Rein funktionelle Implementierung eines CDCL SAT-Solvers

Purely functional implementation of a CDCL SAT solver

Bachelorarbeit

Thanh Nam Pham
Matrikelnummer
Katharina-Mair-Straße 142
85356 Freising

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Vollständiges Wort	Abkürzung
Conflict-driven clause learning	CDCL
Davis-Putnam	DP
Davis-Putnam-Logemann-Loveland	DPLL
Falsch	F
First Unique Implication Point	1UIP
Satisfiability Problem	SAT-Problem
Satisfiable	SAT
Unique Implication Point	UIP
Unsatisfiable	UNSAT
Wahr	T

1 Einleitung

Das Boolean Satisfiability Problem (SAT), auf Deutsch Erfüllbarkeitsproblem der Aussagenlogik, ist das erste Problem, welches durch den „Satz von Cook“ im Jahr 1971 als NP-vollständig bewiesen wurde [4]. Das SAT-Problem ist in der Praxis sehr wichtig, weshalb trotz NP-Vollständigkeit viel Forschung in diesem Bereich betrieben wurde. Mitunter wurden mehrere SAT-Solver entwickelt, wie z.B. zChaff und MiniSAT.

Die Entwicklung von effizienten SAT-Solvern ist seit dem Jahr 2002 stetig angestiegen. Jedoch wird für die Programmierung dieser Solver hauptsächlich eine objektorientierte Programmiersprachen verwendet. Im Gegensatz dazu ist der Anteil von SAT-Solvern, welche komplett in einer rein funktionalen Programmiersprache geschrieben wurden, sehr gering.

Im Rahmen dieser Bachelorarbeit wird der Frage nachgegangen, wie eine mögliche Umsetzung eines „Conflict-driven clause learning“ (CDCL) SAT-Solvers in einer rein funktionalen Programmiersprache aussehen könnte. Das Ziel dieser Arbeit ist eine Implementierung eines CDCL SAT-Solvers in Haskell und mögliche Vorschläge wie deren Implementierung verbessert werden kann.

Anhand einer Literaturarbeit werden bestehende Algorithmen untersucht, wofür verschiedene Arbeiten über CDCL und näherstehende Arbeiten betrachtet werden. Die Literaturarbeit wurde gewählt, um bestehende Erforschungen in diesem Fachbereich zu erhalten.

In dieser Arbeit werden zuerst die verschiedenen Programmierparadigmen und die verwendete Programmiersprache Haskell in Kapitel 2 erläutert. Daraufhin werden SAT und verschiedene SAT-Solver in Kapitel 3 vorgestellt, wobei auch ein Einblick in die SAT-Competitions gewährt wird. Danach wird der Unterschied zwischen dem CDCL-Algorithmus und dem Davis-Putnam-Logemann-Loveland-Algorithmus (DPLL) in Kapitel 4 erklärt. Das darauffolgenden Kapitel 5 beinhaltet eine Beschrei-

bung für eine Umsetzung eines CDCL SAT-Solvers. Ein Vergleich der Implementierung mit anderen CDCL SAT-Solvern wird in Kapitel 6 durgeführt. Im letzten Teil der Arbeit (Kapitel 7) wird ein Fazit über die gewonnenen Erkenntnisse gezogen als auch ein Ausblick über Verbesserungsmöglichkeiten für eine bessere Effizienz des SAT-Solvers gegeben.

2 Funktionale Programmierung

In diesem Abschnitt werden die zwei verschiedenen Programmierparadigmen (imperative und deklarative Programmierung), funktionale Programmierung und die Programmiersprache Haskell kurz vorgestellt.

2.1 Imperative Programmierung

Folgende Definition von der Universität Passau für imperative Programmierung wurde verwendet: „Imperative Programme beschreiben Programmabläufe durch Operationen auf Zuständen“ [11]. Dies bedeutet dass der Ablauf des Programmes durch die Reihenfolge der Befehle maßgeblich für das erwartete Ergebnis ist. Sprachen, die zu diesem Paradigma gehören, sind z.B. Java, C++ oder C.
Die imperative Programmierung kann in weitere Paradigmen unterteilt werden, wie z.B. strukturierte Programmierung, objektoriertierte Programmierung, modulare Programmierung [1].

2.2 Deklarative Programmierung

Weiterführende Definition für deklarative Programmierung wurde von der Passauer Universität übernommen: „Deklarative Programme beschreiben Berechnungen durch eine Ein-/Ausgaberelation. Der Kontrollfluß ist dem Programmierer nicht explizit zugänglich; der Ablauf der Berechnung kann aber trotzdem durch den Programmaufbau beeinflußt werden.“ [11] Sinngemäß bedeutet dies, dass nicht der Weg zum Ergebnis das Entscheidende ist, sondern die Spezifaktion des Problemes und der Ergebnisse selbst.
Die deklarative Programmierung wird wie die imperative Programmierung auch in verschiedene Unterkategorien eingeteilt. Diese sind z.B. logische Programmierung, Constraint Programmierung und funktionale Programmierung. Prolog, Lisp und SQL sind beispielhafte Programmiersprachen, die zu diesem Paradigma gehören. [1].

2.3 Funktionale Programmierung

Wie im vorherigen Abschnitt erwähnt wurde, ist die funktionale Programmierung ein Teil von der deklarativen Programmierparadigmen. Ein Programm in diesem Schema besteht hauptsächlich aus einer Zusammensetzung von Funktionen [11], verwendet unveränderliche Daten und vermeidet Zustandsänderungen.
Die Programmierung mit funktionalen Sprachen bringt mehrere Vorteile. Beispiele für solche Vorteile sind „Lazy Evaluation“ und das explizierte Markieren von Seiteneffekten [17].
Folgende Beschreibung für Lazy Evaluation wurde von Bloss, Hudak und Young sinngemäß übernommen: Lazy Evaluation beurteilt einen Ausdruck erst, wenn der Wert absolut benötigt wird [3]. Dies bedeutet, dass eine Parameterübergabe an eine andere Funktion eine Evaluierung nicht auslöst. Der Wert muss explizit für die Berechnung eines neuen Wertes aufgerufen werden, damit dieser evaluiert werden kann.
Eine Definition für Seiteneffekte wurde von Nokie übernommen: Seiteneffekte sind Änderungen im Programmzustand. Diese können z.B. durch Funktionsaufrufe oder der Veränderung einer globalen Variablen ausgelöst werden [18].

