

# Languages, automata and computation II

## Tutorial 2

Winter semester 2023/2024

In this tutorial we explore weighted automata and linear recursive sequences over a field. In particular, we will be concerned with functions in  $\Sigma^* \rightarrow \mathbb{Q}$  for a finite alphabet  $\Sigma$ .

**Exercise 1.** Show that the set of functions  $\Sigma^* \rightarrow \mathbb{Q}$  can be given the structure of a vector space over  $\mathbb{Q}$ . What is its dimension?

*Solution:* Define the addition of functions as  $(f + g)(w) := f(w) + g(w)$  and scalar multiplication by  $\alpha \in \mathbb{Q}$  as  $(\alpha \cdot f)(w) := \alpha \cdot f(w)$ . It can be checked that these definitions satisfy the requirements of vector spaces.

The space is infinite dimensional: Functions  $f_w$ 's s.t.  $f_w(w) = 1$  and  $f_w(u) = 0$  if  $u \neq w$  are linearly independent.  $\square$

### Rational functions and their linear representations

A *linear representation* over  $\Sigma$  is a triple  $A = (x, M, y)$  where the transition matrix  $M : \Sigma \rightarrow \mathbb{Q}^{k \times k}$  maps each letter  $a \in \Sigma$  to a  $k \times k$  rational matrix  $M_a$ ,  $x : \mathbb{Q}^{1 \times k}$  is a row vector, and  $y : \mathbb{Q}^{k \times 1}$  is a column vector. The transition matrix  $M$  is extended homomorphically to a function  $\Sigma^* \rightarrow \mathbb{Q}^{k \times k}$  (where matrices form a ring with the usual notions of matrix sum and product). The semantics of a linear representation is the function  $f : \Sigma^* \rightarrow \mathbb{Q}$  s.t.

$$f(w) = x \cdot M(w) \cdot y, \quad \text{for every } w \in \Sigma^*.$$

Call a function *rational* if it is of the form above.

**Exercise 2** (name of the game). Consider the special case of a unary alphabet  $\Sigma = \{a\}$ . Define the *generating series* of  $f : \mathbb{N} \rightarrow \mathbb{Q}$  to be

$$f(x) = \sum_{n=0}^{\infty} f(n) \cdot x^n$$

Show that if  $f$  is rational iff its generating series  $f(x)$  is a rational power series. Recall that rational power series are those which can be written as  $p(x)/q(x)$  for two polynomials  $p, q \in \mathbb{Q}[x]$ .

*Solution:* For the “only if” direction, assume  $f$  is rational and thus  $f(n) = u \cdot M^n \cdot v$ . Then its generating series satisfies

$$\begin{aligned} f(x) &= \sum_n (u \cdot M^n \cdot v) x^n = \\ &= u \cdot \sum_n (Mx)^n \cdot v = \\ &= u \cdot (I - Mx)^{-1} \cdot v, \end{aligned}$$

where one observes that  $I - Mx$  is invertible (even over the ring of power series matrices) and that the inverse of a polynomial matrix is a rational matrix.

For the “if” direction, let  $f(x) = \frac{p(x)}{1-x \cdot q(x)}$ . Thus  $f(x) = p(x) + x \cdot q(x) \cdot f(x)$  and one notices that this induces a linear recurrence for  $f(n)$ .  $\square$

A matrix  $A \in \mathbb{Q}^{k \times k}$  is *deterministic* if each row has at most one nonzero entry. A rational function  $f$  with linear representation  $(x, M, y)$  is *deterministic* if  $M_a, M_b$  are deterministic and  $x$  has at most one nonzero entry.

**Exercise 3.** Show that there are rational functions which are not deterministic.

*Solution:* A deterministic rational function never uses the “+” operation. In other words, if  $f$  is deterministic then  $f(w)$  is a *product* of numbers appearing in  $x$ ,  $M$ , and  $y$ . In particular, the image of  $f$  cannot contain numbers with arbitrarily large prime divisors. Now consider the function  $f(w) = |w|$ . It is rational and its image is  $\mathbb{N}$ . Since there are infinitely many primes,  $f$  cannot be deterministic.  $\square$

## q-finite functions

Given a function  $f : \Sigma^* \rightarrow \mathbb{Q}$  and a word  $u \in \Sigma^*$ , let the *left quotient*  $u^{-1}f : \Sigma^* \rightarrow \mathbb{Q}$  be the function defined as

$$(u^{-1}f)(w) = f(uw), \quad \text{for every } w \in \Sigma^*.$$

Call a function  $f$  *q-finite* if the set of left quotients

$$\{u^{-1}f \mid u \in \Sigma^*\}$$

span a finite-dimensional subspace of  $\Sigma^* \rightarrow \mathbb{Q}$ .

