Languages, automata and computation II
Tutorial 5

Winter semester 2023/2024

In this tutorial we study well-quasi orders with some applications in theoretical computer science.

Well-quasi orders

Exercise 1. Let $(X, \preceq)$ be a preorder (a.k.a. quasi-order). Show that the following conditions are equivalent.

1. Every infinite sequence $x_1, x_2, \dots \in X$ contains a *domination*: $x_i \preceq x_j$ for some $i < j$.
2. Every infinite sequence $x_1, x_2, \dots \in X$ contains a *monotone infinite subsequence*: $x_{i_1} \preceq x_{i_2} \preceq \cdots$ for some $i_1 < i_2 < \cdots$.
3. $(X, \preceq)$ is *well-founded* (no infinite strictly decreasing sequences $x_1 \succ x_2 \succ \cdots$) and all *antichains are finite* (an antichain is a set of pairwise incomparable elements).
4. Every upward closed set is the upward closure of a finite set.
5. Every nondecreasing chain of upward closed sets $U_1 \subseteq U_2 \subseteq \cdots \subseteq X$ is finite.

Solution: $(1 \Rightarrow 2)$ Assume each x_i is dominated by finitely many elements to its right. We can then take the subsequence of elements which are not dominated by any element to their right. This sequence is infinite and does not have any domination by construction.
$(2 \Rightarrow 1)$ This is trivial.
$(1 \Rightarrow 3)$ Well-foundedness is obvious. Now consider an antichain $A \subseteq X$. If it is infinite, then we arrange its elements into an infinite sequence. By the assumption we can find (in particular) a domination, contradicting that A is an antichain.
$(3 \Rightarrow 1)$ Consider the set of minimal elements of the infinite sequence. This is an antichain, so it must be finite. Take any element in the sequence not from this finite set, and it is preceded by a smaller element, yielding a domination.
$(3 \Rightarrow 4)$ Let $U \subseteq X$ be upward closed and consider the subset of its elements M which are not dominated by any element in U (minimal elements). Clearly U is the upward closure of M and the latter set is an antichain, thus finite by assumption.

(4 $\Rightarrow$ 3) Clearly antichains must be finite. Regarding well-foundedness, by way of contradiction assume we have an infinite strictly decreasing sequence $x_1 \succ x_2 \succ \cdots$. Then the upward closure of its elements is not the upward closure of a finite set, which is a contradiction.
(4 $\Rightarrow$ 5) The upward closed set $U_1 \cup U_2 \cup \cdots$. By assumption it is the upward closure of finitely many elements $B = \{x_1, \dots, x_n\}$. Take the first U_n s.t. $B \subseteq U_n$ and we have $U_n = U_{n+1} = \cdots$.
(5 $\Rightarrow$ 4) Let $U \subseteq X$ be an upward closed set and consider the set of its minimal elements $M = \{x_1, x_2, \dots\}$ (if there are ties just select arbitrarily an element from each minimal equivalence class). Now consider the chain generated by the upward closure of $\{x_1\}$, $\{x_1, x_2\}$, etc. By assumption, this chain is finite, therefore there is n s.t. the upward closure of $\{x_1, \dots, x_n\}$ is the same as that of M itself, which is just X. □

Exercise 2. Which of the following preorders are well-quasi orders?

1. $\mathbb{N}^2$ with the lexicographic order;
2. $\{a, b\}^*$ with the lexicographic order;
3. $\mathbb{N}$ with the divisibility partial order;
4. $\{a, b\}^*$ with the prefix order;
5. $\{a, b\}^*$ with the infix order;
6. intervals of $\mathbb{N}$ with the following order:
$$[a, b] \preceq [c, d] \quad \text{if } b < c \vee (a = c \wedge b \leq d);$$
7. graphs with the subgraph order (remove some edges and some vertices).

