Languages, automata and computation II
Tutorial 3

Winter semester 2023/2024

In this tutorial we explore ideals, varieties, and polynomial automata. Recall that an *ideal* of a ring R is a subset $I \subseteq R$ which is 1) closed under sum $I + I \subseteq I$, and 2) closed under under product with elements from the ring $R \cdot I \subseteq I$. For a set of vectors $A \subseteq \overline{\mathbb{Q}}^k$, let $I(A) \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ be the set of polynomials vanishing on A. (This is an ideal, justifying the notation). For a set of polynomials $P \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_k]$, let $V(P) \subseteq \overline{\mathbb{Q}}^k$ be the set of vectors where all polynomials in P vanish simultaneously. The *Zariski closure* of a set of vectors A is defined as

$$\overline{A} := V(I(A)).$$

Exercise 1. 1. Show that $A \subseteq \overline{A}$, for every $A \subseteq \overline{\mathbb{Q}}^k$.

2. Find a set of vectors $A \subseteq \overline{\mathbb{Q}}^k$ where the inclusion in the previous point is strict. Can such a set A be finite?

Solution: The first point follows directly from the definitions. For the second point, we first notice that A cannot be finite. Indeed if $A \subseteq \overline{\mathbb{Q}}^k$ is finite, then $I(A) = \langle p \rangle$ is generated by a single polynomial p which vanishes precisely on A, and thus $V(I(A)) = A$. Finally, consider $k = 1$ and the infinite set $A = \mathbb{N}$. Since only nonzero univariate polynomials have finitely many zeroes, $I(A) = \langle 0 \rangle = \{0\}$ is generated by the zero polynomial. Then $\overline{A} = V(\{0\}) = \overline{\mathbb{Q}}$ is the whole set of algebraic numbers. □

Exercise 2 (zero polynomial vs. zero polynomial function)**.** Show that $p : \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ is the zero polynomial iff as a function $\overline{\mathbb{Q}}^k \to \overline{\mathbb{Q}}$ it is constantly zero. Is this true if we replace $\overline{\mathbb{Q}}$ by $\mathbb{F}_2$ (the field consisting just of the elements $\{0, 1\}$)?

Solution: The "only if" direction is obvious (and true also in $\mathbb{F}_2$), For the "if" direction, we proceed by induction on k. The base case $k = 0$ is trivial. For the inductive step, we rely on the isomorphism

$$\overline{\mathbb{Q}}[x_1, \ldots, x_k] \cong \overline{\mathbb{Q}}[x_1, \ldots, x_{k-1}][x_k].$$

In other words, we see p as a univariate polynomial in x_k over the polynomial ring not containing x_k. A univariate nonzero polynomial has finitely many zeros *and the latter ring is infinite.* We can thus find a substitution $x_k \mapsto q$ where q

does not contain x_k s.t. p does not vanish after this substitution. We now have a nonzero polynomial without x_k and we can apply the inductive assumption.

The "if" direction not hold over $\mathbb{F}_2$, for instance $x \cdot (1 - x)$ is not the zero polynomial, however it evaluates to $0 \in \mathbb{F}_2$ for all $x \in \mathbb{F}_2$. □

Exercise 3. Show that I is an ideal of $R[x]$ iff I is a vector subspace of $R[x]$ over R (i.e., $I + I \subseteq I$ and $aI \subseteq I$ for every $a \in R$) s.t. $xI \subseteq I$.

Solution: Easy. □

Exercise 4. We have seen that $I(A)$ is an ideal of $\overline{\mathbb{Q}}[x_1, \ldots, x_k]$ for every $A \subseteq \overline{\mathbb{Q}}^d$. Is every ideal of this ring of this form?

Solution: No. For example $I = \langle x^2 \rangle$ is not of the form $I(A)$. Since x^2 vanishes precisely at $x = 0$, we necessarily have $A = \{0\}$, however $I(\{0\}) = \langle x \rangle$ is strictly larger than I. For instance, $x \notin I$.

