

Általános információk, a diplomaterv szerkezete

A diplomaterv szerkezete a BME Villamosmérnöki és Informatikai Karán:

1. Diplomaterv feladatkiírás
2. Címoldal
3. Tartalomjegyzék
4. A diplomatervező nyilatkozata az önálló munkáról és az elektronikus adatok kezeléséről
5. Tartalmi összefoglaló magyarul és angolul
6. Bevezetés: a feladat értelmezése, a tervezés célja, a feladat indokoltsága, a diplomaterv felépítésének rövid összefoglalása
7. A feladatkiírás pontosítása és részletes elemzése
8. Előzmények (irodalomkutatás, hasonló alkotások), az ezekből levonható következtetések
9. A tervezés részletes leírása, a döntési lehetőségek értékelése és a választott megoldások indoklása
10. A megtervezett műszaki alkotás értékelése, kritikai elemzése, továbbfejlesztési lehetőségek
11. Esetleges köszönetnyilvánítások
12. Részletes és pontos irodalomjegyzék
13. Függelék(ek)

Felhasználható a következő oldaltól kezdődő \LaTeX diplomatervsablon dokumentum tartalma.

A diplomaterv szabványos méretű A4-es lapokra kerüljön. Az oldalak tükörmargóval készüljenek (min-denhol 2,5 cm, baloldalon 1 cm-es kötéssel). Az alapértelmezett betűkészlet a 12 pontos Times New Roman, másfeles sorközzel, de ettől kismértékben el lehet térni, ill. más betűtípus használata is megengedett.

Minden oldalon – az első négy szerkezeti elem kivételével – szerepelnie kell az oldalszámnak.

A fejezeteket decimális beosztással kell ellátni. Az ábrákat a megfelelő helyre be kell illeszteni, fejeze-tenként decimális számmal és kifejező címmel kell ellátni. A fejezeteket decimális aláosztással számozzuk, maximálisan 3 aláosztás mélységben (pl. 2.3.4.1.). Az ábrákat, táblázatokat és képleteket célszerű fejeze-tenként külön számozni (pl. 2.4. ábra, 4.2. táblázat vagy képletnél (3.2)). A fejezetcímeket igazítsuk balra, a normál szövegnél viszont használjunk sorkiegyenlítést. Az ábrákat, táblázatokat és a hozzájuk tartozó címet igazítsuk középre. A cím a jelölt rész alatt helyezkedjen el.

A képeket lehetőleg rajzoló programmal készítsék el, az egyenleteket egyenlet-szerkesztő segítségével írják le (A \LaTeX ehhez kézenfekvő megoldásokat nyújt).

Az irodalomjegyzék szövegközi hivatkozása történhet sorszámozva (ez a preferált megoldás) vagy a Harvard-rendszerben (a szerző és az évszám megadásával). A teljes lista névsor szerinti sorrendben a szö-veg végén szerepeljen (sorszámozott irodalmi hivatkozások esetén hivatkozási sorrendben). A szakirodalmi források címeit azonban mindig az eredeti nyelven kell megadni, esetleg zárójelben a fordítással. A listá-ban szereplő valamennyi publikációra hivatkozni kell a szövegben (a \LaTeX -sablon a Bib \TeX segítségével mindezt automatikusan kezeli). Minden publikáció a szerzők után a következő adatok szerepelnek: folyó-irat cikkeknél a pontos cím, a folyóirat címe, évfolyam, szám, oldalszám tól-ig. A folyóiratok címét csak akkor rövidítsük, ha azok nagyon közismertek vagy nagyon hosszúak. Internetes hivatkozások megadásakor fontos, hogy az elérési út előtt megadjuk az oldal tulajdonosát és tartalmát (mivel a link egy idő után akár elérhetetlenné is válhat), valamint az elérés időpontját.

