teacher redistributes the exercises for correction to the pupils. Let  $b_n$  be the number of ways of distributing the exercises in such a way that no pupil gets his or her own.

1. Compute  $b_1, b_2$  and  $b_3$ .
2. Show that the following equation holds:  $b_n = (n-1)(b_{n-1} + b_{n-2})$ , for  $n > 2$ .
3. Show that  $b_n - nb_{n-1} = (-1)^n$ , for  $n > 1$ .
4. Let  $b_0 = 1$ , and define the exponential generating series by

$$b(z) = \sum_{n=0}^{\infty} \frac{b_n z^n}{n!}.$$

Prove that  $b(z) = \frac{e^{-z}}{1-z}$ . ◇