TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

DIPLOMARBEIT

A fixed-point theorem for Horn formula equations

ausgeführt am Institut für Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter der Anleitung von
Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

durch

Johannes Kloibhofer

Kranzgasse 2/ 10
1150 Wien

November 16, 2020

_____
Unterschrift

Contents

Chapter 1

Introduction

Formula equations are logical equations, where the unknowns are formulas. They are hardly considered in the literature. We claim that they should, as they naturally occur in many areas like program verification or automated theorem proving. In these communities similar problems are treated independently. Our motivation is to state general theorems about formula equations which then will be used to generalize and simplify results in various different applications. In this thesis we treat the special case of Horn formula equations, this restriction is justified as it covers many applications. We will use Horn formula equations to obtain a first-order approximation of second-order formulas as well as to get a different perspective on Hoare triples in program verification and to get more insights in inductive theorem proving.
For Horn formula equations we are able to compute canonical solutions if a solution exists. This will be achieved by defining an operator such that every solution of the Horn formula equation is a fixed point of it. Now the least fixed point, which exists due to the Knaster-Tarski theorem, turns out to be the canonical solution.
This approach, to use fixed-point theorems to get solutions of certain classes of equations, appears in various areas of mathematics. To illustrate how this arguments work we sketch the proof of one well-known example, the Picard-Lindelöf theorem. Here a function y is sought that solves the initial value problem $y'(t) = f(t, y)$ with $y(t_0) = y_0$ in a neighbourhood of t_0. It is shown that y is a solution of this initial value problem iff it is a fixed point of $T(y)(t) = y_0 + \int_{t_0}^{t} f(t, y(s))ds$. If f is sufficiently smooth the Banach fixed-point theorem provides a unique solution.
Our aim is to use a similar method to get solutions of a certain kind of equations in logic: Formula Equations. A formula equation has the form $\exists \overline{X} \psi$, where ψ is a first-order formula which may additionally contain the second order variables $X_1, ..., X_n$.
Under the name of "Boolean unification with predicates" some classes of formula equations were investigated by Eberhard, Hetzl and Weller in [5]. They deal with the problem of finding quantifier-free first-order formulas $\chi_1, ..., \chi_n$ such that $\models \psi[X_1 \backslash \chi_1, ..., X_n \backslash \chi_n]$. It is

shown that for a quantifier-free ψ this problem is Π_2^p-complete. If on the other hand ψ is of the form $\forall \bar{y}\psi'$ or $\exists \bar{y}\psi'$ with ψ' quantifier-free, they prove that the problem is undecidable. In this thesis we consider formula equations of the form $\exists \overline{X} \forall \bar{y}\ \psi'$, where ψ' is either a conjunction of constrained Horn clauses or a conjunction of constrained dual-Horn clauses. We call them Horn formula equations and dual-Horn formula equations, respectively. It turns out that in this cases we can define an operator F_ψ such that every solution of $\exists \overline{X}\psi$ is a fixed point of F_ψ. The least fixed point of F_ψ will always be a solution of the formula equation iff there exists a solution. This canonical solution will be described by least fixed-point formulas. Furthermore the canonical solution implies every solution in the Horn case and is implied by every solution in the dual-Horn case. This main results will then be used in manifold applications.

In Chapter 2 we present the toolkit that we need in this work: Basic definitions of logic, formula equations and fixed-point logics.
Chapter 3 will be the main part of our work. Here we prove the fixed-point theorems for Horn formula equations, dual-Horn formula equations and linear-Horn formula equation. Moreover we will explain why there is no immediate generalization of the results for universal formula equations, where the clauses do not have to be Horn.
In the Chapters 4 - 6 we present applications of the fixed-point theorems.
By considering inflationary fixed points in Chapter 4 we get first-order formulas that approximate the canonical solutions obtained in the previous chapter. In doing so we get first-order formulas that approximate Horn formula equations.
In Chapter 5 we take a look at program verification. We present a different semantics of Hoare triples, which is described by a Horn formula equation. The canonical solutions obtained in Chapter 3 correspond to the classical concepts of weakest precondition and strongest postcondition.
Horn formula equations occur naturally in the subject of inductive theorem proving. In Chapter 6 we show that our fixed-point theorems may be used to shorten some proofs and bring new insights in that area.
In Chapter 7 we deal with a paper, where the decidability of the affine solution problem is proven. This is achieved with a similar method we used to prove our fixed-point theorems. We show how the fixed-point theorems may be generalized to make it applicable for that problem.

Chapter 2

Preliminaries

We will start this chapter with some basic notations and definitions of logic, which will be used in this work. Then formula equations and solution problems are defined. Around this main concepts the whole work will be built up. At last we define fixed-point logics, which will take a key part in the proofs of the fixed-point theorems.

2.1 Notations

A *language* $\mathcal{L}$ consists of constant, predicate and function symbols. *Terms* over $\mathcal{L}$ are built from variables[1], constant and function symbols of $\mathcal{L}$. *First-order formulas* over $\mathcal{L}$ are built from predicate symbols, terms, the logical connectives $\neg, \vee, \wedge$ and the quantifiers $\exists, \forall$. Moreover we use the symbols $\rightarrow$ and $\leftrightarrow$, where $A \rightarrow B$ is defined to be an abbreviation for $\neg A \vee B$ and $A \leftrightarrow B$ to be an abbreviation for $A \rightarrow B \wedge B \rightarrow A$. In addition to first-order logic we often consider *formula variables*, which stand for predicates. To distinguish them from first-order variables we denote them with upper-case letters.
Unless otherwise noted we always talk about logic *with equality*, which means that we have a specified binary predicate symbol " $=$ ", which is interpreted as equality.
A subformula ψ of a formula φ occurs positively in φ if ψ is in the scope of an even number of negations in φ and occurs negatively if it is in the scope of an odd number of negations. For example in the formula $\varphi \equiv A \rightarrow B$ the subformula A occurs negatively and B occurs positively in φ, as φ is an abbreviation for $\neg A \vee B$. A formula variable X *occurs only positively* in φ if every occurrence of X as a subformula in φ occurs positively. Conversely X *occurs only negatively* if every occurrence of X as a subformula in φ occurs negatively.
Now let us define substitution. For a formula φ, variables $x_1, ..., x_n$ and terms $t_1, ..., t_n$ we define $\varphi[x_1 \backslash t_1, ..., x_n \backslash t_n]$ to be the formula φ, where every occurrence of x_j is replaced by t_j for every $j \in \{1, ..., n\}$ simultaneously. This is only allowed if no free variable of $t_1, ..., t_n$ became bound during the substitution process. Similarly for formula variables $X_1, ..., X_n$

[1] In distinction to formula variables sometimes also called *individual variables*.

and formulas $\alpha_1, ..., \alpha_n$ we define $\varphi[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$ to be the formula φ, where every occurrence of X_j is replaced by α_j for every $j \in \{1, ..., n\}$. Again this is forbidden if a free variable of $\alpha_1, ..., \alpha_n$ became bound in the process. We use the usual vector notation, that means we write $\overline{X}$ for $X_1, ..., X_n$ if n is clear from the context or unimportant. Consistently we write $\varphi[\overline{X} \backslash \overline{\alpha}]$ for $\varphi[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$.

An *$\mathcal{L}$-structure* $\mathcal{M}$ is a pair $\mathcal{M} = (M, I)$, where M is a set and I is an interpretation of $\mathcal{L}$, i.e. $I(P) \subseteq M^k$ for a k-ary predicate symbol $P \in \mathcal{L}$ and $I(f) : M^k \to M$ for a k-ary function symbol $f \in \mathcal{L}$.
An *environment* is an interpretation of the set of free variables. For an environment θ, a variable x and $m \in M$ we define $\theta[x := m]$ by $\theta[x := m](x) = m$ and $\theta[x := m](y) = \theta(y)$ for $x \neq y$. $\theta[X := S]$ is defined analogously for a k-ary predicate variable X and $S \subseteq M^k$. For a structure $\mathcal{M}$, an environment θ and a formula φ we define $\mathcal{M}, \theta \models \varphi$ as usual. In particular $\mathcal{M}, \theta \models \exists X \varphi[X]$ holds for a k-ary formula variable X iff there exists an $S \subseteq M^k$ s.t. $\mathcal{M}, \theta[X := S] \models \varphi[X]$. We define $\mathcal{M} \models \varphi$ iff $\mathcal{M}, \theta \models \varphi$ holds for all environments θ. A formula is *valid*, we write $\models \varphi$, iff $\mathcal{M} \models \varphi$ holds for all structures $\mathcal{M}$. We write $\varphi \equiv \psi$, if φ and ψ are logical equivalent, i.e. if $\models \varphi \leftrightarrow \psi$ holds.

To conclude this section about logic we state a lemma where many of these concepts are used. It will be of use later.

Lemma 2.1. *Let $\mathcal{L}$ be a language and $\mathcal{M}$ be an $\mathcal{L}$-structure. Let R be a formula variable and let S and S' be formulas in $\mathcal{L}$ with the same arity as R. Let φ be a second-order formula in $\mathcal{L} \cup \{R\}$, s.t. R occurs only positively in φ. Then*

$$\mathcal{M} \models S(\bar{x}) \to S'(\bar{x}) \quad \Rightarrow \quad \mathcal{M} \models \varphi[R \backslash S] \to \varphi[R \backslash S'].$$

Conversely, if R occurs only negatively in φ, it holds

$$\mathcal{M} \models S(\bar{x}) \to S'(\bar{x}) \quad \Rightarrow \quad \mathcal{M} \models \varphi[R \backslash S'] \to \varphi[R \backslash S].$$

Proof. Let φ be in negation normal form[2] and R occur only positively in φ. We prove the claim by structural induction on φ. Note that there are no negated atomic formulas of the form $\varphi \equiv \neg R(\bar{t})$.[3]

- $\varphi \equiv R(\bar{t})$: It holds $\mathcal{M} \models S(\bar{t}) \to S'(\bar{t})$.
- $\varphi \equiv P(\bar{t})$ for a predicate symbol $P \in \mathcal{L}$: We have $\mathcal{M} \models P(\bar{t}) \to P(\bar{t})$.
- $\varphi \equiv \neg P(\bar{t})$ for a predicate symbol $P \in \mathcal{L}$: Similarly $\mathcal{M} \models \neg P(\bar{t}) \to \neg P(\bar{t})$.

[2] i.e. every negation occurs directly in front of an atomic formula. For every second-order formula there is a logical equivalent formula in negation normal form.
[3] We write $\varphi[S]$ as abbreviation of $\varphi[R \backslash S]$.

- $\varphi \equiv \varphi_1 \vee \varphi_2$: $\mathcal{M} \models \varphi_1[S] \to \varphi_1[S']$ and $\mathcal{M} \models \varphi_2[S] \to \varphi_2[S']$ implies $\mathcal{M} \models \varphi_1[S] \vee \varphi_2[S] \to \varphi_1[S'] \vee \varphi_2[S']$.
- $\varphi \equiv \varphi_1 \wedge \varphi_2$: Same as for " $\vee$ ".
- $\varphi \equiv \exists x \varphi_1$: We got $\mathcal{M}, \theta \models \varphi_1[S] \to \varphi_1[S']$ for all environments θ of x. Hence $\mathcal{M} \models \exists x \varphi_1[S] \to \exists x \varphi_1[S']$.
- Same argumentation as above works for formulas of the form $\varphi \equiv \forall x \varphi_1$ and second-order quantified formulas $\varphi \equiv \exists X \varphi_1$ and $\varphi \equiv \forall X \varphi_1$.

If R occurs only negatively in φ we have negated atomic formulas $\varphi \equiv \neg R(\bar{t})$ instead of $\varphi \equiv R(\bar{t})$. For $\varphi \equiv \neg R(\bar{t})$ it holds $\mathcal{M} \models \neg S'(\bar{t}) \to \neg S(\bar{t})$. The rest of the proof is analogous. □

2.2 Formula equations

Definition 2.2 (Formula equation)**.** *Let $\mathcal{L}$ be a language. A* formula equation *over $\mathcal{L}$ has the form $\exists \overline{X} \varphi$, where $\overline{X} = X_1, ..., X_n$ is a tuple of formula variables and φ is a first-order formula in $\mathcal{L}$ without free individual variables, whose formula variables are among$X_1, ..., X_n$.*

A formula equation $\exists \overline{X} \varphi$ is valid if $\models \exists \overline{X} \varphi$. In contrast, $\exists \overline{X} \varphi$ is first-order solvable if there exist first-order formulas $\chi_1, ..., \chi_n$ s.t. $\models \varphi[\overline{X} \backslash \bar{\chi}]$. Every first-order solvable formula is valid, yet in general the converse is not true.
If we are interested in a specific class of formulas, which solve formula equations, we talk about solution problems. As sometimes it is also interesting to speak about validity modulo a specific theory we have the following general definition.

Definition 2.3 (Solution problem)**.** *Let $\mathcal{L}$ be a first-order language. A* solution problem *over $\mathcal{L}$ consists of*

- *A theory $\mathcal{T}$ (the background theory),*
- *A class $\mathcal{C}$ of formulas (the candidate solutions).*
- *A class Φ of formula equations,*

The solution problem *$\langle \mathcal{T}, \mathcal{C}, \Phi \rangle$ is the set of formula equations in Φ that have solutions in $\mathcal{C}$ modulo the theory $\mathcal{T}$, i.e. the set*

$$\{\varphi \in \Phi \mid \exists F_1, ..., F_n \in \mathcal{C} : \mathcal{T} \models \varphi[X_1 \backslash F_n, ..., X_n \backslash F_n]\}.$$

Example 2.4.
- *Let $\mathcal{L}$ be any language and let Φ be the class of first-order formulas in $\mathcal{L}$, i.e. formula equations without formula variables. Then the solution problem $\langle \emptyset, \emptyset, \Phi \rangle$ is the problem of first-order validity. This is undecidable.*

- *Let $\mathcal{L}$ be any language. Let Φ be the set of quantifier-free formula equations and $\mathcal{C}$ be the set of quantifier-free first-order formulas. Then the solution problem $\langle \emptyset, \mathcal{C}, \Phi \rangle$ is called the* quantifier-free solution problem. *As shown in [5] this problem is Π_2^P-complete.* [4]

- *Let $\mathcal{L}$ be any first-order language. Let Φ be the set of formula equations of the form $\exists \overline{X} \forall \overline{y}\ \psi$, where ψ is a quantifier-free formula and $\mathcal{C}$ be the set of quantifier-free first-order formulas. Then the solution problem $\langle \emptyset, \mathcal{C}, \Phi \rangle$ is called the* universal solution problem. *As shown in [5] this problem is undecidable.* [5]

2.3 Fixed-point logics

We give an overview of least fixed-point logic and inflationary fixed-point logic. This will be enough for our purpose, for a more detailed description we refer to [7] and [3].

Definition 2.5. *Let A be a set.*

- *A function $F : 2^A \to 2^A$ is called an* operator *on A.*

- *An operator is* monotonous *if for all $X \subseteq Y \subseteq A$ it holds that $F(X) \subseteq F(Y)$.*

- *An operator is* inflationary *if $X \subseteq F(X)$ for all $X \subseteq A$.*

- *A set $X \subseteq A$ is a* fixed point *of F if $F(X) = X$.*

- *A set $X \subseteq A$ is the* least fixed point *of F, if X is a fixed point of F and for any fixed point Y it holds that $X \subseteq Y$. This is denoted as* $\mathrm{lfp}(F)$.

Note that there are monotonous operators, which are not inflationary and inflationary operators, which are not monotonous.

Definition 2.6. *Let $\mathcal{L}$ be a first-order language and R a formula variable of arity k. Let $\varphi(R, x_1, ..., x_k)$ be a first-order formula in $\mathcal{L} \cup \{R\}$. For an $\mathcal{L}$-structure $\mathcal{M}$ define an operator F_φ on M^k by*

$$F_\varphi : \quad X \mapsto \{\bar{x} \in M^k \mid \mathcal{M}, [R := X] \models \varphi(R, \bar{x})\}.$$

[4] Other authors also call this problem QFBUP(Quantifier-free boolean unification problem).
[5] The same authors call this problem UBUP.

2.3.1 Monotonous fixed point

Lemma 2.7. *If R occurs only positively in φ, then F_φ is a monotonous operator.*

Proof. Let $A \subseteq B \subseteq M^k$. We have $\mathcal{M}, [S := A, S' := B] \models S(\bar{x}) \to S'(\bar{x})$. The proof of Lemma 2.1, adjusted for sets in M^k instead of formulas, yields
$\mathcal{M}, [S := A, S' := B] \models \varphi[R\backslash S] \to \varphi[R\backslash S']$. Thus $F_\varphi(A) \subseteq F_\varphi(B)$. □

The following theorem is normally presented in the context of a complete lattice $\langle E, \leq \rangle$ (cf. [2]). As $\langle 2^A, \subseteq \rangle$ is a complete lattice we can modify it for our need:

Theorem 2.8 (Knaster-Tarski)**.** *Let F be a monotonous operator on a set A. Then F has a least fixed point and*

$$\mathrm{lfp}(F) = \bigcap \{X \subseteq A \mid F(X) \subseteq X\}.$$

Definition 2.9 (LFP)**.** *Least fixed-point logic(LFP) is an expansion of first-order logic, which in addition to the usual formation rules allows atomic formulas*

$$[\mathrm{lfp}_R\ \varphi(R, \bar{x})](\bar{t}), \tag{2.1}$$

where $\varphi(R, \bar{x})$ is a first-order formula in $\mathcal{L} \cup \{R\}$, s.t. R occurs only positively, R is k-ary and $\bar{t}$ is a k-tuple of terms. The free variables of (2.1) are those of $\bar{t}$.
The semantics is defined as follows:

$$\mathcal{M} \models [\mathrm{lfp}_R\ \varphi(R, \bar{x})](\bar{a}) :\Leftrightarrow\ \bar{a} \in \mathrm{lfp}(F_\varphi).$$

As R occurs only positively, F_φ is a monotonous operator according to Lemma 2.7. Using Theorem 2.8 the least fixed point exists and thus the definition does make sense.

