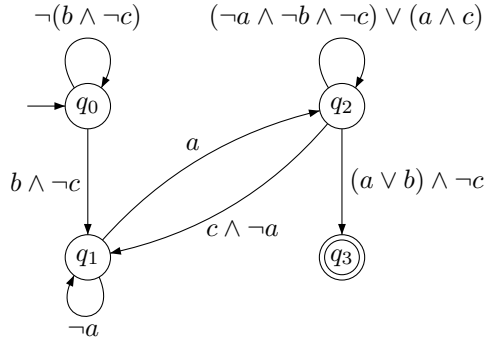


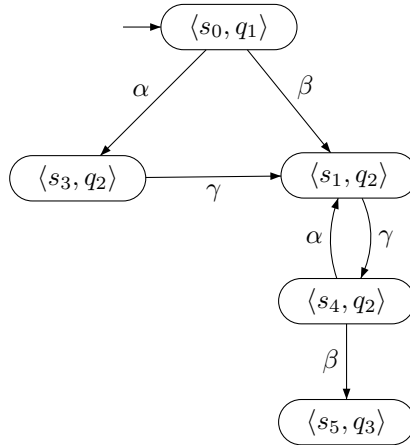
Introduction to Model Checking 2015:

Exercise 4. Solution

Solution 1 • *The NFA that accepts the set of minimal bad prefixes:*



• *First I apply the $TS \otimes \mathcal{A}$ construction which yields:*



A counterexample to $TS \models P_{safe}$ is given by the following initial path fragment in $TS \otimes \mathcal{A}$:

$$\pi_{\otimes} = \langle s_0, q_1 \rangle \langle s_3, q_2 \rangle \langle s_1, q_2 \rangle \langle s_4, q_2 \rangle \langle s_5, q_3 \rangle$$

By projection on the state component, I get a path in the underlying transition system:

$$\pi = s_0 s_3 s_1 s_4 s_5 \text{ with } \text{trace}(\pi) = \{a, b\}\{a, c\}\{a, b, c\}\{a, c\}\{a, b\}$$

Obviously, $\text{trace}(\pi) \in \text{BadPref}(P_{safe})$, so I have $\text{Traces}_{fin}(TS) \cap \text{BadPref}(P_{safe}) \neq \emptyset$. Therefore, $TS \not\models P_{safe}$.

Solution 2

1. For any word w and letter a , $\text{freq}_a(w_n) \leq n$.
 $\therefore \frac{1}{n} \text{freq}_a w_n \leq 1$ for any $n \in \mathbb{N}$.
2. I need to construct a word w where the absence of a becomes rarer but never vanishes. There could be many candidates for such a word w . My personal favourite is the following:

$$w[i] = a \text{ iff } i \text{ is not a prime.}$$

The absence of 'a' at index i in w represent the fact that i is prime. We know that there are infinitely many primes (a theorem proved by Euclid and is arguably the oldest proof in the history of mathematics), thus the absence of 'a' never vanishes. This means, $w \not\models \bigvee_{\infty} a$.

The prime number theorem tells us that the frequency of primes decreases. For sufficiently large N , the number of primes less than the number N is $\approx \frac{N}{\log N}$. Thus, $\text{freq}_a(w_N) = N - \frac{N}{\log N}$.

$$\therefore \lim_{N \rightarrow \infty} \inf \frac{1}{N} \text{freq}_a(w_N) = \lim_{N \rightarrow \infty} \inf \left(1 - \frac{1}{\log N} \right) = 1$$

Thus, $w \models \bigvee_p a$ with $p = 1$.

3. Consider two series $S_n = x_1 + x_2 + \dots + x_n$, where $x_i = 1$ if $w[i] \models a$ else $x_i = 0$, and $T_n = y_1 + y_2 + \dots + y_n$, where $y_i = 1$ if $w[i] \models b$ else $y_i = 0$. Define $U_n = z_1 + z_2 + \dots + z_n$, where $z_i = x_i y_i$. Observe that, $\text{freq}_a(w_n) = S_n$, $\text{freq}_b(w) = T_n$, and $\text{freq}_{a \wedge b}(w) = U_n$. Let $\bar{S}_n$ (similarly, $\bar{T}_n$ and $\bar{U}_n$) is $\bar{x}_1 + \dots + \bar{x}_n$, where $\bar{x}_i = 0$ if $x_i = 1$ else $\bar{x}_i = 1$.

I need to show the following:

$$\text{If } \lim_{n \rightarrow \infty} \inf \frac{1}{n} S_n = 1 \text{ and } \lim_{n \rightarrow \infty} \inf \frac{1}{n} T_n = 1 \text{ then } \lim_{n \rightarrow \infty} \inf \frac{1}{n} U_n = 1$$

Observe that, $S_n = n - \bar{S}_n \therefore \lim_{n \rightarrow \infty} \inf \frac{1}{n} \bar{S}_n = 0$. Similarly, $\lim_{n \rightarrow \infty} \inf \frac{1}{n} \bar{T}_n = 0$.

$$\therefore \lim_{n \rightarrow \infty} \inf \frac{1}{n} (\bar{S}_n + \bar{T}_n) = 0.$$

Also notice that, $\bar{U}_n = \sum_{i=1}^n \lceil \frac{\bar{x}_i + \bar{y}_i}{2} \rceil$.

