

Pflichtenheft

Beste Gruppe

25. November 2016

CBMC C Bounded Model Checker

BMC Bounded Model Checking

GUI Graphical User Interface

Inhaltsverzeichnis

1	Produktübersicht	5
2	Zielbestimmung	7
2.1	Musskriterien	7
2.2	Sollkriterien	8
2.3	Wunschkriterien	8
2.4	Abgrenzungskriterien	8
3	Produkteinsatz	9
3.1	Anwendungsbereiche	9
3.2	Zielgruppen	9
3.3	Betriebsbedingungen	9
4	Produktumgebung	10
4.1	Software	10
4.2	Hardware	10
4.3	Orgware	10
4.4	Produkt-Schnittstellen	10
5	Funktionale Anforderungen	11
5.1	Allgemein	11
5.2	C-Code Editor für Wahlverfahren	11
5.3	Editor für formale Eigenschaften	12
5.4	Editor für Eingabeparameter	13
5.5	Ausgabe der Analyseergebnisse	13
6	Produktdaten	14
6.1	Code-Editor Wahlverfahren	14
6.2	Editor von formalen Eigenschaften	14
7	Nichtfunktionale Anforderungen	15
8	Globale Testfälle	16
8.1	Laden von Wahlverfahren	16
9	Systemmodelle	18
9.1	Szenarien	18
9.2	Anwendungsfälle	18

9.3	Objektmodelle	19
9.4	Dynamische Modelle	19
10	GUI	20
11	Phasenverantwortliche	21
11.1	Pflichtenheft	21
11.2	Entwurf	21
11.3	Implementierung	21
11.4	Qualitätssicherung	21
11.5	Abschlusspräsentation	21
12	Glossar	22

1 Produktübersicht

Wahlverfahren bilden den Grundstein unserer Demokratie. Dabei werden viele Anforderungen an sie gestellt, welche unsere intuitiven Ideen über Gerechtigkeit formalisieren: Proportionalität, Anonymität, etc. Moderne Wahlverfahren sind oft so komplex, dass sie viele überraschende und teils unerwünschte Eigenschaften haben. Nachweisen deren Abwesenheit ist absolut nicht trivial. So wurde beispielsweise 2008 das Bundestagswahlrecht vom BVerfG für verfassungswidrig erklärt, da es unter anderem Gleichheit der Wirkung verschiedener Stimmen verletzte. Auf der anderen Seite ist es auch sehr schwer, Wahlverfahren auf die Anwesenheit erwünschter Eigenschaften zu untersuchen.

Bounded Model Checking (BMC) bietet im allgemeinstem Fall eine Möglichkeit zu verifizieren, ob ein gegebenes System diverse Eigenschaften erfüllt. Es ist vollautomatisch und gibt bei Nichterfüllung ein Gegenbeispiel zurück. Dazu baut es eine boolsche Formel, welche genau dann erfüllbar ist, wenn die zu Untersuchende Eigenschaft vom System nicht erfüllt wird.

In unserem Fall kann BMC konkret dazu verwendet werden, ein C-Programm darauf zu untersuchen ob es im Falle gegebener Vorbedingungen gegebene Nachbedingungen erfüllt. Dies wird dazu verwendet, obige Problemstellung zu lösen: so kann ein in C definiertes Wahlverfahren wie z.B. die einfache Mehrheitswahl darauf geprüft werden, ob es bestimmte Eigenschaften erfüllt. Allerdings ist es sehr kompliziert, dies ohne Weiteres zu tun.

Unser Programm ist im Wesentlichen eine sehr umfangreiche Schnittstelle um mit C Bounded Model Checker (CBMC) zu kommunizieren. Es bietet dem Benutzer über eine Graphical User Interface (GUI) die Möglichkeiten, formale Eigenschaften für Wahlverfahren sowie diese Wahlverfahren selbst anzugeben und zu editieren. Weiterhin liefert es Möglichkeiten die Interaktion mit CBMC zu gestalten: Für wie viele Wähler, Plätze etc geprüft werden soll. Nach erfolgreicher Überprüfung durch CBMC bekommt der Benutzer schließlich eine Antwort des Programms, in der er bei Nichterfüllung der Eigenschaft ein Gegenbeispiel angezeigt bekommt. Sollte die Prüfung jedoch erfolgreich sein, bekommt der Nutzer ein Positivbeispiel präsentiert. All dies wird graphisch über die GUI aufbereitet.

