CR15: Logics, Automata and Games for Advanced Verification

Midterm homework - Solutions

Denis Kuperberg and Matteo Mio

Exercise 1

1. Is it decidable whether a NFA recognize a finite language ?
2. Same question with NBA instead of NFA.

1.
Let $\mathcal{A} = (\Sigma, Q, q_0, F, \Delta)$ be the input NFA, and $n = |Q|$. If $p, q \in Q$, we will note $p \to^* q$ if there is a possibly empty path from p to q, and $p \to^+ q$ if there is a non-empty path from p to q.
We show that $L(\mathcal{A})$ is infinite if and only if there is $(q, q_f) \in Q \times F$ such that there is a path of the form $q_0 \to^* q \to^+ q \to^* q_f$ in $\mathcal{A}$.
First, assume, that such a path exists. Let $(u, v, w) \in \Sigma^* \times \Sigma^+ \times \Sigma^*$ be the words labelling the three subpaths $q_i \to^* q$, $q \to^+ q$, and $q \to^* q_f$, respectively. Then we have $uv^*w \subseteq L(\mathcal{A})$, so $L(\mathcal{A})$ is infinite.
Conversely, assume u is infinite. Then it contains a word u with $|u| \geq n+1$. Any accepting run on u must contain a repeated state, and is therefore a path of the wanted form.
Therefore, checking finiteness of $L(\mathcal{A})$ amounts to checking the existence of a path of the above form, which can be done in NL (nondeterministic logarithmic space).

2.
Let $\mathcal{A} = (\Sigma, Q, q_0, F, \Delta)$ be the input NFA, $n = |Q|$ and $L = L(\mathcal{A})$.
For all $k \in \mathbb{N}$, let $P_k = \{u \in \Sigma^k \mid \exists w \in \Sigma^\omega, uw \in L\}$ be the set of prefixes of length k of words in L. Notice that $|P_k| \leq |P_{k+1}|$ for all k, and $|L| = \sup_{k \in \mathbb{N}} |P_k|$. Moreover, $|P_k| < |P_{k+1}|$ if and only if there exists $(u, a, b) \in \Sigma^k \times \Sigma \times \Sigma$ such that $ua, ub \in P_{k+1}$ and $a \neq b$.

Lemma 1. *L is finite if and only if $|P_{n^2}| = |P_{2n^2}|$.*

Proof. If L has at most one word the result is trivial. Assume L is finite with at least two words, and let k be minimal such that $|L| = |P_k|$. Since $|P_k| > |P_{k-1}|$, there are words $ua_1, ua_2 \in P_k$ with $|u| = k-1$, and a_1, a_2 distincts letters. Let $p_0, p_1, p_2, p_3 \dots$ (resp. $q_0, q_1, q_2 \dots$) be an accepting run of $\mathcal{A}$ on ua_1w_1 for some $w_1 \in \Sigma^\omega$ (resp. on ua_2w_2). If $k > n^2$, then $|u| \geq n^2$, so there exists $i < j < |u|$ such that $(p_i, q_i) = (p_j, q_j)$. By iterating this loop twice, we obtain a word u' with $|u'| > |u|$ such that $u'a_1, u'a_2 \in P_{k'}$, with $k' > k$. This implies $|P_{k'}| > |P_k|$, which is absurd because $|P_k| = |L| \geq |P_{k'}|$. So we must have $k \leq n^2$, and thus $|L| = |P_{n^2}| = |P_{2n^2}|$.
Conversely, assume that L is infinite. We show it implies $|P_{n^2}| < |P_{2n^2}|$. Since L is infinite, there exists $ua_1w_1, ua_2w_2 \in L$ with $|u| \geq n^2$, $a_1, a_2 \in \Sigma$, $w_1, w_2 \in \Sigma^\omega$, and $a_1 \neq a_2$. We choose u to be of minimal length with this property (still imposing $|u| \geq n^2$). As before, let $(p_i)_{i \in \mathbb{N}}$ and $(q_i)_{i \in \mathbb{N}}$ be runs witnessing $ua_1w_1 \in L$ and $ua_2w_2 \in L$ respectively. If $|u| > 2n^2$, we can find $i < j$ in $[n^2, 2n^2]$ such that $(p_i, q_i) = (p_j, q_j)$. By removing this loop, we obtain u' smaller than u satisfying the above property, so this contradicts minimality of u. This means $|u| \leq 2n^2$, and thus the pair ua, ub is a witness that $|P_{n^2}| < |P_{2n^2}|$. □