Fontos:

- A szakdolgozatkészítő / diplomatervező nyilatkozata (a jelen sablonban szereplő szövegtartalom-mal) kötelező előírás, Karunkon ennek hiányában a szakdolgozat/diplomaterv nem bírálható és nem védhető!
- Mind a dolgozat, mind a melléklet maximálisan 15 MB méretű lehet!

Jó munkát, sikeres szakdolgozatkészítést, ill. diplomatervezést kívánunk!

FELADATKIÍRÁS

A feladatkiírást a tanszéki adminisztrációban lehet átvenni, és a leadott munkába eredeti, tanszéki pecséttel ellátott és a tanszékvezető által aláírt lapot kell belefűzni (ezen oldal *helyett*, ez az oldal csak útmutatás). Az elektronikusan feltöltött dolgozatban már nem kell beleszerkeszteni ezt a feladatkiírást.



Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Méréstechnika és Információs Rendszerek Tanszék

Monitor szintézis időzített üzenet szekvencia specifikáció alapján

DIPLOMATERV

Készítette
Bakai István Bálint

Konzulens
Dr. Majzik István

2021. április 29.

Tartalomjegyzék

Kivonat	i
Abstract	ii
1. Bevezetés - Rendszerkomponensek közti kommunikáció monitorozása	1
2. PSC – Property Sequence Charts	2
3. TPSC – Timed Property Sequence Charts	4
4. TPSC scenario-ból automata készítése	5
5. Monitor generálás terv	6
6. Szöveges leíró nyelv PSC kibővítése	7
7. Időzített automata generátor	8
7.1. Az automata generátor célja	8
7.2. Az automata generátor megvalósítása	8
7.3. Minta példa	9
8. Monitor forráskód generátor	10
8.1. A monitor interfészei	10
8.2. A monitor forráskód megvalósítása	10
8.3. Minta példa	11
Köszönetnyilvánítás	12
Függelék	13
F.1. A TeXstudio felülete	13
F.2. Válasz az „Élet, a világmindenség, meg minden” kérdésére	14
Irodalomjegyzék	13

HALLGATÓI NYILATKOZAT

Alulírott *Bakai István Bálint*, szigorló hallgató kijelentem, hogy ezt a diplomatervet meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2021. április 29.

Bakai István Bálint
hallgató

Kivonat

A monitorozással történő hibadetektálás létfontosságú egy rendszer működtetésében és karbantartásában. A monitorozás sok hibát fel tud deríteni, amiket a tesztek nem feltétlenül tudnak kideríteni.

Az önálló laboratórium feladat célja az volt, hogy a „Monitor komponensek generálása kontextusfüggő viselkedés ellenőrzésére” című szakdolgozatomban definiált szöveges PSC (Property Sequence Chart) leíró nyelvet kibővítsem úgy, hogy időzítési feltételeket is meg lehessen adni a követelményben. Ilyen követelményeket egyszerűen specifikálhatunk TPSC (Timed Property Sequence Chart) diagramokkal. Az Xtext alapú nyelvet kiegészítettem a TPSC tulajdonságaival.

A monitor generálás következő lépése, hogy a PSC diagramokból TA időzített automatákat generálunk (Timed Automaton). A TA fogja megadni, hogy a megfigyelt kommunikáció helyes viselkedést jelent-e. A szakdolgozatomban készített automata generátort kibővítettem és most már képes a minta alapú módszert használva TA automatákat generálni a TPSC diagramjainkból. A generátor előállítja az automatát.

A szöveges scenario leírásból generált automata alapján legenerálható a monitor forráskódja. A monitor forráskód generátor előállítja a monitor Java implementációját, ami képes egy rendszer monitorozására adott követelmény alapján.

Abstract

This document is a L^AT_EX-based skeleton for BSc/MSc theses of students at the Electrical Engineering and Informatics Faculty, Budapest University of Technology and Economics. The usage of this skeleton is optional. It has been tested with the *TeXLive* T_EX implementation, and it requires the PDF-L^AT_EX compiler.

