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* $I \subseteq R := \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ 1) contains the zero polynomial $0 \in I$, 2) it is closed under sum $I + I \subseteq I$, and 3) it is closed 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 an 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 nonzero univariate polynomials only 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 $x \in \mathbb{F}_2$. $\square$

Exercise 3.

Solution: $\square$