It now suffices to verify that we can decide the above property. Actually it is even decidable in NL, using the following algorithm:
Guess u of length in $[n^2, 2n^2]$ and follow two simultaneous paths in $\mathcal{A}$ over u on the fly: starting from (q_0, q_0) and just remembering the current pair of states and the number of steps already

performed. This leads to states (p, q). Then guess letters $a \neq b$ and transitions (p, a, p'), (q, a, q') in Δ. Finally, guess accepting lassos from p' and q' (not synchronized), witnessing that ua and ub can be extended to words in L.
This algorithm actually looks for a witness that $|P_{n^2}| < |P_{2n^2}|$, so it decides whether L is infinite in NL. But since NL is closed under complement, we obtain that deciding finiteness of a language given by a NBA is in NL.

Exercise 2
Given an ω-word $w \in \{0,1\}^\omega$, we note $|w|_1$ the number of 1's in w, so $|w|_1 \in \mathbb{N} \cup \{\infty\}$.
If $w = a_0 a_1 \dots$ and $w' = b_0 b_1 \dots$ are in $\{0,1\}^\omega$, we note $\langle w, w' \rangle := (a_0, b_0)(a_1, b_1) \cdots \in \{0,1\}^2$.

1. Is the language $\{\langle w, w' \rangle \mid |w|_1 = |w'|_1\}$ ω-regular ?
2. Is the language $\{w \mid |w|_1$ is a power of $2\}$ ω-regular ?

1.
Assume there is a NBA $\mathcal{A}$ with n states for this language L. Let $u = 0^n 1^n 0^\omega$ and $v = 1^n 0^\omega$. Then $\langle u, v \rangle \in L$, witnessed by an accepting run $(p_i)_{i \in \mathbb{N}}$. But there are $i < j \leq n$ such that $p_i = p_j$. Let $m = n + j - 1$. By repeating the loop from p_i to p_j twice, we obtain an accepting run on $\langle 0^m 1^n 0^\omega, 1^m 0^\omega \rangle$, which is absurd since $m \neq n$. Therefore, L is not ω-regular.

2.
Assume there is a NBA $\mathcal{A}$ with n states for this language P. Let $u = 1^{2^n} 0^\omega$, and $(p_i)_{i \in \mathbb{N}}$ be an accepting run of $\mathcal{A}$ on u. There exists $i < j < 2^n$ such that $p_i = p_j$, so by repeating this loop we can build an accepting run of $\mathcal{A}$ on $u' = 1^{2^n + (j-i)} 0^\omega$. Since $j - i < 2^n$, $u' \notin P$ and we have a contradiction.

Exercise 3
If $L \subseteq \Sigma^*$ is a language, we define $\mathit{Sqrt}(L) = \{u \mid uu \in L\}$.

1. Show that if L is regular then $\mathit{Sqrt}(L)$ is regular *(hint: use finite monoids)*.
2. Show that if L is FO-definable then $\mathit{Sqrt}(L)$ is FO-definable.
3. Same questions with $\mathit{Root}(L) = \{u \mid u^n \in L$ for some $n \in \mathbb{N}\}$.

1.
Let M be a finite monoid, $h : \Sigma \to M$ and $P \subseteq M$ such that (M, h, P) recognizes L. Let $P' = \{m \in M \mid m \cdot m \in P\}$. We extend h to $\Sigma^* \to M$ as usual. Then for any word $w \in \Sigma^*$, we have $w \in \mathit{Sqrt}(L) \Leftrightarrow ww \in L \Leftrightarrow h(ww) \in P \Leftrightarrow h(w)h(w) \in P \Leftrightarrow h(w) \in P'$. This means that (M, h, P') recognizes $\mathit{Sqrt}(L)$, and therefore $\mathit{Sqrt}(L)$ is regular.
2.
We saw that L is FO-definable if and only if it is recognized by an aperiodic monoid. Taking M aperiodic in the above construction shows that $\mathit{Sqrt}(L)$ is also recognized by the same aperiodic monoid, and is therefore FO-definable.
3.
Same construction with $P' = \{m \in M \mid \exists n \in \mathbb{N}, m^n \in P\}$.

Exercise 4
We add to MSO on finite words a quantifier $\exists^n$ for each $n \in \mathbb{N}$. The formula $\exists^n x.\varphi(x)$ is true if and only if the number of positions x such that $\varphi(x)$ is true is a multiple of n. Let us call MSO(Mod) this new logic.

1. Show that MSO(Mod) is expressively equivalent to MSO(ModPrime), where only quantifiers $\exists^p$ with p prime are used.
2. Show that MSO(Mod) is expressively equivalent to MSO.

