TECHNICAL UNIVERSITY MUNICH
Department of Informatics

BACHELOR'S THESIS IN INFORMATICS

The Satisfiability Problem for Fragments of PCTL

Alexej ROTAR

TECHNICAL UNIVERSITY MUNICH
Department of Informatics

BACHELOR’S THESIS IN INFORMATICS

The Satisfiability Problem for Fragments of PCTL

Das Erfüllbarkeitsproblem für Fragmente von PCTL

Author: Alexej ROTAR
Supervisor: Prof. Dr. Jan KŘETÍNSKÝ
Advisor: Prof. Dr. Jan KŘETÍNSKÝ
Submission date: March 15, 2018

Declaration of Authorship

I confirm that this bachelor's thesis is my own work and I have documented all sources and material used.

Abstract

The satisfiability of PCTL-formulae in general is a long standing open problem. Variations of the problem, such as the satisfiability of qualitative PCTL-formulae (Brázdil, Forejt, Křetínskỳ, and Kucera, 2008), the bounded satisfiability (Bertrand, Fearnley, and Schewe, 2012), or the satisfiability for bounded PCTL-formulae (Chakraborty and Katoen, 2016) have been solved already. In this thesis, we tackle the satisfiability problem for various fragments of the quantitative PCTL. For this, we develop several techniques to reduce the size and complexity of models in order to obtain models of regular shape. Thereby, we show the small model property of the considered fragments. In particular, we prove that for those fragments, the general satisfiability problem and the finite satisfiability problem are equivalent. We also provide examples of obstacles for more general fragments. Besides the solutions presented in this thesis, the methods that we develop may serve as a framework to solve other fragments, as they are applicable to more general formulae.

Contents

List of Figures

1 Introduction

For complex systems, it can be rather hard to manually determine, whether or not they meet certain requirements. On the other hand, there are systems, such as safety critical ones, where such guarantees are vital. Therefore, the need for automatic tools to aid the process arises. In this context, various temporal logics, as a means of formalizing requirements to systems, have been thoroughly studied. Examples for such logics include LTL, CTL, TCTL, or PCTL, to name a few. The model checking problem is then to determine, whether some representation of a system meets a requirement—i.e. whether the system is a *model* for the logical formula. In order to construct a system which behaves as specified, one could first formalize the specification in terms of an appropriate logic and then try to iteratively find a model for the resulting formula.

What if, however, the formula cannot be satisfied at all; i.e. the specification is inconsistent and the corresponding formula a contradiction. For complex specifications, contradicting statements can be far from obvious. The procedure of creating a well-behaved system, will become a rather frustrating task—no matter which system one comes up with, it would never satisfy the formula. The task to determine, if there is a model for some formula or not, is called the satisfiability problem. If a solver for this problem existed, one could first check, whether some specification is consistent before trying to find a model for it.

One could go even further and search for a model automatically. That means, we need to solve the following problem: *Given a satisfiable logical formula, construct a system which models the formula.* We will refer to this as the model construction problem. The satisfiability problem is typically solved by showing how to construct a model for a satisfiable formula and, therefore, solve the model construction problem.

The model checking problem has been solved for all of the mentioned temporal logics (Baier and Katoen, 2008). The satisfiability problem turns out to be more complicated. It has been solved for LTL (Baier and Katoen, 2008) and CTL (Emerson and Halpern, 1982). In contrast, finite satisfiability of TCTL formulae has been proven to be undecidable (Alur, Courcoubetis, and Dill, 1993). In the case of PCTL, no general decision procedure has been given so far but neither has its existence been disproved. In the following section, we will discuss some existing approaches to this problem.

1.1 Related Work

We will call formulae of PCTL *qualitative* if they have only the bounds 0 and 1. For these cases, the satisfiability problem and the finite satisfiability problem have been proven to be **EXPTIME**-complete and therefore decidable (Brázdil, Forejt, Křetínský, and Kucera, 2008). Interestingly, the two problems are not equivalent in general; i.e. there are formulae, which are satisfiable but only by infinite models. An example of this case is given in (Brázdil, Forejt, Křetínský, and Kucera, 2008). In order to solve the general satisfiability problem, the authors introduced a finite representation of infinite models, together with an algorithm that can create such representations for satisfiable formulae.

The bounded satisfiability problem is to determine, whether there exists a model of a certain size for a given formula. This problem has been solved by encoding it into an SMT problem (Bertrand, Fearnley, and Schewe, 2012). There is an important implication of this result. Namely, if we are able to determine a maximum required model size for some formula, then it follows that the satisfiability of that formula can also be determined. In many of our proofs, this will be exactly our strategy.

Another interesting problem that has been solved is the satisfiability problem for bounded PCTL formulae (Chakraborty and Katoen, 2016). In bounded PCTL, some operators are restricted in a certain sense. What makes this problem and the bounded satisfiability problem simple, compared to general PCTL satisfiability, is the fact that both avoid the possibility of arbitrarily large (or infinite) models, by explicitly limiting them in certain ways. We will see that this possibility makes the general satisfiability problem particularly challenging.

Typically, model checking cannot directly deal with infinite-state systems. In (Dimitrova, Fioriti, Hermanns, and Majumdar, 2016), the authors introduce an axiomatization for PCTL* and solve the model checking problem for countable-state, non-deterministic systems.

Apart from solutions for various related problems, one such has also been proven to be undecidable; namely, the problem, whether for some PCTL formula there exists a model with a branching degree that is bounded by some integer (Brázdil, Forejt, Křetínský, and Kucera, 2008). However, the authors have not been able to extend their proof and show the undecidability for our considered problem.