1. fejezet

Bevezetés - Rendszerkomponensek közti kommunikáció monitorozása

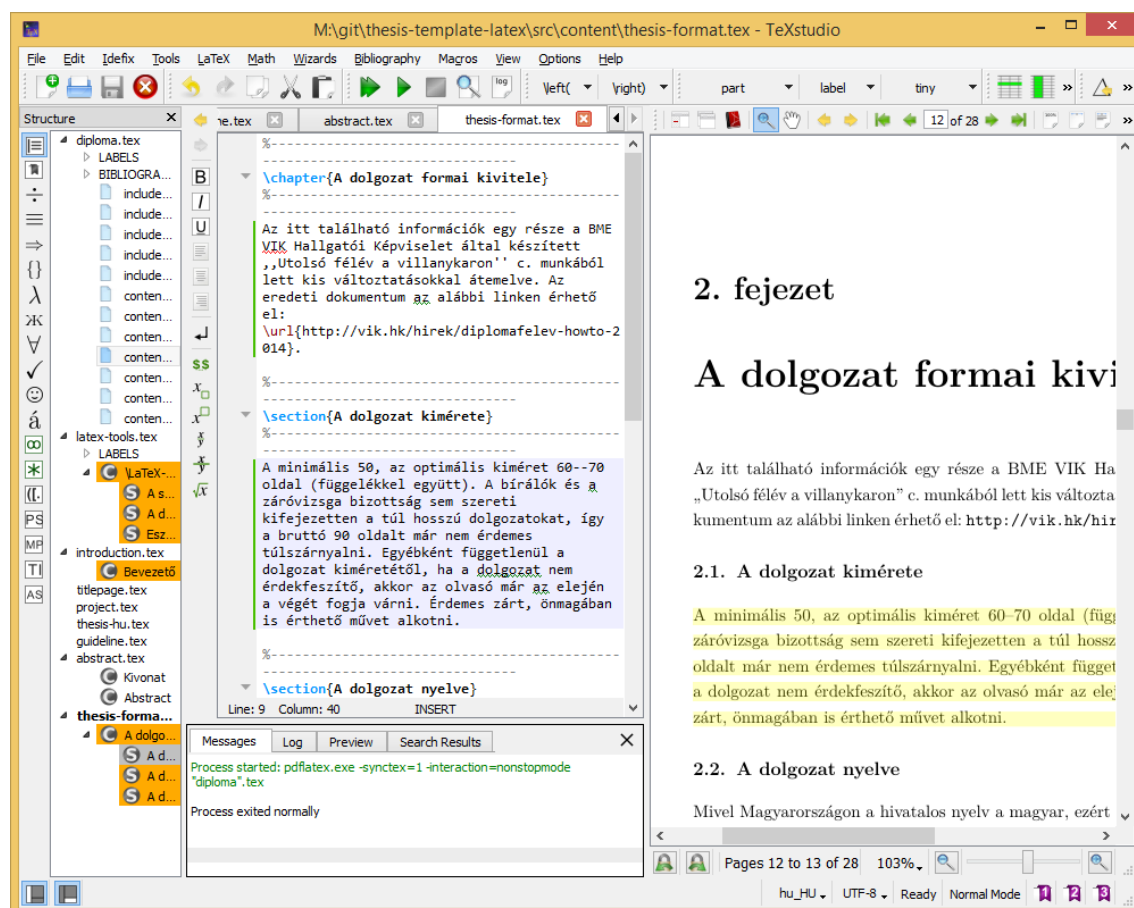
Egy monitor feladata az, hogy futási időben egy rendszert megfigyeljen, elemezzen és egy adott követelmény alapján felismerje a rendszer helytelen viselkedését. Ezt a helytelen viselkedést jelzi a rendszernek, de néhány esetben a rendszer működését is befolyásolhatja. Egy rendszer viselkedése lehet kontextusfüggő, amit a monitornak figyelembe kell venni. Például, egy gépjármű fékezésének vezérlését befolyásolja a terep, amin épp halad. A rendszer működése tehát függ a környezetétől. Ezért, hogy a viselkedését ellenőrizni tudjuk, a monitornak információval kell rendelkeznie a környezetben történő változásokról. Ezen kívül, a monitornak időmérésre is szüksége van, mert a követelmény tartalmazhat időzítéseket is. Az 1. ábra bemutatja a monitorozás koncepcióját.