1.
Disclaimer: It is trivial to notice that answering question 2 also answers question 1. The intention of question 1 was to solve it without the technique of question 2. I will therefore show here a "stronger" result: FO(Mod) is expressively equivalent to FO(ModPrime). This forces to use other techniques than in question 2. No points will be removed for students that only solved question 2.
First, notice that it is enough to have quantifiers for prime powers, since for any $n \in \mathbb{N}$, if we consider its decomposition into prime factors $n = \prod_{i \in I} p_i^{\alpha_i}$, by the chinese remainder theorem we have the following equivalence:

$$\exists^n x.\varphi(x) \equiv \bigwedge_{i \in I} \exists^{p_i^{\alpha_i}} x.\varphi(x).$$

Fix a prime p, we show by induction on α that $\exists^{p^\alpha}$ is expressible in FO(ModPrime) for any $\alpha \geq 1$. For $\alpha = 1$ it is trivial.
We can conclude thanks to the following lemma:

Lemma 2. *Let p be a prime number, $\alpha \geq 1$, and φ a formula. Let*

$$\psi = \exists^p y.(\varphi(y) \wedge \exists^{p^\alpha} x.(x \leq y) \wedge \varphi(x)).$$

Then we have $\exists^{p^{\alpha+1}} x.\varphi(x) \equiv \psi \wedge \exists p^\alpha x.\varphi(x)$.

Proof. First, assume $\exists^{p^{\alpha+1}} x.\varphi(x)$ is true, and let $X = \{x_1, x_2, \ldots, x_{mp^{\alpha+1}}\}$ be the set of positions where $\varphi(x)$ is true, numbered in increasing order. Then ψ is true, witnessed by the set $Y = \{x_i \mid i \equiv 0[p^\alpha]\}$ of cardinal mp. Indeed, if $y = x_{kp^\alpha} \in Y$, then the set $X_y = \{x \mid x \leq y \wedge \varphi(x)\}$ is equal to $\{x_1, x_2, \ldots, x_{kp^\alpha}\}$ so it satisfies the constraint in formula ψ. No other positions than those in Y satisfy this constraint, as the set X_y would not have a required cardinality. Moreover, $\exists p^\alpha x.\varphi(x)$ is also true, as $mp^{\alpha+1}$ is a multiple of p^α.
Conversely, assume ψ is true, witnessed by a set $Y = \{y_1, y_2, \ldots y_{mp}\}$, and $\exists p^\alpha x.\varphi(x)$ is also true. Consider the set $X = \{x_1, x_2, \ldots, x_{np^\alpha}\}$ where $\varphi(x)$ is true. Both sets are numbered in increasing order. By definition, for all i, y_i is the i^{th} position where φ is true, and such that the cardinal of $\{x \in X \mid x \leq y\}$ is a multiple of p^α. This means $y_i = x_{ip^\alpha}$ for all i. Since the last element x_{np^α} is such a position, we have $y_{mp} = x_{np^\alpha}$, so $n = mp$. Thus $|X| = (mp)p^\alpha$ is a multiple of $p^{\alpha+1}$, and therefore $\exists^{p^{\alpha+1}} x.\varphi(x)$ is true. □

2.
We show the following equivalence:

$$\begin{aligned}\exists^n x.\varphi(x) \equiv \quad & \exists X_1, X_2, \ldots, X_n. \\ & \forall x.[(\varphi(x) \Leftrightarrow \bigvee_{1 \leq i \leq n} x \in X_i) \wedge \bigwedge_{1 \leq i < j \leq n} \neg(x \in X_i \wedge x \in X_j)] \\ & \wedge \bigwedge_{i \neq j} \forall x, y.(Cons(x, y, X_i) \Rightarrow \exists! z \in X_j.x < z < y)\end{aligned}$$

Where $\exists! z \in X_j$ is syntactic sugar for "there exists a unique z in X_j", $x < z < y$ is shorthand for $x < z \wedge z < y$, and $Cons(x, y, X_i)$ means that x and y are consecutive in X_i, defined by $Cons(x, y, X_i) := x \in X_i \wedge y \in X_i \wedge x < y \wedge \neg(\exists t \in X_i, x < t < y)$.
The first line expresses that the X_i form a partition of $X := \{x \mid \varphi(x) \text{ is true}\}$, and the last one forces them to be regularly interleaved, i.e. the interval between two positions in X_i contains exactly one position of X_j, for any $i \neq j$. Since the existence of such a partition is equivalent to the fact that $|X|$ is a multiple of n, we obtain the wanted equivalence.

