

PSE: Analyse formaler Eigenschaften von Wahlverfahren

Pflichtenheft

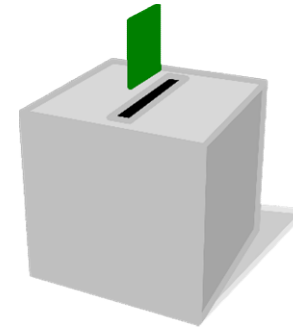
Bearbeiter: Justin Hecht, Holger Klein, Niels Hanselmann, Nikolai Schnell,
Lukas Stapelbroek, Jonas Wohnig

Betreuer: Prof. Bernhard Beckert, Sarah Grebing, Michael Kirsten

INSTITUT FÜR THEORETISCHE INFORMATIK – ANWENDUNGSORIENTIERTE FORMALE VERIFIKATION

Wahlen

- Einfacher Vorgang?
 - X Wähler
 - Y Kandidaten
 - Z Sitze
- Welches Wahlverfahren?
 - 2008 Bundestagswahl für verfassungswidrig erklärt, weil keine Stimmengleichheit vorherrschte
- Andere formale Eigenschaften?
 - Anonymität
 - Monotoniekriterium
 - Mehrheitsprinzip

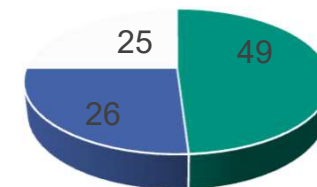


Verletzung Monotoniekriterium

- Überprüfung auf formale Eigenschaften ist im Allgemeinen unentscheidbar
- Suche kann lange dauern
- Beispiel: Instant-Runoff-Voting verletzt Monotoniekriterium

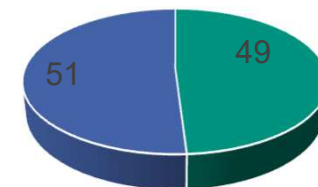
49%	26%	25%
<ul style="list-style-type: none"> • CDU • SPD • AfD 	<ul style="list-style-type: none"> • AfD • CDU • SPD 	<ul style="list-style-type: none"> • SPD • AfD • CDU

1. Durchlauf



■ CDU ■ AfD ■ SPD ■

2. Durchlauf



■ AfD ■ CDU

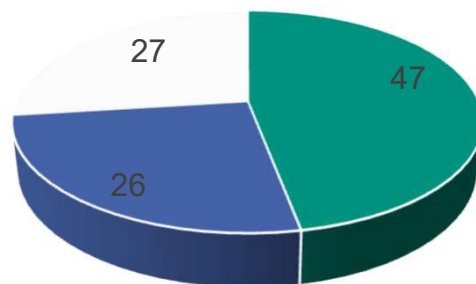
Verletzung Monotoniekriterium

- CDU-Wähler können der eigenen Partei nützen, wenn sie eine andere Partei favorisieren

47%	2%	26%	25%
<ul style="list-style-type: none"> • CDU • SPD • AfD 	<ul style="list-style-type: none"> • SPD • CDU • AfD 	<ul style="list-style-type: none"> • AfD • CDU • SPD 	<ul style="list-style-type: none"> • SPD • AfD • CDU

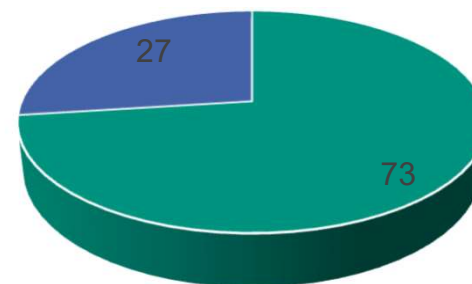
→ Monotoniekriterium verletzt

1. Durchlauf



■ CDU ■ AfD ■ SPD

2. Durchlauf



■ CDU ■ SPD

Auftritt: BEAST

Bounded Election Attribute Structuring Tool

Das Ziel:

- Eingabe Wahlverfahren
- Eingabe formaler Eigenschaften
- Optional: Angabe von Wahlparametern
- Aufruf eines BMC (Bounded Model Checker), um die Erfüllung formaler Eigenschaften zu analysieren
- Graphische Ausgabe der Rückgabe



CBMC

- CBMC: Bounded Model Checker for C
 - Überprüft Vor- und Nachbedingungen innerhalb bestimmter Grenzen
 - Wird über Kommandozeile angesteuert
- Ausgabe soll von BEAST interpretiert werden:
 - Ja, Eigenschaft erfüllt → Erfolgsmeldung.
 - Nein, nicht erfüllt → Präsentiere ein Gegenbeispiel.