1.2 Our Contribution

In this thesis, we will explore different fragments of PCTL and solve the satisfiability problem for those. In order to do so, we will develop general techniques that can help to normalize the shape of a model. Those techniques enable us to prove the small model property for the considered fragments and thereby solve the satisfiability problem. In some cases, we will give methods for model construction, as well. In all other cases, it is easy to derive model construction methods from our proofs. A particularly interesting result is that all satisfiable formulae in the considered fragments are finitely satisfiable.

Moreover, we will discuss some obstacles that arise in other parts of PCTL, along with concrete examples of challenging formulae; i.e. formulae which enforce models of a rather complicated shape. This is important, as it indicates what one would have to deal with when approaching the general problem.

2 Background on Probability Theory

Before we can define PCTL, we shall recap some notions from probability theory. PCTL is a logic that speaks about properties of Markov chains. In this section, we will discuss the definitions of probability spaces and Markov chains. We will also present some results, which we will frequently refer to throughout the thesis.

2.1 Probability Spaces and Markov Chains

In order to properly define Markov chains, we have to look at probability spaces, first.

Definition 2.1 (Probability Spaces)**.** A probability space is a triple $(\Omega, \mathfrak{E}, Pr)$, such that Ω is any non-empty set, $\mathfrak{E} \subseteq 2^{\Omega}$, and $Pr : \mathfrak{E} \to [0,1]$. Additionally,

- $\Omega \in \mathfrak{E}$.
- For $E \in \mathfrak{E}, \overline{E} \in \mathfrak{E}$.
- For $E_1, E_2, \dots \in \mathfrak{E}, \bigcup_i E_i \in \mathfrak{E}$.
- $Pr(\Omega) = 1$.
- For disjoint $E_1, E_2, \dots \in \mathfrak{E}$, $Pr(\bigcup_i E_i) = \sum_i Pr(E_i)$.

We call Ω the sample space, $\mathfrak{E}$ the σ-Algebra, $E \in \mathfrak{E}$ an event, and Pr the probability measure (Rosenthal, 2006).

Markov chains can be described as a set of states together with transition probabilities. They can be used to model uncertainty in systems. Examples can be found in (Baier and Katoen, 2008). Typically, Markov chains are formally defined as sequences of random variables (Rosenthal, 2006). For our purpose, however, we prefer the definition in (Baier and Katoen, 2008).

Definition 2.2 (Discrete Time Markov Chains)**.** A tuple $M := (S, P)$ is called a discrete-time Markov chain if S is a countable set, $P : S \times S \to [0,1]$, and for all $s \in S$, $\sum_{t \in S} P(s,t) = 1$.

For the sake of simplicity, we will write M for a Markov chain, whenever we mean $M := (S, P)$—and similarly for $M' := (S', P')$, etc. In order to reason about Markov chains, we need to associate a probability space with them. For a Markov chain M, and state $s \in S$, we define the set of finite paths from s

$$paths_M(s) := \{\rho \in S^+ \mid \rho[0] = s \text{ and for all } i, P(\rho[i], \rho[i+1]) > 0\}.$$

Moreover, for a finite path $\rho \in paths_M(s)$, we define the cylinder set spanned by ρ

$$Cyl_M(\rho) := \{\pi \in S^\omega \mid \rho \text{ is a prefix of } \pi\}.$$

We can now define a σ-Algebra $\mathfrak{C}^M$ as the least σ-Algebra that contains all $Cyl_M(\rho)$, with $\rho \in paths_M(s)$. The probability measure is uniquely determined by

$$Pr_M(Cyl_M(\rho)) := \prod_{0 \le i < len(\rho)} P(\rho[i], \rho[i+1]).$$

This follows from the well known extension theorem which, for instance, can be found in (Rosenthal, 2006).

Successors and predecessors Now that we can reason about probabilities in Markov chains, we can introduce the notions of successors and predecessors of states. Let $T \subseteq S$. Then, the immediate successors of T are given by

$$post_M(T) := \bigcup_{t \in T} \{s \in S \mid P(t,s) > 0\}$$

and the immediate predecessors are

$$pre_M(T) := \bigcup_{t \in T} \{s \in S \mid P(s,t) > 0\}.$$

Moreover, we will use the recursive notation

$$\begin{aligned} post^1_M(T) &:= post_M(T) \\ post^n_M(T) &:= post_M(post^{n-1}_M(T)) \end{aligned}$$

to denote the states reachable from T within n steps. Finally,

$$post^*_M(T) := \bigcup_{n \in \mathbb{N}} post^n_M(T)$$

denotes the set of all states that are reachable from T with positive probability. Similarly, we denote $pre^n_M(T)$, and $pre^*_M(T)$. If we are only interested in a single state $s \in S$, we will omit the braces and simply write $post_M(s)$. Moreover, we will write $Pr(\cdot), post(\cdot)$, and $pre(\cdot)$, if M is clear from the context.

Trees Every Markov chain can be unfolded into a tree. Formally, for a given Markov chain M, we define the unfolded tree $T_M := (S^+, P')$, with

$$\forall \rho s \in S^+ : P'(\rho s, \rho s s') = P(s, s').$$

In a sense, two states of T_M are equivalent, if the last state of their paths is the same. Therefore, we can define an equivalence relation $\rho s \sim \eta t$ iff $s = t$. In trees, every state has a unique path to each of its predecessors. This property makes them more convenient to handle than general chains. Therefore in our proofs, we will frequently assume that the chain is a tree. For this, we first have to prove that the unfolding behaves the same as the original chain. Proposition 2.3 formalizes this. First, consider a function $f : paths_{T_M}(s) \to paths_M(s), \rho \mapsto \rho[len(\rho)]$. Intuitively, every state of T_M stores the path that led to it. Therefore, if we pick the last state of a path through T_M, we obtain a path through M of the same length. We can extend f to map events of $\mathfrak{C}^{T_M}$ to events in $\mathfrak{C}^M$ in the following way: for $E \in \mathfrak{C}^{T_M}$, let

$$f(E) := \begin{cases} Cyl_M(f(\rho)) & \text{if } E = Cyl_{T_M}(\rho) \\ f(E_1) \cup f(E_2) & \text{if } E = E_1 \cup E_2 \\ \overline{f(E')} & \text{if } E = \overline{E'}. \end{cases}$$

What we have to show, is that the events in T_M occur with the same probability as the corresponding events in M.