Ideals of the form $I(A)$ have the special property that $p^n \in I(A)$ implies $p \in I(A)$ (i.e., they are closed under n-th roots) and those are called *radical ideals*. One can then show that all radical ideals are in fact of the form $I(A)$. □

Principal ideal rings

Recall that a ring R is a *principal ideal ring* if every ideal of R is generated by one element.

Exercise 5. Are the following principal ideal rings?

1. The field of rational numbers $\mathbb{Q}$.
2. The ring of integers $\mathbb{Z}$.
3. The ring of univariate polynomials over the rationals $\mathbb{Q}[x]$.
4. The ring of univariate polynomials over the integers $\mathbb{Z}[x]$.
5. The ring of bivariate polynomials over the rationals $\mathbb{Q}[x, y]$.
6. The quotient ring $\mathbb{Q}[x, y]/\langle x - y \rangle$.

Solution:

1. Yes, a field has two ideals $\{0\}$ and $\mathbb{Q} = \langle 1 \rangle$, which are both principal.
2. Yes, ever ideal is of the form "integer multiples of a basis element $b \in \mathbb{Z}$".
3. Yes, one can compute the GCD of all elements of an ideal $I \subseteq \mathbb{Q}[x]$, and this is its generator.
4. No, for instance the proper ideal $\langle 2, x \rangle \subsetneq \mathbb{Z}[x]$ cannot be generated by a single polynomial $p \in \mathbb{Z}[x]$. Indeed, by way of contradiction we could write $2 = q \cdot p$ for some $q \in \mathbb{Z}[x]$ which forces $p = \pm 2$ since the ideal is proper. But then we cannot have $x = r \cdot p = r \cdot 2$ for any $r \in \mathbb{Z}[x]$.
5. No, since $\langle x, y \rangle$ is not principal.
6. Yes, since the quotient is isomorphic to $\mathbb{Q}[z]$.

□

Exercise 6. If R is a principal ideal ring, does the same hold for $R[x]$?

Solution: No, for instance $\mathbb{Z}[x]$ is a principal ideal ring, however $\mathbb{Z}[x][y]$ is not. □

Noetherian rings

A ring R is *Noetherian* if every ideal $I \subseteq R$ is finitely generated. In the following problem we explore ways to construct Noetherian rings.

Exercise 7.

1. Fields are Noetherian.
2. Finite rings are Noetherian.
3. Principal ideal rings are Noetherian.
4. If R is Noetherian and $I \subseteq R$ is an ideal, then R/I is Noetherian.
5. If R is Noetherian, then $R[x]$ is Noetherian. Does the converse hold?
6. If R is Noetherian, then $R[\![x]\!]$ is Noetherian.

Solution: The first three points are obvious.

For point 4. recall that elements of the quotient ring R/I are of the form $a + I$ (*cosets*) with $a \in R$. One can show that the ideals of R/I are in bijection with the ideals of R containing I. Moreover, $J + I \subseteq K + I$ (as an inclusion of ideals in R/I) iff $J \subseteq K$ (as an inclusion of ideals in I). Consequently, if we have an ideal chain in the quotient ring

$$J_0 + I \subseteq J_1 + I \subseteq \cdots \subseteq R/I$$

then we have also an ideal chain in the original ring

$$J_0 \subseteq J_1 \subseteq \cdots \subseteq R,$$

but since R is Noetherian there is n s.t. $J_n \supseteq J_{n+1} \supseteq \cdots$, and thus for the same n we have $J_n + I \supseteq J_{n+1} + I \supseteq \cdots$.