2.4 Haskell

Haskell ist eine der weitverbreitesten funktionalen Sprachen, die 1988 ihren Namen im „Yale Meeting“ erhielt. Der Name kam vom Mathematiker Haskell B. Curry, wessen Arbeit einer der Anstöße zur Entwicklung von Haskell geführt hat. Im Jahr 1987 begann der Haskell Design Prozess in der „Functional Programming and Computer Architecture Conference“ (FPCA) und am 01. April 1990 wurde der „Haskell version 1.0 report“ veröffentlicht. Über die Jahre entwickelte sich die Sprache weiter und es wurde im Februar 1999 der „Haskell 98 Report“ veröffentlicht, wobei eine Revision im Dezember 2002 veröffentlicht wurde [8]. Mit der Veröffentlichung des „Haskell 2010 Language Report“ wurde eine wichtige Änderung für neue Revisionen beschlossen. Jedes Jahr sollte mindenstens eine neue Revision veröffentlicht werden, die eine kleine Anzahl an Änderungen und Erweiterungen beinhaltet [13].

Im Folgenden werden Beispielfunktionen in Haskell gezeigt, welche die in Kapitel 2.3 vorgeführten Vorteile darstellt.

Listing 2.1: Ein einfaches „Hello World“-Programm

```
1 main :: IO ()
2 make = putStrLn "Hello World"
```

Wie in Zeile 1 im Programmbeispiel 2.1 gezeigt wird, werden Seiteneffekte in Haskell immer durch IO markiert. Wenn eine Funktiondeklaration keine IO beinhaltet, so ist die Funktion Seiteneffektfrei.

Listing 2.2: Beispiele für Lazy Evaluation

```
1 lazy :: Int -> Int -> Int
2 lazy x y = x
3
4 lazy2 :: Int -> Int -> Int
5 lazy2 x y = if x > 2 then y else x
```

Im Programmbeispiel 2.2 würde die „Eager Evaluation“ (das Gegenteil von Lazy Evaluation) die Parameter x und y in Zeile 2 evaluieren. Lazy Evaluation hingegen evaluiert nur den Parameter x, da y nicht weiter verwendet wird in der Funktion. In der Beispielsfunktion „lazy2“ wird der Parameter y in Zeile 5 nur evaluiert, wenn x größer als 2 ist.

3 SAT

Dieses Kapitel gibt eine kurze Einführung zum Thema SAT und einen Einblick in die SAT-Competitions. Des Weiteren werden die bekannten SAT-Solver zChaff und MiniSAT vorgestellt.

3.1 SAT-Problem

Die SAT Assoziation definiert das SAT-Problem als ein Problem, in dem bestimmt werden muss, ob es für ein aussagenlogisches Problem boolesche Wertzuweisungen existieren, die dieses dann zu 1 evaluiert [19]. Stephen A. Cook hat die NP-Vollständigkeit des SAT-Problems 1971 in seiner Publikation bewiesen [4], welche 1973 nochmals von Leonid A. Levin nachgewiesen wurde [12]. Deshalb wird der Beweis oft auch „Satz von Cook-Levin“ genannt. Durch diesen Beweis wurde das SAT als allererstes Problem die NP-Vollständigkeit bewiesen.
Jedes aussagenlogische Problem kann in „Konjunktive Normalform“ oder zu Englisch „Conjunctive Normal Form“ (CNF) umschrieben werden. CNF hierbei ist eine Konjunktion ($\bigwedge$) von Disjunktionen ($\bigvee$).
Ein aussagenlogisches Problem besteht aus folgenden Elementen:

- Literale
- Klauseln
- Formeln

In dieser Arbeit ist ein Literal ein Zeichen, welches mit Wahr (T) oder Falsch (F) belegt werden kann und negiert (-) sein kann. Eine Klausel besteht aus einer Menge von disjunkten Literalen, während eine Formel eine Menge von konjunkten Klauseln ist.

Folgende Beispiele zeigen Formeln, die in CNF oder nicht in CNF sind.

$$A \wedge (B \vee C) \tag{3.1}$$

$$A \wedge -B \tag{3.2}$$

$$A \vee B \tag{3.3}$$

$$A \wedge (B \wedge -C) \tag{3.4}$$

$$A \vee (B \wedge -C) \tag{3.5}$$

Die Beispiele 3.1, 3.2 und 3.3 sind in CNF Form, während 3.4 und 3.5 nicht in CNF sind. Der Grund hierfür liegt daran, dass die Literale innerhalb der Klausel verundet sind. Das Beispiel 3.2 ist in CNF, da die Literale A und B in disjunkter Form sind. Diese Probleme können mit zwei Ergebnissen beurteilt werden. Als Ergebnis können die Probleme entweder mit Satisfiable (SAT) oder Unsatisfiable (UNSAT) evaluiert werden.

Das SAT-Problem findet sich in vielen industriellen Bereichen wieder, die sich mit Informatik beschäftigen. Darunter zählen z.B. Bounded Model Checking, künstliche Intelligenz und Theorembeweise [19].

3.2 SAT-Competition

Die internationale SAT-Competition findet seit dem Jahr 2002 statt. Der Wettbewerb wurde eingeführt, um neue SAT-Solver vorzustellen und Benchmarks zu finden, die nicht einfach zu lösen sind. Dabei werden die Solver auch mit SAT-Solvern verglichen, die den Stand der Technik darstellen. Unter anderem existieren im Wettbewerb auch unterschiedliche Disziplinen, in denen sich die Solver messen können [20].