**Exercise 4.** Show that  $f$  is q-finite iff it is rational.

*Solution:* For the “only if” direction, assume that  $f$  is q-finite. There is a dimension  $d$  and this many basis left quotients

$$f_1 := u_1^{-1}f, \dots, f_d := u_d^{-1}f$$

s.t. every left quotient is a linear combination of  $f_1, \dots, f_d$ . We now construct a linear representation for  $f$ . Consider a basis left quotient  $f_m$  and extend it by reading  $a \in \Sigma$  to the quotient  $(u_m a)^{-1}f$ . This quotient is not necessarily a basis element, however it can be written as a (unique) linear combination of basis elements

$$(u_m a)^{-1}f = \alpha_{m,1} \cdot f_1 + \dots + \alpha_{m,d} \cdot f_d.$$

This defines  $M_a(m, n) := \alpha_{m, n}$ . To define the initial row vector we write  $f$  itself as

$$f = \alpha_1 \cdot f_1 + \cdots + \alpha_d \cdot f_d,$$

giving  $x = (\alpha_1, \dots, \alpha_d)$ , and the final column vector is obtained by evaluating the basis elements at  $\varepsilon$ , giving  $y = (f_1(\varepsilon), \dots, f_d(\varepsilon))^T$ .

Correctness amounts to prove

$$f(w) = x \cdot M(w) \cdot y, \quad \text{for all } w \in \Sigma^*.$$

This will follow at once from the following inductive property:

$$w^{-1}f = x \cdot M(w) \cdot (f_1, \dots, f_d)^T, \quad \text{for all } w \in \Sigma^*.$$

For  $w = \varepsilon$  it holds by the definition of  $x$ . Inductively we have

$$\begin{aligned} (wa)^{-1}f &= a^{-1}w^{-1}f = \\ &= a^{-1}(x \cdot M(w) \cdot (f_1, \dots, f_d)^T) = \\ &= x \cdot M(w) \cdot (a^{-1}f_1, \dots, a^{-1}f_d)^T = \\ &= x \cdot M(w) \cdot (M_a \cdot (f_1, \dots, f_d)^T) = \\ &= x \cdot M_{wa} \cdot (f_1, \dots, f_d)^T. \end{aligned}$$

We have used the inductive assumption, the fact that left quotients act linearly, and the definition of  $M_a$ .

For the “if” direction, assume that  $f$  is rational. There is a  $k$ -dimensional linear representation  $(x, M, y)$  s.t.  $f(w) = x \cdot M(w) \cdot y$  for every  $w \in \Sigma^*$ . The set of  $k \times k$  matrices  $\mathbb{Q}^{k \times k}$  is a vector space of dimension  $k^2$  (with respect to matrix addition and scalar multiplication). Now consider the linear span of all reachable matrices

$$V := \text{span}(M(w) \mid w \in \Sigma^*) \subseteq \mathbb{Q}^{k \times k}.$$

As a subspace of a vector space of dimension  $k^2$  it is itself of some finite dimension  $d \leq k^2$ . Let a basis of  $V$  be  $M_1 := M_{u_1}, \dots, M_d := M_{u_d}$ . We claim that  $f_1, \dots, f_d$  is a basis of the vector subspace generated by left quotients of  $f$ , where for every  $1 \leq i \leq d$ ,

$$f_i(w) := x \cdot M_{u_i \cdot w} \cdot y, \quad \text{for all } w \in \Sigma^*.$$