Proposition 2.3. *For a Markov chain M, its unfolding T_M, and an event $E \in \mathfrak{E}^{T_M}$, $Pr_{T_M}(E) = Pr_M(f(E))$.*

Proof. It is clear that $Pr_{T_M}(E)$ is determined by the probabilities of the single cylinder sets which describe E. Moreover, as we have argued before, the measure is uniquely determined by the probabilities of the cylinder sets. Therefore, it suffices to show that $Pr_{T_M}(Cyl_{T_M}(\rho)) = Pr_M(Cyl_M(f(\rho)))$ because then the probability measure of T_M is entirely determined by the probability measure of M. From the definitions, we can easily see that

$$\begin{aligned} Pr_{T_M}(Cyl_{T_M}(\rho)) &= \prod_{0 \leq i \leq len(\rho)} P'(\rho[i], \rho[i+1]) \\ &= \prod_{0 \leq i \leq len(f(\rho))} P(f(\rho)[i], f(\rho)[i+1]) \\ &= Pr_M(Cyl_M(f(\rho))). \end{aligned}$$

□

Let M' be a tree, $s \in S'$, and $t \in post^*(s)$. We can determine the probability to reach t from s as follows: let ρ be the path from s to t. Then,

$$P^*(s,t) := Pr(Cyl(\rho))$$

2.2 Markov Chains and their underlying Graphs

Markov chains can be visualized as directed graphs: the states of the chain become the vertices of the graph, and every state is linked to its successors by arcs. When reasoning about Markov chains, it is sometimes convenient to refer to the underlying graph. In particular, it is interesting to look at Strongly Connected Components (SCCs) in the graph. An SCC in the original sense is a set of vertices such that every vertex can reach every other vertex therein and no proper superset satisfies this condition. A Bottom SCC (BSCC) is an SCC that cannot be left. We can easily adapt these definitions to Markov chains.

Definition 2.4 ((Bottom) Strongly Connected Components)**.** For a Markov chain M, a set $T \subseteq S$ is called a Strongly Connected Component iff

- For all $s, t \in T$, $t \in post^*(s)$.
- No state $s \in S \setminus T$, can be added without violating the above condition.

If additionally $post^*(T) = T$, then T is bottom.

There is an important result about BSCCs and finite Markov chains.

Theorem 2.5. *For a finite Markov chain M, some BSCC is reached almost surely, and every state in a BSCC is reached from every other state within that BSCC almost surely.*

This theorem is fundamental for our subsequent proofs. A proof can be found in (Baier and Katoen, 2008). Note that for an unfolding of a finite chain, proposition 2.3 yields that theorem 2.5 still holds, in the sense that every run ends up in the unfolding of a BSCC, and every equivalence class within a BSCC is reached almost surely from every other equivalence class.

3 Probabilistic Computational Tree Logic

There exist various formal logics in mathematics and computer science, such as propositional logic, predicate logic, or temporal logic, to name a few. Each of those makes statements about certain structures. Propositional logic is about assignments of truth values to atomic propositions. Predicate logic speaks about domains and interpretations of symbols. Temporal logics typically make statements about various transition systems. If a statement about a given structure is true, then we call this structure a model for this statement. Whenever we define a new formal logic, we need to define two things—the syntax and the semantics. The syntax determines how to form proper statements which we call formulae. Semantics define how to evaluate the truth of a formula for a given structure. For this, we first need to properly define the structures that we consider.

Probabilistic Computational Tree Logic—or PCTL for short—is a temporal logic. It is, in a certain sense, similar to the Computational Tree Logic (CTL), which justifies the name. In CTL, we make statements about Kripke structures, which are basically labeled transition systems. We can express properties of paths in Kripke structures, using Linear Time Logic (LTL). Formulae of LTL typically read somewhat like, *ϕ and ψ never hold in the same state,* or, *Whenever ϕ holds in a state, eventually we will reach a state, where ψ holds.* CTL can then express things such as, *From some state, there is a path that satisfies LTL-formula ϕ,* or, *All paths starting at a state satisfy LTL-formula ϕ*—with certain restrictions on ϕ. The statements expressed by CTL are rather rigorous. Instead of claiming that *all* paths or *no* path satisfy some path formula, in PCTL we can express things such as, *The probability to satisfy path formula ϕ from some state, is greater than* $1/2$. Depending on the use case, such expressions might be more appropriate. The interested reader shall refer to (Baier and Katoen, 2008) for examples on PCTL, or in-depth discussions on LTL and CTL. In this section, we will define the syntax and semantics of PCTL, and we will prove some basic propositions about PCTL.

3.1 Syntax

Let $\mathcal{A}$ be a set of atomic propositions. Then, we define the syntax of PCTL as follows.