Die GUI ist nach Funktionalität in vier Teilen angeordnet:

1. „Rigtime“: Code-Editor für Wahlverfahren in Programmiersprache C.
2. „Properties“: Editor für Spezifikation formaler Eigenschaften in abgespeckter C-Syntax mit speziellen Macros.
3. „Params“: Eingabe von Parametern einer zu analysierenden Wahl mit Anzahl der Wähler, Kandidaten und Sitzen. s

4. „Rigplete“: Ausgabe der Prüfung.

2 Zielbestimmung

Ziel des Programmes ist es, eine komfortable, graphische Lösung zur Untersuchung formaler Eigenschaften von Wahlverfahren zu präsentieren, welche auch von Nicht-Informatikern mit minimalem Aufwand erlernt und eingesetzt werden kann. Es soll Folgendes bereitstellen:

- Eine Möglichkeit zur Beschreibung diverser Wahlverfahren in C-Code
- Eine Möglichkeit zur Beschreibung der formalen Eigenschaften, welche das Wahlverfahren erfüllen soll, in abgespeckter C Syntax
- Eine Möglichkeit zum Angeben der Parameter (Anzahl Wähler, Anzahl Kandidaten, Anzahl Sitze)
- Eine Ausgabe des Ergebnisses der Überprüfung: eine Erfolgsmeldung bei Erfolg und Präsentation eines Gegenbeispiels bei Nichterfolg

Die letztendliche Überprüfung wird durch den CBMC geschehen. Aufgabe des Programmes wird es sein, die gegebenen Eingaben für den CBMC aufzubereiten sowie dessen Ausgabe zu interpretieren und präsentieren.

All diese Aufgaben ließen sich theoretisch auch schon jetzt, ohne Verwendung unseres Programms erledigen. Allerdings wäre der damit verbundene Lern- und Einarbeitungsaufwand sehr hoch, vor allem bei der Angabe der formalen Eigenschaften. Daher ist ein enorm wichtiger Schwerpunkt unseres Programmes einfache Benutzung, auch und besonders für Nicht-Informatiker. Dies soll erreicht werden über eine leicht zu navigierende und intuitive GUI. Dadurch soll das Untersuchen von Wahlverfahren deutlich leichter und schneller werden, was den Mehrwert unseres Programmes ausmacht.

•

2.1 Musskriterien

- Das Programm kann auf aktuellen 32-Bit Versionen von Windows und Linux-Betriebssystemen betrieben werden
- Alle Abhängigkeiten werden mit dem Programm ausgeliefert
- Das Programm bietet einen Code-Editor für das zu prüfende Wahlverfahren
 - Der Code kann abgespeichert und geladen werden
 - Der Code-Editor zeigt Fehler im eingegebenen Code an

- Aktionen können widerrufen und wiederhergestellt werden
- Es können formale Eigenschaften zur Prüfung des Wahlverfahrens eingegeben werden
 - Eine formale Eigenschaft kann abgespreichert und geladen werden
 - Fehler in der Eingabe werden angezeigt
- Die Parameter der Wahl (Anzahl von Wählern, Kandidaten und Sitzen) können festgelegt werden
- Das Ergebnis der Überprüfung wird vom Programm angezeigt. Im Fall der Verletzung einer formalen Eigenschaft wird ein Gegenbeispiel vom Programm angezeigt

2.2 Sollkriterien

- Die Parameter der Wahl können in Intervallen angegeben werden.
- Der Code-Editor bietet folgendes:
 - Syntax-Highlighting
 - Automatisches Einrücken
 - Tastatur-Shortcuts
 - Codevorlagen
- Es gibt Code completion bei der Eingabe der formalen Eigenschaften
- Die Analyse des Wahlverfahrens kann abgebrochen werden.