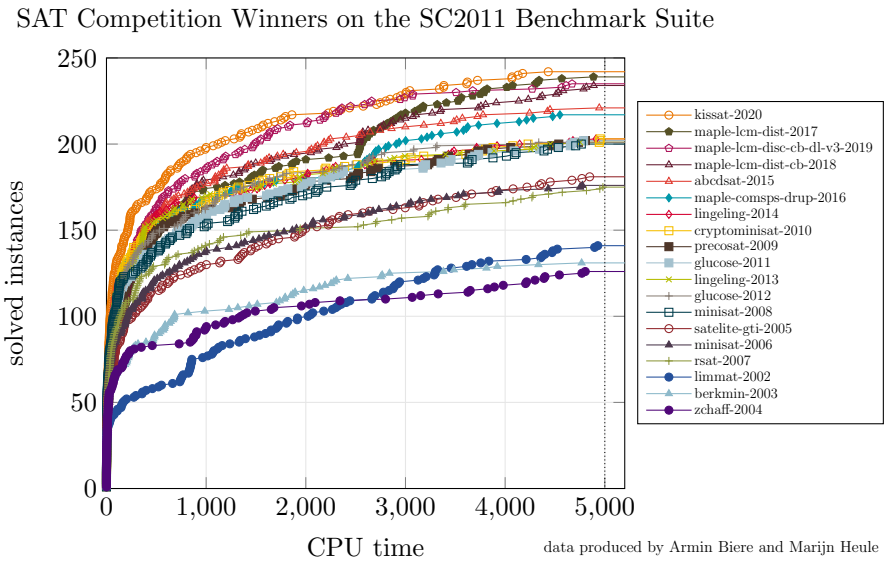

Abbildung 3.1: Benchmark 2011
Bildquelle: http://fmv.jku.at/kissat/winners-2011.pdf

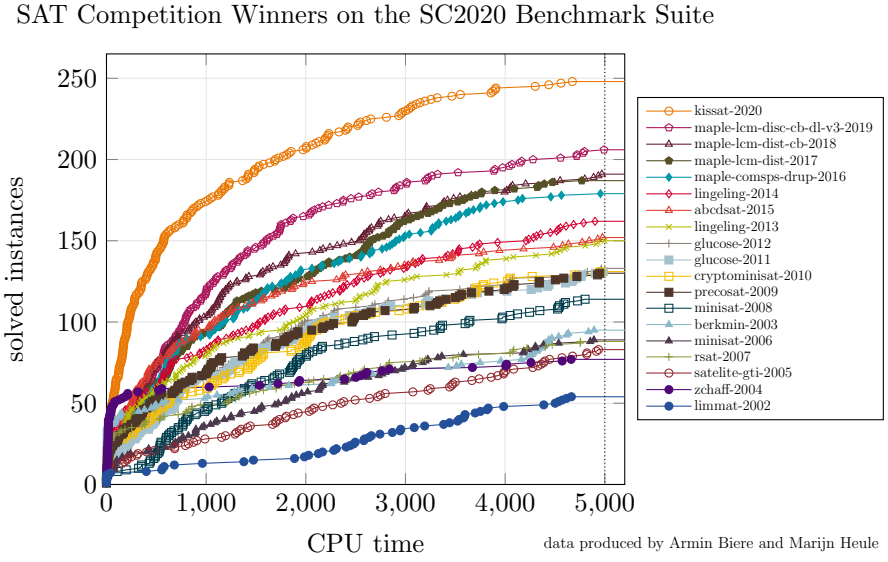

Abbildung 3.2: Benchmark 2020
Bildquelle: http://fmv.jku.at/kissat/winners-2020.pdf

Die x-Achse der Abbildungen 3.1 und 3.2 zeigt die Anzahl der gelösten SAT-Probleme, während die y-Achse die CPU Zeit darstellt. Die Legende stellt die Gewinner der SAT-Competition von 2002 bis 2020 dar. Verglichen mit der Abbildung 3.1 wird ersichtlich, dass die Benchmarks aus Abbildung 3.2 komplexer wurden, was durch die Ausweitung der Graphen wiedergespiegelt wird. Daraus kann geschlossen werden, dass die Solver mit den Jahren einen höhere Leistungsgrad erzielt haben [2].

3.3 SAT-Solver

Es existieren viele SAT-Solver, die gute Leistungen vollbringen beim Lösen von SAT-Problemen. In den folgenden Abschnitten werden zwei Solver vorgestellt, welche an einer SAT-Competition teilgenommen und diese auch zu ihrer Zeit gewonnen haben. Die zwei SAT-Solver, die vorgestellt werden, sind zChaff und MiniSAT.

3.3.1 zChaff

Der SAT-Solver zChaff basiert auf den Chaff-Algorithmus und wurde an der Princeton Universität entwickelt und veröffentlicht. Der Chaff-Solver verwendet einen optimierten „Boolean Constrainst Propagation"-Algorithmus (BCP) mit „Watched Literals" und „Variable State Independent Decaying Sum" (VSIDS) für die Entscheidungsheuristik. Des Weiteren wendet zChaff „Restarts" und „Clause Deletion" an [16]. Viele von diesen Ideen wurden später für den 2003 entwickelten MiniSAT übernommen [7].
zChaff hat 2004 im „Industrial Track" die „ALL (SAT+UNSAT)" und „UNSAT" Kategorien gewonnen [20].

3.3.2 MiniSAT

MiniSAT wurde von Niklas Eén und Niklas Sörensson an der Chalmers University of Technology entwickelt. Hintergrund für die Entwicklung des Solvers ist die Veröffentlichung eines zugänglichen, minimalistischen CDCL-SAT-Solvers, der Watched Literals und „Dynamic Variable Ordering" (VSIDS) verwendet [7]. Durch dieses Konzept sind viele SAT-Solver entstanden, die MiniSAT als Basis für ihre Entwicklung verwendet haben.
MiniSAT gewann den ersten Platz im SAT-Race 2006 [21].