First of all,  $f_i$  is indeed a left quotient of  $f$ . Secondly, let  $u^{-1}f$  be a left quotient for  $f$ . Since  $M(u)$  is in  $V$ , by the spanning property of the basis we can write

$$M(u) = \alpha_1 \cdot M_1 + \cdots + \alpha_d \cdot M_d.$$

For every input word  $w \in \Sigma^*$  we can write

$$\begin{aligned} (u^{-1}f)(w) &= f(uw) = x \cdot M(uw) \cdot y = \\ &= x \cdot M(u) \cdot M(w) \cdot y = \\ &= x \cdot (\alpha_1 \cdot M_1 + \cdots + \alpha_d \cdot M_d) \cdot M(w) \cdot y = \\ &= \alpha_1 \cdot x \cdot M(u_1 \cdot w) \cdot y + \cdots + \alpha_d \cdot x \cdot M(u_d \cdot w) \cdot y = \\ &= \alpha_1 \cdot f(u_1 \cdot w) + \cdots + \alpha_d \cdot f(u_d \cdot w) = \\ &= \alpha_1 \cdot (u_1^{-1}f)(w) + \cdots + \alpha_d \cdot (u_d^{-1}f)(w) = \\ &= \alpha_1 \cdot f_1(w) + \cdots + \alpha_d \cdot f_d(w). \end{aligned}$$

Since  $w$  was arbitrary, we have established  $u^{-1}f = \alpha_1 \cdot f_1 + \cdots + \alpha_d \cdot f_d$ , as required.  $\square$

## Closure properties

**Exercise 5.** Show that the set of all q-finite functions is a vector subspace of  $\Sigma^* \rightarrow \mathbb{Q}$ .

*Solution:* This boils down to showing that q-finite functions are closed under multiplication by constants and by addition. Both verifications are immediate by applying linearity either to linear representations or to left quotients. (Left quotienting acts linearly:  $u^{-1}(\alpha \cdot f) = \alpha \cdot (u^{-1}f)$  and  $u^{-1}(f + g) = u^{-1}f + u^{-1}g$ .)  $\square$

**Exercise 6.** Show that the set of q-finite functions is closed under the following operations.

1. Hadamard product:  $(f \cdot g)(w) := f(w) \cdot g(w)$ .
2. Cauchy product:  $(f * g)(w) := \sum_{uv=w} f(u) \cdot g(v)$ .
3. Iteration, when  $f(\varepsilon) = 0$ :  $f^* := f^0 + f^1 + f^2 + \cdots$ , where  $f^0(w)$  is 1 if  $w = \varepsilon$  and 0 otherwise, and  $f^{n+1} = f^n * f$  for every  $n \geq 0$ .

*Solution:* 1. Let  $f_1, \dots, f_d$  be a basis for  $f$  and  $g_1, \dots, g_e$  one for  $g$ . We claim that quotients of  $f \cdot g$  are in the linear span of

$$\{f_i \cdot g_j \mid 1 \leq i \leq d, 1 \leq j \leq e\}.$$

This follows at once since (a) quotients distribute over Hadamard product, and (b) Hadamard product is bilinear. This shows that the dimension of  $f \cdot g$  is at most  $d \cdot e$ , but it could be less.

2. For words  $u = a_1 \cdots a_n, w \in \Sigma^*$ , by analysing the Cauchy product we have that  $u^{-1}(f * g)$  equals

$$\underbrace{f(\varepsilon)}_{\in \mathbb{Q}} \cdot u^{-1}g + \underbrace{f(a_1)}_{\in \mathbb{Q}} \cdot (a_2 \cdots a_n)^{-1}g + \cdots + \underbrace{f(a_1 \cdots a_{n-1})}_{\in \mathbb{Q}} \cdot a_n^{-1}g + u^{-1}f * g.$$

In other words, left quotients of  $f * g$  are linear combinations of left quotients of  $g$  and  $h * g$  with  $h$  a left quotient of  $f$ . This suggests that if  $f_1, \dots, f_d$  is a basis for  $f$  and  $g_1, \dots, g_e$  one for  $g$ , then left quotients of  $f * g$  are in the linear span of

$$\{f_i * g \mid 1 \leq i \leq d\} \cup \{g_j \mid 1 \leq j \leq e\}.$$

This can be verified thanks to the calculation above and bilinearity of Cauchy product. Incidentally, this shows that the dimension of  $f * g$  is at most  $d + e$ .