Example 2.10. *Let $\mathcal{L} = \{E\}$ be the language of graphs, where E is a binary relation symbol and R be a binary formula variable. Define*

$$\varphi(R, u, v) \equiv E(u, v) \vee \exists w(R(u, w) \wedge E(w, v)).$$

As R occurs only positively in φ we can define $[\mathrm{lfp}_R\ \varphi(R, u, v)](x, y)$, which holds iff there is a path from x to y.

2.3.2 Inflationary fixed point

The least fixed point of an operator is hard to grasp. Therefore we define a sequence of sets, which, if the operator is monotonous, converges to the least fixed point. This yields the notion of inflationary fixed point.

Definition 2.11. *Let F be an operator on a set A. We define the inflationary operator F' by $F'(X) = F(X) \cup X$. By transfinite recursion define the following sequence of subsets of 2^A, where ζ and η are ordinal numbers:*

$$\begin{aligned} S_F^0 &= \varnothing, \\ S_F^{\zeta+1} &= F'(S_F^\zeta), \\ S_F^\zeta &= \bigcup_{\eta<\zeta} S_F^\eta, \quad \textit{for limit ordinals } \zeta. \end{aligned}$$

If it is obvious which operator we talk of, we sometimes omit the subscript and write S^ζ.

Lemma 2.12. *1. $\zeta \leq \eta \Rightarrow S_F^\zeta \subseteq S_F^\eta$,*

2. *There exists an ordinal number ξ s.t. $F'(S_F^\xi) = S_F^\xi$ and $|\xi| \leq |A|$. We call the least such ξ the* closure ordinal *of F and we define the* inflationary fixed point *of F, written* $\mathrm{ifp}(F)$*, to be S_F^ξ.*

3. *$\zeta \geq \xi \Rightarrow S_F^\zeta = S_F^\xi$*

4. *If F is monotonous, then* $\mathrm{ifp}(F) = \mathrm{lfp}(F)$.

5. *If F is monotonous, then $S_F^\zeta \subseteq F(S_F^\zeta)$ for all ordinals ζ, thus we can use F instead of F' in the definition of the sequence (S_F^ζ).*

Proof. As F' is an inflationary operator 1. follows from the definition of the sequence (S_F^ζ). For 2. assume that $F'(S^\zeta) \supsetneq S^\zeta$ for every $|\zeta| \leq |A|$. Then we can choose $x_\zeta \in F'(S^\zeta) \setminus S^\zeta$ for every such ζ. Hence the set

$$\{x_\zeta \mid \zeta \leq |A|\}$$

is a subset of A, yet it has cardinality bigger then A, a contradiction. As $F'(S^\xi) = F(S^\xi) \cup S^\xi \supseteq S^\xi$, the claim follows.
3. follows by induction from the fact that $F'(S^\xi) = S^\xi$.
4. From 2. we get that $F(S^\xi) \subseteq S^\xi$ and thus $\mathrm{lfp}(F) \subseteq S^\xi$ with Theorem 2.8. Now let X be any fixed point of F. We prove by transfinite induction that $S^\zeta \subseteq X$ for every $\zeta \leq \xi$. Obviously $S^0 = \varnothing \subseteq X$. Now assume $S^\zeta \subseteq X$. From the monotonicity of F it follows that $F(S^\zeta) \subseteq F(X)$ and therefore

$$S^{\zeta+1} = F'(S^\zeta) = F(S^\zeta) \cup S^\zeta \subseteq F(X) \cup X = X.$$

For limit ordinals ζ assume $S^\eta \subseteq X$ for all $\eta \leq \zeta$, we got

$$S^\zeta = \bigcup_{\eta<\zeta} S^\eta \subseteq \bigcup_{\eta<\zeta} X = X.$$

Hence $S^\xi \subseteq X$ and in total $S^\xi = \mathrm{lfp}(F)$.
We proof 5. by transfinite induction on ζ. First $S^0 = \varnothing \subseteq S^1$. For a successor ordinal ζ assume $S^{\zeta-1} \subseteq F(S^{\zeta-1})$, in particular $F'(S^{\zeta-1}) = F(S^{\zeta-1})$. Using monotonicity of F we get $F(S^{\zeta-1}) \subseteq F(F(S^{\zeta-1}))$ and hence

$$S^\zeta = F'(S^{\zeta-1}) = F(S^{\zeta-1}) \subseteq F(F(S^{\zeta-1})) = F(S^\zeta).$$

For a limit ordinal ζ assume $x \in S^\zeta$. Thus $x \in S^\eta$ for an ordinal $\eta < \zeta$. Using the induction hypothesis and monotonicity we get

$$S^\eta \subseteq F(S^\eta) \subseteq F(S^\zeta).$$

Therefore $x \in F(S^\zeta)$ and we get $S^\zeta \subseteq F(S^\zeta)$. □

Analogous to the least fixed-point logic we now can define inflationary fixed-point logic, which generalizes least fixed-point logic in the way that it allows negative occurrences of R in φ.

Definition 2.13 (IFP). *Inflationary fixed-point logic(IFP) is an expansion of first-order logic, which in addition to the usual formation rules allows atomic formulas*

$$[\mathrm{ifp}_R\ \varphi(R, \bar{x})](\bar{t}), \tag{2.2}$$

where $\varphi(R, \bar{x})$ is a first-order formula in $\mathcal{L} \cup \{R\}$, R is k-ary and $\bar{t}$ is a k-tuple of terms. The free variables of (2.2) are those of $\bar{t}$.
The semantics is defined as follows:

$$\mathcal{M} \models [\mathrm{ifp}_R\ \varphi(R, \bar{x})](\bar{a}) :\Leftrightarrow\ \bar{a} \in \mathrm{ifp}(F_\varphi).$$

Lemma 2.14. *Let $\mathcal{L}$ be a language. Let $\varphi(R, \bar{x})$ be a first-order formula in $\mathcal{L} \cup \{R\}$, s.t. R occurs only positively. Then for all $i \in \{1, ..., n\}$*

$$[\mathrm{ifp}_R\ \varphi(R, \bar{x})] \equiv [\mathrm{lfp}_R\ \varphi(R, \bar{x})].$$

Proof. Using the definition of IFP and LFP this is equivalent to $\mathrm{ifp}(F_\varphi) = \mathrm{lfp}(F_\varphi)$ for every structure $\mathcal{M}$. From Lemma 2.7 we obtain that F_φ is a monotonous operator, hence the claim follows with Lemma 2.12/4. □

Example 2.15. *We continue Example 2.10 from the previous section, where we defined*

$$\varphi(R, u, v) \equiv E(u, v) \vee \exists w(R(u, w) \wedge E(w, v)).$$

Let G be any graph and $n \in \mathbb{N}$. Then $(x, y) \in S^n_{F_\varphi}$ iff there is a path from x to y of length at most n. Hence $(x, y) \in S^\omega_{F_\varphi}$ iff there is a finite path from x to y. $[\mathrm{ifp}_R\ \varphi(R, u, v)](x, y)$ holds, iff there is any path from x to y, which describes the same relation as $[\mathrm{lfp}_R\ \varphi(R, u, v)](x, y)$.

2.3.3 Simultaneous monotonous fixed point

The previously introduced concepts may be generalized for m-ary operators. We skip the proofs as they are similar, only more technical, to their counterparts in the previous subsections.

Definition 2.16. *Let $A_1, ..., A_n$ be sets.*

- *A function $F : 2^{A_1} \times \cdots \times 2^{A_n} \to 2^{A_1} \times \cdots \times 2^{A_n}$ is called an* n-ary operator *on $A_1 \times \cdots \times A_n$.*
- *For two sequences of sets $\overline{X} := (X_1, ..., X_n)$ and $\overline{Y} := (Y_1, ..., Y_n)$ we write $\overline{X} \subseteq \overline{Y}$ if $X_i \subseteq Y_i$ for all $i \in \{1, ..., n\}$.*
- *F is* monotonous *if for all $\overline{X} \subseteq \overline{Y} \subseteq \overline{A}$ it holds that $F(\overline{X}) \subseteq F(\overline{Y})$.*
- *F is* inflationary *if for all $\overline{X}$ and $i \in \{1, ..., n\}$ it holds that $X_i \subseteq F(\overline{X})_i$.*
- *$\overline{X}$ is a* fixed point *of F if $F(\overline{X}) = \overline{X}$.*
- *If $\overline{X}$ is a fixed point of F and for every fixed point $\overline{Y}$ we have $\overline{X} \subseteq \overline{Y}$, then $\overline{X}$ is called the* least fixed point *of F, written* $\mathrm{lfp}(F)$.

Similarly to Theorem 2.8 we have (cf. [2]):

Theorem 2.17. *Let $A_1, ..., A_n$ be sets and F be a monotonous n-ary operator on $A_1 \times \cdots \times A_n$. Then F has a least fixed point.*

Definition 2.18. *Let $\mathcal{L}$ be a language and $R_1, ..., R_n$ be formula variables, with R_i being of arity k_i. Consider a sequence Φ of first-order formulas in $\mathcal{L} \cup \{R_1, ..., R_n\}$:*

$$\begin{gathered} \varphi_1(R_1, ..., R_n, \overline{x_1}) \\ \vdots \\ \varphi_n(R_1, ..., R_n, \overline{x_n}), \end{gathered}$$

where $|\overline{x_i}| = k_i$.
For a structure $\mathcal{M}$ define

$$\begin{aligned} F_i : \quad & M^{k_1} \times \cdots \times M^{k_n} \to M^{k_i}, \\ & (X_1, ..., X_n) \mapsto \{\overline{x} \in M^{k_i} \mid \mathcal{M}, [R_1 := X_1, ..., R_n := X_n] \models \varphi_i(R_1, ..., R_n, \overline{x})\}. \end{aligned}$$

Now define the n-ary operator $F_\Phi = (F_1, ..., F_n)$.

Lemma 2.19. *If $R_1, ..., R_n$ occur only positively in Φ, then F_Φ is a monotonous n-ary operator on $M^{k_1} \times \cdots \times M^{k_n}$.*

Proof. This proof is analogous to the proof of Lemma 2.7. □

Definition 2.20 (LFP^{SIM}). *Simultaneous least fixed-point logic(LFP^{SIM}) is an expansion of first-order logic, which in addition to the usual formation rules allows atomic formulas*

$$[\mathrm{lfp}_{R_i}\ \Phi](\bar{t}), \tag{2.3}$$

where Φ is defined as in Definition 2.18 with $R_1, .., R_n$ occurring only positively in Φ and $\bar{t}$ is a k_i-tuple of terms. The free variables of (2.3) are those of $\bar{t}$.
The semantics is defined as follows:

$$\mathcal{M} \models [\mathrm{lfp}_{R_i}\ \Phi](\bar{a}) : \Leftrightarrow\ \bar{a} \in \mathrm{lfp}(F_\Phi)_i.$$

Example 2.21. *Again consider the language of graphs $\mathcal{L} = \{E\}$, where E is a binary relation symbol. Let R and S be two 2-ary formula variables. Define Φ as*

$$\varphi_1(R, S, u, v) \equiv E(u, v) \vee \exists w(S(u, w) \wedge E(w, v)),$$
$$\varphi_2(R, S, u, v) \equiv \exists w(R(u, w) \wedge E(w, v)).$$

As R and S occur only positively in Φ, we can define the formulas in LFP^{SIM} $[\mathrm{lfp}_R\ \Phi](x, y)$ and $[\mathrm{lfp}_S\ \Phi](x, y)$. The former holds iff there is an odd path and the latter iff there is an even path from x to y.

In the last example it is easy to see that there are equivalent formulas in LFP. That this is always the case is the content of the next theorem. A proof can be found in [7].

Theorem 2.22. *For every formula φ in LFP^{SIM} there exists a formula ψ in LFP, s.t. $\varphi \equiv \psi$.*

Note that the converse of Theorem 2.22 is also true, as LFP^{SIM} is a generalization of LFP. Thus we can use LFP and LFP^{SIM} interchangeably.

2.3.4 Simultaneous inflationary fixed point

Definition 2.23. *Let $F = (F_1, ..., F_n)$ be an n-ary operator. We define the* inflationary n-ary operator *of F to be $F' = (F'_1, ..., F'_n)$, where $F'_j(\overline{X}) = F_j(\overline{X}) \cup X_j$ for $j \in \{1, ..., n\}$.*

By transfinite recursion define the sequence of sets[6]

$$\begin{aligned} S^0 &= (\varnothing, ..., \varnothing), \\ S^{\zeta+1} &= F'(S^\zeta), \\ S^\zeta &= \bigcup_{\eta<\zeta} S^\eta, \quad \text{for limit ordinals } \zeta. \end{aligned} \tag{2.4}$$

Analogous to Lemma 2.12 we get:

[6] We write S^ζ as abbreviation for S^ζ_F.

Lemma 2.24. *Let F be an n-ary operator and the sequence (S^ζ) defined as above. Then*

1. $\zeta \leq \eta \Rightarrow S^\zeta \subseteq S^\eta$,
2. *There exists an ordinal number ξ s.t. $F'(S^\xi) = S^\xi$ and $|\xi| \leq |A|$. We call the least such ξ the* closure ordinal *of F and we define the* simultaneous inflationary fixed point *of F, written* $\mathrm{ifp}(F)$*, to be S^ξ.*
3. $\zeta \geq \xi \Rightarrow S^\zeta = S^\xi$
4. *If F is monotonous, then* $\mathrm{ifp}(F) = \mathrm{lfp}(F)$.
5. *If F is monotonous, then $S^\zeta \subseteq F(S^\zeta)$ for all ordinals ζ, thus we can use F instead of F' in the definition of S^ζ.*

Proof. This proof is essentially the proof of Lemma 2.12. □

Definition 2.25 (IFP^{SIM})**.** *Simultaneous inflationary fixed-point logic(IFP^{SIM}) is an expansion of first-order logic, which in addition to the usual formation rules allows atomic formulas*

$$[\mathrm{ifp}_{R_i}\ \Phi](\bar{t}), \tag{2.5}$$

where Φ is defined as in Definition 2.18 and $\bar{t}$ is a k_i-tuple of terms. The free variables of (2.5) are those of $\bar{t}$.
The semantics is defined as follows:

$$\mathcal{M} \models [\mathrm{ifp}_{R_i}\ \Phi](\bar{a}) : \Leftrightarrow\ \bar{a} \in \mathrm{ifp}(F_\Phi)_i.$$

Lemma 2.26. *If $R_1, ..., R_n$ occur only positively in Φ, then for all $i \in \{1, ..., n\}$*

$$[\mathrm{ifp}_{R_i}\ \Phi] \equiv [\mathrm{lfp}_{R_i}\ \Phi].$$

Proof. Lemma 2.19 states, that F_Φ is monotonous and hence $\mathrm{ifp}(F_\Phi) = \mathrm{lfp}(F_\Phi)$ for every structure $\mathcal{M}$. This is equivalent to $[\mathrm{ifp}_{R_i}\ \Phi] \equiv [\mathrm{lfp}_{R_i}\ \Phi]$. □

As for LFP^{SIM} we have:

Theorem 2.27. *For every formula φ in IFP^{SIM} there exists a formula ψ in IFP, s.t. $\varphi \equiv \psi$.*

Chapter 3

The fixed-point theorems

This chapter will be the main part of this work. We will take a look at special formula equations: Horn, dual-Horn and linear-Horn formula equations. For those there exist canonical solutions, which are described by least fixed-point formulas. At last we will see that we can not generalize the results for universal formula equations.

3.1 Horn formula equations

The idea to prove the fixed-point theorem is the following: For a Horn formula equation $\exists \overline{X} \psi$ we define an operator F_ψ such that every solution of $\exists \overline{X} \psi$ is a fixed point of F_ψ. It turns out that the least fixed point of F_ψ is always a solution of $\exists \overline{X} \psi$ if there exists one. This canonical solution is described by a least fixed-point logic formula.