3.4 DIMACS Format

Damit SAT-Solver ein generelles Dateiformat einlesen könnnen, um aussagenlogische Probleme zu lösen, wurde das DIMACS Format eingeführt.

Listing 3.1: DIMACS Format

```
1 c simpleExample.cnf
2 c
3 p cnf 3 2
4 1 2 -3 0
5 c Kommentare können auch hier sein
6 -2 -1 0
```

Kommentare werden mit einem kleinem „c“ symbolisiert wie z.B. in Zeile 1 und 5 im Beispiel, während kleine p's die Spezifikationen des SAT-Problemes zeigen. Das Wort nach dem p deutet in welcher Form ein Problem dargestellt ist. Dies kann entwender cnf oder „Disjunktive Normalform“ (dnf) sein. Der erste Integer in Zeile 3 steht für die Anzahl der Literale und der Zweite für die Anzahl der Klauseln. Wenn nach der p-Zeile ein Integer oder ein Minus die Zeile anführt, so beginnt eine Klausel. Integer in diesen Zeilen können entweder positive oder negative Literale darstellen. Wenn eine 0 eingelesen wird, ist die Klausel vollständig und es wird eine neue Zeile eingelesen.
Die decodierte Formel für das obige Beispiel sieht folgendermaßen aus:

$$(1 \vee 2 \vee -3) \wedge (-2 \vee -1)$$

4 Algorithmen

In diesem Kapitel wird der DPLL-Algorithmus und CDCL-Algorithmus vorgestellt. Anhand einer Literaturarbeit werden die Erweiterung erläutert, die das CDCL-Verfahren performanter im Gegensatz zum DPLL machen.

4.1 DPLL-Algorithmus

Martin Davis und Hilary Putnam entwickelten 1960 den Davis-Putnam-Algorithmus (DP) [6], der als Basis für das 1962 entwickelte DPLL-Verfahren verwendet wird. Der Algorithmus wurde von Martin Davis, George Logemann und Donald Loveland präsentiert und besitzt drei Regeln [5].
Die erste Regel ist die Eliminierung von Klauseln mit nur einem Literal [6]. Mit dieser Regel wurden vier Teilregeln eingeführt. Diese sind folgende:

1. Existieren zwei atomare Klauseln mit gegenteiligen Literalen, wie z.B. $\{p\}$ und$\{-p\}$, so ist die Formel F UNSAT.

2. Existiert eine atomare Klausel mit nur einem positiven Literal p, so können alle Klauseln, die ein p beinhalten, gelöscht werden und alle negierten p's können aus den Klauseln entfernt werden.

3. Die dritte Teilregel ist wie die zweite Teilregel, jedoch mit umgekehrten Vorzeichen.

4. Die Formel ist SAT, wenn F nach anwenden der Regeln leer wird.

Die zweite Regel ist die „Affirmative-Negative Rule" [6]. Diese Regel ist ähnlich zur Regel 1.2 und 1.3. Anstelle von atomaren Klauseln wird hier eine Entscheidung für ein Literal in einer Klausel getroffen. Wenn das Literal p mit T belegt wird, so werden alle Klauseln mit einem positiven p gelöscht, während alle negativen p aus den Klauseln gelöscht werden. Dies geschieht auch umgekehrt mit einer Belegung von F.
Als dritte Regel wurde die Teilungs Regel vorgestellt [5]. In dieser Regel wird eine Formel F in $(A \vee p) \wedge (B \vee -p) \wedge R$ aufgeteilt, wobei p nicht in A, B und R vorhanden

ist. A und B stellen hierbei andere Literale dar, während R andere Klauseln in F darstellen. F wird UNSAT, wenn für die Belegungen $p = F$ und $A \wedge R$ und $p = T$ und $B \wedge R$ die Klauseln in der Formel inkonsistenz aufzeigen.
Ein Beispiel wie die Regeln 1 und 2 funktionieren, wird an folgendem Problem gezeigt:

$$F = 1 \wedge (-1 \vee -2) \wedge (1 \vee 2) \wedge (3 \vee 4) \wedge (4 \vee 5) \tag{4.1}$$

$$Setze\, 1 = T$$

$$\Leftrightarrow 2 \wedge (3 \vee 4) \wedge (4 \vee 5) \tag{4.2}$$

$$Setze\, 2 = T$$

$$\Leftrightarrow (3 \vee 4) \wedge (4 \vee 5) \tag{4.3}$$

$$Setze\, 4 = T$$

$$\Rightarrow SAT \tag{4.4}$$

Die zweite Teilregel der ersten Regel wird im ersten Schritt angewendet. Diese löscht alle Klauseln, welche eine positive 1 besitzen, und alle negativen 1 in allen Klauseln. Dadurch kommt die Formel $2 \wedge (3 \vee 4) \wedge (4 \vee 5)$ im zweiten Schritt zustande. Nach der Anwendung der dritten Teilregel für das Literal (-2) kommt die Formel $(3 \vee 4) \wedge (4 \vee 5)$ als Ergebnis heraus. Mit dem Einsetzen von $4 = T$ wird die zweite Regel benutzt, wodurch die leere Menge entsteht. Dadurch wird die gesamte Formel mit SAT evaluiert.
Wenn die Formel F jedoch noch eine atomare Klausel (-1) besitzen würde, würde die Formel F als UNSAT evaluiert werden, da die erste Teilregel von Regel 1 bei zwei atomaren Klauseln mit unterschiedlichen Vorzeichen und gleichen Literalen die Formel als UNSAT beurteilt.

