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* $I \subseteq R$ of a ring R is a set which is 1) closed under sum $I + I \subseteq I$, and 2) closed under under product with the whole ring $I \cdot R = R \cdot I \subseteq I$. 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. 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. □

Exercise 4. We say that a ring is *k-bounded* if every ideal is generated by at most k elements, and *bounded* if it is k-bounded for some $k > 0$. For each of the following rings, decide whether it is bounded.

1. $\mathbb{Z}[x]$.
2. $\mathbb{Q}[x, y]$.
3. $\mathbb{Q}[x, y]/\langle x^2, xy, y^2 \rangle$.

Solution:

1. No. Fix $k > 0$ and consider the ideal... TODO
2. No. Fix $k > 0$ and consider the ideal $\langle x^k y^0, x^{k-1} y^1, \ldots, x^0 y^k \rangle$. It is not possible to generate this ideal with $\leq k$ elements.
3. Yes. The ring is in fact a three-dimensional algebra over $\mathbb{Q}$, where we identify $a \cdot x + b \cdot y + c$ with the triple (a, b, c). This means that every ideal of the ring is generated by at most three elements since sets with at least four elements are linearly dependent.

□

Exercise 5. Are the following rings Noetherian?

1. Ring of polynomials with countably many variables: $\mathbb{Q}[x_1, x_2, \ldots]$.
2. Ring of power series: $\mathbb{Q}[\![x]\!]$.
3. Ring of power series over the integers: $\mathbb{Z}[\![x]\!]$.
4. Ring of rational power series: $\mathbb{Q}[\![x]\!] \cap \mathbb{Q}(x)$.
5. Ring of rational power series over the integers: $\mathbb{Z}[\![x]\!] \cap \mathbb{Q}(x)$.

Solution:

1. No. The ideal $\langle x_1, x_2, \ldots \rangle$ is not finitely generated.
2. Yes. 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, that 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, but this is more difficult. TODO
4. Yes, since this is in fact a field and all fields are Noetherian since they have finitely many ideals (in fact just two).

5. Yes, but this is more difficult. TODO

□

Exercise 6. For every of the following sets $\mathbb{Q}[x] \subseteq A \subseteq \mathbb{Q}[x, y]$ check that A is a ring. Is A Noetherian?

1. $A = 1 + x \cdot \mathbb{Q}[x, y]$.
2. $A = \mathbb{Z} + x \cdot \mathbb{Q}[x]$.
3. $A = xy \cdot \mathbb{Q}[x, y]$.

Solution: 1. No.

2. No.
3. Yes?

□

Exercise 7.

Solution: □