2.3 Wunschkriterien

- Das Programm kann auf einem Mac betrieben werden
- Der Code-Editor bietet folgendes:
 - Code completion
 - Warnung vor nicht unterstützten Elementen der Programmiersprache
- Es kann festgelegt werden, wie lange die Analyse des Wahlverfahrens maximal dauern soll
- Eine Wahl kann eingegeben werden. Das Ergebnis wird angezeigt.

2.4 Abgrenzungskriterien

XXX open

3 Produkteinsatz

Das Programm überprüft Wahlverfahren auf ihre formalen Eigenschaften. Es richtet sich an Kunden, die ein Interesse an der Erforschung oder Entwicklung solcher Verfahren haben. Sie benötigen ein Grundverständnis der Programmiersprache C und Logik.

3.1 Anwendungsbereiche

- Universitärer Bereich
- Forschung

3.2 Zielgruppen

- Wahlforscher
- Softwareentwickler

3.3 Betriebsbedingungen

Das Produkt kommt in einer Büroumgebung zum Einsatz. Es wird auf einem aktuellen Computer mit aktuellen Werten für Arbeitsspeicher und Rechnergeschwindigkeit betrieben.

4 Produktumgebung

4.1 Software

- Das Betriebssystem ist entweder Microsoft Windows oder eine Linux-Distribution

4.2 Hardware

- PC mit Tastatur und Maus

4.3 Orgware

Es kommt keine Orgware zum Einsatz.

4.4 Produkt-Schnittstellen

Über das Produkt wird der SAT-Solver CBMC angesteuert. Es sorgt für die Konfiguration von CBMC und interpretiert die Ergebnisse.

5 Funktionale Anforderungen

5.1 Allgemein

/F10/ Bereitstellen von Editoren zur Beschreibung des Wahlverfahrens sowie zur Beschreibung zu erfüllender formaler Eigenschaften

/F20/ Kommunikation und Überprüfung dieser Eigenschaften via CBMC

/F30/ Bereitstellen von Kommunikationsschnittstellen mit CBMC sowohl für Eingabe von Parametern als auch Ausgabe der Ergebnisse, welche auch für Nicht-Informatiker verständlich ist

/F40/ Möglichkeit des Speicherns von Code, formaler Anforderungen und Eingabeparametern als ein Projekt

5.2 C-Code Editor für Wahlverfahren

/F10/ Darstellung aller für das Programmieren in C benötigten Charaktere

/F20/ Veränderung des dargestellten Textes durch Eingabe anderer Charaktere über die Tastatur wie in Notepad

/F30/ Speichern von erstelltem Code in Dateiformat `datei.c`

/F40/ Laden und Darstellen von `.c` Dateien

/F50/ Automatisches Einrücken des Codes in Schleifen und `if`-Statements

/F60/ Code-Completion

- Automatisches Schließen von Klammern und Anführungszeichen
- Primitiv: Vorschlagen bereits im Code vorgekommener Wörter
- Intelligent: Durch Analysieren eines ASTs nur Vorschlagen der Wörter welche im Kontext Sinn ergeben.

/F70/ Syntax-Highlighting: Darstellung diverser Schlüsselwörter in anderen Farben als den Rest des Codes. Dies beinhaltet, ist jedoch nicht beschränkt auf:

- Typendeklaration (`int`, `float`, `structs...`)
- Kontrollflow-Konstrukte (`if`, `else`, `while...`)
- Kommentare

/F80/ Durch den User konfigurierbares Verhalten:

Tabelle 5.1: Hotkeys und verbundene Operationen

Kürzel	Operation
Strg + c	Kopieren
Strg + x	Auschneiden
Strg + v	Einfügen
Strg + z	Zuletzt ausgeführte Aktion rückgängig machen
Strg + r	Zuletzt rückgängig gemachte Aktion erneut ausführen
Strg + s	Speichern
Strg + o	Öffnen
Strg + Leer	Anzeigen der Code-Completion Vorschläge