Exercise 5
An NFA $\mathcal{A} = (\Sigma, Q, q_0, F, \Delta)$ is said history-deterministic if there is a function $\tau : \Sigma^* \to Q$ such that for any word $u = a_1 a_2 \dots a_n \in L(\mathcal{A})$, the sequence $\tau(\epsilon)\tau(a_1)\tau(a_1 a_2) \dots \tau(u)$ is an accepting run of $\mathcal{A}$ on u. We will assume that $\mathcal{A}$ is complete, i.e. that for any $(p, a) \in Q \times \Sigma$ there is at least one $q \in Q$ such that $(p, a, q) \in \Delta$, by addink a rejecting sink state if necessary.

1. Show that if an NFA $\mathcal{A}$ is history-deterministic, its strategy τ can be replaced by a strategy $\sigma : Q \times \Sigma \to Q$, needing only the current state and letter to choose the next state, but ignoring the rest of the history. *(hint: associate to each state q the language $L(q)$ accepted from this state).*

2. We informally describe the safety game $G_{\mathcal{A}}$, played on $\mathcal{A} \times \mathcal{A}$, as follows:

Start in position (q_0, q_0), and at each round from (p, q):
-Adam chooses a letter $a \in \Sigma$
-Eve chooses a transition $(p, a, p') \in \Delta$
-Adam chooses a transition $(q, a, q') \in \Delta$
-The game moves to position (p', q')
The safe region for Eve is $\{(p, q) \mid q \in F \Rightarrow p \in F\}$.

   - Give a formal description of the game $G_{\mathcal{A}}$ as $(V_{Eve} \cup V_{Adam}, E)$.
   - Show that an NFA A is history-deterministic if and only if Eve wins $G_{\mathcal{A}}$.

3. Show that it is in PTIME to decide whether an NFA is history-deterministic

4. Show that if an NFA is history-deterministic, it can be determinized in PTIME.

1.
Let $Q_\tau = \{q \in Q \mid \exists u \in \Sigma^*, q = \tau(u)\}$. Notice that $\mathcal{A}$ can be restricted to Q_τ, as any word in the language is accepted via τ using only states from Q_τ.
Let $L = L(\mathcal{A})$, and if $q \in Q$, we note $L(q)$ the language accepted from q in $\mathcal{A}$. If $u \in \Sigma^*$ and $X \subseteq \Sigma^*$, let $u^{-1}X = \{v \in \Sigma^* \mid uv \in X\}$.

Lemma 3. *For all $u \in \Sigma^*$ and $a \in \Sigma$, $L(\tau(ua)) = a^{-1}L(\tau(u))$.*

Proof. Let $p = \tau(u)$ and $q = \tau(ua)$. First, since $(p, a, q) \in \Delta$, we have $L(q) \subseteq a^{-1}L(p)$. Now, assume that there is $v \in a^{-1}L(p) \setminus L(q)$. We have $av \in L(q)$, so $uav \in L$, but since v cannot be accepted from $\tau(ua)$, we also have $\tau(uav) \notin F$. This contradicts the assumption on τ, so we can conclude $L(q) = a^{-1}L(p)$. □

We can now define σ on Q_τ: if $q = \tau(u)$ for some u arbitrarily chosen, we define $\sigma(q, a) = \tau(ua)$. By the above Lemma, for any transition (p, a, q) chosen by σ, we have $L(q) = a^{-1}L(p)$. So if $u \in \Sigma^*$ and $q_0, q_1, \dots q_n$ is the run chosen by σ on $u = a_1, \dots a_n$, we have for each $i \in [1, n]$

$L(q_i) = a_i^{-1}L(q_{i-1})$. This means $L(q_n) = u^{-1}L(q_0)$, so $q_n \in F \Leftrightarrow \epsilon \in u^{-1}L(q_0) \Leftrightarrow u \in L$. Thus, σ is also a correct strategy for accepting all words from L in $\mathcal{A}$.