4.2 CDCL-Algorithmus

CDCL SAT-Solver basieren auf den DPLL-Algorithmus und verwenden zusätzlich zu den Regeln mehrere Optimierungen und einen Algorithmus, welches dem CDCL seinem Namen verdankt. CDCL wurde in Publikationen von Marques-Silva und Sakallah 1996 [14] und 1999 [15] und Bayardo und Schrag 1997 [9] vorgeschlagen. Der CDCL-Algorithmus wird immer dann angewendet, wenn nach der Anwendung des Entscheidungsalgorithmus (siehe 5.2.1) und „Boolean Constraint Propagation“ (BCP, siehe 5.2.2) ein Konflikt auftritt. Ein Konflikt ensteht, wenn eine Zuweisung von Literalen bei einer Klausel keine logische wahre Aussage ergibt. Das folgendes Beispiel soll diesen Fall zeigen:

$$F = (-1 \vee -2) \wedge (-1 \vee 2) \wedge (1 \vee 2) \tag{4.5}$$

$$Setze\, 1 = T\, (Entscheidung)$$

$$\Leftrightarrow -2 \wedge 2 \tag{4.6}$$

$$Setze\, 2 = F$$

$$\Rightarrow Konflikt\, bei\, Klausel\, (-1 \vee 2)$$

Die Klausel $(-1 \vee 2)$ hat einen Konflikt für die Belegungen $1 = T$ und $2 = F$ verursacht. In der Publikation von Marques-Silva und Sakallah [15] wird die Verwendung eines Implikationsgraphen [1]vorgeschlagen, um diesen Konflikt zu lösen. Für das Beispiel in Formel 4.5 würde der Graph folgendermaßen aussehen:

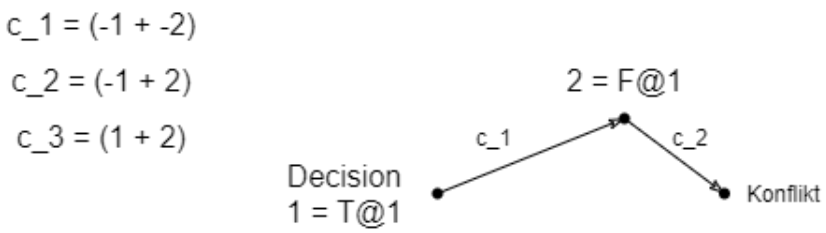

Abbildung 4.1: Beispiel eines Implikationsgraphen
Die Plusse stellen $\vee$ dar

[1]Soll genauer auf Implikationsgraph gegangen werden? Also z.B. die mathematische Definition mit Gerichteter azyklischer Graph mit G(V,E)...?

Der Graph in Abbildung 4.1 ist gleichzeitig auch ein partieller Implikationsgraph, da dieser alle relevanten Entscheidungen und Literalbelegungen zum Konflikt im zurzeitigen Entscheidungslevel zeigt. Ein vollständiger Implikationsgraph dagegen zeigt alle aktuellen Entscheidungen und Wahrheitsbelegungen eines SAT-Problemes an. Um die Konfliktklausel zu lernen wird Resolution [10] verwendet.
Hierbei ist die Resolution folgende Regel:

$$\frac{x_1 \vee x_{...} \vee x_n \vee p \qquad y_1 \vee y_{...} \vee y_n \vee -p}{x_1 \vee x_{...} \vee x_n \vee y_1 \vee y_{...} \vee y_n} \tag{4.7}$$

Die Literale x_1 bis p stellen eine Klausel in der Formel dar, während y_1 bis $-p$ eine andere Klausel darstellt. Diese Klauseln werden auch „resolving clauses“ (RC) genannt. Das Literal p ist hierbei eine „resolution variable“, welche nach der Resolution ihre Literalbelegung verliert. Die Klausel $(x_1 \vee x_{...} \vee x_n \vee y_1 \vee y_{...} \vee y_n)$ wird als „resolvent clause“ bezeichnet und kann als Klausel für die nächste Resolution verwendet werden oder zur Formel als gelernte Konfliktklausel hinzugefügt werden. Damit die Resolution angewendet werden kann, muss ein Literal p mit unterschiedlichen Vorzeichen in den RC existieren.
Die Resolutionschritte gehen einen Implikationsgraphen, der von links nach rechts entwickelt wird, von rechts nach links ab. Dabei gibt es verschiedene Stopkriterien, die verwendet werden können, um die Konfliktklausel zu lernen. In dieser Arbeit wird „First Unique Implication Point“ (1UIP) [10] als Stopkriterium für die Konfliktanalyse verwendet. 1UIP ist ein „Unique Implication Point“ (UIP), der dem Konfliktknoten am nähesten ist. Dies liegt daran, dass die Entscheidung an diesem Knotenpunkt einen Konflikt augelöst hat. Solange die Konfliktklausel nach dem „Backjumping“ nur ein unbelegtes Literal besitzen, können die SAT-Solver in diesem Prozess bis zum zweithöchsten Entscheidungslevel zurückspringen. Dadurch werden alle Literalbelegungen vom höchsten bis zum zweithöchsten + 1 gefundenen Level gelöscht.
In der Abbildung 4.1 werden die Klauseln c_1 (c_1) und c_2 (c_2) für die Resolution verwendet, da die Klausel c_2 den Konflikt verursacht hat und die Klausel c_1 die Belegung für die Variable 2 verantwortlicht ist. Als Ergebnis kommt die neue Klausel (-1) heraus und wird zur Formel 4.5 hinzugefügt. Gleichzeitig werden alle Belegungen die auf dem Entscheidungslevel 1 getroffen wurden gelöscht. Nachdem dies geschehen ist, wird der BCP-Prozess fortgeführt und eine Lösung mit den Belegungen $1 = F$ und $2 = T$ wird gefunden.

5 Implementierung des SAT-Solvers

In diesem Kapitel wird die Implementierung des SAT-Solvers diskutiert. Hierbei werden zunächsts die notwendigen Datenstrukturen beschrieben und danach werden die Algorithmen und der Aufbau des Programmes dargestellt. [1] Die wichtigsten Algorithmen in der Implementierung basieren auf Konzepte, die von zChaff und MiniSAT verwendet werden.