A scenario alapú monitorozás során a kommunikáció megfigyelésével szeretnénk felismerni a problémákat a rendszerünkben. A rendszerben lévő objektumok közti interakciókat, üzeneteket fogja megfigyelni a monitor. A követelményt scenario formájában adjuk meg az üzenet szekvenciák specifikálására. Szekvencia diagramok segítségével egyszerűen megadhatunk ilyeneket. A diagramokat a későbbiekben olyan alakra kell majd hoznunk, hogy abból a monitor létrehozható legyen.

2. fejezet

PSC – Property Sequence Charts

A Message Sequence Chart-nak nagyon sok hiányossága van. Nem lehet vele megkötéseket definiálni vagy egy üzenetről eldönteni, hogy az egy elvárt vagy nem kívánt üzenet. Ebből kifolyólag az MSC nem egy alkalmas nyelv arra, hogy az üzenet szekvenciáinkat részletesebben specifikálni tudjuk vele.



2.1. ábra. A TeXstudio LaTeX-szerkesztő.

A Property Sequence Chart[1] az MSC egy kiterjesztése. Sok új elemet vezet be ami nincs az MSC-ben, melyek megtekinthetők az 1. táblázaton, mint az üzenet típusokat: sima üzenet (e), elvárt üzenet (r) és nem kívánt üzenet (f). Így specifikálhatjuk, hogy mely üzenetek azok amik helyes viselkedésre utalnak és azok amelyek nem. Az elvárt üzenetek azok az üzenetek amelyeknek feltétlenül meg kell történniük a rendszer működése során.

Egy sima üzenetnek nem jelent hibát a monitor szempontjából ha nem történik meg, viszont ha megjelenik, akkor a scenario-ban utána következő üzenetek ellenőrzésére kell áttérni. Szigorú sorrendezésre is ad megoldást a PSC, ami azt jelenti, hogy megadhatjuk explicit az üzenetek sorrendjét a követelményünkben. A PSC-ben egy üzenetre megkötést is rakhatunk. Megadhatjuk, hogy melyek azok az üzenetek amik nem kívántak az üzenetünk előtt vagy után. A különböző PSC tulajdonságok megtalálhatók a 2. ábrán.

Az üzeneteket a következő formában adjuk meg: Feladó.Üzenet.Címzett.

A 3. ábrán láthatunk egy példát arra, hogy egy követelményt hogyan lehet definiálni. Ez a PSC diagram egy ATM rendszer működését figyeli. Először a felhasználó egy login üzenettel bejelentkezik az ATM-be majd egy wReq üzenettel egy lekérdezést hajt végre. Ezen az üzeneten van egy megkötés, még pedig hogy az üzenet előtt nem történt kijelentkezés, logout. Az ATM ezután, ha nem történt logout egy elvárt üzenetet küld a Bank adatbázisába.

A scenario-ink specifikálására most már rendelkezésünkre áll egy grafikus nyelv. A következőkben az lesz a feladatunk, hogy ezeket a diagramokat úgy transzformáljunk, hogy monitor kódot lehessen belőlük készíteni.

3. fejezet

TPSC – Timed Property Sequence Charts

A TPSC[2] a PSC-nek egy kiterjesztése. A PSC üzenetekre időzítési feltételeket specifikálhatunk.

A TPSC óraváltozókat (x , y) használ az időzítéshez. Ezekre meg lehet adni feltételeket, valamint az óraváltozót lehet nullázni. A nullázással adott eseménytől (pl. üzenet vételétől) kezdve lehet időzítést indítani, majd rákövetkező események időbeliségét ellenőrizni.