For point 5., let $I \subseteq R[x]$ be an ideal of the polynomial ring. Let $I_n \subseteq R$ be the set of all leading coefficients $a_{n,i}$ of degree n polynomials in I

$$f_{n,i} = a_{n,i} \cdot x^n + O(x^{n-1}) \in I.$$

One can check that $I_0 \subseteq I_1 \subseteq \cdots \subseteq R$ is an ideal chain, and since R is Noetherian there is $N \in \mathbb{N}$ s.t. $I_N = I_{N+1} = \cdots$. Let $I_n = \langle G_n \rangle$ for some *finite* set of generators $G_n \subseteq R$ and consider the corresponding finite set of degree n polynomials

$$S_n = \{f_{n,i} \in R[x] \mid a_{n,i} \in G_n\}.$$

We claim that $S = S_0 \cup \cdots \cup S_N$ generates the whole polynomial ideal $I = \langle S \rangle$. By way of contradiction consider a polynomial *of minimal degree* d

$$f = a_d \cdot x^d + O(x^{d-1}) \in I \setminus \langle S \rangle.$$

We show that there is a polynomial $g = a_d \cdot x^d + O(x^{d-1}) \in \langle S \rangle$ with the same leading term $a_d \cdot x^d$ as f. Since $f \in I$ has degree d, we have $a_d \in I_d$. We have two cases to consider.

- For small degree $d \leq N$, since $I_d = \langle G_d \rangle$ we write a_d as a R-linear combination of elements from G_d. The same R-linear combination of elements of the corresponding polynomials in S_d gives us the required polynomial $g = a_d \cdot x^d + O(x^{d-1}) \in \langle S_d \rangle \subseteq \langle S \rangle$.
- For large degree $d > N$, we use $\langle G_d \rangle \subseteq \langle G_N \rangle$ and write a_d as a R-linear combination of elements from G_N. The same R-linear combination of elements of the corresponding polynomials in S_N gives us a polynomial $h = a_d \cdot x^N + O(x^{N-1}) \in \langle S_N \rangle \subseteq \langle S \rangle$ of degree N. We then define $g = x^{d-N} \cdot h = a_d \cdot x^d + O(x^{d-1}) \in \langle S \rangle$.

But then $f - g \in I \setminus \langle S \rangle$ has strictly smaller degree than f, which is a contradiction.

The converse holds as well. An ideal chain $I_0 \subseteq I_1 \subseteq \cdots \subseteq R$ in the underlying ring induces an ideal chain $\langle I_0 \rangle \subseteq \langle I_1 \rangle \subseteq \cdots \subseteq R[x]$ in the polynomial ring. But the latter is Noetherian so $\langle I_n \rangle = \langle I_{n+1} \rangle = \cdots$, for some $n \in \mathbb{N}$. Since the constant terms of the sum and product of polynomials depend only on their constant terms, $I_n = I_{n+1} = \cdots$.

The argument for point 6. is similar as in the previous point, but instead of looking at coefficients of terms of highest degree we look at coefficients of terms of smallest order. We omit the details. □

Exercise 8. Are the following rings Noetherian?

1. Ring of polynomials with countably many variables: $\mathbb{Q}[x_1, x_2, \dots]$.
2. Ring of power series: $\mathbb{Q}[\![x]\!]$.
3. Ring of rational power series: $\mathbb{Q}[\![x]\!] \cap \mathbb{Q}(x)$.
4. Noncommutative ring of power series in noncommuting variables: $R := \Sigma^* \to \mathbb{Q}$, $|\Sigma| \geq 2$, with sum and convolution (Cauchy) product.

Solution:

1. No. The ideal $\langle x_1, x_2, \dots \rangle$ is not finitely generated.
2. Yes. This follows from Exercise 7, but we can also give a quick argument in this particular case since $\mathbb{Q}$ is a field. Every power series can be written as $f = x^n \cdot (a_0 + a_1 x + \cdots)$ where $a_0 \neq 0$. Since the constant term of the series on the right is nonzero, the series has an inverse in the ring (i.e., it is a *unit* of the ring). It follows that this is even a principal ideal ring, where every ideal is generated by $\langle x^n \rangle$ for some $n \in \mathbb{N}$.
3. Yes, since this is in fact a field and all fields are Noetherian.
4. No. Let $\Sigma = \{a, b\}$ and consider the right ideal

$$I := a \cdot R + ba \cdot R + b^2 a \cdot R + \cdots .$$

I cannot be generated by finitely many $\{b^0 a, \dots, b^n a\}$ since $b^{n+1} a \in I$ cannot be written as a right linear combination of the generators.