Definition 3.1 (PCTL Syntax)**.** PCTL formulae are composed of *state formulae* and *path formulae.* The syntax for state formulae is

$$\Phi ::= a \mid \neg\Phi \mid \Phi \wedge \Phi \mid \mathbf{P}_{\bowtie r}[\Psi]$$

where $r \in [0,1]$, $\bowtie \in \{<, \leq, =, \geq, >\}$, and $a \in \mathcal{A}$. Path formulae are of the form

$$\Psi ::= \neg\Psi \mid \mathbf{X}\ (\Phi) \mid (\Phi)\ \mathbf{U}\ (\Phi) \mid (\Phi)\ \mathbf{R}\ (\Phi)$$

In fact, the **R**-operator is just an abbreviation, namely:

$$(\phi)\ \mathbf{R}\ (\psi) := \neg((\neg\phi)\ \mathbf{U}\ (\neg\psi)).$$

Therefore, it suffices to include either the negation or the **R**-operator. Later on, we will prove that we can assume that formulae are in a certain normal form, where we will not have such overlaps. For this proof, however, we found it more convenient to consider the above syntax. Other common abbreviations are:

$$\begin{aligned}\phi \vee \psi &:= \neg(\neg\phi \wedge \neg\psi)\\ \top &:= \phi \vee \neg\phi\\ \mathbf{F}\ (\phi) &:= (\top)\ \mathbf{U}\ (\phi)\\ \mathbf{G}\ (\phi) &:= \neg\mathbf{F}\ (\neg\phi).\end{aligned}$$

Remark. Note, that we could have also defined the weak until operator as $\phi\ \mathbf{W}\ \psi := ((\phi)\ \mathbf{U}\ (\psi)) \vee \mathbf{G}\ (\phi)$. However, we could not define a state formula out of this operator using the above syntax because it is not allowed to have a disjunction in a path formula. Therefore, a probabilistic weak until is rather a new operator than an abbreviation.

We will refer to the set of state formulae as $\mathcal{F}_s$ and to the set of path formulae as $\mathcal{F}_p$. Moreover, we will denote $\mathcal{L} := \mathcal{A} \cup \{\neg a \mid a \in \mathcal{A}\}$ for the set of literals. Sometimes, it will be useful to consider the subformulae of a formula. Intuitively, this is the set of all formulae in the syntactic tree of a formula. Concretely, we define

Definition 3.2 (Subformulae)**.** The set $sub(\phi)$ is recursively defined as follows

- $\phi \in sub(\phi)$
- if $\neg\psi \in sub(\phi)$ and $\psi \neq a$, then $\psi \in sub(\phi)$
- if $\psi \wedge \xi \in sub(\phi)$, then $\psi, \xi \in sub(\phi)$
- if $\psi \vee \xi \in sub(\phi)$, then $\psi, \xi \in sub(\phi)$
- if $\mathbf{P}_{\bowtie r}[\mathbf{X}\ (\psi)] \in sub(\phi)$, then $\psi \in sub(\phi)$
- if $\mathbf{P}_{\bowtie r}[(\psi)\ \mathbf{U}\ (\xi)] \in sub(\phi)$, then $\psi, \xi \in sub(\phi)$
- if $\mathbf{P}_{\bowtie r}[(\psi)\ \mathbf{R}\ (\xi)] \in sub(\phi)$, then $\psi, \xi \in sub(\phi)$

where ψ and ξ are PCTL-formulae, $a \in \mathcal{A}$, and $r \in [0,1]$.

This definition slightly deviates from the usual definition of subformulae—e.g. the one in (Brázdil, Forejt, Křetínský, and Kucera, 2008)—as typically $\neg a \in sub(\phi)$ implies $a \in sub(\phi)$. However, for our purpose the above definition is more convenient.

$sub(\phi)$ contains the subformulae in exactly the same way, as they occur in ϕ. In some cases, this purely syntactical construction is insufficient. Instead, we might need, what we will call *closure-subformulae.*

Definition 3.3 (Closure-Subformulae)**.** The set of closure-subformulae satisfies $sub^*(\phi) \supseteq sub(\phi)$ and

- if $\mathbf{P}_{\bowtie r}[\varphi] \in sub^*(\phi)$, then $\mathbf{P}_{\bowtie' r'}[\varphi] \in sub^*(\phi)$ for all r', and $\bowtie'$.

- if $\mathbf{P}_{\bowtie r}[(\psi)\ \mathbf{R}\ (\xi)] \in sub^*(\phi)$, then $\mathbf{P}_{\bowtie_1 r_1}[(\xi)\ \mathbf{U}\ (\psi \wedge \xi)] \in sub^*(\phi)$, and $\mathbf{P}_{\bowtie_2 r_2}[\mathbf{G}\ (\xi)] \in sub^*(\phi)$, for all r_1, r_2, and $\bowtie_1, \bowtie_2$.

The set $sub^*(\phi)$ is in some sense a closure of $sub(\phi)$, as it shall not only contain the subformulae as they occur in ϕ, but additionally include the probabilistic operators with all possible probabilities.

3.2 Semantics

PCTL formulae are evaluated over Markov chains. However, all of the mentioned temporal logics require some sort of labeling of the states. Intuitively, the labels express, which formulae hold at a state. Hence, we will extend our notion of Markov chains by labeling the states.

Definition 3.4 (Labelled Markov chain)**.** A labeled Markov chain is a tuple $M := (S, P, L)$, where $MC := (S, P)$ is a Markov chain, and $L : S \to 2^{\mathcal{F}_s}$ is a labeling function.