A 4. ábrán látható, hogy például az e : a sima üzenet e : a; $x < t$, $y := 0$ üzenetre bővül. Elvárjuk, hogy az a üzenet t idő előtt történjen meg és egy y óraváltozót nullázunk. Az e : a üzenet egy sima üzenet, szóval ha nem történik meg a specifikált idő intervallumban az nem jelent hibát. Viszont r : a üzenetnél már elvárt, hogy t időn belül megtörténjen. f : a üzenet esetében viszont akkor jelez hibát a monitor, ha üzenet megtörtént t időn belül.

Egy megkötésre is meg lehet adni időzítési feltételt. Így megadhatjuk, hogy mennyi ideig nem szabad jönnie a megkötésben szereplő nem kívánt üzenetek egyikének. Ha a feltételben megadott idő után történik akkor az nem jelent hibát a monitor szempontjából.

4. fejezet

TPSC scenario-ból automata készítése

A monitorozás alapja, hogy TPSC scenario-kból időzített automatákat (Timed Automata) tudjunk készíteni. Egy TA állapotokból, elfogadó állapotokból, feltételekből, akciókból és bemenetekkel címkézett állapotátmenetekből áll. Akkor fogad el egy bemenet sorozatot, ha ennek során elérünk az automata végállapotába. Ha elfogadó állapotot érünk el, akkor az a monitor szempontjából hibát jelent. Az alapelv az az, hogy minden TPSC elemhez tartozik egy minta automata (pattern) ami leírja a szemantikáját. Például a 5. és 6. ábrákon láthatóak a különböző PSC üzenetekhez tartozó minták.

A minta automatánkban található szürke állapotok reprezentálják a végállapotokat. A megkötéseket az automatáknál egy átmenettel definiáljuk ami a nem kívánt üzenetek negáltjainak az ÉS kapcsolata. Például az 5. ábrán lévő 3. automata mintán látható „b, $\delta' \&!a, \delta$ ” címkéjű hurokélen, a „b” azt jelzi, hogy amíg nem jött nem kívánt üzenet addig maradjunk az S0 állapotban. A címke teljes jelentése az, hogy ha δ' időn belül nem jött nem kívánt üzenet és δ időn belül nem az „a” üzenet jött akkor maradjunk az s0 állapotban. Ezekből az automata részekből lesznek meghatározott illesztési szabályokkal a scenario-hoz tartozó teljes időzített automaták. Ennek az az alapelve, hogy a scenario-n végig menve az előző minta végállapotát a következő minta kezdőállapotával kell egyesíteni. Ezt a folyamatot mutatják be a 7., 8. és 9. ábrák.

5. fejezet

Monitor generálás terv

A cél az, hogy a „Monitor komponensek generálása kontextusfüggő viselkedés ellenőrzése” című szakdolgozatom során elkészített monitor komponens generátort kibővíteni úgy, hogy támogassa időzítési feltételek megadását. A monitor generálás terve látható a 10. ábrán. Először az a feladatunk, hogy a szakdolgozat során definiált szöveges PSC diagram leíró nyelvet kibővítsük a TPSC elemeivel. Ezután az automata generátort kell úgy kibővíteni, hogy a TPSC diagramokból tudjon TA automatákat generálni. Ebből az időzített automatából előallítható a monitor konkrét modellje, ami egy UPPAAL időzített automata. Egy monitor forráskód generátor pedig az automata alapján elkészítheti a monitor forráskódját. Az önálló laboratórium 1 tárgy keretében az első három ponttal, majd az önálló laboratórium 2 tárgy keretében a tervnek a harmadik és negyedik részével foglalkoztam.