5.1 Datenstrukturen

In der Implementierung werden verschiedene Datenstrukturen verwendet.

Listing 5.1: Wichtige Datenstrukturen für die Implementierung

```
1  -- | Literal defined as Integer
2  newtype Literal = Lit Integer
3      deriving (Show, Eq, Ord)
4
5  -- | Clause defined as a List of Literal
6  type Clause = [Literal]
7
8  -- | Tuple of 2 Clauses
9  --   First clause in tuple is reduced via Unitresolution
10 --   Second clause is the clause in its original form
11 type ReducedClauseAndOGClause = (Clause, Clause)
12
13 -- | ClauseList defined as a List of ReducedClauseAndOGClause
14 type ClauseList = [ReducedClauseAndOGClause]
```

Zum Zeitpunkt der Implementierung wurde entschieden keine „Watched Literals“ zu implementieren, da die Permutation von Listen in Haskell kompliziert ist. Der Grund hierfür ist, das Haskell keine Kontrollstrukturen, wie z.B. for-Schleifen, besitzt und nicht direkt auf die einzelnen Listenelemente zugreifen kann. Aus diesem Grund

[1] Ist die Struktur von Kapitel 5.2 so ok? Oder wäre es besser, wenn Programmaufbau das erste Unterkapitel ist. Im Programmaufbau würde ich die auf die anderen Unterkapitel wieder aufgreifen.

wird stattdessen ReducedClauseAndOGClause verwendet, wobei das erste Element eine veränderliche Klausel darstellt, während das zweite Element eine unveränderte Klausel ist.

5.2 Algorithmen

5.2.1 Entscheidungsalgorithmus / Decision

5.2.2 Unitpropagation

Die Unitpropagation, oder auch BCP, ist einer der wichtigsten Algorithmen für moderne SAT-Solver. In der Unitpropagation werden Klauseln, die nur ein unbelegtes Literal besitzen und noch nicht als SAT evaluiert sind, so belegt, dass Sie wahr werden (siehe 4.1).

Listing 5.2: Unitpropagation

```
1  unitPropagation :: ClauseList -> TupleClauseList -> Level ->
       MappedTupleList -> TriTuple
2  unitPropagation clist tlist lvl mapped
3
4      -- Case: no UnitClause found or no more clauses in ClauseList
5      | null clist || null fstElem = (clist, tlist, mapped)
6      | otherwise = unitPropagation resolutionC
7                    (tlist ++ [(calcTuple, ogClause)]) lvl updatedMap
8      where
9            unitClause = getUnitClause clist
10           fstElem = getClauseFromReducedClauseAndOGClause unitClause
11           calcTuple = setVariable fstElem
12           ogClause = Reason (getOGFromReducedClauseAndOGClause
                 unitClause)
13           updatedMap = pushToMappedTupleList mapped lvl calcTuple
                 ogClause
14           subsumptionC = unitSubsumption clist calcTuple
15           resolutionC = unitResolution subsumptionC calcTuple
```

Zunächst wird überprüft, ob die ClauseList Elemente besitzt. Wenn dies der Fall ist, wird nach einer Klausel gesucht, die nur ein unbelegtes Literal (Unit-Clause) besitzt. Wenn jedoch keine Elemente mehr vorhanden sind oder keine Unit-Clause gefunden wird, werden die übergebenen Daten zurückgegeben und der Algorithmus wird beendet. Ansonsten setzt der Algorithmus das Literal so, dass die Klausel wahr wird und wendet Subsumption auf die ClauseList an. Die neue ClauseList wird dann mit Resolution verändert. Gleichzeitig wird der Grund für die Entscheidung des Algorithmus in die MappedTupleList aufgenommen.. Solange der erste Fall nicht eintritt, arbeitet der Algorithmus rekursiv mit den bearbeiteten Daten weiter.
Subsumption ist das Löschen einer ganzen Klausel, während die Resolution das Löschen eines gegenteiligen Literals ist (siehe 2)

5.2.3 Konfliktanalyse / Conflict analysis

5.2.4 Programmaufbau

6 Auswertung der Implementierung

In diesem Kapitel wird die Richtigkeit des SAT-Solvers mit dem PicoSAT-Solver verglichen. Nach dem Vergleich wird eine Auswertungen der Zeiten für das Lösen von SAT-Problemen erstellt, wobei die Implementierung mit zChaff und MiniSAT verglichen wird.

7 Fazit

Dokumentation für Code[1]

Für eine umfangreichere Dokumentation des Codes wird auf Haddock Dokumentation hingewiesen. Diese Dokumentation dient nur als grober Überblick für die hauptsächlichen Funktionen, die implementiert wurden.

Types.hs

Die Datei enthält alle nötigen Datentypen, die für die Implementierung des CDCL Programms notwendig sind.
data
CDCLResult
Rückgabewert von CDCL Funktion. Folgende Datentypen können hier zurückgegeben werden:

- SAT TupleList
- SAT_WITH_STATS TupleList MappedTupleList Integer [Clause] (Liste von Clause sind gelernte Klauseln)
- UNSAT
- UNSAT_WITH_STATS [Clause] [Clause] (Die erste Liste sind gelernte Klauseln, während die zweite Klauseln sind, die Konflikte hervorgeführt haben)

Reason
Reason zeigt an, aus welchem Grund eine Belegung für eine Variable entschieden wurde. Diese können folgende sein:

- Decision
- Reason Clause

[1] soll ich den Anhang rausnehmen? Oder soll ich den Codeanhang auch im Verzeichnis haben?