In literature, the signature of L is often different from ours. Instead of labeling the states with state formulae, one could also assign atomic propositions; i.e. $L : S \to 2^{\mathcal{A}}$—see (Brázdil, Forejt, Křetínský, and Kucera, 2008). Due to the definition of PCTL semantics, which follows next, there is not much difference between those seemingly different notions of labels. We will assign state formulae because this will help us to manipulate models more easily, which we will have to do quite frequently. We can define the semantics of PCTL as follows

Definition 3.5 (PCTL Semantics)**.** Let M be a labeled Markov chain, $s \in S$, $a \in \mathcal{A}$, $\phi, \psi \in \mathcal{F}_s$, and $\varphi \in \mathcal{F}_p$. We define the modeling relation $\models$ as follows

(MS1) $M, s \models a$ iff $a \in L(s)$.

(MS2) $M, s \models \neg\phi$ iff $M, s \not\models \phi$.

(MS3) $M, s \models \phi \wedge \psi$ iff $M, s \models \phi$ and $M, s \models \psi$.

(MS4) $M, s \models \mathbf{P}_{\bowtie r}[\varphi]$ iff $Pr(\{\pi \in Cyl(s) \mid \pi \models_p \varphi\}) \bowtie r$.

Here, $\models_p$ is the satisfaction relation for path formulae, i.e.

(MP1) $\pi \models_p \neg\varphi$ iff $\pi \not\models_p \varphi$.

(MP2) $\pi \models_p \mathbf{X}\ (\phi)$ iff $M, \pi[1] \models \phi$.

(MP3) $\pi \models_p (\phi)\ \mathbf{U}\ (\psi)$ iff there is an $i \in \mathbb{N}_0$, such that $M, \pi[i] \models \psi$ and for all $j < i$, $M, \pi[j] \models \phi$.

(MP4) $\pi \models_p (\phi)\ \mathbf{R}\ (\psi)$ iff $\pi \not\models_p (\neg\phi)\ \mathbf{U}\ (\neg\psi)$.

M is a model, if for all formulae $\xi \in \mathcal{F}_s$, and all states $t \in S$, $\xi \in L(t)$ iff $M, t \models \xi$.

We will call M a model for ϕ, if M is a model and $\phi \in L(s)$ for some s. In fact, the definition for models is slightly less technical if one labels only atomic propositions instead of state formulae, as described above. In that case, the condition for proper labeling can be omitted, and a model for ϕ is any Markov chain M, such that

$M, s \models \phi$. One might wonder, why we, nevertheless, decided for our notion of labeling although it adds unnecessary overhead. This overhead will pay off in later definitions and proofs. The intuitive reason for this is that the modeling relation cannot be modified without performing non-trivial manipulations to the whole Markov chain. The labeling, on the other hand, can be easily adjusted. In subsequent chapters, we will introduce a slightly modified notion of models that will allow us to do so.

Remark. At this point, we want to make a remark on the sets sub, sub^*, and L. In some of our proofs, we will use conditions that assume those to be multi-sets. For the subformulae, this means that if the same subformula occurs several times in a formula, then it will also occur that many times in the sets sub and sub^*. Unless explicitly stated differently, we will assume that whenever we remove a formula from L, we remove only one specific instance of this formula. It will be clear from the context, which one is to be removed.

Before we can continue reasoning about PCTL formulae, we first have to argue that the satisfaction relation is measurable. Our proof is just a slight variation of the proof found in (Baier and Katoen, 2008).

Proposition 3.6 (Measurability of PCTL-events). *For Markov chain M, a state $s \in S$, and a path formula $\varphi \in \mathcal{F}_p$, $E_\varphi := \{\pi \in Cyl(s) \mid \pi \models \varphi\} \in \mathfrak{E}$.*

Proof. All we have to show here is that E_φ can be described in terms of countable unions of events or complements thereof. We will apply structural induction over φ.

I $\varphi = \neg\vartheta$. By induction hypothesis, $E_\vartheta \in \mathfrak{E}$. Then $E_\varphi = \overline{E_\vartheta} \in \mathfrak{E}$.

II $\varphi = \mathbf{X}\ (\psi)$. Let $T := \{t \in post(s) \mid M, t \models \psi\}$. If there is no path formula in ψ, then it is clear that the set T is well defined. If ψ does contain a path formula, this is due to the induction hypothesis. Now, $E_\varphi = \bigcup_{t \in T} Cyl(st) \in \mathfrak{E}^M$.

III $\varphi = (\psi)\ \mathbf{U}\ (\xi)$. For an integer $n \in \mathbb{N}$, let $paths^n(s)$ be the set of paths from s of length n and $E^n_\varphi := \{\rho \in paths^n(s) \mid \rho \models \varphi\}$. Obviously, $E_\varphi = \bigcup_{n \in \mathbb{N}} E^n_\varphi$. Hence, we only have to argue that all E^n_φ are measurable. Let $F := \{\rho \in paths^n(s) \mid \exists k \leq n. M, \rho[k] \models \xi \land \forall j < k. M, \rho[j] \models \psi\}$. We can determine whether $M, t \models \xi$ or not (and similarly for ψ), due to the induction hypothesis. Then, $E^n_\varphi = \bigcup_{\rho \in F} Cyl(\rho)$.

□

Next, we will introduce the satisfiability problem, which is the main topic of the thesis.

Definition 3.7 (The Satisfiability Problem for PCTL). A formula $\phi \in \mathcal{F}_s$ is called (finitely) satisfiable, if there is a (finite) model for ϕ and (finitely) unsatisfiable otherwise. The (finite) satisfiability problem is to determine, whether or not a formula is (finitely) satisfiable.

A solution has already been given for the bounded satisfiability problem (Bertrand, Fearnley, and Schewe, 2012); i.e. given a formula ϕ and an integer n, one can determine, whether or not there is a model for ϕ that has at most n states. Due to this, it suffices to determine the maximum required size for a model of some formula in order to be able to find a finite model. Therefore, our main goal will be to find bounds for formulae. For this, we will introduce general methods, which can be applied to rather general formulae, as well as specialized methods that will help us solve the problem for specific formulae only.

