Testování stavového automatu

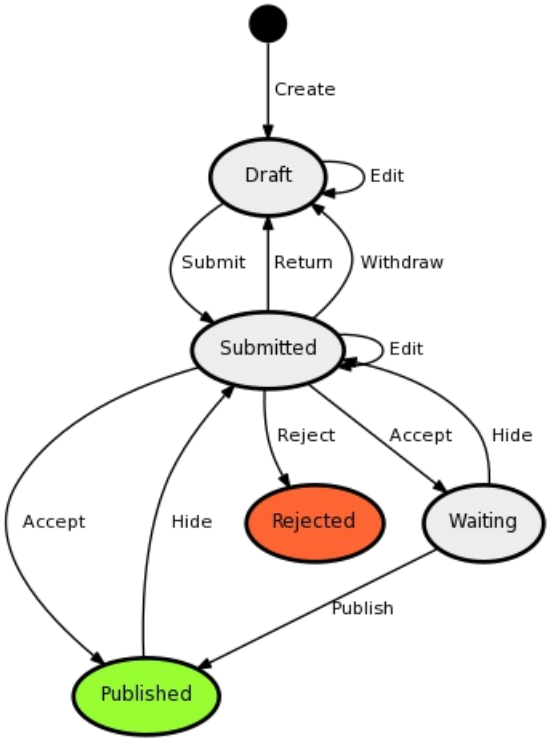
Skupina: **10**
Řešitelé: **Stanke Michal**, **Timr Marek**, **Voříšek Lukáš**

Zadání semestrální úlohy

1. Z aplikace získejte definici stavového automatu (jednu entitu dle vašeho téma) a importujte ji do Uppallu.
2. Vymodelujte v Uppallu další entity, například uživatele, tak aby byly použity alespoň dvoje hodiny.
3. Simulujte chování systému a dokažte nějaké zajímavé vlastnosti.

Naše skupina zpracovala úlohu 1, tedy Články redakčního systému. V této úloze jsme vytvořili model, který reprezentuje stavy pro *článek*, *autora* a *nakladatelství*, kde každá z entit má vlastní hodiny `clk` (body 1 a 2 ze zadání). Na tomto modelu jsme simulovali průchod tvorby článku od autora až po vydání.

Znázornění automatu úlohy 1, ze kterého jsme vycházeli:



Automaty

V této sekci budou popsány jednotlivé entity. Tedy lokace a přechody, které reprezentují tyto entity.

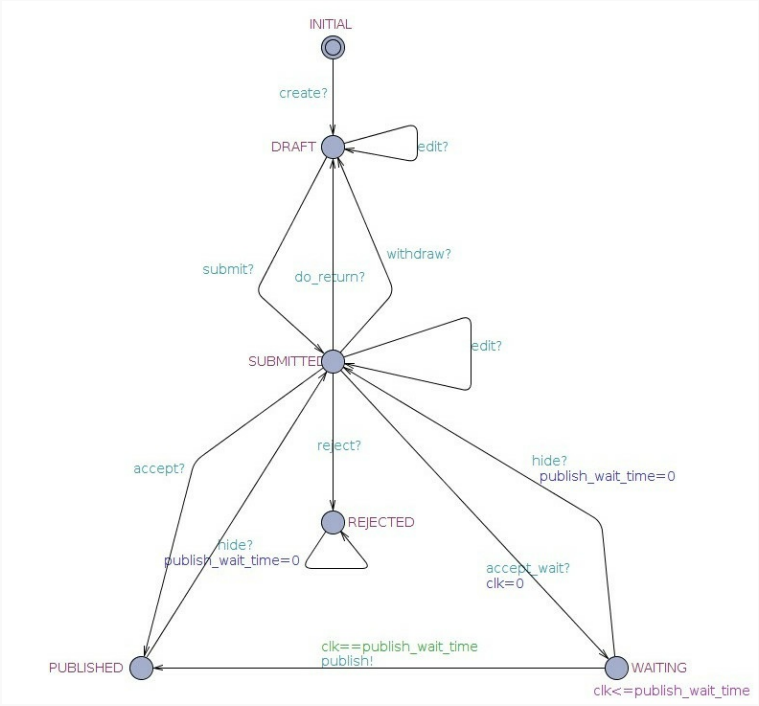
Článek

Lokace tohoto automatu představují stavy, ve kterých se může článek nacházet během svého života.