Definition 3.1. *Let $\mathcal{L}$ be a language and $X_1, ..., X_n$ formula variables. A* variable atom *in $\mathcal{L} \cup \{X_1, ..., X_n\}$ is an atom starting with a formula variable, i.e. it is of the form $X_i(\overline{t_i})$, where $i \in \{1, ..., n\}$ and $\overline{t_i}$ is a tuple of terms in $\mathcal{L}$ with the same arity as X_i.*
A constrained Horn clause *in $\mathcal{L} \cup \{X_1, ..., X_n\}$ is a disjunction of a first-order formula in $\mathcal{L}$, negated variable atoms and at most one variable atom, i.e. it has the form*

$$\gamma \vee \neg X_{i_1}(\overline{t_{i_1}}) \vee \cdots \vee \neg X_{i_m}(\overline{t_{i_m}}) \vee X_{i_0}(\overline{t_{i_0}}),$$

where γ is a first-order formula, $\overline{t_{i_0}}, .., \overline{t_{i_m}}$ are tuples of terms in $\mathcal{L}$ of appropriate arity and $i_0, i_1, ..., i_m \in \{1, ..., n\}$.
Conversely, a constrained dual-Horn clause *in $\mathcal{L} \cup \{X_1, ..., X_n\}$ is a disjunction of a first-order formula in $\mathcal{L}$, variable atoms and at most one negated variable atom.*
A constrained linear-Horn clause *in $\mathcal{L} \cup \{X_1, ..., X_n\}$ is a clause which is both a constrained Horn clause and a constrained dual-Horn clause, i.e. it is of the form*

$$\gamma \vee \neg X_{i_1}(\overline{t_{i_1}}) \vee X_{i_0}(\overline{t_{i_0}}).$$

Definition 3.2. *Let $\mathcal{L}$ be a language. A* Horn formula equation *is a formula equation of the form $\exists\overline{X}\forall\bar{y}\ \bigwedge_{i=1}^{m} H_i$, where H_i is a constrained Horn clause for $i \in \{1,...,m\}$.*

Let $\exists\overline{X}\psi$ be a Horn formula equation with formula variables $X_1,...,X_n$. There are three different types of clauses in ψ:

$$\begin{array}{lll} (B) & \gamma & \to X_{i_0}(\bar{s}), \\ (I) & \gamma \wedge X_{i_1}(\overline{t_1}) \wedge \cdots \wedge X_{i_m}(\overline{t_m}) & \to X_{i_0}(\bar{s}), \\ (E) & \gamma \wedge X_{i_1}(\overline{t_1}) \wedge \cdots \wedge X_{i_m}(\overline{t_m}) & \to \bot, \end{array}$$

where γ is a first-order formula in $\mathcal{L}$, $m \geq 1$, $\overline{t_1},..,\overline{t_m},\bar{s}$ are tuples of terms in $\mathcal{L}$ of appropriate arity and $i_0, i_1, ..., i_m \in \{1,...,n\}$. Note that the variables $\bar{y}$ may occur in the formulas γ and the terms $\bar{s}, \overline{t_1}, ..., \overline{t_m}$. We call the first base clauses, the second induction clauses, and the third end clauses. The idea now is to build an inductive relation from the base and induction clauses for every formula variable.

Let B_j and I_j be the sets of clauses of the form (B) and (I), respectively, where $i_0 = j$, for $j \in \{1,...,n\}$. For shorter notation we write $\iota := \{i_1,...,i_m\}$ and $\tau := \{\overline{t_1},...,\overline{t_m}\}$. A clause in I_j is determined by the tuple $(\gamma,\iota,\tau,\bar{s})$, thus we write $(\gamma,\iota,\tau,\bar{s})$ for the clause $\gamma \wedge X_{i_1}(\overline{t_1}) \wedge \cdots \wedge X_{i_m}(\overline{t_m}) \to X_j(\bar{s})$ in I_j. Analogously we write $(\gamma,\bar{s})$ for the clause $\gamma \to X_j(\bar{s})$ in B_j.
Every Horn formula equation $\exists\overline{X}\psi$ defines a sequence of first-order formulas Φ_ψ as follows:

$$\begin{aligned} \varphi_1(X_1,...,X_n,\overline{x_1}) &\equiv \exists\bar{y}\left(\bigvee_{(\gamma,\bar{s})\in B_1}(\gamma\wedge\overline{x_1}=\bar{s}) \vee \bigvee_{(\gamma,\iota,\tau,\bar{s})\in I_1}\left(\gamma\wedge\bigwedge_{k=1}^{m}X_{i_k}(\overline{t_k})\wedge\overline{x_1}=\bar{s}\right)\right), \\ &\vdots \\ \varphi_n(X_1,...,X_n,\overline{x_n}) &\equiv \exists\bar{y}\left(\bigvee_{(\gamma,\bar{s})\in B_n}(\gamma\wedge\overline{x_n}=\bar{s}) \vee \bigvee_{(\gamma,\iota,\tau,\bar{s})\in I_n}\left(\gamma\wedge\bigwedge_{k=1}^{m}X_{i_k}(\overline{t_k})\wedge\overline{x_n}=\bar{s}\right)\right), \end{aligned} \tag{3.1}$$

where $\overline{x_j}$ is a tuple of variables s.t. $|\overline{x_j}|$ equals the arity of X_j for $j \in \{1,...,n\}$. Notice that $X_1,...X_n$ only occur positively in Φ_ψ, hence we can introduce the simultaneous fixed-point formulas $[\mathrm{lfp}_{X_j}\ \Phi_\psi]$ for $j \in \{1,...,n\}$.

Lemma 3.3. *Let $\exists\overline{X}\psi$ be a Horn formula equation and $\alpha_j := [\mathrm{lfp}_{X_j}\ \Phi_\psi]$ for $j \in \{1,...,n\}$. Then:*

1. $\models \exists\overline{X}\ \psi \leftrightarrow \psi[X_1\backslash\alpha_1,...,X_n\backslash\alpha_n]$,
2. *If for a structure $\mathcal{M}$ and relations $\chi_1,...,\chi_n$ it holds $\mathcal{M} \models \psi[X_1\backslash\chi_1,...,X_n\backslash\chi_n]$, then $\mathcal{M} \models \bigwedge_{j=1}^{n}\alpha_j \to \chi_j$.*

3. *If* $\models \exists \overline{X}\ \psi \leftrightarrow \psi[X_1 \backslash \chi_1, ..., X_n \backslash \chi_n]$ *for LFP-formulas* $\chi_1, ..., \chi_n$, *then* $\models \exists \overline{X}\ \psi \rightarrow \left(\bigwedge_{j=1}^{n} \alpha_j \rightarrow \chi_j\right)$.

Proof. 1. The right-to-left direction is clear. For the other direction we first state that the formulas $\alpha_1, ..., \alpha_n$ satisfy all clauses in (B) and (I), i.e. for all $j \in \{1, ..., n\}$ it holds

$$\begin{aligned} &\models \forall \bar{y}\ (\gamma \rightarrow \alpha_j(\bar{s})), && \forall (\gamma, \bar{s}) \in B_j, \\ &\models \forall \bar{y}\ (\gamma \wedge \alpha_{i_1}(\overline{t_1}) \wedge \cdots \wedge \alpha_{i_m}(\overline{t_m}) \rightarrow \alpha_j(\bar{s})), && \forall (\gamma, \iota, \tau, \bar{s}) \in I_j. \end{aligned}$$

To see this let $\mathcal{M}$ be a structure and $\overline{y_0}$ s.t.

$$\mathcal{M}, [\bar{y} := \overline{y_0}] \models \gamma \wedge \alpha_{i_1}(\overline{t_1}) \wedge \cdots \wedge \alpha_{i_m}(\overline{t_m}),$$

then, as $(\alpha_1, ..., \alpha_n)$ is a fixed point of F_Φ, we have

$$\mathcal{M}, [\bar{y} := \overline{y_0}] \models \alpha_j(\bar{s}).$$

The argumentation is analogous for clauses of the form (B).
Now let $\mathcal{M}$ be a structure s.t. $\mathcal{M} \models \exists \overline{X}\ \psi$. Let $\chi_1, ..., \chi_n$ be relations s.t. $\mathcal{M} \models \psi[X_1 \backslash \chi_1, ..., X_n \backslash \chi_n]$, thus it holds for all $j \in \{1, ..., n\}$:

$$\mathcal{M} \models \forall \bar{y}\ (\gamma \rightarrow \chi_j(\bar{s})), \qquad \forall (\gamma, \bar{s}) \in B_j, \tag{3.2}$$

$$\mathcal{M} \models \forall \bar{y}\ (\gamma \wedge \chi_{i_1}(\overline{t_1}) \wedge \cdots \wedge \chi_{i_m}(\overline{t_m}) \rightarrow \chi_j(\bar{s})), \qquad \forall (\gamma, \iota, \tau, \bar{s}) \in I_j. \tag{3.3}$$

Assume $\overline{x_j} \in F_\Phi(\chi_1, ..., \chi_n)_j$. Then there either exists $(\gamma, \bar{s}) \in B_j$ s.t

$$\mathcal{M} \models \exists \bar{y}\ (\gamma \wedge \overline{x_j} = \bar{s})$$

or $(\gamma, \iota, \tau, \bar{s}) \in I_j$ s.t.

$$\mathcal{M}, [\overline{X} := \overline{\chi}] \models \exists \bar{y}\ (\gamma \wedge \bigwedge_{k=1}^{m} X_{i_k}(\overline{t_k}) \wedge \overline{x_j} = \bar{s})$$

We assume the latter, the proof for the former is analogous. Thus let $\overline{y_0}$ be s.t.

$$\mathcal{M}, [\overline{X} := \overline{\chi}, \bar{y} := \overline{y_0}] \models \gamma \wedge \bigwedge_{k=1}^{m} X_{i_k}(\overline{t_k}) \wedge \overline{x_j} = \bar{s}.$$

From (3.3) we obtain $\mathcal{M}, [\bar{y} := \overline{y_0}] \models \chi_j(\bar{s})$ and thus $\mathcal{M} \models \chi_j(\overline{x_j})$.

Hence $F_\Phi(\chi_1, ..., \chi_n) \subseteq (\chi_1, ..., \chi_n)$ and as $(\alpha_1, ..., \alpha_n)$ is the least fixed point of F_Φ we obtain $\mathcal{M} \models \bigwedge_{j=1}^{n} \alpha_j \rightarrow \chi_j$.
For all clauses in (E) it holds that

$$\mathcal{M}, [\overline{X} := \overline{\chi}] \models \forall \bar{y}\ (\gamma \wedge X_{i_1}(\overline{t_1}) \wedge \cdots \wedge X_{i_m}(\overline{t_m}) \rightarrow \bot),$$

and therefore, as $X_1, ..., X_n$ only occur positively, we get with Lemma 2.1

$$\mathcal{M}, [\overline{X} := \overline{\alpha}] \models \forall \overline{y}\ (\gamma \wedge X_{i_1}(\overline{t_1}) \wedge \cdots \wedge X_{i_m}(\overline{t_m}) \rightarrow \bot).$$

Thus $\mathcal{M}, [\overline{X} := \overline{\alpha}]$ satisfies all clauses in ψ and we conclude that $\mathcal{M} \models \psi[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$.
For 2. we get $\mathcal{M} \models \bigwedge_{j=1}^{n} \alpha_j \rightarrow \chi_j$ analogous as in the proof of 1.
3. holds, as for every structure $\mathcal{M}$, which fulfils $\mathcal{M} \models \exists \overline{X}\ \psi$, we can use 2. □

We have proven Lemma 3.3/3 for LFP-formulas. Yet this holds for an arbitrary class of formulas, as it is an immediate consequence of 3.3/2, where we have shown $\mathcal{M} \models \bigwedge_{j=1}^{n} \alpha_j \rightarrow \chi_j$ for any relations $\chi_1, ..., \chi_n$.

Theorem 3.4 (Horn fixed-point theorem)**.** *Let $\exists \overline{X} \psi$ be a valid Horn formula equation, i.e. $\models \exists \overline{X} \psi$, and $\alpha_j := [\mathrm{lfp}_{X_j}\ \Phi_\psi]$ for $j \in \{1, ..., n\}$. Then:*

1. *$\models \psi[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$,*
2. *If $\models \psi[X_1 \backslash \chi_1, ..., X_n \backslash \chi_n]$ for LFP-formulas $\chi_1, ..., \chi_n$, then $\models \bigwedge_{j=1}^{n} \alpha_j \rightarrow \chi_j$.*

Proof. As we got $\models \exists \overline{X} \psi$ by assumption, 1. follows directly from Lemma 3.3/1. and 2. follows from Lemma 3.3/3. □

For Horn formula equations we got three concepts: validity, first-order solvability and LFP-solvability. A priori these are all different. Now Theorem 3.4/1 shows that a Horn Formula equation is valid iff it is LFP-solvable.

To illustrate Lemma 3.3 and Theorem 3.4 we take a look at the following example:

Example 3.5. *Let $\mathcal{L} = \{E, s, t\}$ be the language of graphs with two specified vertices s and t. Consider the Horn formula equation $\exists X, Y \psi$ with two unary formula variables X and Y:*

$$\psi \equiv \forall u, v \bigwedge \begin{cases} X(s) \\ Y(t) \\ X(u) \wedge E(u, v) \rightarrow X(v) \\ Y(u) \wedge E(u, v) \rightarrow Y(v) \\ X(u) \wedge Y(u) \rightarrow \bot \end{cases} .$$

There are two base clauses, two induction clauses and one end clause. It is easy to see that a graph satisfies ψ iff there is no vertex v s.t. there is a path from s to v and from t to v. The sequence of formulas Φ_ψ is

$$\varphi_1(X, Y, x_1) \equiv \exists u, v(x_1 = s \vee (X(u) \wedge E(u, v) \wedge x_1 = v)),$$
$$\varphi_1(X, Y, x_2) \equiv \exists u, v(x_2 = t \vee (Y(u) \wedge E(u, v) \wedge x_2 = v)).$$

Thus for every structure $\mathcal{M}$ we have $F_{\Phi_\psi}(\varnothing,\varnothing) = (s,t)$ and $F^{n+1}_{\Phi_\psi}(\varnothing,\varnothing)$ is the pair of sets of vertices for which there is a path from s and t, respectively, with length at most n. The formulas $\alpha_X := [\mathrm{lfp}_X\ \Phi_\psi]$ and $\alpha_Y := [\mathrm{lfp}_Y\ \Phi_\psi]$ describe the sets of vertices reachable from s and t, respectively. Hence Lemma 3.3 states that a structure $\mathcal{M}$ satisfies $\exists X, Y\psi$ iff α_X and α_Y are disjoint.

Note that in general there is no greatest fixed point such that there is a similar theorem to Theorem 3.3. As counterexample take the following Horn formula equation $\exists X\psi$ with one unary formula variable X:

$$\psi \equiv \neg X(c_1) \vee \neg X(c_2),$$

where c_1 and c_2 are constant symbols. Consider the structure

$$\mathcal{M} = \{\{a,b\}; I(c_1) = a, I(c_2) = b\}.$$

For the sets $S_1 = \{a\}$ and $S_2 = \{b\}$ we have

$$\mathcal{M}, [X := S_1] \models \psi \quad \text{and} \quad \mathcal{M}, [X := S_2] \models \psi, \quad \text{yet} \quad \mathcal{M}, [X := S_1 \cup S_2] \not\models \psi.$$

Hence there can not be a greatest set S in $\mathcal{M}$ s.t. $\mathcal{M}, [X := S] \models \psi$. As ψ only consists of one end clause the least fix point in $\mathcal{M}$ is $S = \varnothing$.

3.2 Dual-Horn formula equations

In the last section we have seen that for Horn formula equations there is a solution, which implies every solution. If we consider dual-Horn clauses instead of Horn clauses the converse is true: We obtain a solution which is implied by every solution.

Definition 3.6. *Let $\mathcal{L}$ be a language. A* dual-Horn formula equation *is a formula equation of the form $\exists\overline{X}\forall\overline{y}\ \bigwedge_{i=1}^m H_i$, where H_i is a constrained dual-Horn clause for $i \in \{1,...,m\}$.*

Let $\exists\overline{Y}\psi$ be a dual-Horn formula equation with formula variables $Y_1,...,Y_n$. Define ψ^D by replacing every occurrence of Y_j by $\neg X_j$ for every $j \in \{1,...,n\}$ in ψ. We call ψ^D the dual formula of ψ. Then up to logical equivalence every clause in ψ^D has at most one positive formula variable and hence $\exists\overline{X}\psi^D$ is a Horn formula equation. We define, as in the last section, $\alpha_j := [\mathrm{lfp}_{X_j}\ \Phi_{\psi^D}]$ for $j \in \{1,...,n\}$. Now define the LFP-formulas $\beta_j := \neg\alpha_j$ for $j \in \{1,...,n\}$.

Lemma 3.7. *Let $\exists\overline{Y}\psi$ be a dual-Horn formula equation and $\beta_j := \neg[\mathrm{lfp}_{X_j}\ \Phi_{\psi^D}]$ for $j \in \{1,...,n\}$. Then:*

1. $\models \exists\overline{Y}\ \psi \leftrightarrow \psi[Y_1\backslash\beta_1,...,Y_n\backslash\beta_n]$,

2. *If for a structure* $\mathcal{M}$ *and relations* $\chi_1, ..., \chi_n$ *it holds* $\mathcal{M} \models \psi[Y_1 \backslash \chi_1, ..., Y_n \backslash \chi_n]$*, then* $\mathcal{M} \models \bigwedge_{j=1}^{n} \chi_j \to \beta_j$.