Earlier, we mentioned that we will most of the time consider unfolded Markov chains. For this, we first need to properly extend the labeling function and show that the resulting chain is still a model for the same formulae. Luckily, this is straight forward. For a labeled Markov chain M, we define the unfolded Markov chain $T_M := (S^+, P', L')$, where P' is defined as usual and for all $\rho \in S^*$ and $s \in S$, $L'([s]) = L(s)$. Here, $[s]$ denotes the equivalence class according to the equivalence relation $\sim$; i.e. $[s] := \{\rho s \in S^+\}$. The following proposition states that T_M behaves as expected.

Proposition 3.8. *Let T_M, be the unfolding of a model M. Then, T_M is a model itself.*

Proof. We will show that $\psi \in L'([s])$ iff $T_M, [s] \models \psi$, by induction over the structure of ψ.

I $\psi = a$. Then, $a \in L'([s])$ iff $T_M, [s] \models a$ is due to the definition of models.

II $\psi = \neg\xi$. Then, $\neg\xi \in L(s)$ iff $M, s \not\models \xi$ iff $\xi \notin L(s) = L'([s])$. Moreover, from the induction hypothesis follows that $\xi \in L'([s])$ iff $T_M, [s] \models \xi$. Finally, $\neg\xi \in L'([s])$ iff $T_M, [s] \models \neg\xi$.

III $\psi = \xi \wedge \zeta$. Then, $\xi \wedge \zeta \in L(s)$ iff $M, s \models \xi$ and $M, s \models \zeta$, and therefore, $\xi, \zeta \in L(s) = L'([s])$. From the induction hypothesis follows that $\xi, \zeta \in L'(\rho s)$ iff $T_M, [s] \models \xi$ and $T_M, [s] \models \zeta$, and thus, $T_M, [s] \models \xi \wedge \zeta$. Finally, it follows that $\xi \wedge \zeta \in L'([s])$ iff $T_M, [s] \models \xi \wedge \zeta$.

IV $\psi = \mathbf{P}_{\bowtie r}[\varphi]$. Then, $\mathbf{P}_{\bowtie r}[\varphi] \in L(s) = L'([s])$ iff $M, s \models \mathbf{P}_{\bowtie r}[\varphi]$. From proposition 2.3 we know that $Pr_{T_M}(E_\varphi) = Pr_M(f(E_\varphi))$. Therefore, $Pr_M(f(E_\varphi)) \bowtie r$ iff $Pr_{T_M}(E_\varphi) \bowtie r$ iff $T_M, [s] \models \mathbf{P}_{\bowtie r}[\varphi]$.

□

3.3 Normal Form

In order to reason about formulae, it is helpful to transform them into some normal form which is easier to handle, first. For this, we shall define the notion of equivalence of PCTL formulae.

Definition 3.9 ((Finite) Equivalence)**.** Let $\phi, \psi \in \mathcal{F}_s$. We say that ϕ is (finitely) equivalent to ψ and write $\phi \equiv \psi$ (or $\phi \equiv_{fin} \psi$, resp.), if for every (finite) model $M := (S, P, L)$, and every state $s \in S$, $\phi \in L(s)$ iff $\psi \in L(s)$.

We will also use the notation $\phi \Rightarrow \psi$ and $\phi \Rightarrow_{fin} \psi$ to express that every (finite) model for ϕ is also a model for ψ.

We will now prove a first proposition about PCTL formulae that will simplify our proofs later on. It is sometimes inconvenient to consider the syntax, as we introduced it before. In particular, negations and comparison operators other than $>$ or $\geq$, can be hard to handle. The following proposition allows us to consider formulae of a certain normal form.

Proposition 3.10 (Normalization)**.** *Every PCTL-formula is equivalent to a formula of the form*

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[\Psi]$$
$$\Psi ::= \mathbf{X}\ (\Phi) \mid (\Phi)\ \mathbf{U}\ (\Phi) \mid (\Phi)\ \mathbf{R}\ (\Phi)$$

where $a \in \mathcal{A}$, $r \in [0,1]$, and $\rhd \in \{>, \geq\}$.

Proof. Let $\phi \in \mathcal{F}_s$. We apply induction over $n := |\phi|$. For $n = 1$, $\phi = a$, and therefore is normalized already. Assume $n = n' + 1$. Now we have to distinguish several cases.

I $\phi = \neg\psi$.
Consider the following subcases.

(a) $\psi = a$. Since $\neg a$ is in the normal form, there is nothing to show.

(b) $\psi = \xi \wedge \zeta$. From the definition, it immediately follows that $\neg(\xi \wedge \zeta) \equiv \neg\xi \vee \neg\zeta$. Since $|\neg\xi| \leq n'$ and $|\neg\zeta| \leq n'$, it follows from the induction hypothesis, that there are normalized ξ' and ζ', with $\xi' \equiv \neg\xi$, and $\zeta' \equiv \neg\zeta$. Then, $\neg\psi \equiv \xi' \vee \zeta'$ is normalized.