2.
Let A, E be fresh symbols, $V_{Adam} = (Q \times Q) \cup (Q \times Q \times \Sigma \times \{A\})$ and $V_{Eve} = Q \times Q \times \Sigma \times \{E\}$. The game $G_{\mathcal{A}}$ is played on (V, E) with $V = V_{Eve} \cup V_{Adam}$, and

$$\begin{aligned} E = \quad & \{((p,q),(p,q,a,E)) \mid (p,q,a,E) \in V_{Eve}\} \\ & \cup \{((p,q,a,E),(p',q,a,A)) \mid (p,a,p') \in \Delta, q \in Q\} \\ & \cup \{((p',q,a,A),(p',q')) \mid (q,a,q') \in \Delta, p' \in Q\} \end{aligned}$$

The safety region for Eve is $S = V \setminus \{(p,q) \mid p \notin F \text{ and } q \in F\}$.
Now, assume that $\mathcal{A}$ is history-deterministic. From question 1, this is witnessed by a strategy $\sigma : Q \times \Sigma \to Q$. Define the positional strategy σ_E for Eve in $G_{\mathcal{A}}$ by $\sigma_E(p,q,a,E) = (\sigma(p,a),q,a,A)$. Assume Adam has a strategy to win against σ_E, i.e. he can choose a word u letter by letter and transitions on the second component such that the play reaches $(p,q) \notin S$ when Eve plays according to σ_E. Since $q \in F$, the run built by Adam witnesses that $u \in L$. However, Eve failed to accept u with strategy σ, contradicting the definition of σ. This is absurd, so σ_E is a winning strategy for Eve in $G_{\mathcal{A}}$.
Conversely, assume Eve wins $G_{\mathcal{A}}$. We know safety games are positionally determined, so Eve has a winning strategy of the form $\sigma_E : V_{Eve} \to Q \times Q \times \Sigma \times \{A\}$. We define a strategy σ for building runs in $\mathcal{A}$ by $\sigma(p,a) = \pi_1(\sigma_E(p,p,a,E))$, where π_1 is the projection onto the first component. I.e. to process letter a from state p, we do the same choice of transition as Eve would do from (p,p) in $G_{\mathcal{A}}$. Let $\sigma^* : \Sigma^* \to Q$ be defined inductively by $\sigma^*(\epsilon) = q_0$ and $\sigma^*(ua) = \sigma(\sigma^*(u),a)$.

Lemma 4. *For all $u \in \Sigma^*$, $L(\sigma^*(u)) = u^{-1}L$.*

Proof. First, for any $(p,a,q) \in \Delta$, we have $L(q) \subseteq a^{-1}L(p)$, so by induction on u, we have $L(\sigma^*(u)) \subseteq u^{-1}L$ for all $u \in \Sigma^*$. Now assume for contradiction that there is $u \in \Sigma^*$ such that $L(\sigma^*(u)) \neq u^{-1}L$. We choose u of minimal length with this property. Since $L(\sigma^*(\epsilon)) = \epsilon^{-1}L$, there is $(v,a) \in \Sigma^* \times \Sigma$ such that $u = va$. By minimality of u, we have $L(\sigma^*(v)) = v^{-1}L$. Let $w \in u^{-1}L \setminus L(\sigma^*(u))$, $p = \sigma^*(v)$ and $q = \sigma^*(u)$. Consider the play of $G_{\mathcal{A}}$ where Eve plays σ_E, and Adam plays v and follows all transitions taken by Eve. This play reaches the vertex $(p,p) \in V_{Adam}$. Adam can now move to (p,p,a,E), and according to σ_E, Eve moves to vertex (q,p,a,A). Since $w \in u^{-1}L$, there is a transition $(p,a,q') \in \Delta$ such that $w \in L(q')$. Adam can move to (q,q') and from there play w together with an accepting run on it from q', reaching $q_f \in F$. Answering with σ_E, Eve will reach a state $q'' \notin F$, because it is impossible to accept w from q. This means this play is losing for Eve, contradicting the fact that σ_E is a winning strategy in $G_{\mathcal{A}}$. □

This shows that $\mathcal{A}$ is history-deterministic witnessed by the strategy σ (or σ^*).

3.
By question 2, it suffices to build the safety game $G_{\mathcal{A}}$, which is polynomial in the size of $\mathcal{A}$, and decide its winner, which can be done in linear time in $|G_{\mathcal{A}}|$. We answer that $\mathcal{A}$ is history-deterministic if and only if Eve wins $G_{\mathcal{A}}$.

4.
In the above algorithm, if the answer is Yes, we can also compute a positional winning strategy σ_E for Eve. We saw in the question 2 how to turn this strategy into a witness $\sigma : Q \times \Sigma \to Q$ that $\mathcal{A}$ is history-deterministic, by defining $\sigma(p,a) = \pi_1(\sigma_E(p,p,a,E))$. Restricting $\mathcal{A}$ to the transitions defined by σ yields an equivalent DFA, so this is a PTIME algorithm to determinize an history-deterministic NFA.