□

Exercise 9. For every of the following sets A check that it is a ring. Is it Noetherian?

1. $A = x \cdot \mathbb{Q}[x] \subseteq \mathbb{Q}[x]$.
2. $A = \mathbb{Z} + x \cdot \mathbb{Q}[x] \subseteq \mathbb{Q}[x]$.

Solution: 1. Yes, since this is isomorphic to the polynomial ring $\mathbb{Q}[x]$.

2. No, the ideal of elements with *zero* constant term $I = x \cdot \mathbb{Q}[x]$ is not finitely generated over A. By way of contradiction, suppose it was finitely generated by $f_1, \ldots, f_n \in I$. We can write $f_i = \alpha_i \cdot x + O(x^2)$ with $\alpha_i \in \mathbb{Q}$. Then an arbitrary $f = \alpha \cdot x + O(x^2) \in I$ can be written as a linear combination of the generators $f = g_1 \cdot f_1 + \cdots + g_n \cdot f_n$ for some $g_1, \ldots, g_n$ with integer constant terms $k_1, \ldots, k_n \in \mathbb{Z}$. It follows that $\alpha = k_1 \cdot \alpha_1 + \cdots + k_n \cdot \alpha_n$, however the rational numbers on the right can only generate finitely many denominators.

□

Polynomial automata

Recall that a *polynomial automaton* is a tuple

$$A = (d, Q, \Sigma, q_I, F)$$

where $d \in \mathbb{N}$ is the *dimension*, $Q = \overline{\mathbb{Q}}^d$ is the set of *states*, Σ is a finite alphabet inducing a polynomial action

$$q \in Q \mapsto q \cdot a \in Q, \quad \text{for every } a \in \Sigma,$$

$q_I \in Q$ is the *initial state*, and $F : Q \to \overline{\mathbb{Q}}$ is the polynomial *output function*. The action of Σ is extended to words $w \in \Sigma^*$ homomorphically: $q \cdot \varepsilon := q$ and $q \cdot (a \cdot w) := (q \cdot a) \cdot w$. The *semantics* of state $q \in Q$ is the mapping $[\![q]\!] : \Sigma^* \to \overline{\mathbb{Q}}$ defined as

$$[\![q]\!]_w = F(q \cdot w), \quad \text{for every } w \in \Sigma^*.$$

The semantics of the automaton A is $[\![A]\!] = [\![q_I]\!]$. The automaton is *zero* if $[\![A]\!] = 0$.

The set $\Sigma^* \to \mathbb{Q}$ has the structure of a commutative ring w.r.t. addition and Hadamard product (pointwise product). This gives us an alternative presentation of the semantics of polynomial automata.

Exercise 10. A function $f : \Sigma^* \to \mathbb{Q}$ is recognisable by a polynomial automaton iff it belongs to a finitely generated subring of $S := \Sigma^* \to \mathbb{Q}$ closed under left quotients $u^{-1}(\cdot)$.

Solution: For the "only if" direction, let A be the automaton recognising f. Let the transition function of A for coordinate $i \in \{1, \ldots, d\}$ and letter $a \in \Sigma$ be realised by $p_i^a \in \mathbb{Q}[x_1, \ldots, x_d]$. Let $f_i : S$ be defined as $f_i(w) = \pi_i(q_I \cdot w)$, i.e. the value of state i after reading w from the initial state. Then the subring $\mathbb{Q}[f_1, \ldots, f_d]$ of S generated by $f_1, \ldots, f_d$ satisfies the following properties:

1. f is in R since $f = F(f_1, \ldots f_d)$.