3. *If* $\models \exists \overline{Y}\ \psi \leftrightarrow \psi[Y_1 \backslash \chi_1, ..., Y_n \backslash \chi_n]$ *for LFP-formulas* $\chi_1, ..., \chi_n$*, then* $\models \exists \overline{Y}\ \psi \to \left(\bigwedge_{j=1}^{n} \chi_j \to \beta_j \right)$.

To prove this, we first need the following lemma:

Lemma 3.8. *Let* $\exists \overline{X} \psi$ *be a formula equation. Then*

$$\models \exists \overline{X} \psi \ \leftrightarrow\ \exists \overline{Y} \psi[X_1 \backslash \neg Y_1, ..., X_n \backslash \neg Y_n].$$

Proof. This follows as for any structure $\mathcal{M}$ and sets $S_1, ..., S_n$ it holds $\mathcal{M}, [X_1 := S_1, ..., X_n := S_n] \models \psi[X_1, ..., X_n]$ iff $\mathcal{M}, [Y_1 := S_1^C, ..., Y_n := S_n^C] \models \psi[X_1 \backslash \neg Y_1, ..., X_n \backslash \neg Y_n]$ □

Proof of Lemma 3.7. 1. Considering $\alpha_j := [\mathrm{lfp}_{X_j}\ \Phi_{\psi^D}]$ for $j \in \{1, ..., n\}$ we first note that $\psi[Y_1 \backslash \beta_1, ..., Y_n \backslash \beta_n]$ is syntactically equivalent to $\psi^D[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$. Hence $\exists \overline{X} \psi^D$ is a Horn formula equation, Lemma 3.3/1 yields $\models \exists \overline{X} \psi^D \leftrightarrow \psi[Y_1 \backslash \beta_1, ..., Y_n \backslash \beta_n]$. Using Lemma 3.8 it follows $\models \exists \overline{Y}\ \psi \leftrightarrow \psi[Y_1 \backslash \beta_1, ..., Y_n \backslash \beta_n]$.
2. Define the formulas $\chi'_j := \neg \chi_j$ for $j \in \{1, ..., n\}$. In doing so we got $\mathcal{M} \models \psi^D[X_1 \backslash \chi'_1, ..., X_n \backslash \chi'_n]$ and Lemma 3.3/2 yields $\mathcal{M} \models \bigwedge_{j=1}^{n} \alpha_j \to \chi'_j$. Using the tautology $A \to B \Leftrightarrow \neg B \to \neg A$ we obtain $\mathcal{M} \models \bigwedge_{j=1}^{n} \chi_j \to \beta_j$.
Again 3. is an immediate consequence of 2. □

Analogously to the Horn formula equations we get the following theorem:

Theorem 3.9 (Dual-Horn fixed-point theorem)**.** *Let* $\exists \overline{Y} \psi$ *be a valid dual-Horn formula equation, i.e.* $\models \exists \overline{Y} \psi$*, and* $\beta_j := \neg[\mathrm{lfp}_{X_j}\ \Phi_{\psi^D}]$ *for* $j \in \{1, ..., n\}$*. Then:*

1. $\models \psi[Y_1 \backslash \beta_1, ..., Y_n \backslash \beta_n]$,

2. *If* $\models \psi[Y_1 \backslash \chi_1, ..., Y_n \backslash \chi_n]$ *for LFP-formulas* $\chi_1, ..., \chi_n$*, then* $\models \bigwedge_{j=1}^{n} \chi_j \to \beta_j$.

3.3 Linear-Horn formula equations

A linear-Horn clause is a clause which is both a Horn and a dual-Horn clause. Thus for linear-Horn formula equations we can apply the results for Horn as well as for dual-Horn formula equations. Considering that they often occur in applications(e.g. Chapter 5) we will state the combinations of the theorems for linear-Horn formula equations.

Definition 3.10. *Let* $\mathcal{L}$ *be a language. A* linear-Horn formula equation *is a formula equation of the form* $\exists \overline{X} \forall \overline{y}\ \bigwedge_{i=1}^{m} H_i$*, where* H_i *is a constrained linear-Horn clause for* $i \in \{1, ..., m\}$.

Theorem 3.11 (Linear-Horn fixed-point theorem)**.** *Let $\exists\overline{X}\psi$ be a valid linear-Horn formula equation, i.e. $\models \exists\overline{X}\psi$. Let $\alpha_j := [\mathrm{lfp}_{X_j}\ \Phi_\psi]$ and $\beta_j := \neg[\mathrm{lfp}_{Y_j}\ \Phi_{\psi^D}]$ for $j \in \{1,...,n\}$. Then:*

1. *$\models \psi[X_1\backslash\alpha_1,...,X_n\backslash\alpha_n]$ and $\models \psi[X_1\backslash\beta_1,...,X_n\backslash\beta_n]$,*
2. *If $\models \psi[X_1\backslash\chi_1,...,X_n\backslash\chi_n]$ for LFP-formulas $\chi_1,...,\chi_n$, then $\models \bigwedge_{j=1}^n \alpha_j \to \chi_j \wedge \chi_j \to \beta_j$.*

Thus if we try to find solutions for linear-Horn formula equations we got an upper bound solution $\overline{\beta}$ and a lower bound solution $\overline{\alpha}$. This will be illustrated in the next example.

Example 3.12. *Let $\mathcal{L} = \{0,1,+,\cdot\}$ be the language of arithmetic. Take a look at the linear-Horn formula equation $\exists X\psi$ with one unary formula variable X, where*

$$\psi \equiv \forall n \bigwedge \begin{cases} X(0) \\ X(n) \to X(n+2) \\ \neg X(7) \end{cases} .$$

The dual formula of ψ is

$$\psi^D \equiv \forall n \bigwedge \begin{cases} Y(7) \\ Y(n+2) \to Y(n) \\ \neg Y(0) \end{cases} .$$

Let us consider the structure $\mathbb{N}$. The formulas $\alpha = [\mathrm{lfp}_X\ \Phi_\psi]$ and $\beta = \neg[\mathrm{lfp}_Y\ \Phi_{\psi^D}]$ define the sets

$$\alpha^{\mathbb{N}} = 2\cdot\mathbb{N}, \quad \beta^{\mathbb{N}} = \mathbb{N}\setminus\{1,3,5,7\}.$$

Thus for every χ s.t. $\mathbb{N} \models \psi[X\backslash\chi]$ we have

$$2\cdot\mathbb{N} \subseteq \chi^{\mathbb{N}} \subseteq \mathbb{N}\setminus\{1,3,5,7\}.$$

3.4 Universal formula equations

The question arises if we can generalize Theorem 3.3 for universal formula equations, where the clauses in general are not Horn nor dual-Horn. The most obvious idea would be to split every clause in Horn-clauses and then compute a fixed point similar as in Chapter 3. We will show that in general this does not work as universal formula equations are substantially more complicated than Horn formula equations.

Definition 3.13. *Let $\mathcal{L}$ be a language. An* universal formula equation *is a formula equation of the form $\exists\overline{X}\forall\overline{y}\ \psi'$, where ψ' is a quantifier-free formula in $\mathcal{L}\cup\{X_1,...,X_n\}$.*

Let $\exists X\psi$ be an universal formula equation. For simplicity we only consider formula equations with one formula variable X, as we will see that already in this case problems occur. Assume $\psi \equiv \forall \bar{y}\ \psi'$, where ψ' is in conjunctive normal form. A clause in ψ' has the form

$$\gamma \wedge X(\overline{t_1}) \wedge \cdots \wedge X(\overline{t_m}) \to X(\overline{s_1}) \vee \cdots \vee X(\overline{s_l}),$$

where γ is a first-order formula and $m, l \geq 0$. Now the idea would be to split every such clause in l Horn-clauses of the form

$$\gamma \wedge X(\overline{t_1}) \wedge \cdots \wedge X(\overline{t_m}) \to X(\overline{s_h}),$$

where $h \in \{1, ..., l\}$. For these Horn-clauses we can construct an operator similarly as to what we did in (3.1). If we do so for every clause in ψ we get operators $F_0, ..., F_k$. One may try to build an inflationary fixed point, where in every step one operator from $\{F_0, ..., F_k\}$ is applied. We will not go into detail how such a fixed point may look like, but demonstrate with an example that in general there is no fixed point which is a solution of $\exists X\psi$.

Example 3.14. *Let $\mathcal{L} = \{0, 1, +, c\}$ be the language of arithmetic with one extra constant symbol c. We are only interested in models $\mathcal{M}$, s.t. the domain is $\mathbb{N}$ and 0,1 and + are interpreted as in the natural numbers. Hence the models only differ in the interpretation of c. Consider the universal formula equation $\exists X\psi$ with one unary formula variable X:*

$$\psi \equiv \forall n \bigwedge \begin{cases} X(0) \\ X(n) \to X(n+1) \vee X(n+2) \\ \neg X(c) \end{cases} .$$

If we split the clauses we get three operators defined as in Definition 2.6: F_0 defined from the formula

$$\varphi_0(X, n) \equiv X(n) \vee n = 0,$$

an operator F_1 defined from the formula

$$\varphi_1(X, n) \equiv X(n) \vee \exists z(X(z) \wedge n = z + 1)$$

and another operator F_2 defined from

$$\varphi_2(X, n) \equiv X(n) \vee \exists z(X(z) \wedge n = z + 2).$$

Now we can build an inflationary sequence of subsets of $\mathbb{N}$, where in every step we apply one of the three operators, for example

$$F_2(F_1(\varnothing)) = \{0, 2\}, \quad F_3(F_1(\varnothing)) = \{0, 3\}.$$

Depending on the interpretation of c it is true that

$$\mathcal{M}, [X := F_2(F_1(\varnothing))] \models \neg X(c).$$

Thus we can not build a fixed point S_F of F_1, F_2, F_3, s.t. $\mathcal{M}, [X := S_F] \models \psi$ for every structure $\mathcal{M}$ s.t. $\mathcal{M} \models \exists X \psi$, as the set S_F has to be different for every structure.

In the last example we have seen that there is no fixed point s.t. a similar result to Theorem 3.3 holds. Still one might think that if we fix one structure $\mathcal{M}$ it is possible to compute a fixed point S_F s.t. $\mathcal{M}, [X := S_F] \models \psi$ if $\mathcal{M} \models \exists X \psi$. That this does not work either will show the next example.

Example 3.15. *Let $\mathcal{L} = \{0, 1, +, \cdot\}$ be the language of arithmetic and $\mathbb{N}$ be the natural numbers. Let $\exists X \psi$ be the universal formula equation with one formula variable X and*

$$\psi \equiv \forall n \bigwedge \begin{cases} X(3 \cdot n) \\ X(n) \to X(n+1) \vee X(n+2) \\ \neg X(1) \\ \neg X(5) \end{cases}.$$

If we split the clauses again we got three operators, F_0 defined from the formula

$$\varphi_0(X, n) \equiv X(n) \vee \exists z (X(z) \wedge n = 3 \cdot z),$$

and the operators F_1 and F_2, which are identical as in the last example. We got $F_0(\varnothing) = 3\mathbb{N}$, which does not satisfy the second clause. Furthermore we have

$$F_1(F_0(\varnothing)) = 3\mathbb{N} \cup (3\mathbb{N} + 1) \quad \textit{and} \quad F_2(F_0(\varnothing)) = 3\mathbb{N} \cup (3\mathbb{N} + 2).$$

They both satisfy the first two clauses of ψ, yet $1 \in F_1(F_0(\varnothing))$ and $5 \in F_2(F_0(\varnothing))$, thus they do not satisfy ψ. All other sequences of F_0, F_1, F_2 applied on $\varnothing$ do not satisfy ψ either. Yet $\mathbb{N} \models \exists X \psi$, as $\mathbb{N}, [X := R] \models \psi$ for

$$R = \{0, 2, 3, 4, 6, 7, 8, 9, ...\}.$$

Thus we see that there are no canonical solutions for universal formula equations as there are for Horn formula equations.

Chapter 4

Fixed-point approximation

The problem of finding first-order formulas, which approximate a second-order formula is an intensively studied topic in the history of logic. For second-order formulas of the form $\exists \overline{X} \forall \overline{y}\ \psi$, where ψ is quantifier-free, it has been investigated by Ackermann in 1935 [1]. Under the assumptions that the language $\mathcal{L}$ is only relational[1] and there is only one unary formula variable X, an infinite conjunction of first-order formulas is computed, that is equivalent to the second-order formula $\exists X \forall \overline{y}\ \psi$. This is achieved with a method similar to modern resolution. That result is extended to any number of formula variables of arbitrary arity in [9], yet the assumption of a relational language remains. We want to show a similar result for any language $\mathcal{L}$, but with another assumption: We only consider Horn formula equations. Moreover, this is attained with a completely different method, as the most important tool will be the Horn fixed-point theorem from the previous chapter.

Let $\exists \overline{X} \psi$ be a Horn formula equation. In the last chapter we found least fixed-point logic formulas $\alpha_1, ..., \alpha_n$ s.t. $\models \exists \overline{X}\ \psi \leftrightarrow \psi[X_1 \backslash \alpha_1, ..., X_n \backslash \alpha_n]$. The question emerges if there are first-order formulas, which approximate $\alpha_1, ..., \alpha_n$ and therefore lead to an approximation of the second-order formula $\exists \overline{X} \psi$. To do so we take a look at the inflationary fixed point. Yet first we have to define infinite conjunctions and disjunctions.

Definition 4.1. *Let $\mathcal{L}$ be a language and $\mathcal{M}$ be an $\mathcal{L}$-structure. Let Ψ be a set of first-order formulas in $\mathcal{L}$. Define*

$$\mathcal{M} \models \bigvee_{\varphi \in \Psi} \varphi \ :\Leftrightarrow\ \exists \varphi \in \Psi :\ \mathcal{M} \models \varphi,$$

$$\mathcal{M} \models \bigwedge_{\varphi \in \Psi} \varphi \ :\Leftrightarrow\ \forall \varphi \in \Psi :\ \mathcal{M} \models \varphi,$$

[1] i.e. $\mathcal{L}$ contains no function symbols.

Lemma 4.2. *Let $\mathcal{L}$ be a language and let Ψ_1, Ψ_2 be sets of first-order formulas in $\mathcal{L}$. Then*

1. $\neg \bigvee_{\varphi \in \Psi_1} \varphi \equiv \bigwedge_{\varphi \in \Psi_1} \neg\varphi$,
2. $\bigvee_{\varphi_1 \in \Psi_1} \varphi_1 \vee \bigvee_{\varphi_2 \in \Psi_2} \varphi_2 \equiv \bigvee_{\varphi \in \Psi_1 \cup \Psi_2} \varphi$,
3. $\bigvee_{\varphi_1 \in \Psi_1} \varphi_1 \wedge \bigvee_{\varphi_2 \in \Psi_2} \varphi_2 \equiv \bigvee_{(\varphi_1,\varphi_2) \in \Psi_1 \times \Psi_2} \varphi_1 \wedge \varphi_2$,

Let $\exists \overline{X} \psi$ be a Horn formula equation and Φ_ψ be the sequence of formulas defined as in (3.1). We know that F_{Φ_ψ} is monotonous and hence $\alpha_j = [\mathrm{lfp}_{X_j}\ \Phi_\psi] = [\mathrm{ifp}_{X_j}\ \Phi_\psi]$ for all $j \in \{1, ..., n\}$. Now we want to express the inflationary fixed point with, possibly infinite, first-order formulas. We will write Φ for Φ_ψ if the context is clear and use the notations from Chapter 3.

Lemma 4.3. *Let $\exists \overline{X} \psi$ be a Horn formula equation. Let $\mathcal{M}$ be a structure and let F_{Φ_ψ} be the operator defined in Definition 2.18 from the sequence of formulas Φ_ψ. Let $(S^\zeta_{F_\Phi})$ be the sequence defined in (2.4). Then $F_\Phi(S^\omega_{F_\Phi}) = S^\omega_{F_\Phi}$.*

Proof. As F_Φ is monotonous Lemma 2.24/5 states, that $F_\Phi(S^\omega) \supseteq S^\omega$. So let $(\overline{a_1}, ..., \overline{a_n}) \in F_\Phi(S^\omega)$. Then for every $j \in \{1, ..., n\}$ there are two possibilities:

- There exists $\overline{y_0}$ and $(\gamma, \bar{s}) \in B_j$ s.t. $\mathcal{M}, [\overline{y} := \overline{y_0}] \models \gamma \wedge \overline{a_j} = \bar{s}$. In this case define $\zeta_j := 0$.
- There exists $\overline{y_0}$, $(\gamma, \iota, \tau, \bar{s}) \in I_j$ and $\zeta_j \in \omega$ s.t. $\mathcal{M}, [\overline{y} := \overline{y_0}] \models \gamma \wedge \bigwedge_{k=1}^m (S^{\zeta_j})_{i_k}(\overline{t_k}) \wedge \overline{a_j} = \bar{s}$.