- Festlegen der Farben, welche beim Syntax-Highlighting verwendet werden
- Festlegen des verwendeten Fonts

/F90/ Anzeigen von Syntaktischen Fehlern im Code, welche durch einen Lexer oder Parser erkannt werden können:

- Verwendung von Schlüsselwörtern als Variablennamen
- Vergessene Semikolons am Ende von Anweisungen

/F100/ Reaktion auf typische Tastenkürzel (siehe 5.1)

/F110/ Bereitstellen von Wahl-Templates

- Jeder Wähler wählt genau einen Kandidaten
- Jeder Wähler ordnet Kandidaten nach Präferenz in absteigender Reihenfolge
- Jeder Wähler ordnet Kandidaten eine Nummer zwischen 100 (maximale Zustimmung) und 0 (maximale Abneigung) zu

5.3 Editor für formale Eigenschaften

/F10/ Darstellung aller für das Programmieren in C benötigten Charaktere

/F20/ Veränderung des dargestellten Textes durch Eingabe anderer Charaktere über die Tastatur wie in Notepad

/F21/ Beschreibung formaler Eigenschaften als Vor- und Nachbedingung in abgespeckter C-Syntax

/F30/ Bereitstellung von Makros zur Beschreibung der Eigenschaften (siehe 5.2)

/F40/ Bereitstellen symbolischer Variablen für Wähler, Kandidaten und Sitze

/F50/ Bereitstellen von Operatoren für Implikation und Äquivalenz

/F60/ Beliebig tiefe, lediglich von Hardware begrenzte, Schachtelung dieser Konstrukte

Tabelle 5.2: Makros zur Beschreibung formaler Eigenschaften

Makro	Effekt
FOR_ALL_VOTERS(E)	checkt ob E für alle Wähler gilt
FOR_ALL_CANDIDATES(E)	checkt ob E für alle Kandidaten gilt
FOR_ALL_SEATS(E)	checkt ob E für alle Sitze gilt
EXISTS_ONE_VOTER(E)	checkt ob E für zumindest einen Wähler gilt
EXISTS_ONE_CANDIDATE(E)	checkt ob E für zumindest einen Kandidaten gilt
EXISTS_ONE_SEAT(E)	checkt ob E für zumindest einen Sitz gilt
VOTE_SUM_FOR_CANDIDATE(c)	gibt die Anzahl Stimmen für Kandidaten c zurück

/F70/ Syntax-Highlighting

/F80/ Anzeigen von Syntaktischen Fehlern im Code

/F90/ Code-Completion

- Auto-Vervollständigung der Makros
- Analyse des Codes und Anzeigen relevanter, bereits definierter Eigenschaften und symbolischer Variablen

5.4 Editor für Eingabeparameter

/F10/ Möglichkeit zur Angabe der zu analysierenden Anzahl von Wählern, Kandidaten und Sitzen

/F20/ Möglichkeit zum Eingeben einer Zeitspanne nach welcher die Berechnung abgebrochen wird

5.5 Ausgabe der Analyseergebnisse

/F10/ Ausgabe einer Erfolgsmeldung bei Erfolg

/F20/ Graphische Darstellung eines Gegenbeispiels

6 Produktdaten

6.1 Code-Editor Wahlverfahren

/D10/ Das Wahlverfahren ist als Methode „unsigned int voting(params)“ einer C-Headerdatei definiert und wird mit der Endung .h gespeichert.

6.2 Editor von formalen Eigenschaften

/D20/ Die formale Eigenschaft, derer das Wahlverfahren genügen muss ist als C-Datei definiert, die einmal die Methode voting(params) aus einer Headerdatei aufruft, und wird mit der Endung .c gespeichert.