Počáteční lokací je `INITAL`, ve které žádný článek ještě neexistuje. V této lokaci čeká na příjem signálu `create`. Přijetí tohoto signálu dovolí článku přejít do stavu `DRAFT`, tedy konceptu. Článek v tomto stavu je rozpracovaný autorem.

Jakákoliv editace článku (událost `edit`) zanechá článek ve stavu konceptu. Přechod do jiného stavu způsobí až autor článku tím, že se jej pokusí odevzdat redakci (akce `submit`), kdy se článek považuje za odevzdaný `SUBMITTED`.

Odevzdaný článek (`SUBMITTED`) je následně editován vydavatelem. Tato editace je však časově omezena. Následně je článek redakcí buď přijat (hrana `accept?`) nebo odmítnut (hrana `reject?`).



Obrázek 1: Stav článku

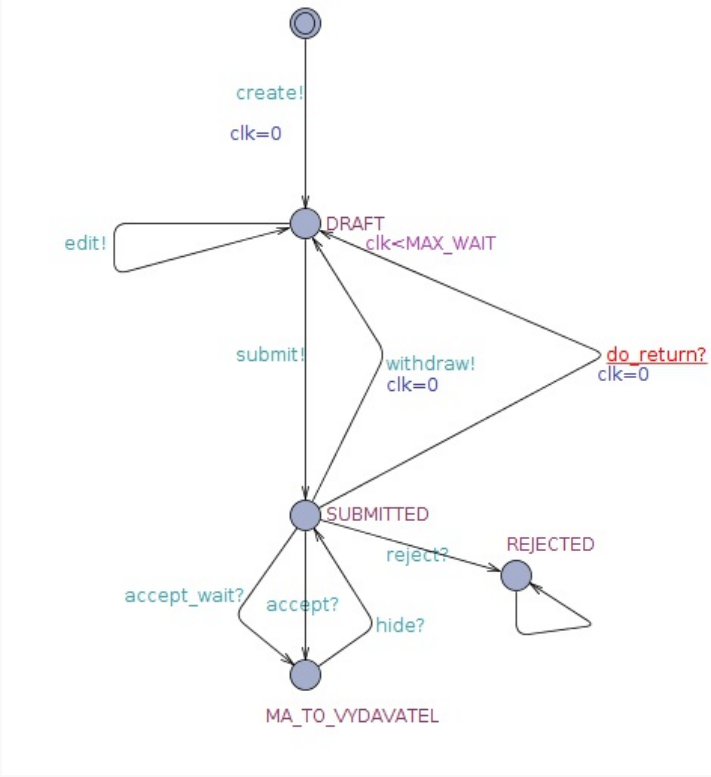
Článek, který je jednou odmítnut, je odmítnut již napořád. Naopak publikovaný článek (ve stavu `PUBLISHED`) může být stažen zpět do redakce (stavu `SUBMITTED`) pomocí hrany `hide?`, která je řízena rozhodnutím vydavatele.

Autor

Autor začíná ve svém počáteční lokaci a s přechodem do lokace `DRAFT` vyvolá zprávu `create`, která informuje ostatní automaty o vytvoření článku. Tedy v předchozím automatu dojde k přechodu na hraně `create?`.

V lokaci `DRAFT` může dojít ke spuštění dvou akcí (dvou hran) a to buď hrany `edit!` a nebo `submit!`. Akce `edit!`, která informuje o tom, že autor upravil článek a nebo akce `submit!`, která informuje o tom, že autor odevzdal článek redakci.

V odevzdaném stavu (`SUBMITTED`) již nemůže autor na článku pracovat. Všechny přechody zrcadlí rozhodnutí ostatních automatů tedy akceptaci článku, jeho odmítnutí a nebo čekání.