For $\zeta_{\max} := \max\{\zeta_1, ..., \zeta_n\}$ we claim that $(\overline{a_1}, ..., \overline{a_n}) \in F_\Phi(S^{\zeta_{\max}})$. As the sequence S^ζ is increasing we have $S^{\zeta_j} \subseteq S^{\zeta_{\max}}$, hence the same statement as for S^ω hold for $S^{\zeta_{\max}}$ for every $j \in \{1, ..., n\}$. Thus $(\overline{a_1}, ..., \overline{a_n}) \in F_\Phi(S^{\zeta_{\max}}) \subseteq S^\omega$. □

Let $\exists \overline{X} \psi$ be a Horn formula equation. Let B_j and I_j be the sets of base clauses and induction clauses, respectively, where the positive formula variable is X_j for $j \in \{1, ..., n\}$. For $j \in \{1, ..., n\}$ define the following sequence of first-order formulas, where $|\overline{x_j}|$ equals the arity of X_j:

$$\varphi_j^0(\overline{x_j}) \equiv \bot$$

$$\varphi_j^{l+1}(\overline{x_j}) \equiv \exists \overline{y} \left(\bigvee_{(\gamma,\bar{s}) \in B_j} (\gamma \wedge \overline{x_j} = \bar{s}) \vee \bigvee_{(\gamma,\iota,\tau,\bar{s}) \in I_j} \left(\gamma \wedge \bigwedge_{k=1}^m \varphi_{i_k}^l(\overline{t_k}) \wedge \overline{x_j} = \bar{s} \right) \right). \quad (4.1)$$

At last define

$$\varphi_j^\omega(\overline{x_j}) \equiv \bigvee_{l \in \omega} \varphi_j^l(\overline{x_j}).$$

Lemma 4.4. *Let $\exists\overline{X}\psi$ be a Horn formula equation and $\mathcal{M}$ be a structure. Let $(S^{\zeta}_{F_\Phi})$ be the sequence defined in (2.4) from the operator F_{Φ_ψ}. For every $j \in \{1,...,n\}$ and $\bar{a} \in M^{k_j}$, where k_j equals the arity of X_j, it holds*

$$\mathcal{M} \models \varphi^l_j(\bar{a}) \quad \Leftrightarrow \quad \bar{a} \in (S^l_{F_\Phi})_j,$$

for every $l \in \omega \cup \{\omega\}$.

Proof. The proof goes by induction on l: For $l = 0$ we have $\mathcal{M} \models \bot$ iff $\bar{a} \in \varnothing$, which is valid. For $l+1$ we got

$$\begin{aligned}
\mathcal{M} \models \varphi^{l+1}_j(\bar{a}) &\Leftrightarrow \mathcal{M} \models \exists\bar{y}\left(\bigvee_{(\gamma,\bar{s})\in B_j}(\gamma \wedge \bar{a} = \bar{s}) \vee \bigvee_{(\gamma,\iota,\tau,\bar{s})\in I_j}\left(\gamma \wedge \bigwedge_{k=1}^{m}\varphi^l_{i_k}(\overline{t_k}) \wedge \bar{a} = \bar{s}\right)\right)\\
&\Leftrightarrow \mathcal{M} \models \exists\bar{y}\left(\bigvee_{(\gamma,\bar{s})\in B_j}(\gamma \wedge \bar{a} = \bar{s}) \vee \bigvee_{(\gamma,\iota,\tau,\bar{s})\in I_j}\left(\gamma \wedge \bigwedge_{k=1}^{m}(S^l)_{i_k}(\overline{t_k}) \wedge \bar{a} = \bar{s}\right)\right)\\
&\Leftrightarrow \bar{a} \in F_\Phi(S^l)_j\\
&\Leftrightarrow \bar{a} \in (S^{l+1})_j.
\end{aligned}$$

The last equivalence holds because of Lemma 2.24/5.
The statement for ω holds as

$$\mathcal{M} \models \varphi^\omega_j(\bar{a}) \;\Leftrightarrow\; \mathcal{M} \models \bigvee_{l\in\omega}\varphi^l_j(\bar{a}) \;\Leftrightarrow\; \bar{a} \in \bigcup_{l\in\omega}(S^l)_j \;\Leftrightarrow\; \bar{a} \in (S^\omega_{F_\Phi})_j.$$

□

Theorem 4.5. *Let $\exists\overline{X}\psi$ be a Horn formula equation and $\alpha_j := [\mathrm{lfp}_{X_j}\,\Phi_\psi]$ for $j \in \{1,...,n\}$. Then $\alpha_j \equiv \varphi^\omega_j$ for all $j \in \{1,...,n\}$.*

Proof. As F_{Φ_ψ} is monotonous we know from Lemma 2.24/4, that $\alpha_j = [\mathrm{lfp}_{X_j}\,\Phi_\psi] = [\mathrm{ifp}_{X_j}\,\Phi_\psi]$ for $j \in \{1,...,n\}$. Lemma 4.3 states that for every structure $\mathcal{M}$ the closure ordinal ξ of F_Φ fulfils $\xi \leq \omega$. With Lemma 2.24/3 we got for every structure $\mathcal{M}$, that $S^\omega_{F_\Phi} = S^\xi_{F_\Phi}$ and hence for every $\bar{a} \in M^{k_j}$, where k_j equals the arity of X_j, we have $\mathcal{M} \models [\mathrm{ifp}_{X_j}\,\Phi_\psi](\bar{a})$ iff $\bar{a} \in (S^\omega_{F_\Phi})_j$. Now Lemma 4.4 concludes the proof. □

Theorem 4.6. *Let $\exists\overline{X}\psi$ be a Horn formula equation. Then there exists a, possibly infinite, set of first-order formulas Ψ s.t.*

$$\exists\overline{X}\psi \equiv \forall\bar{y}\bigwedge_{\varphi\in\Psi}\varphi.$$

Proof. Applying Lemma 3.3/1 and Theorem 4.5 we have

$$\exists \overline{X} \psi \equiv \psi[X_1 \backslash \varphi_1^\omega, ..., X_n \backslash \varphi_n^\omega].$$

As in every structure $(\varphi_1^\omega, ..., \varphi_n^\omega)$ is a fixed point of F_{Φ_ψ}, the formulas $\varphi_1^\omega, ..., \varphi_n^\omega$ satisfy all the clauses of the form (B) and (I) in ψ. Hence it suffices to check clauses of the form (E), i.e. of the form $\neg\gamma \vee \neg X_{i_1}(\overline{t_1}) \vee \cdots \vee \neg X_{i_m}(\overline{t_m})$. Let E be the set of clauses of the form (E) in ψ. We denote a clause in E by the determining tuple (γ, ι, τ), where $\iota := \{i_1, ..., i_m\}$ and $\tau := \{\overline{t_1}, ..., \overline{t_m}\}$. Then

$$\psi[X_1 \backslash \varphi_1^\omega, ..., X_n \backslash \varphi_n^\omega] \equiv \forall \bar{y} \bigwedge_{(\gamma,\iota,\tau) \in E} \left(\neg\gamma \vee \neg\varphi_{i_1}^\omega(\overline{t_1}) \vee \cdots \vee \neg\varphi_{i_m}^\omega(\overline{t_m}) \right).$$

Per definition there is a set of first-order formulas Ψ_j s.t. $\varphi_j^\omega \equiv \bigvee_{\varphi \in \Psi_j} \varphi$ for every $j \in \{1, ..., n\}$. Thus with repeated application of Lemma 4.2 there exists a set of first-order formulas Ψ s.t.

$$\forall \bar{y} \bigwedge_{(\gamma,\iota,\tau) \in E} \left(\neg\gamma \vee \neg(\bigvee_{\varphi \in \Psi_{i_1}} \varphi(\overline{t_1})) \vee \cdots \vee \neg(\bigvee_{\varphi \in \Psi_{i_m}} \varphi(\overline{t_m})) \right) \equiv \forall \bar{y} \bigwedge_{\varphi \in \Psi} \varphi.$$

□

Note that the set Ψ in Theorem 4.6 is given constructively, hence we constructed first-order formulas, which approximate the second-order formula $\exists \overline{X} \psi$.

Chapter 5

Partial Correctness of while-programs

In this chapter we take a look at while-programs, which is a well studied topic in computer science. We are only interested in partial correctness, which means that we only consider runs of programs that terminate, this is justified as usually it is much easier to check termination than correctness of a program. First we will state some basic definitions and results from computer science. Then we will take a different approach, where we define the verification condition of a program, which turns out to be equivalent to the classical semantics of partial correctness. The verification condition is a linear-Horn formula equation, hence we can apply our results form Chapter 3.

Definition 5.1. *In this chapter we work in the language of arithmetic* $\mathcal{L} = \{0, 1, +, -, \cdot, \leq\}$*, where* "0" *and* "1" *are constant symbols,* "$+$", "$-$" *and* "$\cdot$" *are binary function symbols and* "$\leq$" *is a binary relation symbol. We mainly consider the standard model* $\mathbb{Z}$ *of* $\mathcal{L}$*, the integers. We define* Z *to be the domain of* $\mathbb{Z}$*.*

Definition 5.2. *A* program[1] p *is a string of symbols. The set of programs, written in Backus-Naur*[2] *form, is*

$$p ::= \textbf{\textit{skip}} \mid x_j := t \mid p_0; p_1 \mid \textbf{\textit{if}}\ B\ \textbf{\textit{then}}\ p_0\ \textbf{\textit{else}}\ p_1 \mid \textbf{\textit{while}}\ B\ \textbf{\textit{do}}\ p_0,$$

where t *is an* $\mathcal{L}$*-term,* B *a quantifier-free first-order formula in* $\mathcal{L}$ *and* x_j *a variable.*

Definition 5.3. *Define* $\mathrm{Var} = \{x_0, x_1, ...\}$ *to be the set of variables which may occur in a program. A function* $\sigma : \mathrm{Var} \to Z$ *is called a* state[3]*. We denote the set of all states with* Σ*. We write* $\sigma[x_j \to n]$ *for the unique state* σ' *s.t.* $\sigma'(x_j) = n$ *and* $\sigma'(x_i) = \sigma(x_i)$ *for* $i \neq j$*.*

[1] This is usually called while-program. As we do not talk about other types of programs, we abbreviate it to program.

[2] i.e. p is defined recursively, where one program consists of one of the six options divided by |. Here p_0 and p_1 are programs themselves.

[3] Later we will talk of formulas, in which the variables of a program occur. In this sense a state may also be seen as an environment.

Definition 5.4 (Denotational semantics)**.** *For every program p we define a relation $C(p)$ on $\Sigma \times \Sigma$ by structural induction.*

$$C(\textbf{\textit{skip}}) = \{(\sigma, \sigma) \mid \sigma \in \Sigma\}$$

$$C(x_j := t) = \{(\sigma, \sigma[x_j \to n]) \mid \sigma \in \Sigma,\ n \in Z \text{ and } \mathbb{Z}, \sigma \models t = n\}$$

$$C(p_0; p_1) = C(p_1) \circ C(p_0)$$

$$\begin{aligned} C(\textbf{\textit{if}}\ B\ \textbf{\textit{then}}\ p_0\ \textbf{\textit{else}}\ p_1) = {} & \{(\sigma, \sigma') \mid \mathbb{Z}, \sigma \models B \text{ and } (\sigma, \sigma') \in C(p_0)\} \cup \\ & \{(\sigma, \sigma') \mid \mathbb{Z}, \sigma \models \neg B \text{ and } (\sigma, \sigma') \in C(p_1)\} \end{aligned}$$

$$C(\textbf{\textit{while}}\ B\ \textbf{\textit{do}}\ p_0) = \mathrm{lfp}(\Gamma),$$

where Γ is an operator on $\Sigma \times \Sigma$ defined as

$$\begin{aligned} \Gamma(X) = {} & \{(\sigma, \sigma') \mid \mathbb{Z}, \sigma \models B \text{ and } (\sigma, \sigma') \in C(p_0) \circ X\} \cup \\ & \{(\sigma, \sigma) \mid \mathbb{Z}, \sigma \models \neg B\}. \end{aligned}$$

We see that Γ is a monotonous operator and thus $\mathrm{lfp}(\Gamma)$ is well-defined. Then we can convince ourselves that $C(p)$ is actually a partial function from $\Sigma \to \Sigma$. If $C(p)(\sigma)$ is not defined, this means that a while-loop is not terminating. To make it a total function, we extend the set of states Σ with the state $\perp$, which is associated with a non-terminating computation, i.e. we define $\Sigma_\perp := \Sigma \cup \{\perp\}$. For every σ s.t. $C(p)(\sigma)$ is not defined yet, we define $C(p)(\sigma) := \perp$ and in that way $C(p)$ is a total function from $\Sigma \to \Sigma_\perp$.

Definition 5.5. *A Hoare triple is a triple (φ, p, ψ) consisting of a program p and two first-order formulas φ and ψ. This is traditionally denoted as $\{\varphi\}p\{\psi\}$.*

Now we define the meaning of partial correctness of a Hoare triple:

Definition 5.6 (Semantics of Hoare triples)**.** *Let σ be a state. For a Hoare triple define*

$$\sigma \models \{\varphi\}p\{\psi\} \quad :\Leftrightarrow \quad (\mathbb{Z}, \sigma \models \varphi \ \Rightarrow\ \mathbb{Z}, C(p)(\sigma) \models \psi)\,.$$

Here $\mathbb{Z}, \perp \models \psi$ is defined to be true. In doing so we only check validity for states, in which the computation terminates. Now define

$$\models \{\varphi\}p\{\psi\} \quad :\Leftrightarrow \quad \forall \sigma \in \Sigma\ (\sigma \models \{\varphi\}p\{\psi\})\,.$$

Definition 5.7 (Hoare rules)**.** *In order to get a proof calculus for Hoare triples let us define the following rules, called Hoare rules. We write* $\vdash \{\varphi\}p\{\psi\}$ *if* $\{\varphi\}p\{\psi\}$ *is provable by the Hoare rules. Here* $\varphi, \psi, \chi, B, I$ *are first-order formulas in* $\mathcal{L}$*,* p, p_0, p_1 *are programs,* t *is an* $\mathcal{L}$*-term and* x_j *is a variable.*

$$\frac{}{\{\varphi\}\textbf{\textit{skip}}\{\varphi\}} \text{ (skip)}$$

$$\frac{}{\{\varphi[x_j \backslash t]\}x_j := t\{\varphi\}} \text{ (assign)}$$

$$\frac{\{\varphi\}p_0\{\chi\} \quad \{\chi\}p_1\{\psi\}}{\{\varphi\}p_0; p_1\{\psi\}} \text{ (sequence)}$$

$$\frac{\{\varphi \wedge B\}p_0\{\psi\} \quad \{\varphi \wedge \neg B\}p_1\{\psi\}}{\{\varphi\}\textbf{\textit{if}}\ B\ \textbf{\textit{then}}\ p_0\ \textbf{\textit{else}}\ p_1\{\psi\}} \text{ (conditional)}$$

$$\frac{\mathbb{Z} \models \varphi \to I \quad \{I \wedge B\}p\{I\} \quad \mathbb{Z} \models I \wedge \neg B \to \psi}{\{\varphi\}\textbf{\textit{while}}\ B\ \textbf{\textit{do}}\ p\{\psi\}} \text{ (while)}$$

$$\frac{\mathbb{Z} \models \varphi \to \varphi' \quad \{\varphi'\}p\{\psi'\} \quad \mathbb{Z} \models \psi' \to \psi}{\{\varphi\}p\{\psi\}} \text{ (consequence)}$$

In most of the literature the (while)-rule is replaced with

$$\frac{\{\varphi \wedge B\}p\{\varphi\}}{\{\varphi\}\textbf{while}\ B\ \textbf{do}\ p\{\varphi \wedge \neg B\}} \textit{ (while')}$$

This leads to an equivalent proof calculus as (while') is a special case of (while) for $I = \varphi$ and $\psi = \varphi \wedge \neg B$. In the other direction (while) can be obtained by combining the (while') and (consequence) rule. Yet for our usage the first definition suits better.

Theorem 5.8. *The Hoare rules are a sound and relatively complete proof system for Hoare triples, i.e.*

$$\vdash \{\varphi\}p\{\psi\} \quad \Leftrightarrow \quad \models \{\varphi\}p\{\psi\}.$$

Proof. Soundness can be proven by a structural induction on the Hoare rules. Proving relatively completeness is more complicated and relies on the fact that it is possible to encode finite sequences of arbitrary length in $\mathbb{Z}$. A proof can be found in [11]. □

Note that there can not be a complete proof system for $\models \{\varphi\}p\{\psi\}$, as this would yield a complete proof system for validity in $\mathbb{Z}$, which is impossible due to Gödel's incompleteness theorem. Hence we will always talk about relative completeness.

5.1 Verification condition

Now we will define a Horn formula equation from a Hoare triple, called the verification condition[4]. It turns out that a Hoare triple is valid iff its verification condition holds in $\mathbb{Z}$.