(c) $\psi = \mathbf{P}_{>r}[\varphi]$. Let $M, s \models \neg\psi$. Then, $M, s \not\models \mathbf{P}_{>r}[\varphi]$. Hence, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \varphi\}) \leq r$. Thus, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \neg\varphi\}) \geq 1 - r$, and this means that $M, s \models \mathbf{P}_{\geq 1-r}[\neg\varphi]$. If $\varphi = \mathbf{X}\ (\xi)$, then $\neg\varphi \equiv \mathbf{X}\ (\neg\xi)$. If $\varphi = (\zeta)\ \mathbf{U}\ (\vartheta)$, then $\neg\varphi \equiv (\neg\zeta)\ \mathbf{R}\ (\neg\vartheta)$. As $|\xi| \leq n'$, $|\zeta| \leq n'$, and $|\vartheta| \leq n'$, there exists a normalized $\xi' \equiv \neg\xi$, or normalized $\zeta' \equiv \neg\zeta$, and $\vartheta' \equiv \neg\vartheta$, respectively. In any case, there is a normalized $\varphi' \equiv \neg\varphi$, so $\neg\psi \equiv \mathbf{P}_{\geq 1-r}[\varphi']$ is normalized, too.

(d) $\psi = \mathbf{P}_{\geq r}[\varphi]$. Analogous to Ic we obtain a normalized φ', such that $\neg\psi \equiv \mathbf{P}_{>1-r}[\varphi']$.

(e) $\psi = \mathbf{P}_{<r}[\varphi]$. Let $M, s \models \neg\psi$. Then, $M, s \not\models \mathbf{P}_{<r}[\varphi]$. Thus, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \varphi\}) \geq r$, and $M, s \models \mathbf{P}_{\geq r}[\varphi]$. From the induction hypothesis follows that $\neg\psi \equiv \mathbf{P}_{\geq r}[\varphi']$, where φ' is in the normal form.

(f) $\psi = \mathbf{P}_{\leq r}[\varphi]$. Similar to Ie, we obtain a normalized $\varphi' \equiv \varphi$, such that $\neg\psi \equiv \mathbf{P}_{>r}[\varphi']$.

(g) $\psi = \mathbf{P}_{=r}[\varphi]$. Obviously, $\psi \equiv \mathbf{P}_{\geq r}[\varphi] \wedge \mathbf{P}_{\leq r}[\varphi]$. Thus, $\neg\psi \equiv \neg\mathbf{P}_{\geq r}[\varphi] \vee \neg\mathbf{P}_{\leq r}[\varphi]$. And then, Id and If yield normalized φ_1 and φ_2, such that $\neg\mathbf{P}_{\geq r}[\varphi] \equiv \mathbf{P}_{>1-r}[\varphi_1]$ and $\neg\mathbf{P}_{\leq r}[\varphi] \equiv \mathbf{P}_{>r}[\varphi_2]$. Finally, this means $\neg\psi \equiv \mathbf{P}_{>1-r}[\varphi_1] \vee \mathbf{P}_{>r}[\varphi_2]$.

II $\phi = \psi \wedge \xi$. Since $|\psi| \leq n'$, and $|\xi| \leq n'$, induction hypothesis yields normalized $\psi' \equiv \psi$, and $\xi' \equiv \xi$. Therefore, $\phi \equiv \psi' \wedge \xi'$ is normalized, as well.

III $\phi = \mathbf{P}_{\rhd r}[\varphi]$. By induction hypothesis, there is a $\varphi' \equiv \varphi$, where φ' is in the normal form. Then, so is $\phi \equiv \mathbf{P}_{\rhd r}[\varphi']$.

IV $\phi = \mathbf{P}_{<r}[\varphi]$. Let $M, s \models \phi$. Then, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \varphi\}) < r$. Hence, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \neg\varphi\}) > 1 - r$, and that means, $M, s \models \mathbf{P}_{>1-r}[\neg\varphi]$. Then, similar to Ic, we obtain a normalized $\varphi' \equiv \neg\varphi$. Therefore, $\phi \equiv \mathbf{P}_{>1-r}[\varphi']$ is in the normal form.

V $\phi = \mathbf{P}_{\leq r}[\varphi]$. In a similar way as in case IV, we get a normalized φ', such that $\phi \equiv \mathbf{P}_{\geq 1-r}[\varphi']$.

VI $\phi = \mathbf{P}_{=r}[\varphi]$. It is clear that $\mathbf{P}_{=r}[\varphi] \equiv \mathbf{P}_{\geq r}[\varphi] \wedge \mathbf{P}_{\leq r}[\varphi]$. Then, from III and V follows that $\mathbf{P}_{\geq r}[\varphi] \equiv \mathbf{P}_{\geq r}[\varphi_1]$, and $\mathbf{P}_{\leq r}[\varphi] \equiv \mathbf{P}_{\geq 1-r}[\varphi_2]$, where φ_1 and φ_2 are normalized. Hence, $\phi \equiv \mathbf{P}_{\geq r}[\varphi_1] \wedge \mathbf{P}_{\geq 1-r}[\varphi_2]$ is also normalized.

□

From now on, we will always assume that formulae are normalized.

4 General Model Properties

In the previous section, we introduced the syntax and semantics of PCTL, as well as the satisfiability problem. The aim of this section is to explore techniques that work for general PCTL formulae and will help us to solve the satisfiability problem for specific fragments of PCTL later on. Although not all results of this section will be important for subsequent proofs, they might still be of use for future work. The section is divided into two parts. In section 4.1, we introduce an alternative concept of models, and in section 4.2 we describe methods that can be used to normalize the shape of models for general formulae.

4.1 Hintikka Chains

In chapter 3, we introduced the notion of models with the remark that our particular way of defining it will allow us to easily manipulate the models by simply changing the labels. It is not quite that simple, though. Assume that for some model M, and formula ϕ, $\phi \in L(s)$. We define another Markov chain $M' := (S, P, L')$, with $L'(s) := L(s) \setminus \{\phi\}$, and for all other states $s \in S \setminus \{s\}$, $L'(s) = L(s)$. If $\phi \notin \mathcal{A}$, then M' violates the conditions for models, since $M', s \models \phi$, but $\phi \notin L'(s)$. This means that models are too restrictive for this kind of modification. In our proofs, however, we will frequently have to do such operations in order to get rid of unnecessary formulae. In this section, we will introduce a slightly weaker notion of models that will allow us to do so in a certain way. We will refer to them as *Hintikka chains*, since they are inspired by the Hintikka structures in (Emerson and Halpern, 1982).