/D30/ Ein Projekt wird als Dateiliste gespeichert

7 Nichtfunktionale Anforderungen

/F10/ Nicht mehr als 0,5 Sekunden Verzögerung bei Erfragen der Code-Completion

8 Globale Testfälle

8.1 Laden von Wahlverfahren

1. Stand: Das Programm wartet auf eine Aktion. Der Nutzer will ein Wahlverfahren laden.

Aktion: Der Nutzer betätigt mit der Maus einen Button mit einem Ladeicon innerhalb des GUIs für Wahlverfahren.

Reaktion: Das Programm öffnet einen Dateibrowser.

2. Stand: Der Dateibrowser ist geöffnet.

Aktion: Der Nutzer wählt eine zu ladende C-Datei aus und bestätigt diese durch den Tastendruck

Enter oder durch einen Klick auf den Ladebutton mit der Maus Reaktion: Falls die Änderungen im vorherigen Wahlverfahren nicht gespeichert wurden öffnet ein neues Pop-up-Fenster. (2.1) Sonst folgt (2.2)

2.1 Je nachdem wie sich der Nutzer entscheidet werden entweder Punkt 2.1.1 Punkt 2.1.2, oder Punkt 2.1.2 ausgeführt.

2.1.1 Stand: Der Nutzer will die Änderungen verwerfen. Aktion: Der Nutzer betätigt den Button Verwerfen des Pop-Ups Reaktion: Das neue C-Programm wird in den Wahlverfahreneditor geladen. Das zuvor geladene C-Programm wird verworfen. Das Pop-up sowie der Dateibrowser schließen sich

2.1.2 Stand: Der Nutzer will das Laden abbrechen Aktion: Der Nutzer betätigt den Button abbrechen des Pop-Ups Reaktion: Pop-up sowie Dateibrowser schließen sich

2.1.3 Stand: Der Nutzer will die Änderungen an seinem alten C-Programm speichern und das neue Dokument laden Aktion: Der Nutzer betätigt den Button Änderungen speichern Reaktion: Die Änderungen am vorherigen C-Programm werden gespeichert. Das neue C-Programm wird in den Wahlverfahreneditor geladen.

2.2 Nur falls keine Aktion 2.1 ausgeführt wurde: Stand: Der Nutzer hat bereits das Laden bestätigt Aktion: - Reaktion: Das neue C-Programm wird in den Wahlverfahreneditor geladen. Laden von zu testenden Eigenschaften:

1. Stand: Das Programm wartet auf eine Aktion. Der Nutzer will eine Eigenschaft von Wahlverfahren (EvW) laden Aktion: Der Nutzer betätigt mit der Maus einen Button mit einem Ladeicon innerhalb des GUIs für die Eigenschaften von Wahlverfahren Reaktion: Das Programm öffnet einen Dateibrowser 2. Stand: Der Dateibrowser ist geöffnet: Aktion: Der Nutzer wählt eine zu EvW aus und bestätigt diese durch den Tastendruck Enter oder durch einen Klick auf den Ladebutton mit der Maus Reaktion: Falls die Änderungen im vorherigen Wahlverfahren nicht gespeichert wurden öffnet ein neues Pop-up-Fenster. (2.1) Sonst folgt 2.2 2.1 Je nachdem wie sich der Nutzer entscheidet werden entweder

Punkt 2.1.1 Punkt 2.1.2, oder Punkt 2.1.2 ausgeführt.

2.1.1 Stand: Der Nutzer will die Änderungen verwerfen. Aktion: Der Nutzer betätigt den Button Verwerfen des Pop-Ups Reaktion: Die neue EvW wird in den Editor für Eigenschaften von Wahlverfahren geladen. Die zuvor geladene EvW werden verworfen. Das Pop-up sowie der Dateibrowser schließen sich 2.1.2 Stand: Der Nutzer will das Laden abbrechen Aktion: Der Nutzer betätigt den Button abbrechen des Pop-Ups Reaktion: Pop-up sowie Dateibrowser schließen sich