6. fejezet

Szöveges leíró nyelv PSC kibővítése

A nyelvet az Xtext technológia segítségével definiáltam. A nyelv két új elemmel bővült:

- időzített feltétel
- óraváltozó nullázása

A 11. ábrán látható, hogy egy TPSC diagramot hogyan tudunk leírni a nyelvünk segítségével. Definiálhatjuk a diagramban szereplő objektumokat, a megkötéseket amiket használni fogunk és végül, hogy milyen üzenetek vannak a követelményünkben. A 12. ábrán látszik, hogy megjelenik a clockConstraint kulcsszó ami egy időzítési feltétel megadására szolgál. A kulcsszó után kapcsos zárójelek közt megadható a feltétel. A reset kulcsszó az óraváltozó nullázására szolgál.

7. fejezet

Időzített automata generátor

7.1. Az automata generátor célja

A diplomatervezés során elkészített automata generátort kibővítettem úgy, hogy támogassa a TPSC elemekhez tartozó automata minták generálását. Bemenetként egy TPSC scenario szöveges leírását kapja meg amiből a minta alapú módszerrel generál egy TA automatát.

A 13. ábrán látható, hogy a monitor generátor támogatja az alt, par és loop operátorokat tartalmazó TPSC-khez tartozó TA-k generálását is. Továbbá a generátor képes az üzenet paraméterek kezelésére. Például az alt operátor feltételét képes feldolgozni és azt elhelyezni a generált automata megfelelő élén.

7.2. Az automata generátor megvalósítása

A generátorhoz az Xtend technológiát használtam. Minden egyes TPSC üzenethez legenerálja a hozzá tartozó minta automatát, majd elvégzi azok összezsátolását.

Az időzített automaták generálásához egy adatstruktúrát definiáltam, amely a következő Java osztályokból áll:

- State
- StateType
- Transition
- Automaton
- Specification

A 14. ábrán látható az adatstruktúra UML osztály diagramja.

Az automatában lévő állapotok implementációja a State osztályban található. Két attribútuma van: id(String), a címkéje tárolására, és type(StateType), az állapot típusa.

Az állapot típusának a megadására a StateType enum osztályt definiáltam. NORMAL, ACCEPT, FINAL értékeket lehet benne eltárolni. Az átmenetek implementációjáért felelős osztály a Transition. Három tag változója van: id(String) az üzenet, sender(State), a feladó állapot, és receiver(State) a fogadó állapot.

Az időzített automata implementációja az Automaton osztályban található. Itt tároljuk az automatában lévő állapotokat és a köztük lévő átmeneteket egy-egy listában. Az Automaton osztály addState(State) és addTransition(Transition) függvényeivel lehet új állapotot és átmenetet hozzáadni az automatához, a collapse(Automaton) függvényével

pedig két automatát egyesíteni. Ezt a függvényt használtam az implementációban a minta automaták egyesítésére. Ezen kívül az osztálynak van egy `merge(ArrayList<Automaton>)` függvénye. Ez az előző fejezetben definiált `merge` függvény implementációja.

A `Specification` osztály feladata, hogy összeállítsa a szöveges leírásban specifikált TPSC scenariohoz tartozó időzített automatát. Ezt követően az automata `Never Claim` leírását egy `.txt` kiterjesztésű fájlba írja.

7.3. Minta példa

A fenti 14., 15. és 16. ábrákon látható, hogy a generátor milyen időzített automatát generál a megadott TPSC scenario-ból.

8. fejezet

Monitor forráskód generátor

8.1. A monitor interfészei

A monitorozás alatt lévő rendszer egy közös interfészen keresztül kommunikál a monitorral. Az interfész Java implementációja a 19. ábrán tekinthető meg. A monitor azt vizsgálja, hogy a rendszer a scenario szerint működik-e.