Angabe formaler Eigenschaften

Eigenschaft:

Kandidat mit den meisten Stimmen gewinnt.

Symbolische Variable: Kandidat x

Vorbedingung:

- $\text{FOR_ALL_CANDIDATES}(i) : \text{VOTE_SUM_FOR_CANDIDATE}(x) > \text{VOTE_SUM_FOR_CANDIDATE}(i);$

Nachbedingung:

- $\text{ELECT} == x;$

Einsatz von BEAST

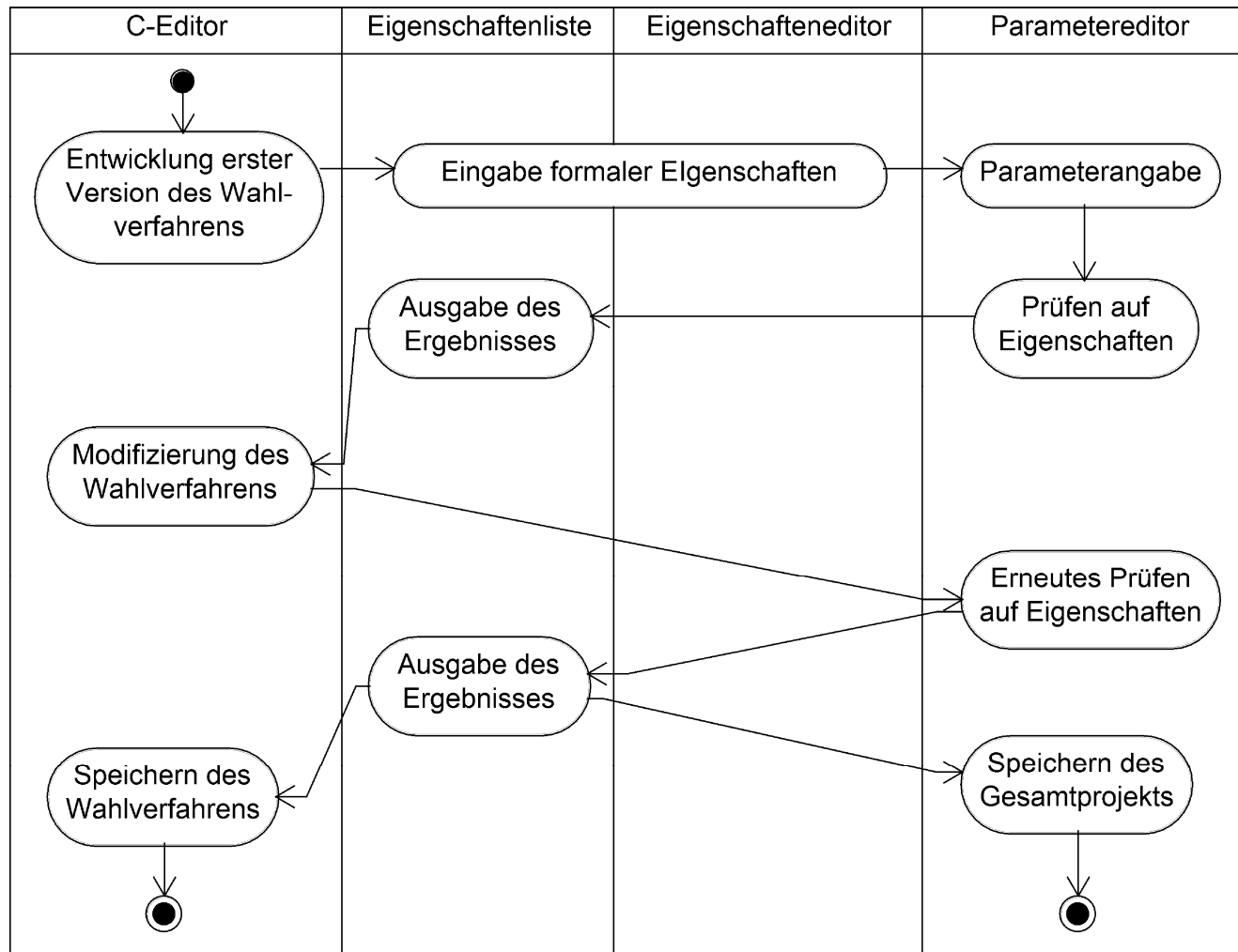
Zielgruppen:

- Wahlforscher
- Mitarbeiter in Prüfstellen
- Entwickler
- Interessierte

Produktumgebung:

- Windows / Linux (Arch und Ubuntu)
- Java SRE 8
- Schnittstellen: ANTLR, CBMC, GCC

Aktivitätsdiagramm

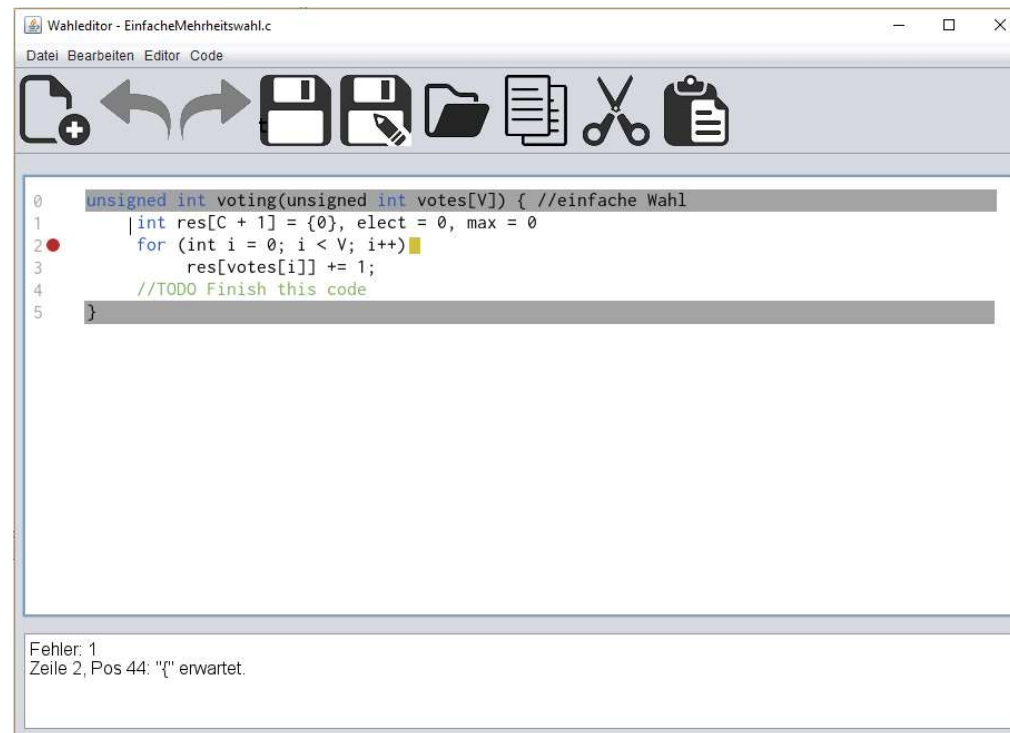


GUI und Anforderungen: C-Editor

Muss: Editorfunktionen und synchrone Fehleranzeige

Soll: Formatüberprüfung, Kürzel und Wahl-Templates

Kann: Code-Completion und asynchrone Fehleranzeige



```
0 unsigned int voting(unsigned int votes[V]) { //einfache Wahl
1     int res[C + 1] = {0}, elect = 0, max = 0
2     for (int i = 0; i < V; i++)
3         res[votes[i]] += 1;
4     //TODO Finish this code
5 }
```