2.1.3 Stand: Der Nutzer will die Änderungen seiner vorherigen EvW speichern und die neuen EvW laden. Aktion: Der Nutzer betätigt den Button Änderungen speichern Reaktion: Die Änderungen an den vorherigen EvW werden gespeichert. Die neuen EvW werden in werden in den Editor für EvW geladen. Pop-up sowie Dateibrowser schließen sich

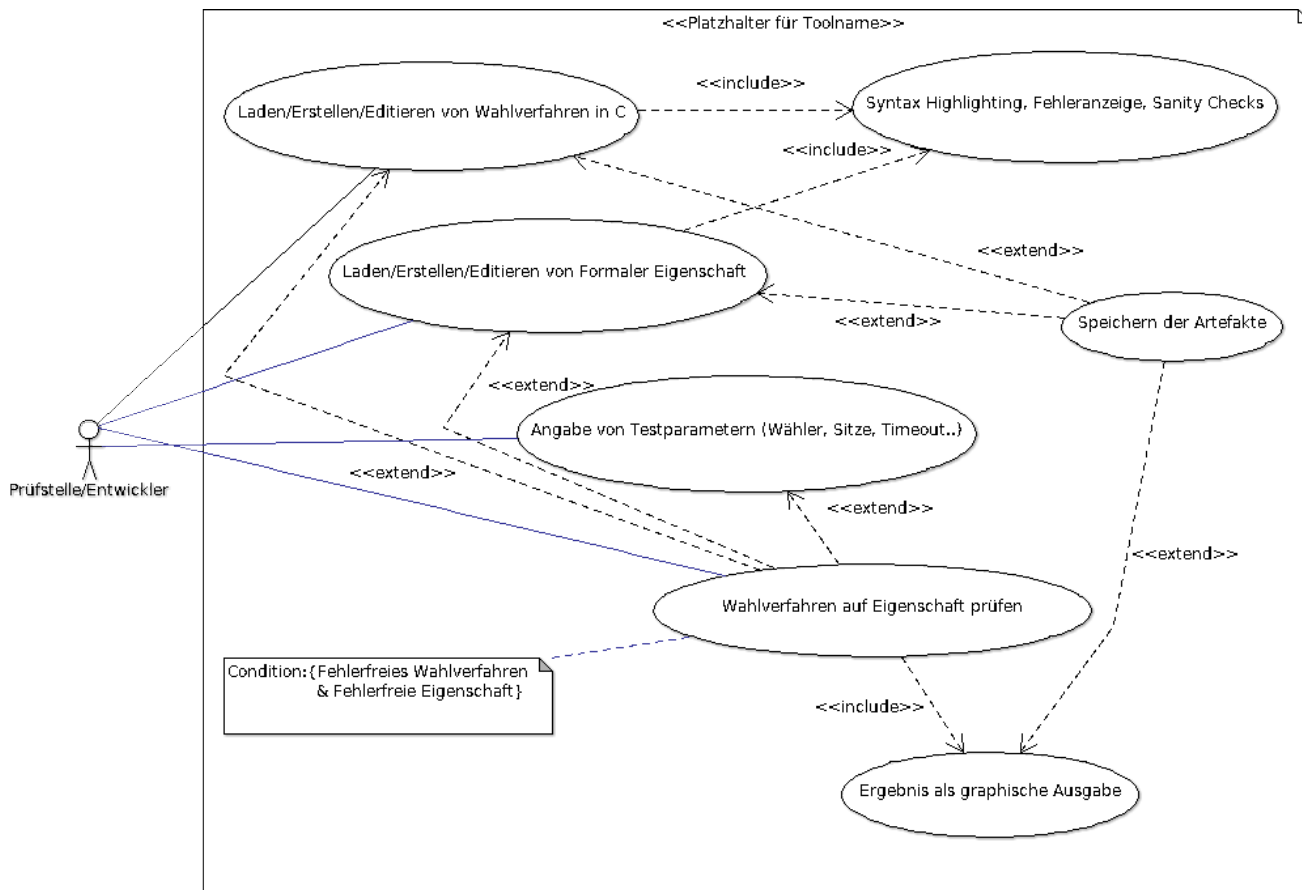
2.2 Nur falls keine Aktion 2.1 ausgeführt wurde: Stand: Der Nutzer hat bereits das Laden bestätigt Aktion: - Reaktion: Die neue EvW wird in den Wahlverfahreneditor geladen. SSpeichern von Wahlverfahren (WV) oder von EvW 1. Stand: Das Programm wartet auf eine Eingabe Aktion: Der Nutzer betätigt das Saveicon im entsprechenden Fenster Reaktion: Das Programm speichert das WV oder die EvW. Falls für dieses Dokument noch kein Speicherort definiert wurde öffnet sich die Reaktion von SSpeichern unterSSpeichern unter von WV oder EvW 1. Stand: Das Programm wartet auf eine Eingabe Aktion: Der Nutzer betätigt das Save-as-icon im entsprechenden Fenster Reaktion: Ein Dateibrowser wird geöffnet 2. Stand: Der Dateibrowser ist geöffnet Aktion: Der Nutzer gibt einen Speicherort und einen Namen für das zu speichernde Dokument an und bestätigt seine Eingabe Reaktion: Das Dokument wird mit dem genannten Namen an den gewählten Ort gespeichert. Eingabe der Anzahl der Wähler 1. Stand: Das Programm wartet auf eine Eingabe: Aktion: In einem Eingabe-Fenster verändert der Nutzer die Anzahl der Wähler und bestätigt diese. Reaktion: Die neue Anzahl der Wähler wird gespeichert Eingabe der Anzahl der Kandidaten 1. Stand: Das Programm wartet auf eine Eingabe: Aktion: In einem Eingabe-Fenster verändert der Nutzer die Anzahl der Kandidaten und bestätigt diese Reaktion: Die neue Anzahl der Kandidaten