Obrázek 2: Autor

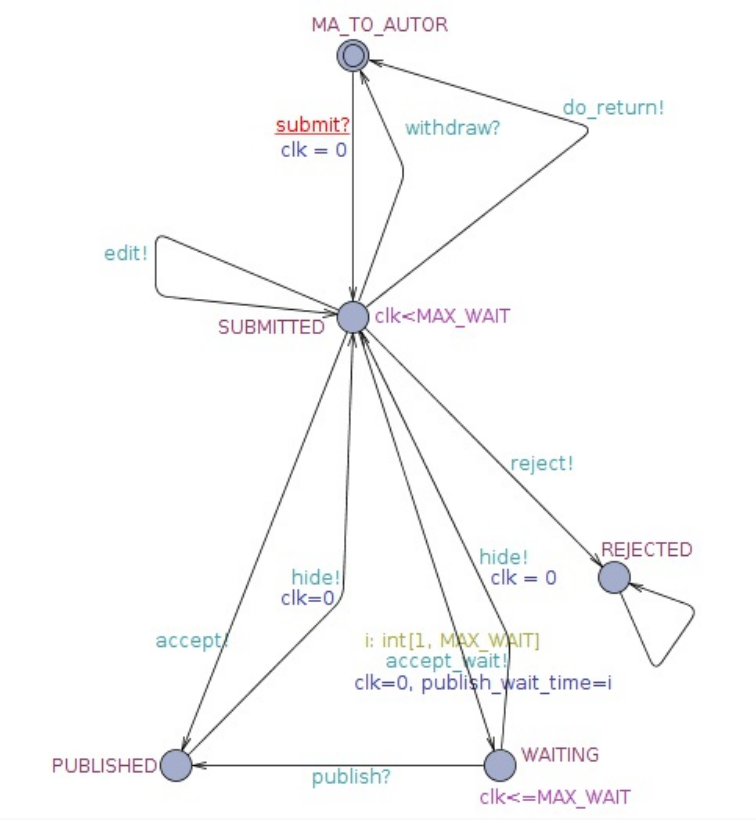
Vydavatel

Úvodní lokací pro vydavatele je uzel `MA_TO_AUTOR`. Jedinou přechodovou hranou z tohoto uzlu je reakce na zprávu `submit?`, která je vyslána autorem.

V odevzdaném stavu (`SUBMITTED`) může vydavatel článek editovat, odmítnout, akceptovat a nebo započít nádhodně dlouhé čekaní.

Publikovaný článek (`PUBLISHED`) může být redakcí odvolán (`hide!`).

Pokud redakce článek jednou odmítne (`reject!`) zůstane již navždy odmítnutý.



Obrázek 3: Vydavatel

Ověřování

K ověřování tvrzení jsme využili Verifier, který je dostupný v UPPAALU.