3. First notice that iteration is well-defined, thanks to the condition  $f(\varepsilon) = 0$ . Let  $f_1, \dots, f_d$  be a basis for left quotients of  $f$  and let  $f_0 := f^0$ . We claim that left quotients of  $f^*$  are in the linear span of

$$\{f_0 * f^*, f_1 * f^*, \dots, f_d * f^*\}.$$

We show that every left quotient  $u^{-1}f^*$  is a linear combination of elements above by induction on the length of  $u$ . In the base case,  $u = \varepsilon$  and thus  $\varepsilon^{-1}f^* = f^*$  is already the basis element  $f_0 * f^*$ .

In the inductive case, let  $u = a_1 \cdots a_n$  have positive length  $n \geq 1$ . We use again  $f^* = f^0 + f * f^*$  to write

$$\begin{aligned} u^{-1}f^* &= u^{-1}(f^0 + f * f^*) = \underbrace{u^{-1}f^0}_0 + u^{-1}(f * f^*) = \\ &= \underbrace{f(\varepsilon) \cdot u^{-1}f^*}_0 + f(a_1) \cdot (a_2 \cdots a_n)^{-1}f^* + \cdots + f(a_1 a_2 \cdots a_{n-1}) \cdot a_n^{-1}f^* + u^{-1}f * f^*. \end{aligned}$$

This shows that  $u^{-1}f^*$  is a linear combination of shorter quotients of  $f^*$  and  $u^{-1}f * f^*$ . By the inductive assumption shorter quotients of  $f^*$  are in the span of the perspective basis. Regarding  $u^{-1}f * f^*$ , since  $u^{-1}f$  is a linear combination of  $f_1, \dots, f_d$ , by left linearity  $u^{-1}f * f^*$  is a linear combination of  $f_1 * f^*, \dots, f_d * f^*$ .

□

**Exercise 7** (Inverses). 1. Under which condition does  $f$  have an inverse w.r.t. Hadamard product? Is Hadamard-invertibility decidable?

2. Under which condition does  $f$  have an inverse w.r.t. Cauchy product?

3. In the latter case, find an expression for the Cauchy inverse of  $f$ .

*Solution:* 1. First of all the unit for the Hadamard product is the constantly 1 function. The function  $f$  has a Hadamard inverse iff  $f(w) \neq 0$  for all  $w$ , in which case the Hadamard inverse of  $f$  is  $g$  defined as  $g(w) = 1/f(w)$  for every  $w \in \Sigma^*$ . Hadamard invertibility is undecidable, since the complement problem (is there some  $w$  s.t.  $f(w) = 0$ ) is undecidable for weighted automata.

2. The unit for the Cauchy product is the function  $f$  s.t.  $f(\varepsilon) = 1$  and that is zero everywhere else. Call this function  $\mathbf{1}$  for convenience. In order for  $f * g$  to be the Cauchy unit, it is necessary that  $f(\varepsilon) \neq 0$ . In fact this condition is also equivalent to the existence of a Cauchy inverse, which we will compute in the next point.

3. First we show how to invert  $f$  s.t.  $f(\varepsilon) = 1$ . Let  $g = \mathbf{1} - f$  and we claim that  $g^*$  is the Cauchy inverse of  $f$ . Indeed  $g^*$  is well defined since  $g(\varepsilon) = 0$ , and we have

$$f * g^* = (\mathbf{1} - g) * (g^0 + g^1 + \cdots) = g^0 = \mathbf{1}. \quad \square$$

## Regular expressions

**Exercise 8** (Kleene-Schützenberger theorem). Call a function *regular* if it can be generated by the following abstract grammar

$$f, g ::= p \mid \alpha \cdot f \mid f + g \mid f * g \mid f^*,$$

where  $p$  is a polynomial (function with finite support) and iteration  $f^*$  is only applied when defined. Show that a function is regular iff it is rational.

*Solution:* The “only if” direction follows by the closure properties of rational functions. The converse direction is more involved and we give only the proof idea. Let  $f$  be rational, thus there is a linear representation  $(x, \{M_a, M_b\}, y)$ , with  $M_a, M_b \in \mathbb{Q}^{k \times k}$ , s.t.  $f(w) = x \cdot M(w) \cdot y$ . Here  $M$  is in  $\Sigma^* \rightarrow \mathbb{Q}^{k \times k}$ . The latter set is naturally endowed by a Kleene algebra structure by the operations of sum, product, iteration (when defined), and constants 0 and 1:

$$\mathbb{S} = (\Sigma^* \rightarrow \mathbb{Q}^{k \times k}, +_{\mathbb{S}}, \cdot_{\mathbb{S}}, (-)_{\mathbb{S}}^*, 0_{\mathbb{S}}, 1_{\mathbb{S}}).$$