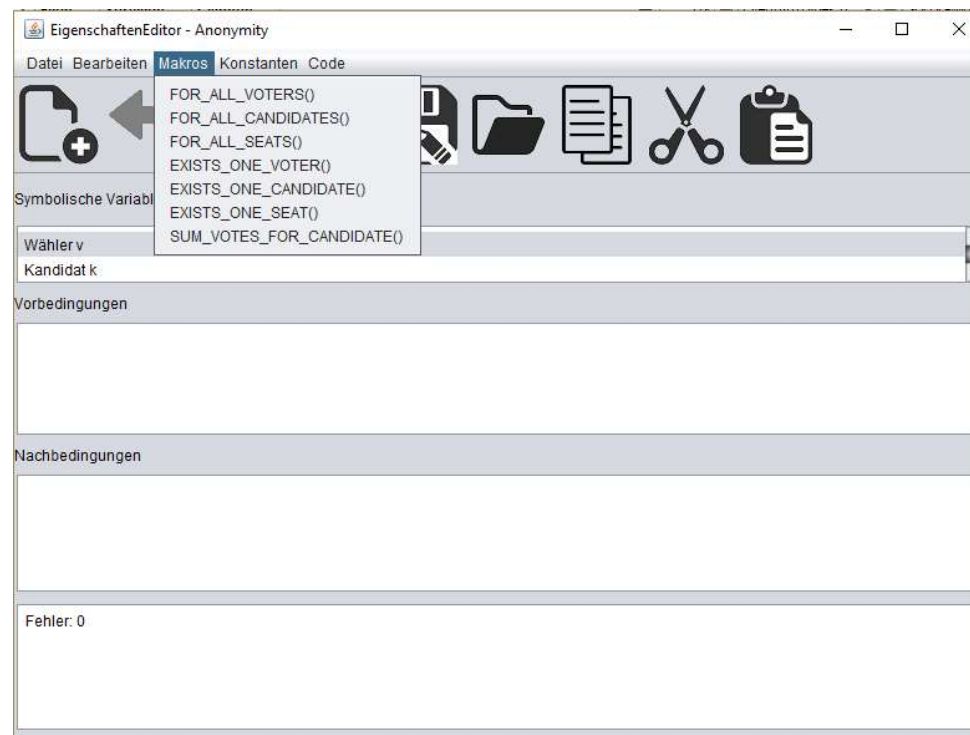
Fehler: 1
Zeile 2, Pos 44: "{" erwartet.

GUI und Anforderungen: Eigenschafteneditor

Muss: Editorfunktionen, Makros, Operatoren und Sanity Checks

Soll: Kürzel und Fehleranzeige

Kann: Code-Completion



GUI und Anforderungen: Eigenschaftenliste

Muss:

- Eigenschaften in Listenform
- Individuelles An- und Ausschalten der Überprüfung
- Listen speichern und laden



GUI und Anforderungen: Parametereditor

Muss:

- Angabe von Wahlparametern
- Dauer der Überprüfung
- Erweiterte Parametereingabe
- Projekte
- Eigentliche Startmöglichkeit für Analyse



Ein Testfall für den Parametereditor

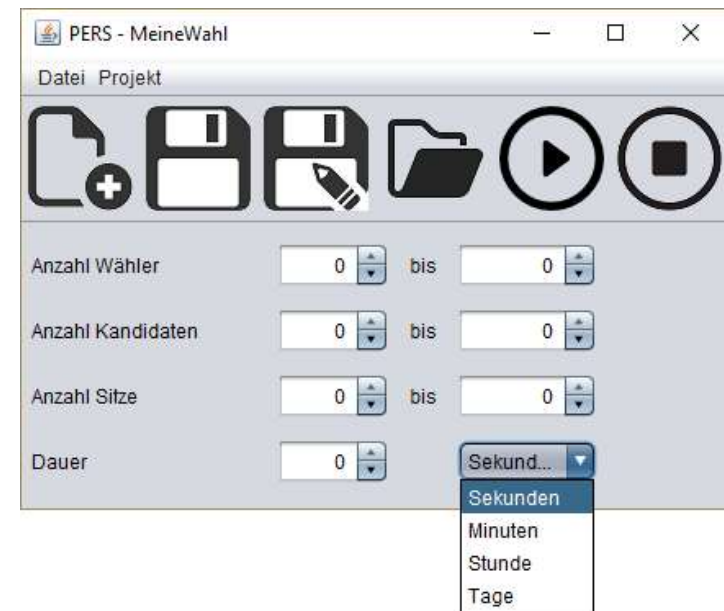
/T620/ Eingabe einer maximalen Zeitspanne

/FM4020/ Sanity-Checks: Alle Parameter größer 0, $\text{Min} < \text{Max}$

/FM4030/ Angabe einer Zeitspanne, nach der Berechnung abgebrochen wird

Nachbedingung (Erfolg):