- **E<> deadlock**
  Ověřuje zda může dojít k deadlocku. Mělo by vyjít FALSE.
- **A[] not deadlock**
  Říká, že nikdy nenastane deadlock.
- **A[] nakladatelstvi.MA_TO_AUTOR imply (clanek.DRAFT or clanek.SUBMITTED or clanek.INITIAL)**
  Pokud má článek autor, tak musí být koncept (DRAFT), odevzdaný (SUBMITTED) a nebo v počátečním stavu (INITIAL).
- **A[] autor.MA_TO_VYDAVATEL imply (clanek.PUBLISHED or clanek.WAITING)**
  Pokud má článek vydavatel, tak musí být publikovaný nebo čekající.
- **A[] nakladatelstvi.PUBLISHED imply (autor.MA_TO_VYDAVATEL and clanek.PUBLISHED)**
  Článek je publikovaný. Má ho tedy vydavatel a je publikován.
- **A[] clanek.PUBLISHED imply (autor.MA_TO_VYDAVATEL and nakladatelstvi.PUBLISHED)**
  Článek je publikovaný (druhé ověření). Je publikovaný pro nakladatelství a má jej vydavatel.
- **A[] nakladatelstvi.WAITING imply (autor.MA_TO_VYDAVATEL and clanek.WAITING)**
  Článek je pro vydavatele ve stavu čekání, je tedy u vydavatele a ve stavu čekání.
- **A[] clanek.WAITING imply (autor.MA_TO_VYDAVATEL and nakladatelstvi.WAITING)**
  Článek je čekající, pro autora je u vydavatele a vydavatel čeká.
- **A[] nakladatelstvi.SUBMITTED imply (autor.SUBMITTED and clanek.SUBMITTED)**
  A[] autor.SUBMITTED imply (clanek.SUBMITTED and nakladatelstvi.SUBMITTED)
  A[] clanek.SUBMITTED imply (autor.SUBMITTED and nakladatelstvi.SUBMITTED)
  Pro všechny subjekty musí být článek odevzdatelný a být odevzdaný.
- **A[] autor.DRAFT imply (clanek.DRAFT and nakladatelstvi.MA_TO_AUTOR)**
  A[] clanek.DRAFT imply (autor.DRAFT and nakladatelstvi.MA_TO_AUTOR)
  Článek je pro všechny koncept (DRAFT).
- **A[] nakladatelstvi.REJECTED imply (clanek.REJECTED and autor.REJECTED)**
  A[] autor.REJECTED imply (clanek.REJECTED and nakladatelstvi.REJECTED)
  A[] clanek.REJECTED imply (autor.REJECTED and nakladatelstvi.REJECTED)
  Článek je odmítnutý (REJECTED) pro všechny automaty.
- **E<> clanek.REJECTED**
  Článek může být odmítnutý.
- **E<> clanek.PUBLISHED**
  Článek může být publikovaný.
- **E<> clanek.WAITING**
  Článek může být ve stavu čekání.
- **E<> clanek.SUBMITTED**
  Článek může být odevzdaný.
- **E<> clanek.DRAFT**
  Článek může být kocept.
- **E<> clanek.WAITING and clanek.clk == publish_wait_time**
  Článek může čekat až do nastaveného wait_time.
- **E<> clanek.WAITING and clanek.clk == nakladatelstvi.MAX_WAIT**
  Článek může čekat až do maximalního wait_time.

- **E<> clanek.WAITING and !(clanek.clk > nakladatelstvi.MAX_WAIT)**
  Článek nikdy nebude v čekání déle než je maximální wait_time.
- **A[] clanek.WAITING imply publish_wait_time>0**
  Pokud je článek v čekání (WAITING) pak má i přiřazen čas čekání.
- **E<> clanek.PUBLISHED imply publish_wait_time==0**
  Do publikovaného stavu (PUBLISHED) se lze přesunout bez čekání.
- **E<> clanek.PUBLISHED and publish_wait_time>0**
  Do publikovaného stavu (PUBLISHED) se lze přesunout s čekáním.
- **A[] (clanek.PUBLISHED and publish_wait_time>0) imply (clanek.clk>=publish_wait_time)**
  Pokud je článek publikován po čekání, tak doba čekání již uběhla.
- **A[] !(clanek.WAITING or clanek.PUBLISHED) imply publish_wait_time==0**
  Pokud článek není ani v čekání a ani publikovaný, pak je doba čekání článku nulová.

Zajímavé pozorování

Konfliktním stavem je u nás stav `SUBMITTED` ve kterém článek náleží jak autorovi, tak vydavateli a oba na něm smějí provádět úpravy.

V nefinální implementaci, před testováním pomocí verifier nám vznikl stav, kdy článek byl zamítnut vydavatelem, ale autor se na něm snažil provádět úpravy. Tento stav jsme napravili hranou `reject?` v automatu autora.

Ve stavu `SUBMITTED` je potřeba zanést veškeré hrany, jelikož se jedná o konfliktní stav, ve kterém jsou ovlivňovány všechny automaty a všechny se mohou nějak rozhodnout.

Diagram neodpovídá chování v reálném světě, jelikož při "nekonečně" dlouhé době trvání se všechny články přesunou, dříve nebo později, do stavu zamítnutého článku `REJECTED`.