wird gespeichert Eingabe der Timeoutzeit 1. Stand: Das Programm wartet auf eine Eingabe: Aktion: In einem Eingabe-Fenster gibt der Nutzer eine Anzahl an Minuten für den Timeout an und bestätigt diese. Reaktion: Das Programm speichert die neue Timeoutzeit Überprüfung des WV auf EvW: 1. Stand: In beiden Editoren sind gültige Dokumenten. Es sind Werte für die Anzahl der Stimmen, der Sitze, der Kandidaten und der Timeoutzeit gesetzt Aktion: Der Nutzer betätigt die Auf Eigenschaften prüfenTaste Reaktion: Das Programm bestätigt die Eigenschaft mit anschaulichen Werten oder gibt ein konkretes Gegenbeispiel im Ausgabefenster. Bearbeiten des WV: 1. Stand: Das Programm wartet auf eine Eingabe Aktion: Der Nutzer ändert das C-Programm Reaktion: Im Interface sieht man, dass sich das Programm geändert hat. Das Programm highlighted korrekte C-Syntax Bearbeiten der EvW: 1. Stand: Das Programm wartet auf eine Eingabe Aktion: Der Nutzer ändert die EvW Reaktion: Macros werden als Vorschläge ergänzt.

9 Systemmodelle

9.1 Szenarien

9.2 Anwendungsfälle

Eine Prüfstelle oder ein Entwickler gibt dem Tool ein Wahlverfahren in C und eine formale Eigenschaft über beziehungsweise entwickelt diese selbst in den jeweiligen Editoren des Tools. Werden diese als plausibel erkannt kann er das Wahlverfahren, auch mit Angabe eigener Testparameter (Wähler, Sitze, Timeout...), auf die Eigenschaft prüfen und erhält das Ergebnis als graphische Ausgabe. Diese kann dann, sowie auch Wahlverfahren und formale Eigenschaft, abgespeichert werden.



9.3 Objektmodelle

9.4 Dynamische Modelle

10 GUI

11 Phasenverantwortliche

11.1 Pflichtenheft

Justin Hecht

11.2 Entwurf

11.3 Implementierung

11.4 Qualitätssicherung

11.5 Abschlusspräsentation

12 Glossar

Abbildungsverzeichnis