It is fruitful to notice that the latter is isomorphic to the matrix Kleene algebra

$$\mathbb{M} = ((\Sigma^* \rightarrow \mathbb{Q})^{k \times k}, +_{\mathbb{M}}, \cdot_{\mathbb{M}}, (-)_{\mathbb{M}}^*, 0_{\mathbb{M}}, 1_{\mathbb{M}}).$$

where the definitions of sum, product, and 0, 1 are automatically inherited from the base ring  $\Sigma^* \rightarrow \mathbb{Q}$ ; iteration is defined as  $M^* := \sum_n M^n$  (when it exists). Indeed, we can map a function  $M \in \mathbb{S}$  to the matrix  $\widetilde{M} \in \mathbb{M}$  s.t.  $\widetilde{M}_{ij}(w) := M(w)_{ij}$ .

The *support* of a matrix  $M \in \mathbb{M}$  is the union of the supports of all its entries. Call a matrix  $M \in \mathbb{M}$  *regular* if it can be finitely generated from matrices of finite support by the algebra operations. For instance, if  $M \in \mathbb{S}$  is generated by matrices  $M_a, M_b \in \mathbb{Q}^{k \times k}$  in the sense of linear representations, then  $\widetilde{M} \in \mathbb{M}$  is regular since

$$\widetilde{M} = (A + B)^*,$$

where  $A, B \in \mathbb{M}$  have finite support and are defined as follows:  $A_{ij}$  maps  $a$  to the  $i, j$  component of  $M_a$ , and maps any other word to zero; similarly for  $B$ .

Then one shows that if  $M, N \in \mathbb{M}$  are two matrices with all entries regular (in the sense of  $\mathbb{S}$ ), then the same holds for  $M + N$ ,  $M \cdot N$ , and  $M^*$ . Only the last case is non-trivial, but it can be shown by induction on the dimension of  $M$  by a suitable rule expressing  $M^*$  in terms of iteration, sum, and product of submatrices.  $\square$

## Supports

The *support* of a function  $f : \Sigma^* \rightarrow \mathbb{Q}$ , denoted  $\text{supp } f$ , is the set of words where  $f$  is nonzero. A *rational support* is the support of a rational function. Since we do not consider any other kind of support, we just say “support” for “rational support” in the following.

**Exercise 9.** 1. Show that the class of supports includes all regular languages.

2. Are there nonregular supports?

*Solution:* For a language  $L \subseteq \Sigma^*$ , we can define its *characteristic function*  $f_L : \Sigma^* \rightarrow \mathbb{Q}$  by mapping words in the language to 1, and the rest to 0. Clearly the support of  $f_L$  is  $L$ . We now argue that if  $L$  is regular, then  $f_L$  is a rational function. It will be convenient to use regular expressions and notice how

characteristic functions interact with rational operations on languages:

$$\begin{aligned}
f_{\{\varepsilon\}} &= \mathbf{1} \\
f_{L \cap M} &= f_L \cdot f_M && \text{(Hadamard product)} \\
f_{\Sigma^* \setminus L} &= 1 - f_L && \text{(where 1 is one everywhere)} \\
f_{L \cup M} &= f_L + f_M - f_L \cdot f_M \\
f_{L \cdot M} &= f_L * f_M && \text{(Cauchy product)} \\
f_{L^*} &= f_L^* && \text{(if } \varepsilon \notin L)
\end{aligned}$$

Finite languages are clearly supports (of polynomials). The proof is concluded by writing  $L$  as a regular expression  $e$  and applying the rules above by structural induction on  $e$ , using the closure properties of rational functions.