Monitor interfész:

- `update()`: a monitorban tárolt rendszer állapotát frissíti a paraméterben kapott üzenet alapján.
- `goodStateReached()`: a rendszer aktuális állapotát jelzi.
- `requirementSatisfied()`: jelzi hogy a rendszer megfelel-e a követelménynek
- `errorDetected()`: detektált hiba jelzésére szolgál

Az `update()` függvényt a rendszer hívja, hogy továbbítsa az üzenetet a monitornak. Paraméterként az üzenet küldőjét (`sender`), fogadóját (`receiver`), üzenet nevét (`messageType`) és az üzenet paramétereit várja (`parameters`). A `goodStateReached()` függvényt a monitor hívja amikor a rendszer állapota változik. Ha a rendszer nem elfogadó állapotban van akkor igazat ad vissza, ha pedig nem akkor hamisat. A `requirementSatisfied()` függvényt is a monitor hívja. Ha a követelménynek megfelelt a rendszer viselkedése akkor igazat ad vissza, amúgy hamisat.

Az üzenetek megfigyeléséhez szükséges segédfüggvényeket a kommunikációs infrastruktúrához kézzel kell megírni. Ezek a monitort az `update()` függvényen keresztül hívják.

Az időzítő komponenshez tartozik egy időzítő interfész amin keresztül elérhető a komponens. Ezen az interfészen keresztül lehet az óraváltozokat lekérdezni vagy nullázni. Két függvénye van:

- `getClockVariable(String name)`: óraváltozó lekérdezése név alapján
- `resetClockVariable(String name)`: óraváltozó nullázása név alapján

8.2. A monitor forráskód megvalósítása

A generált forráskód struktúrája egy statikus és egy dinamikus részből áll. A statikus részbe az időzített automata java osztályai kerülnek:

- `State`: egy állapotot leíró osztály
- `Transition`: egy élet reprezentáló osztály

- Automaton: egy automatát megvalósító osztály

A monitor interfész és a monitor java osztálya is ebbe a részbe tartozik.

A dinamikus részben található a Specification Java osztály, ami a scenario alapján generált automata forráskódját tartalmazza. Ezt a 20. ábra mutatja be. A dinamikus rész pirosan van bekeretezve és a statikus rész pedig feketén.

A szükséges forráskódok generálásához az Xtend technológiát használtam. Az előző fejezetben ismertetett generátort kiegészítettem egy Monitor Java osztállyal, ami a monitor forráskódjának implementációját tartalmazza.

8.3. Minta példa

A 21. ábrán látható egy scenario követelmény, amit egy példa okos telefon működésére specifikáltunk. Az okos telefonon van egy zene lejátszási lista generáló alkalmazás. A követelményben azt várjuk el, hogy ha a felhasználó megnyitja az alkalmazást akkor a belső kamera készít az arcáról egy képet. A kép alapján eldönti, hogy milyen a felhasználó kedve és az alapján előállít egy zene lejátszási listát.

A 23. ábrán látható az okos telefon és a monitor közti kapcsolat megvalósítása Java kódban és a 22. ábrán pedig egy monitor kimenet. A monitor a rendszertől kapott üzenetek alapján jelzi, hogy a követelmény alapján mi a rendszer állapota.

A 24. ábrán látható az okos telefon Java osztálya. Megtekinthető a monitor és az eszköz közti kommunikáció megvalósítása is.