BoolVal
BoolVal gibt den gesetzten Wert einer Variablen zurück. Diese sind BTrue, BFalse or BNothing. Equivalente Werte für diese sind 1, 0 und -1.
InterpretResult
InterpretResult ist das Ergebnis von der Interpret Funktion. Ergebnisse können Folgende sein:

- OK
- NOK Clause
- UNRESOLVED

newtype
Variable
Datentyp für Variable. Die Darstellung für diesen Datentyp ist Variable Integer.
Level
Datentyp für Level. Die Darstellung für diesen Datentyp ist Level Integer.
Activity
Datentyp für Activity. Die Darstellung für diesen Datentyp ist Activity Integer
Period
Datentyp für Period. Die Darstellung für diesen Datentyp ist Period Integer
Type
Clause
Clause ist eine Liste bestehend aus Variable.
ReducedClauseAndOGClause
Synonym für Tupel, die aus zwei Clause bestehen. Die erste Clause wird durch Funktionen gekürzt, während die zweite Clause im Tupel in ihrem Originalzustand bleibt.
ClauseList
ClauseList ist eine Liste aus ReducedClauseAndOGClause.
Tuple
Synonym für Tupel, die aus Variable und BoolVal bestehen.
TupleList
Liste aus Tuple. Wird für den Datentyp CDCLResult verwendet.
TupleClause
Synonym für Tupel, die aus Tuple und Reason bestehen.
TupleClauseList
Liste aus TupleClause.

MappedTupleList
Eine Map, die Level als Key verwendet und TupleClauseList als Value besitzt.
ActivityMap
Variablen sind in dieser Map Keys, während Activity Values darstellen
VariableActivity
Synonym für Tupel, die aus Variable und Activity bestehen.
TriTuple
Eine Tupel aus drei Elementen. Diese enthält ClauseList, TupleClauseList und MappedTupleList.

Algorithm.hs

cdcl
Funktion benötigt einen Parameter. Der erwartete Parameter ist eine Liste aus Listen, welche mit Integern gefüllt ist. Ruft die rekursive cdcl' Funktion auf.
Als Ergebnis kommt dann ein CDCLResult zurück.
calculateClauseList
Funktion benötigt ClauseList und TupleClauseList als Parameter. Diese Funktion wird aufgerufen, wenn eine Variable BoolVal durch eine Decision
erhält und berechnet ihr Ergebnis mithilfe von unitSubsumption und unitResolution.
Der Rückgabewert ist eine ClauseList.
interpret
Interpretiert eine gegebene ClauseList mithilfe einer übergebenen TupelClauseList. Dabei wird rekursiv nach der Reihe eine Clause interpretiert, bis alle Klauseln interpretiert sind oder eine Klausel nicht zu OK evaluiert wird.
Rückgabewerte für diese Funktion sind InterpretResult.
searchTupel
Gibt den Wert eines Tupelpaares zurück basiered auf dem gegebenen Variablenwert und der TupelList. Dabei wird ein BoolVal zurückgegeben.

Unitpropagation.hs

unitPropagation
Führt das Unit-Propagation Verfahren durch. Die Funktion erwartet ClauseList, TupelClauseList, Level und MappedTupleList als Argumente. Als Ergebnis wird ein TriTuple zurückgegeben.
getUnitClause

Gibt eine ReducedClauseAndOGClause durch das überprüfen einer ClauseList zurück. Dabei wird überprüft ob das erste Element im ReducedClauseAndOGClause die Länge 1 besitzt.
setVariable
Setz einen Wert von BFalse oder BTrue in einem Tuple und gibt dieses zurück.
unitSubsumption
Löscht Klauseln aus ClauseList, wenn Klauseln gefunden werden, die Variablen enthalten, welche bei einem eingesetzem Tupelwert zu 1 evaluiert werden. Die bearbeitete ClauseList wird dann zurückgegeben.
unitResolution
Löscht Variablen aus den Clauseln, die zu 0 evaluiert werden. Als Ergebnis wird die bearbeitete ClauseList weitergegeben.

Decisionalalgorithm.hs

initialActivity
Die Funktion wird initial bei der Verwendung von cdcl benutzt und erwartet eine ClauseList und ActivityMap als Paremeter. Mithilfe von rekursiven Aufrufen von initialActivity und updateActivity wird dann eine ActivityMap berechnet und zurückgegeben.
updateActivity
UpdateActivity benötigt eine Clause und ActivityMap als Parameter. Durch Rekursion erhalten neue Variablen einen Eintrag in die ActivityMap, während bestehende um eins aktualisiert werden.
halveActivityMap
Die Funktion halbiert alle Activity nach einer bestimmten Periode. Als Parameter werden eine ActivityMap und eine Liste von allen Variablen benötigt.
getHighestActivity
Erwartet ClauseList, ActivityMap und eine Liste von VariableActivity als Parameter und gibt eine Liste von VariableActivity mit der höchsten Activity als Ergebnis zurück.
getShortestClauseViaActivity
Beim Aufruf der Funktion werden zwei ClauseList und eine Liste von VariableActivity benötigt. Die Funktion gibt eine ClauseList mit den kürzesten Clause zurück, die die gegebenen VariableActivity enthalten.
setVariableViaActivity

SetVariableViaActivity benötigt eine Clause und VariableActivity. Basierend auf der Variable in der Clause wird ein TupleClause als Ergebnis zurückgegeben.

MapLogic.hs

pushToMappedTupleList
Die Funktion erwartet MappedTupleList, Level, Tuple und ein Reason. Anhand der übergebenen Parameter wird die MappedTupleList aktualisiert und anschließend zurückgegeben.
deleteLvl
Die Funktion löscht das gegebenene Level aus einer gegebenen MappedTupleList und gibt diese zurück.

7.0.1 Conflict.hs

analyzeConflict
Die Funktion erwartet folgende Argumente: Level, Clause, MappedTupleList, ClauseList und ActivityMap. Mithilfe von calcReason wird eine neue Clause berechnet und durch addClause zu der gegebenen ClauseList hinzugefügt. Dabei wird durch deleteLvl das letzte Level aus MappedTupleList gelöscht. Level, ClauseList, MappedTupleList und ActivityMap wird am zurückgegeben.
calcReason
Berechnet mithilfe von Level, Clause und MappedTupleList eine 1UIP-Clause.