Definition 5.9. *The* verification condition *of a Hoare triple* $\{\varphi\}p\{\psi\}$*, written* $\mathrm{vc}(\{\varphi\}p\{\psi\})$*, is a formula equation* $\exists \bar{I} \forall \bar{x}\ \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$*, where* $\widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ *is defined by structural induction on* p*. Here* I *is a fresh new formula variable, which does not appear in* φ *and* ψ*.*

$$\begin{aligned}
\widetilde{\mathrm{vc}}(\{\varphi\}\textbf{\textit{skip}}\{\psi\}) &= (\varphi \to \psi)\\
\widetilde{\mathrm{vc}}(\{\varphi\}x_j := t\{\psi\}) &= (\varphi \to \psi[x_j \backslash t])\\
\widetilde{\mathrm{vc}}(\{\varphi\}p_0; p_1\{\psi\}) &= \widetilde{\mathrm{vc}}(\{\varphi\}p_0\{I\}) \wedge \widetilde{\mathrm{vc}}(\{I\}p_1\{\psi\}),\\
\widetilde{\mathrm{vc}}(\{\varphi\}\textbf{\textit{if}}\ B\ \textbf{\textit{then}}\ p_0\ \textbf{\textit{else}}\ p_1\{\psi\}) &= \widetilde{\mathrm{vc}}(\{\varphi \wedge B\}p_0\{\psi\}) \wedge \widetilde{\mathrm{vc}}(\{\varphi \wedge \neg B\}p_1\{\psi\})\\
\widetilde{\mathrm{vc}}(\{\varphi\}\textbf{\textit{while}}\ B\ \textbf{\textit{do}}\ p_0\{\psi\}) &= \widetilde{\mathrm{vc}}(\{I \wedge B\}p_0\{I\}) \wedge (\varphi \to I) \wedge (I \wedge \neg B \to \psi)
\end{aligned}$$

Then $\mathrm{vc}(\{\varphi\}p\{\psi\}) = \exists \bar{I} \forall \bar{x}\ \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ *is defined by universal quantification of every variable occurring in* $\widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ *and existential quantification of every formula variable in* $\widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$*.*

Note that this is an purely syntactic definition, thus we can define $\mathrm{vc}(\{\varphi\}p\{\psi\})$ analogously for a program p and second-order formulas φ, ψ. This will be needed for Lemma 5.13.

Lemma 5.10. *Let* $\{\varphi\}p\{\psi\}$ *be Hoare triple. Then* $\mathrm{vc}(\{\varphi\}p\{\psi\})$ *is a linear-Horn formula equation.*

Proof. $\mathrm{vc}(\{\varphi\}p\{\psi\})$ is a formula equation $\exists \bar{I} \forall \bar{x}\ \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$, where $\widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ is a conjunction of clauses. Each clause has the form $\gamma \vee \neg C \vee D$, where γ is a first-order formula (it is a disjunction of the first-order formulas B or $\neg B$) and C and D are either formula variables or the first-order formulas φ or ψ. □

Lemma 5.11. *Let* $\{\varphi\}p\{\chi\}$ *be a Hoare triple.* φ *occurs only negatively and* ψ *occurs only positively in* $\mathrm{vc}(\{\varphi\}p\{\chi\})$*, respectively.*

Proof. The proof goes by structural induction on $\widetilde{\mathrm{vc}}(\{\varphi\}p\{\chi\})$. It holds as in every step of the construction φ only appears on the left side of an implication, which is a negative occurrence. Conversely ψ only appears on the right side of an implication, which is a positive occurrence. The claim now follows as there are no other negations added, which are in the scope of φ or ψ. □

[4] In the literature mostly the term verification conditions is used for the set of conditions. As we talk about the conjunction of that conditions we will use singular.

Definition 5.12. *For every formula φ in $\mathcal{L}$ define a subset of Σ:*

$$[\varphi] := \{\sigma \in \Sigma \mid \mathbb{Z}, \sigma \models \varphi\}.$$

The next aim will be to show $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\}) \Rightarrow \models \{\varphi\}p\{\psi\}$. If we try to prove this directly with induction on p there arise problems, as in the definition of the verification condition we have expressions of the form $\mathrm{vc}(\{I\}p\{\psi\})$, where I is a formula variable. As $\models \{\varphi\}p\{\psi\}$ is only defined for first-order formulas φ and ψ, we have to prove a more general lemma, where we speak about sets of states instead of formulas.
First we introduce some notations. Let $x_1, ..., x_n$ be the variables occurring in p. Let $S \subseteq \Sigma$ be a set of states. Every such S defines a set $S^Z \subseteq Z^n$ and vice versa as follows

$$(k_1, ..., k_n) \in S^Z \quad \Leftrightarrow \quad \sigma_{\overline{k}} \in S,$$

where $\sigma_{\overline{k}}(x_j) = k_j$ for all $j \in \{1, ..., n\}$.

Lemma 5.13. *Let S_1, S_2 be subsets of Σ. If $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \mathrm{vc}(\{X_1\}p\{X_2\})$, then*

$$\sigma \in S_1 \;\Rightarrow\; C(p)(\sigma) \in S_2 \cup \{\bot\}.$$

Proof. We prove the Lemma by structural induction on p:

- $p \equiv$ **skip**: We have $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \forall \overline{x}(X_1 \to X_2)$, which means, that for all $\sigma \in S_1$ it follows that $C(p)(\sigma) = \sigma \in S_2$.

- $p \equiv x_j := t$: We have $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \forall \overline{x}(X_1 \to X_2[x_j \backslash t])$. Let $\sigma \in S_1$, then there exists an unique $n \in Z$ s.t. $\mathbb{Z}, \sigma \models t = n$. Thus $C(p)(\sigma) = \sigma[x_j \to n] \in S_2$.

- $p \equiv p_0; p_1$: The assumption is $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \exists I \ \mathrm{vc}(\{X_1\}p_0\{I\}) \wedge \mathrm{vc}(\{I\}p_1\{X_2\})$. Let S^Z be a set s.t. $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z, I := S^Z] \models \mathrm{vc}(\{X_1\}p_0\{I\}) \wedge \mathrm{vc}(\{I\}p_1\{X_2\})$. Using the induction hypothesis we get

  $$\begin{aligned} \sigma \in S_1 \quad &\Rightarrow \quad C(p_0)(\sigma) \in S \cup \{\bot\} \quad \text{and} \\ \sigma \in S \quad &\Rightarrow \quad C(p_1)(\sigma) \in S_2 \cup \{\bot\}. \end{aligned}$$

  Combining these statements we obtain

  $$\sigma \in S_1 \quad \Rightarrow \quad C(p)(\sigma) = C(p_1) \circ C(p_0) \in S_2 \cup \{\bot\}.$$

- $p \equiv$ **if** B **then** p_0 **else** p_1: Let $S_1, S_2 \subseteq \Sigma$ s.t. $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \mathrm{vc}(\{X_1 \wedge B\}p_0\{X_2\}) \wedge \mathrm{vc}(\{X_1 \wedge \neg B\}p_1\{X_2\})$. Let $\sigma \in S_1$. If $\mathbb{Z}, \sigma \models B$ the induction hypothesis states $C(p_0)(\sigma) \in S_2$, else $\mathbb{Z}, \sigma \models \neg B$ and we have $C(p_1)(\sigma) \in S_2$. Combining these yields the claim.

- $p \equiv$ **while** B **do** p_0: We have $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \exists I \text{ vc}(\{I \wedge B\}p_0\{I\}) \wedge \forall \bar{x}(X_1 \to I) \wedge \forall \bar{x}(I \wedge \neg B \to X_2)$, hence let $S^Z \subseteq Z^n$ be s.t.

$$\begin{aligned}\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z, I := S^Z] \models \\ \text{vc}(\{I \wedge B\}p_0\{I\}) \wedge \forall \bar{x}(X_1 \to I) \wedge \forall \bar{x}(I \wedge \neg B \to X_2). \end{aligned} \tag{5.1}$$

The semantics of p is defined as $C(p) = \text{lfp}(\Gamma)$, where Γ is the monotonous operator

$$\begin{aligned}\Gamma(X) = &\{(\sigma, \sigma') \mid \mathbb{Z}, \sigma \models B \wedge (\sigma, \sigma') \in C(p_0) \circ X\} \cup \\ &\{(\sigma, \sigma) \mid \mathbb{Z}, \sigma \models \neg B\}.\end{aligned}$$

As Γ is monotonous we know from Theorem 2.12 that $\text{lfp}(\Gamma) = \text{ifp}(\Gamma) = S_\Gamma^\xi$, where ξ is the closure ordinal of Γ. To prove the Lemma we first prove the following statement with induction on m:

Let S_1, S_2, S be s.t. (5.1) is satisfied. For every $m \in \mathbb{N}$ it holds

$$\sigma \in S_1 \text{ and } (\sigma, \sigma') \in S_\Gamma^m \Rightarrow \sigma' \in S. \tag{5.2}$$

$\underline{m = 1}$: $(\sigma, \sigma') \in S_\Gamma^1$ iff $\sigma = \sigma' \wedge \mathbb{Z}, \sigma \models \neg B$. From (5.1) we obtain $\mathbb{Z}, [X_1 := S_1^Z, I := S^Z] \models \forall \bar{x}(X_1 \to I)$, hence $\sigma \in S_1 \Rightarrow \sigma \in S$.

$\underline{m \to m+1}$: $(\sigma, \sigma') \in S_\Gamma^{m+1}$ iff $\sigma = \sigma' \wedge \mathbb{Z}, \sigma \models \neg B$, which we already checked, or

$$\mathbb{Z}, \sigma \models B \wedge \exists \sigma'' : (\sigma, \sigma'') \in S_\Gamma^m \wedge (\sigma'', \sigma') \in C(p_0).$$

Let $\sigma \in S_1$, by induction hypothesis we got $\sigma'' \in S$. (5.1) yields $\mathbb{Z}, [I := S^Z] \models \text{vc}(\{I \wedge B\}p_0\{I\})$ and, as $\mathbb{Z}, \sigma \models B$, we obtain by induction hypothesis of the structural induction $\sigma' = C(p_0)(\sigma'') \in S$.

Now let $\sigma \in S_1$. If there exists $m \in \mathbb{N}$ s.t. $S_\Gamma^m(\sigma)$ is defined and $\Gamma(S_\Gamma^m)(\sigma) = S_\Gamma^m(\sigma)$, then we have $C(p)(\sigma) = \text{lfp}(\Gamma)(\sigma) = S_\Gamma^m(\sigma)$. From (5.2) we obtain that $S_\Gamma^m(\sigma) \in S$. From (5.1) we get $\mathbb{Z}, [X_2 := S_2^Z, I := S^Z] \models \forall \bar{x}(I \wedge \neg B \to X_2)$. As $\Gamma(S_\Gamma^m)(\sigma) = S_\Gamma^m(\sigma)$ it holds that $Z, S_\Gamma^m(\sigma) \models \neg B$ and thus this yields $S_\Gamma^m(\sigma) \in S_2$.
If there is no $m \in \mathbb{N}$ s.t. $S_\Gamma^m(\sigma)$ is defined and $\Gamma(S_\Gamma^m)(\sigma) = S_\Gamma^m(\sigma)$, then $C(p)(\sigma)$ is not defined as well. Hence $C(p)(\sigma) = \perp$ and the proof is finished.

□

Theorem 5.14. *Let $\{\varphi\}p\{\psi\}$ be a Hoare triple. Then*

$$\models \{\varphi\}p\{\psi\} \quad \Leftrightarrow \quad \mathbb{Z} \models \text{vc}(\{\varphi\}p\{\psi\}).$$

Proof. " $\Rightarrow$ ": As the Hoare rules are a relatively complete proof system we may assume $\vdash \{\varphi\}p\{\psi\}$. What we want to prove is that $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$. We accomplish that if we show that every rule yields Hoare triples, whose verification condition is true in $\mathbb{Z}$. In other words, we show that the Hoare rules are sound with respect to the semantics $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$.

- (skip): $\varphi \to \varphi$ is a tautology, thus $\mathbb{Z} \models \forall\bar{x}(\varphi \to \varphi)$
- (assign): By definition $\mathrm{vc}(\{\varphi[x_j\backslash t]\}x_j := t\{\varphi\}) = \forall\bar{x}(\varphi[x_j\backslash t] \to \varphi[x_j\backslash t])$, which $\mathbb{Z}$ always fulfils.
- (sequence): The induction hypothesis states, that $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p_0\{\chi\}) \wedge \mathrm{vc}(\{\chi\}p_1\{\psi\})$. Therefore $\mathbb{Z} \models \exists I\ \mathrm{vc}(\{\varphi\}p_0\{I\}) \wedge \mathrm{vc}(\{I\}p_1\{\psi\})$, which is, by definition and shifting of quantifiers, equivalent to $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p_0; p_1\{\psi\})$.
  Here it is crucial that the formula variables occurring in $\mathrm{vc}(\{\varphi\}p_0\{I\})$ are different to the formula variables in $\mathrm{vc}(\{I\}p_1\{\psi\})$[5]. This is achieved by renaming and thus may be assumed to be always the case. Similar assumptions will also be made in the other cases.
- (conditional): The claim is $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}\textbf{if } B \textbf{ then } p_0 \textbf{ else } p_1\{\psi\})$. By induction hypothesis we have $\mathbb{Z} \models \mathrm{vc}(\{\varphi \wedge B\}p_0\{\psi\}) \wedge \mathrm{vc}(\{\varphi \wedge \neg B\}p_1\{\psi\})$, which is, by definition and shifting of quantifiers, equivalent to the claim.
- (while): Assume that $\mathbb{Z} \models (\varphi \to I) \wedge \mathrm{vc}(\{I \wedge B\}p\{I\}) \wedge (I \wedge \neg B \to \psi)$. In particular $\mathbb{Z} \models \exists I\ (\varphi \to I) \wedge \mathrm{vc}(\{I \wedge B\}p\{I\}) \wedge (I \wedge \neg B \to \psi)$, which is, modulo shifting of quantifiers, the definition of $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}\textbf{while } B \textbf{ do } p_0\{\psi\})$.
- (consequence): By induction hypothesis we have $\mathbb{Z} \models (\varphi \to \varphi')$, $\mathbb{Z} \models (\psi' \to \psi)$ and $\mathbb{Z} \models \mathrm{vc}(\{\varphi'\}p\{\psi'\})$. From Lemma 5.11 we know that φ' occurs only negatively and ψ' occurs only positively in $\mathrm{vc}(\{\varphi'\}p\{\psi'\})$, hence with Lemma 2.1 it follows $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$.

" $\Leftarrow$ ": Let $\{\varphi\}p\{\psi\}$ be a Hoare triple s.t. $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$. Define $S_1 := [\varphi]$ and $S_2 := [\psi]$. Then $\mathbb{Z}, [X_1 := S_1^Z, X_2 := S_2^Z] \models \mathrm{vc}(\{X_1\}p\{X_2\})$ and Lemma 5.13 yields

$$\sigma \in [\varphi] \ \Rightarrow\ C(p)(\sigma) \in [\psi] \cup \{\bot\}.$$

As $\mathbb{Z}, \bot \models \psi$ for every formula ψ, this implies

$$\mathbb{Z}, \sigma \models \varphi \quad \Rightarrow \quad \mathbb{Z}, C(p)(\sigma) \models \psi,$$

which is the definition of $\models \{\varphi\}p\{\psi\}$.

□

[5] except the newly introduced formula variable I.

As $\mathrm{vc}(\{\varphi\}p\{\psi\})$ is a linear-Horn formula we can state an immediate corollary from Lemma 3.3 and Lemma 3.7. Here π^D is the dual formula of π with formula variables $K_1, ..., K_n$.

Corollary 5.15. *Let $\{\varphi\}p\{\psi\}$ be a Hoare triple. Consider the linear-Horn formula equation $\exists \bar{I}\ \pi \equiv \mathrm{vc}(\{\varphi\}p\{\psi\})$ with formula variables $I_1, ..., I_n$ and assume $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$. Define $\alpha_j := [\mathrm{lfp}_{I_j}\ \Phi_\pi]$ and $\beta_j := \neg[\mathrm{lfp}_{K_j}\ \Phi_{\pi^D}]$ for $j \in \{1, ..., n\}$. Then*

1. *$\mathbb{Z}, [I_1 := \alpha_1, ..., I_n := \alpha_n] \models \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ and $\mathbb{Z}, [I_1 := \beta_1, ..., I_n := \beta_n] \models \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$.*
2. *If $\mathbb{Z}, [I_1 := \chi_1, ..., I_n := \chi_n] \models \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$ for relations $\chi_1, ..., \chi_n$, then $\mathbb{Z} \models \bigwedge_{j=1}^n \alpha_j \to \chi_j \wedge \chi_j \to \beta_j$.*

In computer science it is a common problem to find first-order formulas $\chi_1, ..., \chi_n$ s.t. $\mathbb{Z}, [I_1 := \chi_1, ..., I_n := \chi_n] \models \widetilde{\mathrm{vc}}(\{\varphi\}p\{\psi\})$. Corollary 5.15 reduces this to an interpolation problem: Finding first-order formulas $\chi_1, ..., \chi_n$ s.t. $\mathbb{Z} \models \bigwedge_{j=1}^n \alpha_j \to \chi_j \wedge \chi_j \to \beta_j$.

5.2 Weakest precondition/Strongest postcondition

In the last section we have defined the verification condition. As this is a linear-Horn formula equation we can now apply our results from Chapter 3. We will see that the canonical solutions from the verification condition correspond to the weakest precondition and strongest postcondition.