Abbruch der Überprüfung nach Zeitspanne



Daten und Qualität

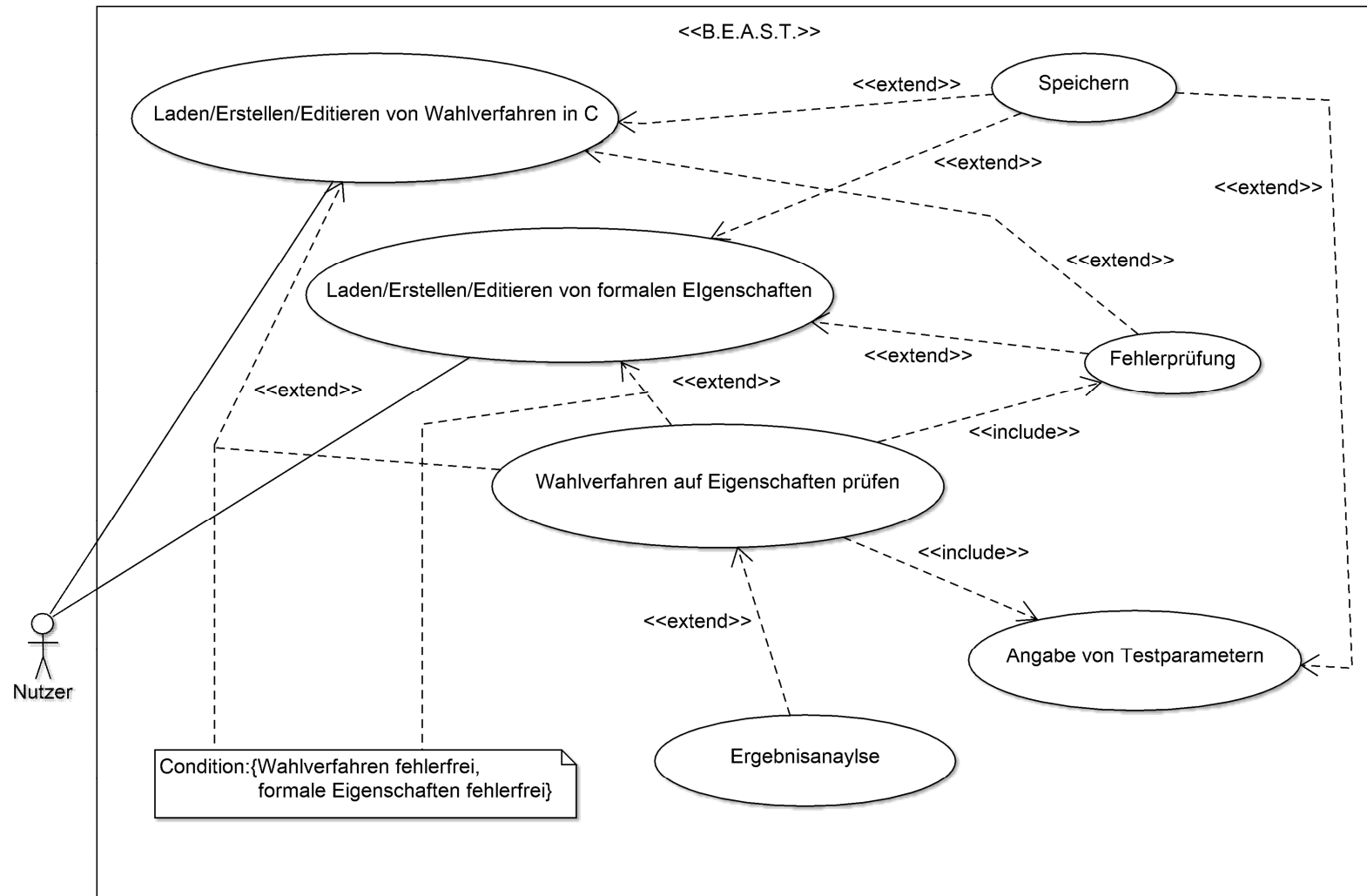
Produktdaten:

- Wahlverfahren (Vorlagen und eigens erstellte)
- Formale Eigenschaften
- Parameterdaten
- Eigenschaftenliste
- Projekte

Qualitätsanforderungen:

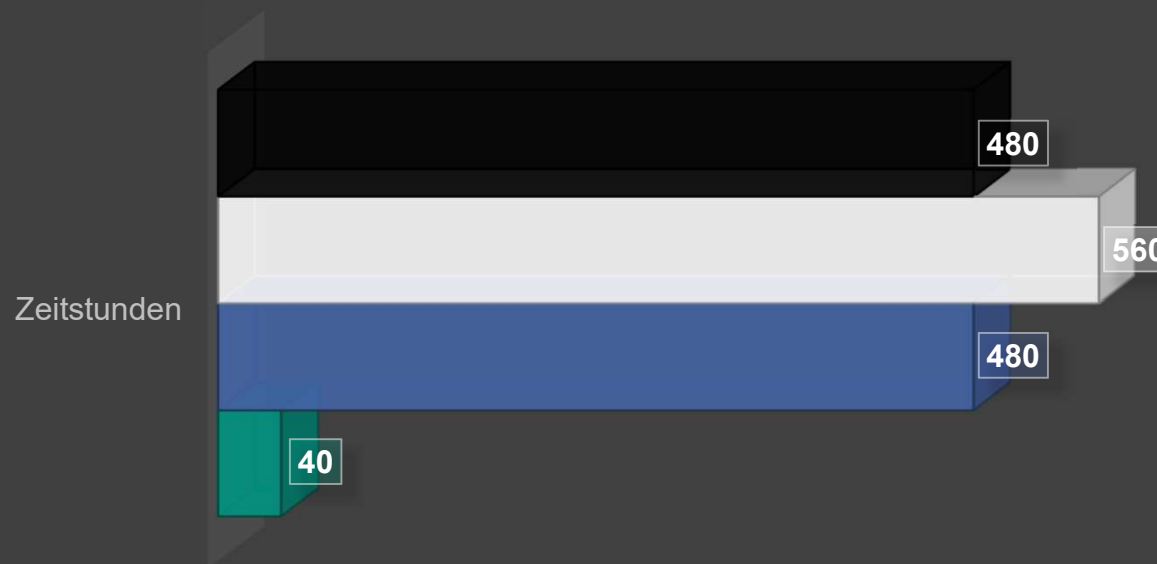
Sehr relevante Anforderungen sind Fehlertoleranz, Bedienbarkeit und Modifizierbarkeit des Programms.

Systemmodelle: Use-Case-Diagramm



REST DES PROJEKTS: CA. 1500 ZEITSTUNDEN

■ Entwurf ■ Implementierung ■ Qualitätssicherung ■ Abschlusspräsentation



Unteraufteilung Entwurfsphase

Subphase	Anteil
Parametereditor	10%
C-Editor	15%
Eigenschafteneditor	15%
Eigenschaftenliste	10%
CBMC-Schnittstelle	10%
Dateiverwaltung	5%
Input-Manager	10%
Rest	25%

Phasenverantwortlicher: Holger Klein

Unteraufteilung Implementierungsphase

Subphase	Anteil
GUI	35%
C-Code-Analyse	30%
Dateiverwaltung	10%
Rest	25%

Phasenverantwortliche: Niels Hanselmann, Nikolai Schnell

Unteraufteilung Qualitätssicherung

Subphase	Anteil
Test der GUI	25%
Testfälle für die Codeanalyse	25%
Testfälle für CBMC	15%
Test des Datensystems	10%
Rest	25%

Phasenverantwortlicher: Lukas Stapelbroek

Unteraufteilung Abschlusspräsentation

Subphase	Anteil
Nachbearbeitung aller Phasen	75%
Erstellen der Präsentation	25%

Phasenverantwortlicher: Jonas Wahnig

Ende der Präsentation

Die Entwickler von BEAST sagen: Vielen Dank für die Aufmerksamkeit!

Wer sich im deutschen Wahlrecht ein bißchen auskennt und dies auch noch anderen Leuten kundtun will, kann sehr schnell sehr einsam werden. Denn die sicherste Methode, eine muntere Gesprächsrunde zu sprengen, ist, einen kleinen Monolog über das Zustandekommen von Überhangmandaten sowie über den Unterschied zwischen Erst- und Zweitstimme zu halten. So etwas will kaum jemand wissen, was – nebenher gesagt – schon seit Jahren dazu führt, daß die FDP es immer wieder in den Bundestag schafft, und zwar, weil die Leute glauben, die Zweitstimme sei weniger wichtig und könne deshalb mildtätigen Zwecken zukommen. Selbst die tapfersten Zuhörer kramen an dieser Stelle normalerweise nach ihrem Autoschlüssel, spätestens aber ergreifen sie die Flucht bei den unglaublich öden Details der Stimmenauszählmethoden nach d'Hondt und/oder Hare/Niemeyer.

(Aus dem Spiegel 44/1997)