There are nonregular supports. We show a rational function  $f$  whose co-support is  $L = \{a^n b^n \mid n \in \mathbb{N}\}$  (the complement of which is nonregular). Let  $f = (g - h)^2 + \ell$  (Hadamard square), where  $g(a^m b^n) = 2^m 3^n$  (and zero otherwise),  $h(a^m b^n) = 2^n 3^m$  (and zero otherwise), and  $\ell$  is the characteristic function of  $\Sigma^* \setminus a^* b^*$ . We have  $f(w) = 0$  if  $w = a^n b^n$  and  $f$  is nonzero otherwise.  $\square$

**Exercise 10** (Weak cancellation property [1]). A language  $L \subseteq \Sigma^*$  has the *weak cancellation property* if there exists a  $n \in \mathbb{N}$  s.t. no matter how we split a word  $w \in L$  as  $w = xy_1 \cdots y_n z$  with  $y_1, \dots, y_n$  nonempty, we can always find  $i, j \in \mathbb{N}$  s.t.  $1 \leq i \leq j \leq n$  and  $xy_1 \cdots y_{i-1} y_{j+1} \cdots y_n z \in L$ .

1. Show that supports have the weak cancellation property.
2. Find a context-free language which is not a support.

*Solution:* 1. Let  $L = \text{supp } f$  be the support of a rational function  $f$  with linear representation  $(u, M, v)$  of dimension  $k$ . We show that  $L$  has the weak cancellation property for  $n := k$ . Consider  $w = xy_1 \cdots y_k z \in L$ . Thus  $uM(w)v \neq 0$ , and in particular row vectors in the following sequence are nonzero:

$$uM(x), uM(xy_1), \dots, uM(xy_1 \cdots y_k) \in \mathbb{Q}^{1 \times k}.$$

Since there are  $k+1$  vectors in the sequence above and they lie in a  $k$ -dimensional vector space, there is  $1 \leq j \leq k$  s.t. the  $j$ -th vector is a linear combination of preceding vectors,

$$uM(xy_1 \cdots y_j) = \sum_{0 \leq i < j} \alpha_i \cdot uM(xy_1 \cdots y_i).$$

We now right multiply both sides by  $M(y_{j+1} \cdots y_k)v$  and obtain

$$uM(w)v = \sum_{0 \leq i < j} \alpha_i \cdot uM(xy_1 \cdots y_i y_{j+1} \cdots y_k)v.$$

Since  $w \in L$ , the r.h.s. is nonzero, thus there is  $0 \leq i < j$  s.t.

$$uM(xy_1 \cdots y_i y_{j+1} \cdots y_k)v \neq 0.$$

This means  $xy_1 \cdots y_i y_{j+1} \cdots y_k \in L$ , as required.

2. Consider the context-free language  $L = \{a^n b^n \mid n \in \mathbb{N}\}$ . We show that it does not satisfy the weak cancellation property. For  $n \in \mathbb{N}$  consider  $w = a^n b^n$  split as  $w = xy_1 \cdots y_n z$  where  $x = \varepsilon$ ,  $y_1 = \cdots = y_n = a$ , and  $z = b^n$ . Clearly there is no way to remove any infix  $u_i \cdots u_j$  of  $a^n$  from  $w$  and remain in  $L$ .  $\square$

**Exercise 11.** Are the following problems decidable for supports:

1. emptiness?
2. universality?
3. equivalence?
4. inclusion?

*Solution:* Emptiness is the same as non-zeroness, thus it is decidable. Non-universality on the other hand asks whether some word has zero semantics, which is undecidable. Equivalence and inclusion are more general than universality, so also undecidable.  $\square$

**Exercise 12.** Are supports closed under

1. intersection?
2. union?
3. concatenation?
4. Kleene star?
5. complement?

*Solution:* The closure properties for the first four points follow by the equations (since rational functions are closed under the respective operations)

$$\begin{aligned}
 \text{supp } f \cap \text{supp } g &= \text{supp } (f \cdot g), & (\text{Hadamard product}) \\
 \text{supp } f \cup \text{supp } g &= \text{supp } (f \cdot f + g \cdot g), & (\text{Hadamard square}) \\
 \text{supp } f \cdot \text{supp } g &= \text{supp } (f * g), & (\text{Cauchy product}) \\
 \text{supp } f^* &= \text{supp } f^*. & (\text{Cauchy iteration})
 \end{aligned}$$

Supports are not closed under complement: We have seen that  $a^n b^n$  is not a support, however its complement is.  $\square$

## References

- [1] Antonio Restivo and Christophe Reutenauer. On cancellation properties of languages which are supports of rational power series. *J. Comput. Syst. Sci.*, 29(2):153–159, October 1984.