Definition 5.16. *Let p be a program and φ, ψ be first-order formulas in $\mathcal{L}$. The* weakest precondition[6] *of p and ψ, written $\mathrm{wp}(p, \psi)$, is defined as*

$$\mathrm{wp}(p, \psi) = \{\sigma \in \Sigma \mid \mathbb{Z}, C(p)(\sigma) \models \psi\}.$$

The strongest postcondition *of p and φ, written $\mathrm{sp}(p, \varphi)$, is defined as*

$$\mathrm{sp}(p, \varphi) = \{\sigma \in \Sigma \mid \exists \sigma' \in \Sigma : \mathbb{Z}, \sigma' \models \varphi \text{ and } C(p)(\sigma') = \sigma\}.$$

Lemma 5.17. *Let $\{\varphi\}p\{\psi\}$ be a Hoare triple. Then*

1. *$\models \{\varphi\}p\{\psi\}$ iff $[\varphi] \subseteq \mathrm{wp}(p, \psi)$,*
2. *$\models \{\varphi\}p\{\psi\}$ iff $[\psi] \supseteq \mathrm{sp}(p, \varphi)$.*

[6] In the literature this is mostly called weakest liberal precondition and the term weakest precondition is reserved for the context of total correctness. As we only talk about relative correctness of programs there is no need for us to do so.

Proof. 1. Let $\sigma \in [\varphi]$, thus $\mathbb{Z}, \sigma \models \varphi$. As $\sigma \models \{\varphi\}p\{\psi\}$, we got $\mathbb{Z}, C(p)(\sigma) \models \psi$, hence $\sigma \in \mathrm{wp}(p, \psi)$.
If $[\varphi] \subseteq \mathrm{wp}(p, \psi)$ it holds for all $\sigma \in \Sigma$, that $\mathbb{Z}, \sigma \models \varphi$ implies $\mathbb{Z}, C(p)(\sigma) \models \psi$, which is the definition of $\models \{\varphi\}p\{\psi\}$.
2. Assume $\sigma \in \mathrm{sp}(p, \varphi)$, that means that there exists σ' s.t. $\mathbb{Z}, \sigma' \models \varphi$ and $C(p)(\sigma') = \sigma$. As $\sigma' \models \{\varphi\}p\{\psi\}$, we have $\mathbb{Z}, C(p)(\sigma') \models \psi$ which means $\sigma = C(p)(\sigma') \in [\psi]$.
If on the other hand $[\psi] \supseteq \mathrm{sp}(p, \varphi)$ it holds $\mathbb{Z}, \sigma \models \varphi \Rightarrow \mathbb{Z}, C(p)(\sigma) \models \psi$ for every $\sigma \in \Sigma$, hence $\models \{\varphi\}p\{\psi\}$. □

Lemma 5.18. *Let p be a program and φ, ψ be first-order formulas. Then*

$$\mathbb{Z} \models \mathrm{vc}(\{\bot\}p\{\psi\}) \quad \textit{and} \quad \mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\top\}).$$

Proof. From Theorem 5.14 we know that $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$ is equivalent to $\models \{\varphi\}p\{\psi\}$, which means that for all states $\sigma \in \Sigma$ it holds $(\mathbb{Z}, \sigma \models \varphi \;\Rightarrow\; \mathbb{Z}, C(p)(\sigma) \models \psi)$. If we replace φ with $\bot$ or ψ with $\top$, this is always a true statement. □

Theorem 5.19 ([11], Theorem 7.5)**.** *Let φ and ψ be first-order formulas in $\mathcal{L}$ and p be a program. Then there exist first-order formulas φ_{wp} and ψ_{sp} s.t.*

$$[\varphi_{\mathrm{wp}}] = \mathrm{wp}(p, \psi) \quad \textit{and} \quad [\psi_{\mathrm{sp}}] = \mathrm{sp}(p, \varphi).$$

To get the first-order formulas φ_{wp} and ψ_{sp} it is necessary to encode runs of programs, in particular arbitrary many iterations of a while-loop. This is achieved by encoding arbitrary large finite sequences, which is possible in $\mathbb{Z}$. However these encodings are not very descriptive. Our aim will be to construct LFP-formulas that define the weakest precondition and the strongest postcondition. Even if this are not first-order formulas, they better reflect the runs of a program and therefore lead to a better understanding of the program.

Consider the formula $\exists X\ \mathrm{vc}(\{\varphi\}p\{X\})$, which asks for a formula X s.t. all states satisfying φ fulfil X after running the program p. Similarly we are interested in solutions of the formula $\exists Y\ \mathrm{vc}(\{Y\}p\{\psi\})$. Note that this are linear-Horn formula equations and therefore we can apply the results from Chapter 3. In general there also occur formula variables in $\mathrm{vc}(\{\varphi\}p\{\psi\})$, yet here we are only interested in the formula variables that are stated specifically.

Theorem 5.20. *Let p be a program and ψ be a first-order formula. Consider the linear-Horn formula equation $\exists Y\ \pi \equiv \exists Y\ \mathrm{vc}(\{Y\}p\{\psi\})$. Let $\beta := \neg[\mathrm{lfp}_X\ \Phi_{\pi^D}]$, where Φ_{π^D} is the sequence of formulas defined in (3.1) from the dual formula of π. Then*

$$[\beta] = \mathrm{wp}(p, \psi).$$

Proof. As $\mathbb{Z} \models \mathrm{vc}(\{\bot\}p\{\psi\})$ we know that $\mathbb{Z} \models \exists Y\ \mathrm{vc}(\{Y\}p\{\psi\})$. Hence with Lemma 3.7/1 we obtain $\mathbb{Z} \models \mathrm{vc}(\{\beta\}p\{\psi\})$, which is, due to Theorem 5.14, equivalent to $\models \{\beta\}p\{\psi\}$. Now Lemma 5.17 states $[\beta] \subseteq \mathrm{wp}(p, \psi)$.
For the other inclusion let φ_{wp} be the formula from Theorem 5.19 s.t. $[\varphi_{\mathrm{wp}}] = \mathrm{wp}(p, \psi)$. From Lemma 5.17 we obtain $\models \{\varphi_{\mathrm{wp}}\}p\{\psi\}$, thus it holds $\mathbb{Z} \models \mathrm{vc}(\{\varphi_{\mathrm{wp}}\}p\{\psi\})$ and we can apply Lemma 3.7/2. This yields $\mathbb{Z} \models \forall \bar{x}\ (\varphi_{\mathrm{wp}}(\bar{x}) \to \beta(\bar{x}))$. In particular we got $\mathbb{Z}, \sigma \models \varphi_{\mathrm{wp}} \to \beta$ for all $\sigma \in \Sigma$. Hence $[\beta] \supseteq [\varphi_{\mathrm{wp}}] = \mathrm{wp}(p, \psi)$. □

Theorem 5.21. *Let p be a program and φ be a first-order formula. Consider the linear-Horn formula equation $\exists X\ \pi \equiv \exists X\ \mathrm{vc}(\{\varphi\}p\{X\})$. Let $\alpha := [\mathrm{lfp}_X\ \Phi_\pi]$, where Φ_π is the sequence of formulas defined in (3.1) from π. Then*

$$[\alpha] = \mathrm{sp}(p, \varphi).$$

Proof. From Lemma 5.18 we got $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\top\})$, in particular $\mathbb{Z} \models \exists X\ \mathrm{vc}(\{\varphi\}p\{X\})$. Using Lemma 3.3/1 it follows $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\alpha\})$, which is equivalent to $\models \{\varphi\}p\{\alpha\}$. Lemma 5.17 concludes $[\alpha] \supseteq \mathrm{sp}(p, \varphi)$.
Now take the formula ψ_{sp} from Theorem 5.19. With Lemma 5.17 we got $\models \{\varphi\}p\{\psi_{\mathrm{sp}}\}$, which is equivalent to $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi_{\mathrm{sp}}\})$. Now Theorem 3.3/2 states $\mathbb{Z} \models \forall \bar{x}(\alpha(\bar{x}) \to \psi_{\mathrm{sp}}(\bar{x}))$, that yields $[\alpha] \subseteq [\psi_{\mathrm{sp}}] = \mathrm{sp}(p, \varphi)$. □

Chapter 6

Inductive theorem proving

As an application of the Horn fixed-point theorem we take a deeper look at [4], a paper called "Inductive theorem proving based on tree grammars" by Sebastian Eberhard and Stefan Hetzl. Their aim is to generate a proof of an universal statement, which is generated in two phases. In the first phase proofs of small instances are computed, from which a second-order unification problem is deduced. Each solution of the unification problem is an induction invariant. We will not go into depth about phase one as we are more interested in phase two, in which solutions of the second-order unification problem are computed. We will see that the second-order unification problem is in fact a Horn formula equation, where we can apply our results from Chapter 3 to get solutions.

In this chapter we work in a language $\mathcal{L}$, which contains the constant symbol 0 and the unary function symbol s. We define $\overline{n} = \overline{s^n(0)}$.

Definition 6.1. *Let $F_1, ..., F_n, G_1, ..., G_m$ be formulas. A formula of the form $F_1 \wedge \cdots \wedge F_n \rightarrow G_1 \vee \cdots \vee G_m$ is called a* sequent *and is written as $\Gamma \Rightarrow \Delta$, where $\Gamma = \{F_1, ..., F_n\}$ and $\Delta = \{G_1, ..., G_m\}$.*

Definition 6.2 ([4],Definition 6.1.)**.** *Let $\alpha, \beta, \nu, \gamma$ be variables only occurring where indicated. Let $\Gamma_0(\alpha, \beta), \Gamma_1(\alpha, \nu, \gamma), \Gamma_2(\alpha)$ be multisets of quantifier-free first-order formulas and let $B(\alpha)$ be a quantifier-free formula. Let $t_i(\alpha, \nu, \gamma)$ and $u_j(\alpha)$ be terms for $i \in \{1, ..., n\}$ and $j \in \{1, ..., m\}$, where $n, m \geq 1$. Let X be a ternary formula variable. Then the list of the following three sequents is a* schematic simple induction proof(schematic s.i.p.)*:*

- $\Gamma_0(\alpha, \beta) \Rightarrow X(\alpha, 0, \beta)$
- $\Gamma_1(\alpha, \nu, \gamma), \bigwedge_{1 \leq i \leq n} X(\alpha, \nu, t_i(\alpha, \nu, \gamma)) \Rightarrow X(\alpha, s(\nu), \gamma)$
- $\Gamma_2(\alpha), \bigwedge_{1 \leq j \leq m} X(\alpha, \alpha, u_j(\alpha)) \Rightarrow B(\alpha)$

Note that every schematic s.i.p. defines a Horn formula equation $\exists X \forall \alpha, \beta, \nu, \gamma\, \psi$, where ψ is the conjunction of the three sequents. A solution of a schematic s.i.p. S is defined to

be a quantifier-free formula $F(x, y, z)$, such that the three sequents of S with X replaced by F are quasi-tautological, which means it is valid in first-order logic with equality. This means exactly $\models \forall \alpha, \beta, \nu, \gamma\ \psi[X \backslash F]$, as we always talk about logic with equality.

For solving a schematic s.i.p., $\Gamma_0, \Gamma_1, \Gamma_2$ may be arbitrary multisets of first-order formulas. Of particular interest is the case, when $\Gamma_0, \Gamma_1, \Gamma_2$ are instances of a theory Γ. In applications this is an arithmetic theory, e.g. Robinson arithmetic. Assume we have a solution F of a schematic s.i.p. S in that specific case. Then we can deduce a proof of $\forall \Gamma \Rightarrow \forall \beta\ F(\alpha, 0, \beta)$ from the first sequent of S, where $\forall \Gamma$ is the universal closure of Γ. Similarly we obtain $\forall \Gamma, \forall \beta F(\alpha, \nu, \beta) \Rightarrow \forall \beta F(\alpha, s(\nu), \beta)$ from the second sequent. As we are interested in proofs with an induction rule, we then are able to deduce $\forall \Gamma \Rightarrow \forall \nu, \beta F(\alpha, \nu, \beta)$. Thus using the third sequent of S yields a proof of $\forall \Gamma \Rightarrow B(\alpha)$ and therefore of $\forall \Gamma \Rightarrow \forall \alpha B(\alpha)$. In [4] the aim is to prove an universal statement $\forall \alpha B(\alpha)$. To do so an appropriate schematic s.i.p. is defined, where a Solution of it yields a proof of $\forall \alpha B(\alpha)$, as we sketched here.
Next we investigate how to get a solution of a schematic s.i.p.

Definition 6.3 ([4], Definition 6.10.)**.** *Let S be a schematic s.i.p. with premises given as in Definition 6.2. By recursion define the following sequence of formulas.*

$$C_{S,0}(x, z) := \bigwedge \Gamma_0(x, z)$$
$$C_{S,q+1}(x, z) := \bigwedge \Gamma_1(x, \bar{q}, z) \wedge \bigwedge_{1 \leq i \leq n} C_{S,q}(x, t_i(x, \bar{q}, z))$$

$C_{S,q}(x, z)$ is called the q-th canonical solution of S.

Lemma 6.4. *Let S be a schematic s.i.p. and $C_{S,q}$ be defined as in Definition 6.3. Let $\exists X \psi$ be the formula equation defined from S. Let $(\varphi^l)_{l \in \omega}$ be the sequence of first-order formulas defined as in (4.1) from ψ. Then for all $q \in \mathbb{N}$ it holds*

$$C_{S,q}(x, z) \equiv \varphi^{q+1}(x, \bar{q}, z).$$

Proof. We show the equivalence by induction on q. The definition of $(\varphi^l)_{l \in \omega}$ is $\varphi^0 \equiv \bot$ and for $l \in \omega$

$$\varphi^{l+1}(x, y, z) \equiv \exists \alpha, \beta, \nu, \gamma \Big(\Big(\bigwedge \Gamma_0(\alpha, \beta) \wedge x = \alpha \wedge y = 0 \wedge z = \beta \Big) \vee \Big(\bigwedge \Gamma_1(\alpha, \nu, \gamma) \wedge \bigwedge_{1 \leq i \leq n} \varphi^l(\alpha, \nu, t_i(\alpha, \nu, \gamma)) \wedge x = \alpha \wedge y = s(\nu) \wedge z = \gamma \Big) \Big).$$

In particular it holds that $\varphi^1(x, 0, z) \equiv \bigwedge \Gamma_0(x, z) \equiv C_{S,0}(x, z)$. For $q \geq 0$ we have

$$\varphi^{q+2}(x, \overline{q+1}, z) \equiv \bigwedge \Gamma_1(x, \bar{q}, z) \wedge \bigwedge_{1 \leq i \leq n} \varphi^{l+1}(x, \bar{q}, t_i(x, \bar{q}, z))$$
$$\equiv \bigwedge \Gamma_1(x, \bar{q}, z) \wedge \bigwedge_{1 \leq i \leq n} C_{S,q}(x, t_i(x, \bar{q}, z)) \equiv C_{S,q+1}(x, z).$$

□

Now we want to present Lemma 6.12. from [4] as a direct corollary of Lemma 3.7.

Lemma 6.5 ([4], Lemma 6.12.)**.** *Let S be a schematic s.i.p. Then for any solution F of S and any $q \in \mathbb{N}$, the q-th canonical solution $C_{S,q}(x,z)$ logically implies $F(x,\bar{q},z)$.*

Proof. From the definition of φ^ω in (4.1) it follows that $\models \varphi^q \to \varphi^\omega$ for all $q \in \omega$. Theorem 4.5 states that $\varphi^\omega \equiv [\mathrm{lfp}_X\ \Phi_\psi]$ and thus Lemma 6.4 yields $\models C_{S,q}(x,z) \to [\mathrm{lfp}_X\ \Phi_\psi]$ for all $q \in \omega$. Now Lemma 3.7/3 concludes $\models C_{S,q}(x,z) \to F(x,\bar{q},z)$ for all $q \in \omega$. □

Thus we see that using the results from Chapter 3 and 4 shortens the proofs of this paper and brings more insights to it.

Chapter 7

Decidability of affine solution problems

In this chapter we want to deal with the affine solution problem, which is shown to be decidable in [6]. This is proven by computing a fixed point similarly to how we did in Chapter 3. The main difference is that the fixed point is not computed on the level of logic, but in a lattice of affine subspaces of $\mathbb{Q}^n$. The question emerges if it is possible to lift up this computation and use the results of Chapter 3. It turns out that this is not possible. Yet we will give some guideline how to generalize the Horn fixed point theorem in order to be applicable for this problem.

We start by presenting the algorithm for the affine solution problem. Here we work in the language $\mathcal{L}_{\text{aff}}$, which consists of

- the constant symbols 0 and 1,
- the binary function symbol $+$,
- the unary function symbols $\{c \mid c \in \mathbb{Q}\}$.

We are only interested in the structure $\mathbb{Q}$, where 0, 1 and $+$ are interpreted in the usual way and the unary function symbol c is interpreted as multiplication with c for each $c \in \mathbb{Q}$. Note that in $\mathcal{L}_{\text{aff}}$ it is only possible to multiplicate with constants, but not with variables. As we are only working in $\mathbb{Q}$ we can assume without loss of generality, that every term $t(x_1, ..., x_n)$ is of the form $c_0 + \sum_{i=1}^{m} c_i x_i$ and every atomic formula $A(x_1, ..., x_n)$ is of the form $c_0 + \sum_{i=1}^{m} c_i x_i = 0$. We call such atomic formulas *linear equations* and conjunctions of linear equations *linear equation systems*.