Thus, $\lim_{n \rightarrow \infty} \inf \frac{1}{n} \bar{U}_n = \lim_{n \rightarrow \infty} \inf \frac{1}{n} \sum_{i=1}^n \lceil \frac{\bar{x}_i + \bar{y}_i}{2} \rceil \leq \lim_{n \rightarrow \infty} \inf \frac{1}{n} (\bar{S}_n + \bar{T}_n) = 0$. Consequently,

$$\lim_{n \rightarrow \infty} \inf \frac{1}{n} U_n = \lim_{n \rightarrow \infty} \inf \frac{1}{n} (n - \bar{U}_n) = 1 - \lim_{n \rightarrow \infty} \inf \frac{1}{n} \bar{U}_n = 1$$

Solution 3 For the purpose of this exercise it suffices to consider the alphabet $\Sigma = \{\{\varphi\}, \emptyset\}$.

1. The deterministic finite automaton (DFA) for,

$$L_{\varphi, d'}^{fin} = \{w \in (2^{AP})^* \mid \text{if } w[i] \models \varphi \text{ then } i \text{ is a multiple of } d'\}$$

is shown in the figure 1. Each of the two cycle of the DFA A contains exactly d' distinct states. The

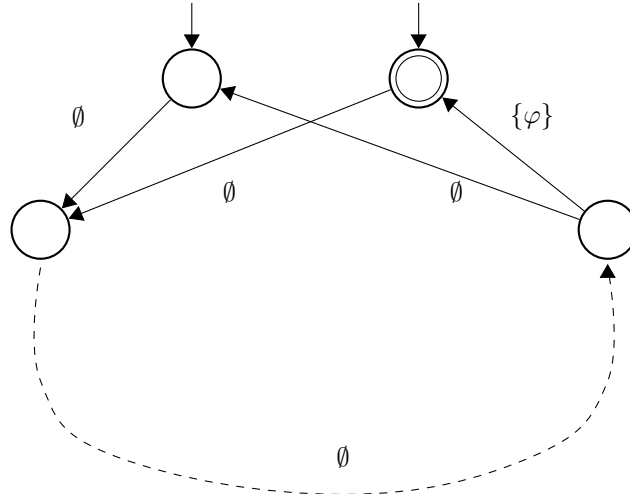


Figure 1: The DFA accepting $L_{\varphi, d'}^{fin}$

BadPref of $L_{\varphi, d'}$ is the language accepted by the complement $\bar{A}$ of A . $\bar{A}$ is constructed by making the non-accepting state accepting and accepting state non-accepting. There are $O(d')$ states in $\bar{A}$. The cross product with $T_{c, d}$ will yield a NFA with $O(cd' + dd')$ states. Thus checking empty-ness can be done time $O(cd' + dd')$.

2. Consider the only infinite path w of $T_{c,d}$. Observe, $w[i] \models \varphi$ iff $i = c + dx$ for every $x \in \mathbb{N}$. I need to verify:

$$\forall x, \exists y : c + dx = d'y. \quad (1)$$

The trick is to find a sufficient and necessary condition for the equation 1 to be true, which can be checked efficiently.

$$\forall x, \exists y : c + dx = d'y \text{ if and only if } (c \equiv 0 \pmod{d'}) \text{ and } (d \equiv 0 \pmod{d'}) \quad (2)$$

The condition is obviously sufficient.

If $(c \equiv 0 \pmod{d'})$ and $(d \equiv 0 \pmod{d'})$ then $c + dx = q_1 d' + q_2 d' x$.

$\therefore$ for every x I can find $y = q_1 + q_2 x$ such that $c + dx = d'y$.

Proving that the condition is necessary requires a bit of effort (not really).

* After talking about it at the exercise class, I felt that there was way too much unnecessary $c^* @ p$. So here is a lean (and mean) version. Basically, we want this:

$$\forall x, \exists y : c + dx = d'y \text{ implies } (c \equiv 0 \pmod{d'}) \text{ and } (d \equiv 0 \pmod{d'})$$

For $x = 0$, we have $c = d'y$, thus, $c \equiv 0 \pmod{d'}$. If $c \equiv 0 \pmod{d'}$ then $c = qd'$. Or, $\forall x : dx = d'(y - q)$. For $x = 1$, we get $d = d'(y - q)$. Thus, $d \equiv 0 \pmod{d'}$.

Returning to the model checking problem, we now trust the following equivalence:

$$T_{c,d} \models L_{\varphi,d'} \text{ iff } (c \equiv 0 \pmod{d'}) \text{ and } (d \equiv 0 \pmod{d'}).$$

Checking whether m divides n can be done in time $O(\log m \log n)$. This gives us our sort after complexity bound $O(\log c \log d' + \log d \log d')$.