Solution: 1. Yes, by Dickson's lemma even the smaller pointwise order is a wqo.
2. No, we have the ill-founded sequence $b \succ ab \succ aab \succ \cdots$.
3. No, the set of primes forms an infinite antichain.
4. No, we have the infinite antichain $\{a, ba, bba, \dots\}$.
5. No, we have the infinite antichain $\{aba, abba, abbba, \dots\}$.
6. Yes. The order is well-founded since $[a, b] \prec [c, d]$ implies $a + b < c + d$ in $\mathbb{N}$. There are no infinite antichains: By way of contradiction, let A be an infinite antichain. Fix an element $[a, b] \in A$. Now look at some other $[c, d] \in A$. Since these two elements are incomparable, from the first condition we have $0 \leq c \leq b$. This yields only finitely many options for c, so there must be two elements $[c, d_1]$ and $[c, d_2]$ in A, which are comparable, yielding a contradiction.
7. No. The order is well-founded by it contains the infinite antichain consisting of cycles of length 2, of length 3, etc. □

Exercise 3. Show that if $(X, \preceq_X)$ and $(Y, \preceq_Y)$ are well-quasi orders, then the following are also well-quasi orders:

1. The *product order* $(X \times Y, \preceq_{X \times Y})$, where
$$(x_0, y_0) \preceq_{X \times Y} (x_1, y_1) \text{ if } x_0 \preceq_X x_1 \text{ and } y_0 \preceq_Y y_1.$$
Deduce Dickson's lemma on $\mathbb{N}^k$.

2. The *subword order* $(X^*, \preceq_{X^*})$, where

$$x_0 \cdots x_m \preceq_X^* y_0 \cdots y_n$$

if there exists a subsequence $y_{i_0}, \ldots, y_{i_m}$ s.t. $x_0 \preceq_X y_{i_0}, \ldots, x_m \preceq_X y_{i_m}$. Deduce Higman's lemma on Σ^*.

3. What about the suborder over infinite words $(X^\omega, \preceq_{X^\omega})$?

Solution: 1. Let $(x_0, y_0), (x_1, y_1), \ldots$ be an infinite sequence in $X \times Y$. By looking at the first component we can find an infinite monotone subsequence $x_{i_0} \preceq_X x_{i_1} \preceq_X \cdots$. Now we look at the second component $y_{i_0}, y_{i_1}, \cdots \in Y$ and we can find a domination $y_{i_j} \preceq_Y y_{i_k}$. We thus get the required domination in the product order $\left(x_{i_j}, y_{i_j}\right) \preceq_{X \times Y} (x_{i_k}, y_{i_k})$.
2. Call a sequence $u_0, u_1, \ldots$ *bad* if there is no domination $u_i \preceq^* u_j$ with $i < j$. By way of contradiction, assume we have a bad sequence as above. We can also assume that each u_n has minimal length amongst all bad sequences starting with the same prefix $u_0, \ldots, u_n$. Since not u_n can be empty, we can write $v_n := a_n \cdot u_n$. By the well quasi ordering on X, there is an infinite ordered subsequence

$$a_{n_0} \preceq_X a_{n_1} \preceq_X \cdots .$$

Consider now the new sequence

$$u_0, u_1, \ldots, u_{n_0 - 1}, v_{n_0}, v_{n_1}, \ldots .$$

This sequence is bad, since a domination therein would result in a domination in the original sequence, and it is not minimal since v_{n_0} is strictly shorter than u_{n_0}, leading to a contradiction.
3. The new quasi-order $\preceq_{X^\omega}$ needs not be a well-quasi order. TODO. □

Applications

Exercise 4. Let V be a d-dimensional VASS and consider a target configuration $t \in P \times \mathbb{N}^d$, where P is a finite set of control locations. Show that one can compute the set of *all configurations* s which can cover t.

Solution: Consider the following chain of sets:

$$U_0 \subseteq U_1 \subseteq \cdots \subseteq \mathbb{N}^d,$$

where U_n is the set of all configurations that can cover s is $\leq n$ steps. Order configurations by $(p, \bar{x}) \leq (q, \bar{y})$ if $p = q$ and $\bar{x} \leq_{\mathbb{N}^k} \bar{y}$. This is a well quasi order. Clearly, U_n is upward closed w.r.t. "$\leq$". It follows that the chain terminates, yielding finitely many minimally elements $B = \{s_1, \ldots, s_m\}$ whose upward closure generates $\bigcup_n U_n$. One can thus guess B and for element $s_i \in B$ thereof check that the set of one-step predecessors of s_i (finitely many) is in the upward closure of B. □

Exercise 5. Let V be a d-dimensional VASS and consider a source configuration $s \in \mathbb{N}^d$. Show that one decide whether there are only *finitely many* configurations reachable from s.

