Solutions to DM 4

Homework 1. Build the Büchi automaton for the following formulae using the method seen during the course: (1) $\mathsf{G}(a \to (b \,\mathsf{U}\, c))$, and (2) $\mathsf{G}\,\mathsf{F}\,b \to \mathsf{F}\,\mathsf{G}\,a$.

Solution. Too big to do without losing sanity. Apologies for having given this question. □

Homework 2. Give an LTL formula φ_n of size $O(n)$ over $\mathrm{AP} = \{p_0, \ldots, p_{n-1}\}$ that simulates an n-bit counter. To be more precise, the models of φ_n are exactly the infinite words in $(2^{AP})^\omega$ where, at each position i, the valuation of $(p_0, \ldots, p_{n-1})$ encodes an n-bit binary number v_i, and for all $i \geq 0$, $v_{i+1} = (v_i + 1) \pmod{2^n}$.

Also provide a tight lower bound on the size of any equivalent Büchi automaton.

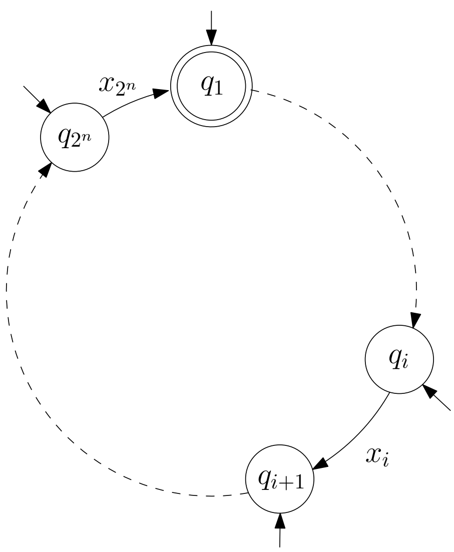
Solution. One possible LTL formula would be

$$\mathsf{G}(p_{n-1} \not\leftrightarrow \mathsf{X}\,p_{n-1}) \wedge \bigwedge_{i=0}^{n-2} \mathsf{G}\left((p_i \not\leftrightarrow \mathsf{X}\,p_i) \leftrightarrow (p_{i+1} \wedge \neg \mathsf{X}\,p_{i+1})\right).$$

Here we assume that if $i < j$ then p_i represents a more significant bit than p_j. Essentially, the LTL formula says that the least significant bit always alternates between words, and that the i-th bit changes only when the $(i+1)$-th bit changes from 1 to 0.

Any corresponding Büchi automaton $\mathcal{A}$ must have at least 2^n states. Assume the contrary. There are exactly 2^n words $\{w_i\}_{1 \leq i \leq 2^n}$ that can be accepted by $\mathcal{A}$; each w_i satisfies the counter behavior and its first letter is interpreted as the binary representation of i. Each word w_i can be written as b_i^ω where $|b_i| = 2^n$. As $\mathcal{A}$ has less than 2^n states, there exist $i \neq j$ and a state q such that the accepting runs of $\mathcal{A}$ on w_i and w_j both reach q after the first iteration of b_i and b_j respectively. It follows that the word $b_i b_j^\omega$ is also accepted by $\mathcal{A}$. However it violates the expected behavior of an n-bit counter, so we have a contradiction.

The lower bound of 2^n is a tight lower bound, as demonstrated by the following automaton where all states are initial states, q_i is the only final state, and $x_i \in 2^{AP}$ is naturally obtained from the n-bit binary representation of i.



□