Definition 7.1. *An* affine formula equation *is a formula equation of the form* $\exists \overline{X}\ \psi$*, where* ψ *is a quantifier-free first-order formula in* $\mathcal{L}_{\text{aff}} \cup \{X_1, ..., X_n\}$.

Definition 7.2. *The solution problem* $\langle \mathrm{Th}(\mathbb{Q}), \mathcal{C}, \Phi \rangle$*, where* $\mathcal{C}$ *is the class of linear equation systems and* Φ *is the class of affine formula equations, is called the* affine solution problem.

The aim of [6] is to prove decidability of the affine solution problem. We now sketch the proof and state the most interesting parts from our point of view. For a detailed and complete proof see [6].

Definition 7.3. *Let* V *be a vector space over* $\mathbb{Q}$*. Then* $\mathrm{Aff}V$ *is the set of all subsets of* V *that are either empty or affine subspaces of* V*.*

$\mathrm{Aff}V$ is a complete lattice with least element $\varnothing$ and greatest element V. Let $\mathscr{A}, \mathscr{B} \in \mathrm{Aff}V$, then the intersection $\mathscr{A} \cap \mathscr{B} \in \mathrm{Aff}V$, we write $\mathscr{A} \vee \mathscr{B}$ for the supremum in $\mathrm{Aff}V$.
Let $A(x_1, ..., x_n)$ be a linear equation system. Then $A^{\mathbb{Q}} \in \mathrm{Aff}\mathbb{Q}^n$. Thus, as we are interested in solutions of affine formula equations, which are linear equation systems, we are searching for solutions in $\mathrm{Aff}\mathbb{Q}^n$.
We write affine spaces, affine transformations and variables in an affine space in calligraphic typeface, e.g. $\mathscr{A}, \mathscr{T}, \mathscr{X}$.

Definition 7.4. *Let* $m, n, l, r \in \mathbb{N}$ *and let* $\mathscr{A}, \mathscr{B}_1, ..., \mathscr{B}_m \in \mathrm{Aff}\mathbb{Q}^n$*. Let* $\mathscr{X}_i$ *be a variable ranging over* $\mathrm{Aff}\mathbb{Q}^{k_i}$ *and* $\mathscr{T}_i : \mathbb{Q}^n \to \mathbb{Q}^{k_i}$ *be an affine transformation for* $i \in \{1, ..., l + r\}$*. An* affine condition $\mathscr{C}$ *is a statement of the form*

$$\mathscr{A} \cap \bigcap_{i=1}^{l} \mathscr{T}_i^{-1}(\mathscr{X}_i) \subseteq \bigcup_{i=1}^{m} \mathscr{B}_i \cup \bigcup_{j=l+1}^{l+r} \mathscr{T}_j^{-1}(\mathscr{X}_j).$$

A tuple $\overline{\mathscr{F}} \in \mathrm{Aff}\mathbb{Q}^{k_1} \times \cdots \times \mathrm{Aff}\mathbb{Q}^{k_{l+r}}$ *is a* solution *of* $\mathscr{C}$ *if* $\mathscr{C}[\overline{\mathscr{X}} \backslash \overline{\mathscr{F}}]$ *is true.*

Let $\exists \overline{X}\ \psi$ be an affine formula equation, where w.l.o.g. ψ is in conjunctive normal form. From every clause C in ψ an affine condition $\mathscr{C}$ can be derived, s.t. for every tuple of linear equation systems $\overline{F}$ we have $\mathbb{Q} \models C[\overline{X} \backslash \overline{F}]$ iff $\overline{F}^{\mathbb{Q}}$ is a solution of $\mathscr{C}$. Thus the affine solution problem is reduced to solving affine conditions.

Definition 7.5. *Let* $\mathscr{C}$ *be an affine condition as in Definition 7.4. We call the affine conditions*

$$\begin{array}{lllll} (U) & \mathscr{A} \cap \bigcap_{i=1}^{l} \mathscr{T}_i^{-1}(\mathscr{X}_i) & \subseteq \mathscr{B}_{i_0}, & & i_0 \in \{1, ..., m\}, \\ (L) & \mathscr{A} \cap \bigcap_{i=1}^{l} \mathscr{T}_i^{-1}(\mathscr{X}_i) & \subseteq \mathscr{T}_{j_0}^{-1}(\mathscr{X}_{j_0}), & & j_0 \in \{l+1, ..., l+r\} \end{array}$$

projections *of* $\mathscr{C}$*. Such affine conditions are called* affine Horn conditions*. We call affine Horn conditions of the form (L)* lower bound conditions *and of the form (U)* upper bound conditions.[1] *Let* S *be a set of affine conditions. We call a set of affine Horn conditions a* projection *of* S *if it consists of exactly one projection of each element of* S*.*

[1] Note the similarity to Section 3.1, where the upper bound conditions correspond to the end clauses and the lower bound conditions correspond to the base and induction clauses.

Theorem 7.6. *Let $\mathscr{C}$ be an affine condition. Then $\overline{\mathscr{F}}$ is a solution of $\mathscr{C}$ iff it is a solution of some projection of $\mathscr{C}$.*

This theorem further reduces the problem to solving affine Horn conditions. It basically follows from the fact that an affine space is in the union of affine spaces iff it is in one of them.

Now we get to the part of the proof that is most interesting for us: Solving a set of affine Horn conditions.

Let P be a set of affine Horn conditions with unknowns $\mathscr{X}_1, ..., \mathscr{X}_n$ of arity $k_1, ..., k_n$. As we are only interested in solutions that are affine spaces it follows that the candidate solutions of P are the elements of $\mathrm{Aff}\mathbb{Q}^{k_1} \times \cdots \times \mathrm{Aff}\mathbb{Q}^{k_n}$. We write $\mathrm{Lat}(P)$ for the lattice $\mathrm{Aff}\mathbb{Q}^{k_1} \times \cdots \times \mathrm{Aff}\mathbb{Q}^{k_n}$. We now define an operator F_P on $\mathrm{Lat}(P)$. Let $j \in \{1, ..., n\}$ and

$$\mathscr{A}_1 \cap \bigcap_{i=1}^{m_1} \mathscr{T}_{1,i}^{-1}(\mathscr{X}_{j_{1,i}}) \subseteq \mathscr{T}_1^{-1}(\mathscr{X}_j)$$

$$\vdots$$

$$\mathscr{A}_l \cap \bigcap_{i=1}^{m_l} \mathscr{T}_{l,i}^{-1}(\mathscr{X}_{j_{l,i}}) \subseteq \mathscr{T}_l^{-1}(\mathscr{X}_j)$$

be the lower bound conditions in P, where the unknown on the right side is $\mathscr{X}_j$. Define

$$F_P(\overline{\mathscr{X}})_j := \mathscr{X}_j \vee \bigvee_{i'=1}^{l} \mathscr{T}_{i'} \left(\mathscr{A}_{i'} \cap \bigcap_{i=1}^{m_{i'}} \mathscr{T}_{i',i}^{-1}(\mathscr{X}_{j_{i',i}}) \right).$$

Similarly to Lemma 3.3 we get:

Theorem 7.7. *Let P be a set of affine Horn conditions and $\alpha_j := \mathrm{lfp}(F_P)_j$ for $j \in \{1, ..., n\}$. Then there exists a solution of P iff $\bar{\alpha}$ is a solution of P.*

Let P be a set of affine Horn conditions. As F_P is a monotonous operator it follows from Lemma 2.24 that $\mathrm{lfp}(F_P) = \mathrm{ifp}(F_P) = S_{F_P}^{\xi}$, where $(S_{F_P}^{\zeta})$ is the sequence defined in (2.4) and ξ is the closure ordinal of F_P. As $\mathrm{Lat}(P)$ has finite height, which follows from the dimensions of the affine spaces being finite, we obtain $\xi < \omega$ and hence we can compute $S_{F_P}^{\xi}$ in finite time. Thus we can decide if P is solvable by checking whether $\bar{\alpha}$ satisfies the upper bound conditions. Hence the following is shown:

Theorem 7.8. *The affine solution problem is decidable.*

The method of finding a solution of affine Horn conditions and the definition of the operator F_P reminds one of solving Horn formula equations as we did in Section 3.1. Thus one might think that we can find linear equation systems, which solve affine formula equations with Lemma 3.3. The next example shows that this does not work.

Example 7.9. *Consider the affine formula equation ψ with one binary formula variable X:*

$$\psi \equiv \bigwedge \begin{cases} X(0,0) \\ X(1,0) \\ X(2,0) \to X(0,1) \end{cases}.$$

Let P be the set of affine conditions obtained from ψ

$$\begin{aligned} \mathbb{Q}^2 &\subseteq \mathscr{T}_0^{-1}(\mathscr{X}) \\ \mathbb{Q}^2 &\subseteq \mathscr{T}_1^{-1}(\mathscr{X}) \\ \mathscr{T}_2^{-1}(\mathscr{X}) &\subseteq \mathscr{T}_3^{-1}(\mathscr{X}), \end{aligned}$$

where $\mathscr{X}$ is a variable ranging over $\mathrm{Aff}\mathbb{Q}^2$ and

$$\mathscr{T}_0 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \mathscr{T}_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathscr{T}_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \quad \mathscr{T}_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

All the affine conditions in P are affine Horn conditions, thus we can define the operator F_P on $\mathrm{Aff}\mathbb{Q}^2$:

$$F_P(\mathscr{X}) = \mathscr{X} \vee \mathscr{T}_0(\mathbb{Q}^2) \vee \mathscr{T}_1(\mathbb{Q}^2) \vee \mathscr{T}_3(\mathscr{T}_2^{-1}(\mathscr{X})).$$

We have $F_P(\varnothing) = \left[\binom{1}{0}\right]$ and $F_P(F_P(\varnothing)) = \mathbb{Q}^2$, hence $\mathrm{lfp}(F_P) = \mathbb{Q}^2$. This is a solution of P.

On the other hand, as ψ is a Horn formula equation, we could try to solve ψ as we did in Section 3.1. Doing so we define $\alpha := [\mathrm{lfp}_X\ \Phi_\psi]$, where Φ_ψ is the operator defined in (3.1). In $\mathbb{Q}$ the formula α defines the set

$$\alpha^{\mathbb{Q}} = \{(0,0),(1,0)\}.$$

This is a solution of ψ, yet we are only interested in solutions, which are affine subspaces of $\mathbb{Q}^2$, which $\alpha^{\mathbb{Q}}$ is not. Thus it is natural to take a look at the affine hull of $\alpha^{\mathbb{Q}}$, which is

$$\mathrm{aff}(\alpha^{\mathbb{Q}}) = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right].$$

This is not a solution of ψ, as $\mathbb{Q}, [X := \mathrm{aff}(\alpha^{\mathbb{Q}})] \not\models X(2,0) \to X(0,1)$.

In the previous example we have seen, that the fixed point theorem from Chapter 3 is not directly applicable for affine solution problems. The reason why this does not work is, that the operator F_{Φ_ψ} used in Chapter 3 and the operator F_P are defined on different lattices. In solving affine solution problems we are only interested in solutions, which are affine subspaces of $\mathbb{Q}^n$. Therefore an operator F_P is defined on the lattice $\mathrm{Aff}\mathbb{Q}^n$ to find a

solution. However in Chapter 3 the operator F_{Φ_ψ} is defined on the lattice of all subsets of $\mathbb{Q}^n$. An idea would be to generalize Lemma 3.3 in the following way:[2]

Let $\exists X\ \psi$ be a Horn formula equation and $\mathcal{M}$ be a structure. Let $(L, \subseteq)$ be a sublattice of $(P(M), \subseteq)$. If a monotonous operator F on M satisfies $F(A) \in L$ for all $A \in L$, then we can apply the Knaster-Tarski theorem on $(L, \subseteq)$ and F and obtain a fixed point $\alpha \in L$ of F. Thus, if the operator defined in (3.1) fulfils this condition, it should be possible to obtain a canonical solution α of $\exists X\ \psi$ s.t. $\alpha \in L$. As this thesis is not the place to work this out in detail we refer to future work.
In the context of affine solution problems we then could apply this result with the sublattice $\mathrm{Aff}\mathbb{Q}^n$ of $\mathbb{Q}^n$. Here the operator F defined in (3.1) does not satisfy $F(A) \in \mathrm{Aff}\mathbb{Q}^n$ for all $A \in \mathrm{Aff}$, thus the operator has to be adjusted accordingly.

Another application of this generalized lemma would be in the context of abstract interpretation. This is a theory of an approximation of the semantics of a computer program. To get a small idea of how this works take for instance a program p, where only the sign of an integer variable x is important, but the exact value does not matter. Then the only information of x that is of interest in abstract interpretation is the sign of x. Therefore the set of accepted states of x of the program p is an element of the sublattice $(P(\{-1, 0, 1\}), \subseteq)$ of $(P(\mathbb{Z}), \subseteq)$, thus we can utilize the generalized Lemma. If this is worked out in full detail it should be possible to get similar results as in Chapter 5 for abstract interpretation.

[2]For simplicity we state this for one unary formula variable X. Yet this should be easy to generalize for finitely many formula variables of arbitrary arity.

Chapter 8

Conclusion

The main results of this thesis are the fixed-point theorems for Horn formula equations and dual-Horn formula equations. These are new results, which describe the solution space of formula equations. We obtained the theorems by defining an operator such that every solution of the formula equation is a fixed point of it. The least fixed point turned out to always be a solution if there exists one. This canonical solution is described by a least fixed-point formula.
In applications one is usually interested in solutions, which are first-order formulas. For the special case of linear-Horn formula equations the fixed-point theorem reduces the problem of finding first-order solutions to an interpolation problem: Finding first-order formulas $\overline{\chi}$, such that $\overline{\alpha} \to \overline{\chi} \wedge \overline{\chi} \to \overline{\beta}$, where $\overline{\alpha}$ and $\overline{\beta}$ are the least fixed-point formulas we got from Theorem 3.11.
Multiple applications of the fixed-point theorems are shown in this thesis. In Chapter 4 we dealt with the problem of finding first-order formulas which approximate existential second-order formulas, which has been investigated since Ackermann in 1935. We managed to extend this results for the special case of Horn formula equations.
The verification conditions of a program are a well-known concept in program verification. Yet, normally they are not treated as a second-order formula like we did in Chapter 5. By doing so we were able to define a new semantics for Hoare triples, which turned out to be equivalent to the classical one. This semantics is specified by a linear-Horn formula equation, thus we could apply our fixed-point theorems. As corollaries we got formulas that correspond to the classical concepts of weakest precondition and strongest postcondition.
By generalizing the fixed-point theorems it should be possible to get similar results for abstract interpretation. We sketched an idea of how to generalize the theorems to make them applicable for this problem, as well as for proving decidability of the affine solution problem. This is left as future work.
The fixed-point theorems were used in many areas, we got new results for approximating second-order formulas, in program verification and in inductive theorem proving. Further

research on Horn formula equations may lead to more insights, especially in abstract interpretation and automated theorem proving.

Bibliography

[1] Wilhelm Ackermann. Untersuchungen über das Eliminationsproblem der mathematischen Logik. *Mathematische Annalen*, 110(1):390–413, December 1935.

[2] A. Arnold and D. Niwinski. *Rudiments of Calculus*. Elsevier Science, 2001.

[3] Anuj Dawar and Yuri Gurevich. Fixed point logics. *The bulletin of symbolic logic*, 8(1):65–88, 2002.

[4] Sebastian Eberhard and Stefan Hetzl. Inductive theorem proving based on tree grammars. *Annals of Pure and Applied Logic*, 166(6):665 – 700, 2015.

[5] Sebastian Eberhard, Stefan Hetzl, and Daniel Weller. Boolean unification with predicates. *Journal of Logic and Computation*, 27(1):109–128, 2015.

[6] Stefan Hetzl and Sebastian Zivota. Decidability of affine solution problems. *Journal of Logic and Computation*, 30(3):697–714, 2019.

[7] Leonid Libkin. *Elements Of Finite Model Theory (Texts in Theoretical Computer Science. An Eatcs Series)*. SpringerVerlag, 2004.

[8] Y. N. Moschovakis. *Elementary Induction on Abstract Structures*. North-Holland Publishing Company, 1974.

[9] Christoph Wernhard. Approximating resultants of existential second-order quantifier elimination upon universal relational first-order formulas. In Patrick Koopmann, Sebastian Rudolph, Renate A. Schmidt, and Christoph Wernhard, editors, *Proceedings of the Workshop on Second-Order Quantifier Elimination and Related Topics (SOQE 2017)*, volume 2013 of *CEUR Workshop Proceedings*, pages 82–98. CEUR-WS.org, 2017.

[10] Christoph Wernhard. The boolean solution problem from the perspective of predicate logic - extended version. *CoRR*, abs/1706.08329, 2017.

[11] G. Winskel. *The Formal Semantics of Programming Languages: An Introduction*. Zone Books, U.S., 1993.