Solution: Consider the following *reachability tree*. The root is labelled by the initial configuration $s \in \mathbb{N}^d$. Whenever a node is labelled by a configuration $x \in \mathbb{N}^d$ and there is a transition $x \to x + v$ with $v \in V$, then this node has a children node labelled with $x+v$. The reachability tree is infinite in general. We now prune the reachability tree as follows. On every infinite branch, stop as long as a configuration y has a smaller ancestor $x \geq y$. We call this a *domination*. In this way all branches become finite. Since the tree is finitely branching, overall we get a finite tree by König's lemma. There are infinitely many reachable configurations iff there is a strict domination $y \geq x$ with $y \neq x$. □

In the next exercise we apply well-quasi orders to deciding the universality problem of nonguessing register automata with one register, over equality atoms. Since the problem is undecidable for two registers, or one register with guessing, this completes the decidability border for the universality problem of register automata.

Exercise 6. Consider a nonguessing register automaton with one register, control locations in L, initial locations $I \subseteq L$, and final locations $F \subseteq L$. The set of *states* is $S = L \times \mathbb{A}_\perp$ and the set of *macrostates* is $M = 2^S_{\mathrm{fin}}$. For two macrostates $P, Q \in M$, write $P \to Q$ if there exists an input letter $a \in \mathbb{A}$ s.t.

$$Q = \left\{ q \in S \mid p \xrightarrow{a} q \text{ for some } p \in P \right\}.$$

1. A macrostate is *rejecting* if it does not intersect $F \times \mathbb{A}_\perp$. Argue that the automaton is not universal iff there is a rejecting macrostate Q s.t. $I \times \{\perp\} \to^* Q$.

2. A *simulation relation* on macrostates is a binary relation $\sqsubseteq \subseteq M \times M$ s.t. for every macrostate $P, Q \in M$ with $P \sqsubseteq Q$:

   (a) Q rejecting implies P rejecting, and

   (b) for all $Q \to Q'$ there is $P \to P'$ s.t. $P' \sqsubseteq Q'$.

   Show that $\subseteq$ is a simulation relation on macrostates. Is it a well quasi order?

3. For two macrostates P, Q, write $P \leq Q$ iff there is an atom automorphism α s.t. $\alpha(P) \subseteq Q$. Show that $\leq$ is a simulation relation on macrostates.

4. Show that $\leq$ is a well quasi order.

5. Show that $\leq$ is decidable.

6. Deduce an algorithm to decide the universality problem.

Solution: 1. This is clear.

2. This is also clear. It is not a well quasi order since there are infinite antichains such as $\{\{(q, a_1)\}, \{(q, a_2)\}, \ldots\}$.

3. Let $P \leq Q$ and $Q \to Q'$. There is an automorphism α s.t. $\alpha(P) \subseteq Q$ Since $\subseteq$ is a simulation, there is $P' \subseteq Q'$ s.t. $\alpha(P) \to P'$. Since α is an automorphism, we can apply its inverse to both sides of $\alpha(P) \to P'$ and we obtain $P \to \alpha^{-1}(P')$. If we define $P'' := \alpha^{-1}(P')$ we have $P'' \leq Q'$.

4. For a macrostate P and a location $\ell \in L$, let $\mathsf{atoms}(P, \ell) = \{a \in \mathbb{A} \mid (\ell, a) \in P\}$ be the set of atoms appearing with location ℓ in P. The *profile* of a macrostate P records the following information:

1. For each control location $\ell \in L$ of P, whether $(\ell, \perp)$ is in P.
2. For each nonempty set of control locations $Z \subseteq L$ of P, the number of distinct atoms jointly appearing in Z,

$$|\mathsf{atoms}(Z)|, \quad \text{where } \mathsf{atoms}(P, Z) := \bigcap_{\ell \in Z} \mathsf{atoms}(P, \ell).$$

Let $\mathsf{profile}(P) \in 2^L \times \mathbb{N}^{2^L \setminus \{\emptyset\}}$ be the profile of P. Let $\mathsf{profile}(P) \preceq \mathsf{profile}(Q)$ with subset inclusion in the first component and point-wise ordering in the second one. Clearly atom renamings do not change the profile $\mathsf{profile}(P) = \mathsf{profile}(\alpha(P))$ and $P \subseteq Q$ implies $\mathsf{profile}(P) \preceq \mathsf{profile}(Q)$. Consequently, $P \leq Q$ implies $\mathsf{profile}(P) \preceq \mathsf{profile}(Q)$. In fact, the converse implication holds as well. Let $\mathsf{profile}(P) \preceq \mathsf{profile}(Q)$. Note that sets $\mathsf{atoms}(P, Z)$ as Z ranges over nonempty sets of locations of P form a partition of all atoms appearing in P (and the same for Q). By the ordering on profiles, $\mathsf{atoms}(Q, Z)$ contains at least as many elements as $\mathsf{atoms}(P, Z)$. Build a partial bijection mapping atoms in $\mathsf{atoms}(P, Z)$ to atoms in $\mathsf{atoms}(Q, Z)$, for every Z. Because of the partitioning property, this process does not create naming conflicts wherby two atoms would be mapped to the same atom (by the partitioning on Q) or an atom would be mapped to two atoms (by the partitioning on P). Extend this partial bijection to an automorphism of atoms α and we have $\alpha P \subseteq Q$, as required.