CDCLFilereader.hs

readCdclFile
Die Funktion erwartet einen String Input und gibt eine IO Ausgabe zurück. Der String Input soll hierbei eine existierende cnf-Datei sein. Bei einem richtigen Input ruft die Funktion loopCheck auf und gibt ihr Ergebnis aus.
loopCheck
Die Funktion überprüft, ob eine Zeile mit einem Integer oder einem - anfängt. Wenn dies der Fall ist, wird die gesamte Zeile in ein Integerliste hinzugefügt. Diese Liste wird dann zu einer Liste von Integerlisten beigefügt. Wenn die Funktion das Ende der Datei erreicht, wird die die Liste von Integerlisten der cdcl-Funktion übergeben. Das Ergebnis wird dann als IO (Maybe CDCLResult) zurückgegeben.

Literatur

[1] Stephan Augsten. *Was ist ein Programmierparadigma?* de. URL: https://www.dev-insider.de/was-ist-ein-programmierparadigma-a-864056/ (besucht am 22.06.2021).

[2] Armin Biere. *Kissat SAT Solver*. URL: http://fmv.jku.at/kissat/ (besucht am 03.07.2021).

[3] Adrienne Bloss, Paul Hudak und Jonathan Young. "Code optimizations for lazy evaluation". en. In: *Lisp and Symbolic Computation* 1.2 (Sep. 1988), S. 147–164. ISSN: 0892-4635, 1573-0557. DOI: 10.1007/BF01806169. URL: http://link.springer.com/10.1007/BF01806169 (besucht am 13.07.2021).

[4] Stephen A. Cook. "The complexity of theorem-proving procedures". In: *In Stoc*. ACM, 1971, S. 151–158.

[5] Martin D. Davis, G. Logemann und D. Loveland. "A machine program for theorem-proving". In: *Commun. ACM* 5 (1962), S. 394–397.

[6] Martin D. Davis und H. Putnam. "A Computing Procedure for Quantification Theory". In: *J. ACM* 7 (1960), S. 201–215.

[7] Niklas Eén und Niklas Sörensson. *An Extensible SAT-solver*. en. 2003. URL: http://minisat.se/downloads/MiniSat.pdf (besucht am 02.07.2021).

[8] Paul Hudak u.a. "A history of Haskell: being lazy with class". en. In: *Proceedings of the third ACM SIGPLAN conference on History of programming languages*. San Diego California: ACM, Juni 2007, S. 3–5. ISBN: 978-1-59593-766-7. DOI: 10.1145/1238844.1238856. URL: https://dl.acm.org/doi/10.1145/1238844.1238856 (besucht am 30.06.2021).

[9] Roberto J Bayardo Jr und Robert C Schrag. "Using CSP Look-Back Techniques to Solve Real-World SAT Instances". en. In: (), S. 6.

[10] Daniel Kroening und Ofer Strichman. "Decision Procedures for Propositional Logic". In: *Decision Procedures: An Algorithmic Point of View*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, S. 27–58. ISBN: 978-3-662-50497-0. DOI: 10.1007/978-3-662-50497-0_2. URL: https://doi.org/10.1007/978-3-662-50497-0_2.

[11] Christian Lengauer. *Was ist funktionale Programmierung?* URL: https://www.infosun.fim.uni-passau.de/cl/lehre/funcprog05/wasistfp.html (besucht am 22.06.2021).

[12] L A Levin. "Universal Sequential Search Problems". ru. In: *Probl. Peredachi Inf.* 9.3 (1973), S. 115–116.

[13] Simon Marlow. *Haskell 2010 Language Report*. Juli 2021. URL: https://www.haskell.org/definition/haskell2010.pdf (besucht am 01.07.2021).

[14] Jo Marques u. a. "GRASP—A New Search Algorithm for Satisfiability". In: *in Proceedings of the International Conference on Computer-Aided Design*. 1996, S. 220–227.

[15] J.P. Marques-Silva und K.A. Sakallah. "GRASP: a search algorithm for propositional satisfiability". en. In: *IEEE Transactions on Computers* 48.5 (Mai 1999), S. 506–521. ISSN: 00189340. DOI: 10.1109/12.769433. URL: http://ieeexplore.ieee.org/document/769433/ (besucht am 16.07.2021).

[16] Matthew W Moskewicz u. a. "Chaff: Engineering an Efficient SAT Solver". en. In: (), S. 6. URL: http://www.princeton.edu/~chaff/publication/DAC2001v56.pdf (besucht am 23.02.2021).

[17] Stefania Loredana Nita und Marius Mihailescu. "Functional Programming". In: *Haskell Quick Syntax Reference: A Pocket Guide to the Language, APIs, and Library*. Hrsg. von Stefania Loredana Nita und Marius Mihailescu. Berkeley, CA: Apress, 2019, S. 1–3. ISBN: 978-1-4842-4507-1. DOI: 10.1007/978-1-4842-4507-1_1. URL: https://doi.org/10.1007/978-1-4842-4507-1_1.

[18] Edward G. Nokie. *Side Effects*. URL: https://www.radford.edu/nokie/classes/320/Tour/side.effects.html (besucht am 14.07.2021).

[19] Hrsg: Satisfiability: Application and Theory (SAT) e.V. *SAT Basics*. URL: http://satassociation.org/articles/sat.pdf (besucht am 05.07.2021).

[20] Hrsg: Satisfiability: Application and Theory (SAT) e.V. *SAT Competitions*. URL: http://satcompetition.org/ (besucht am 03.07.2021).

[21] Carsten Sinz. *SAT-Race 2006*. URL: http://fmv.jku.at/sat-race-2006/results.html (besucht am 06.07.2021).