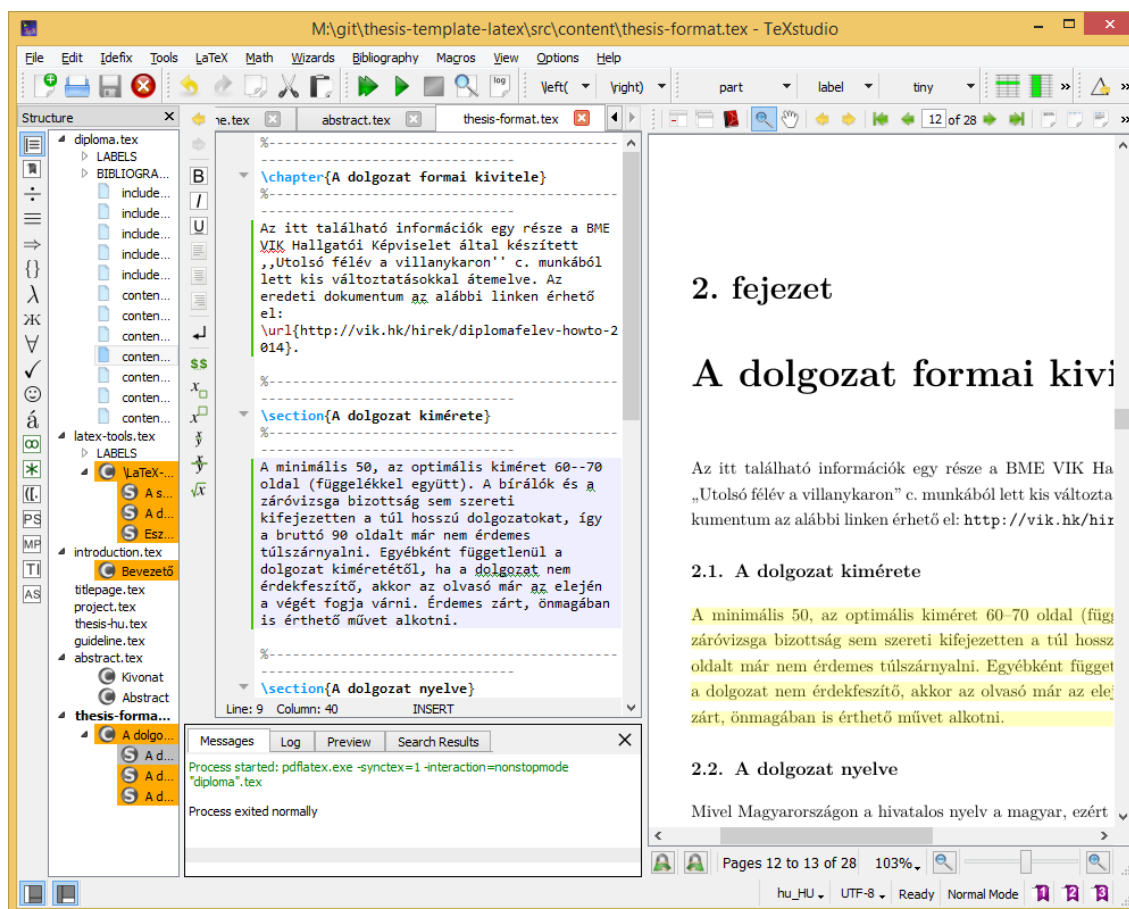
A 25. ábrán látszik, hogy a rendszer a működése elején nem felelt meg a monitor követelményének. Amikor a működése végére ért akkor a monitor jelezte, hogy a követelmény teljesült a „Good state” üzenettel. A mintához tartozó Specification osztály a függelékben található. A generált automatát a konstruktorában állítja elő.

Köszönetnyilvánítás

Ez nem kötelező, akár törölhető is. Ha a szerző szükségét érzi, itt lehet köszönetet nyilvánítani azoknak, akik hozzájárultak munkájukkal ahhoz, hogy a hallgató a szakdolgozatban vagy diplomamunkában leírt feladatokat sikeresen elvégezze. A konzulensnek való köszönetnyilvánítás sem kötelező, a konzulensnek hivatalosan is dolga, hogy a hallgatót konzultálja.

Függelék

F.1. A TeXstudio felülete



F.1.1. ábra. A TeXstudio \LaTeX -szerkesztő.

F.2. Válasz az „Élet, a világmindenség, meg minden” kérdésre

A Pitagorasz-tételből levezetve

$$c^2 = a^2 + b^2 = 42. \quad (\text{F.2.1})$$

A Faraday-indukciós törvényből levezetve

$$\text{rot } E = -\frac{dB}{dt} \quad \longrightarrow \quad U_i = \oint_{\mathbf{L}} \mathbf{E} d\mathbf{l} = -\frac{d}{dt} \int_A \mathbf{B} d\mathbf{a} = 42. \quad (\text{F.2.2})$$