2. R is closed under single letter quotients (and thus under arbitrary quotients): Quotients commute with Hadamard product, so it suffices to show that $a^{-1}f_i$ is in R. This clearly holds since $a^{-1}f_i(w) = f_i(aw) = p_i^a(f_1(w), \ldots, f_d(w))$.

For the "if" direction, let $R = \mathbb{Q}[f_1, \ldots, f_d]$ be closed under left quotients and $f \in R$. It follows that $a^{-1}f_i$ can be written as a polynomial combination of $f_1, \ldots, f_d$ say $a^{-1}f_i = p_i^a(f_1, \ldots, f_d)$. This gives us the transition structure of a polynomial automaton of dimension d. The output function is the polynomial F s.t. $f = F(f_1, \ldots, f_d)$ which exists since $f \in R$. □

A *variety* is a subset $V \subseteq \overline{\mathbb{Q}}^d$ which is the set of common zeros of a set of polynomials: $V = V(P)$ for some $P \subseteq \mathbb{Q}[x_1, \ldots, x_d]$.

Exercise 11. For $d = 2$ find a non-trivial infinite variety.

Solution: Take $V = V(\{x \cdot y\})$, then V is the union of the x and y axes. □

Exercise 12. Let $V \subseteq \overline{\mathbb{Q}}^d$ be a variety.

1. Let $G : \overline{\mathbb{Q}}^e \to \overline{\mathbb{Q}}^d$ be a polynomial map. Is $G^{-1}(V) \subseteq \overline{\mathbb{Q}}^e$ a variety?
2. Let $G : \overline{\mathbb{Q}}^d \to \overline{\mathbb{Q}}^e$ be a polynomial map. Is $G(V) \subseteq \overline{\mathbb{Q}}^e$ a variety?

Solution:
1. Yes. Let $V = V(P)$ for a set of polynomials $P \subseteq \mathbb{Q}[x_1, \ldots, x_d]$. If we see P as a polynomial map $\overline{\mathbb{Q}}^d \to \overline{\mathbb{Q}}$ we have $V = P^{-1}(\{0\})$. Since polynomial maps are closed under composition, the following set is also a variety:
$$G^{-1}(V) = G^{-1}(P^{-1}(\{0\})) = (P \circ G)^{-1}(\{0\}).$$
2. No, already for $d = e = 1$. Take $G(x) = x^2$ and the trivial variety $V = V(\{0\}) = \overline{\mathbb{Q}}$. Then $G(V) = \overline{\mathbb{Q}}_{\geq 0}$, which is not a variety.

□

Exercise 13. Show that all varieties $V \subseteq \overline{\mathbb{Q}}^d$ are generated by *a single* polynomial. Is this true for varieties of $\mathbb{C}^d$?

Solution: By Hilbert finite basis theorem we can write $V = V(p_1, \ldots, p_n)$. We then observe that $V = V(p)$ with
$$p = p_1^2 + \cdots + p_n^2.$$
This trick does not work over the complex numbers, and in fact one can show that single polynomials are not sufficient to generate all complex varieties. □

Exercise 14. Let $U, V \subseteq \overline{\mathbb{Q}}^d$ be a varieties. Are the following varieties?

1. $U \cap V$. What about possibly infinite intersections?
2. $U \cup V$. What about possibly infinite intersections?
3. $U \setminus V$.

Solution: 1. Yes, since $V(P) \cap V(Q) = V(P \cup Q)$. In fact this shows that varieties are closed under arbitrary intersections.

2. Yes. By Hilbert finite basis theorem we can write $U = V(p_1, \ldots, p_m)$ and $V = V(q_1, \ldots, q_n)$. Then $U \cup V = V(\{p_i \cdot q_j \mid 1 \leq i \leq m, 1 \leq j \leq n\})$.

   Varieties are not closed under infinite unions. For instance $V_i := \{i\} \subseteq \mathbb{Q}$ are singleton varieties for $i \in \mathbb{Z}$, however their union $\mathbb{Z}$ is not a variety.