5. By the previous point, we can just decide the ordering on profiles.

6. We build a finite tree labelled with macrostates. The root is labelled with the initial macrostate $I \times \{\perp\}$. If a node is labelled with a macrostate P and $P \to Q_1, \ldots, Q_n$ are all successors of P, then there are n children labelled with $Q_1, \ldots, Q_n$. If we find a node labelled with a rejecting macrostate, then we halt and declare that the automaton is not universal. If on the same branch we find two nodes labelled with macrostates $P \leq Q$, then we do not further explore the tree from Q. (This is correct: If Q can reach a rejecting macrostate, so can P.) Finally, if we cannot further extend the tree, then we declare that the automaton is universal.

The previous algorithm was based on *forward reachability*. We now present an alternative *backward reachability* algorithm. A macrostate is *accepting* if it contains some accepting state $(p, \_)$ with $p \in F$. The set of accepting macrostates is upward closed. Let U_n be the set of all macrostates necessarily reaching an accepting macrostate after $\leq n$ steps. In other words, U_0 is the set of accepting macrostates and if we define the *controller predecessor opertor*

$$\mathsf{pre}^{-1}(U) := \{P \in M \mid P \to Q \text{ implies } Q \in U\},$$

we can write

$$U_{n+1} = U_n \cup \mathsf{pre}^{-1}(U_n).$$

This gives rise to an nondecreasing chain of upward closed sets $U_0 \subseteq U_1 \subseteq \cdots$. It stabilises after finitely many steps at some $U_N = U_{N+1}$, we can detect this, and the automaton is universal if the initial macrostate is in U_N. □

Exercise 7. A *rewrite system* over a finite alphabet Σ is a finite set of pairs $u \to v$ with $u, v \in \Sigma^*$. Consider the least reflexive and transitive congruence $\to^*$ on Σ^* containing $\to$. A rewrite system is *lossy* if it contains transitions $a \to \varepsilon$ for every $a \in \Sigma$. Show that the relation $\to^*$ is decidable when $\to$ is lossy.

Solution: For a set of configurations $X \in \Sigma^*$, let $\mathsf{pre}^*(X)$ be the set of all configurations y which can reach some configuration $x \in X$, i.e., $y \to^* x$. We want to decide whether for given configurations x, y we have $x \in \mathsf{pre}^*(\{y\})$. Notice that $\mathsf{pre}^*(X)$ is upward closed *for every* X. Indeed, for two configurations $x \preceq^* y$ (in the Higman ordering) we have $y \to^* x$ by dropping all additional letters. Consequently, $x \to^* X$ and $x \preceq^* y$ implies $y \to^* x \to^* X$. In particular $\mathsf{pre}^*(\{y\})$ is upward closed and we can compute a finite basis B for it. If $x \in \mathsf{pre}^*(\{y\})$ then just find a path witnessing this. If $x \notin \mathsf{pre}^*(\{y\})$, then verify $x \notin B\uparrow$ by just checking that x does not dominate any element in the basis. $\square$

$\mathbb{Z}$-VASSes

This part is unrelated with well quasi orders. We show that reachability in VASSes is considerably simpler if we relax the requirement that counters cannot become negative.

Exercise 8. Let a $\mathbb{Z}$-*VASS* of dimension $d \in \mathbb{N}$ be a finite set of location-vector pairs $V \subseteq_{\text{fin}} L \times \mathbb{Z}^d$. The semantics is as in VASS, except that now configurations are in $L \times \mathbb{Z}^d$ (instead of the more restrictive $L \times \mathbb{N}^d$). Show that reachability is decidable for $\mathbb{Z}$-VASSes.

Solution: The case without states (control locations) $|L| = 1$ easily reduces to integer linear programming. If $|L| \geq 2$, then we need to additionally ensure that the number of times we enter a control location is the same as the number of times we exit it, plus or minus one when the location is the initial, resp., final one. $\square$