3. No. For instance nonempty finite sets are varieties of $\overline{\mathbb{Q}}$, however their complements are not.

□

Exercise 15. For each direction of the statements below, prove it if it holds, or find a counter-example otherwise.

1. For sets $A, B \subseteq \overline{\mathbb{Q}}^d$: $A \subseteq B$ iff $I(B) \subseteq I(A)$.
2. For sets of polynomials $P, Q \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_d]$: $P \subseteq Q$ iff $V(Q) \subseteq V(P)$.
3. For varieties $U, V \subseteq \overline{\mathbb{Q}}^d$: $U \subseteq V$ iff $I(V) \subseteq I(U)$.

Solution: 1. The "only if" direction clearly holds. The other direction is false: For $d = 1$, $A = \mathbb{Q}$ and $B = \mathbb{Z}$ generate the same (trivial) ideal $I = \{0\}$

2. The "only if" direction clearly holds. The other direction is false, *even for ideals*: Take $d = 1$, $P = \langle x \rangle$, $Q = \langle x^2 \rangle$ s.t. $V(Q) = V(P) = \{0\}$ but $x \in P \setminus Q$.

3. We just need to check the "if" direction. Let $U = V(I)$ and $V = V(J)$ for polynomial ideals I, J which can be chosen to be radical, so that $I(U) = I$ and $I(V) = J$. Thus we have $J \subseteq I$, and we conclude $U \subseteq V$ by the previous point.

□

Exercise 16. Consider the set of states $V_n \subseteq Q$ which give zero after reading words of length $\leq n$:

$$V_n = \left\{ q \in Q \mid \forall w \in \Sigma^{\leq n} : [\![q]\!]_w = 0 \right\}.$$

1. Show that the automaton is zero iff $q_I \in \bigcap_n V_n$.
2. Show that $V_0 \supseteq V_1 \supseteq \cdots \supseteq \bigcap_n V_n$ is a nonincreasing chain of varieties.
3. Conclude that the chain stabilises at some finite level $V_N = V_{N+1} = \cdots = \bigcap_n V_n$.

Solution: The first point is clear. For the second point, V_0 is a variety since $V_0 = F^{-1}(\{0\})$, $\{0\}$ is a variety, and inverse polynomial maps preserve varieties. Then inductively

$$V_{n+1} = V_n \cap \bigcap_{a \in \Sigma} a^{-1} V_n$$

is also a variety since varieties are closed under intersection and inverse images of polynomial maps. To the nonincreasing chain of varieties we associate a nondecreasing chain of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_d], \quad \text{with } I_i := I(V_i) \text{ for all } i \in \mathbb{N}.$$

By Hilbert finite basis theorem, there is $N \in \mathbb{N}$ s.t.$I_N = I_{N+1} = \cdots$. Since $I(U) = I(V)$ implies $U = V$ for any two varieties U, V, we have $V_N = V_{N+1} = \cdots$. □

Exercise 17. Provide a coRP algorithm (randomised polynomial time) for the following problem: Given a polynomial automaton A and an input word $w \in \Sigma^*$, decide whether $[\![A]\!]_w = 0$.

Solution: We can write an arithmetic circuit of polynomial size computing $[\![A]\!]_w$. We then invoke the fact that zeroness testing is in coRP (this a special case of polynomial identity testing). □

Exercise 18. Give an algorithm for the following problem: In input we are given a polynomial automaton A and a finite automaton B recognising a regular language $L \subseteq \Sigma^*$. In output we answer whether for every $w \in L$ we have $[\![A]\!]_w = 0$.

Solution: We can assume B is deterministic, so that as a weighted automaton it takes values in $\{0, 1\}$. We then take the Hadamard product C of A and B, which is again a polynomial automaton, whose support is the intersection of supports. This means that no counter-example to zeroness is lost. We then solve zeroness for C. □