Definition 4.1 (Hintikka Chain)**.** Let M be a labeled Markov chain, $s \in S$, $a \in \mathcal{A}$, and $\phi, \psi \in \mathcal{F}_s$. M is a Hintikka chain if it satisfies the following conditions.

(H1) If $a \in L(s)$, then $\neg a \notin L(s)$

(H2) If $\neg a \in L(s)$, then $a \notin L(s)$

(H3) If $\phi \wedge \psi \in L(s)$, then $\phi \in L(s)$ and $\psi \in L(s)$

(H4) If $\phi \vee \psi \in L(s)$, then $\phi \in L(s)$ or $\psi \in L(s)$

(H5) If $\mathbf{P}_{\rhd r}[\mathbf{X}\ (\psi)] \in L(s)$, then $\sum_{t \in post(s), \psi \in L(t)} P(s,t) \rhd r$

(H6) (a) If $\mathbf{P}_{>r}[(\phi)\ \mathbf{U}\ (\psi)] \in L(s)$, then $\psi \in L(s)$ or $\phi \in L(s)$ and there is a set $T \subseteq post(s)$, such that for every $t \in T$, there is a r_t, and $\rhd_t$ such that $\mathbf{P}_{\rhd_t r_t}[(\phi)\ \mathbf{U}\ (\psi)] \in L(t)$ and $p := \sum_{t \in T} P(s,t) \cdot r_t > r$ or $p = r$ and for some $t \in T, \rhd_t =>$.

(b) If $\mathbf{P}_{\geq r}[(\phi)\ \mathbf{U}\ (\psi)] \in L(s)$, then $\psi \in L(s)$ or $\phi \in L(s)$ and there is a set $T \subseteq post(s)$, such that for every $t \in T$, there is a r_t, and $\rhd_t$, such that $\mathbf{P}_{\rhd_t r_t}[(\phi)\ \mathbf{U}\ (\psi)] \in L(t)$ and $\sum_{t \in T} P(s,t) \cdot r_t \geq r$.

(H7) (a) If $\mathbf{P}_{>r}[(\phi)\ \mathbf{R}\ (\psi)] \in L(s)$, then $\phi \wedge \psi \in L(s)$ or $\psi \in L(s)$ and there is a set $T \subseteq \mathit{post}(s)$, such that for every $t \in T$, there is a r_t, and $\rhd_t$, such that $\mathbf{P}_{\rhd_t r_t}[(\phi)\ \mathbf{R}\ (\psi)] \in L(t)$ and $p := \sum_{t \in T} P(s,t) \cdot r_t > r$ or $p = r$ and for some $t \in T, \rhd_t =>$.

(b) If $\mathbf{P}_{\geq r}[(\phi)\ \mathbf{R}\ (\psi)] \in L(s)$, then $\phi \wedge \psi \in L(s)$ or $\psi \in L(s)$ and there is a set $T \subseteq \mathit{post}(s)$, such that for every $t \in T$, there is a r_t, and $\rhd_t$, such that $\mathbf{P}_{\rhd_t r_t}[(\phi)\ \mathbf{R}\ (\psi)] \in L(t)$ and $\sum_{t \in T} P(s,t) \cdot r_t \geq r$.

(H8) If $\mathbf{P}_{\rhd r}[(\phi)\ \mathbf{U}\ (\psi)] \in L(s)$, then $Pr\{\pi \in Cyl(s) \mid \exists i.\psi \in L(\pi[i]) \wedge \forall j < i.\phi \in L(\pi[j])\}) \rhd r$.

This definition is quite similar to that of models. However, unlike models, Hintikka chains do not necessarily have to contain all formulae in their labels which they actually satisfy. On the other hand, if a formula is in a label, Hintikka chains must satisfy it. So, in a sense, Hintikka chains transform a bidirectional condition into an implication. For our next definition, we shall first introduce some notation. For two formulae $\phi, \psi \in \mathcal{F}_s$, let $\psi \prec \phi$ iff $\psi \in \mathit{sub}^*(\phi)$ and $\psi \neq \phi$. Moreover, for a set $\Phi \subseteq \mathcal{F}_s$, we denote

$$\begin{aligned} \mathit{top}(\Phi) := \{\phi \in \Phi \mid \text{for all } \psi \in \Phi.(&\phi \not\prec \psi \text{ or} \\ &\psi = \phi \wedge \xi \text{ or} \\ &\psi = \phi \vee \xi)\} \end{aligned}$$

Intuitively, the set top denotes the set of temporal top formulae. We will use this set to determine which formulae can be safely omitted from the labels without violating the Hintikka conditions.

Definition 4.2 (Minimal Hintikka Chain)**.** Let M be a tree Hintikka chain, and $\phi \in \mathcal{F}_s$, such that $\phi \in L(s_0)$ for $s_0 \in S$. M is minimal with respect to ϕ if for all $s \in S$ it satisfies

(MH1) $L(s) \subseteq \mathit{sub}^*(\phi)$.

(MH2) $\bigcup_{\psi \in L(s)} \mathit{sub}^*(\psi) \subseteq \bigcup_{\psi \in L(\mathit{pre}(s))} \mathit{sub}^*(\psi)$

(MH3) For all $\mathbf{P}_{\rhd r}[(\phi)\ \mathbf{U}\ (\psi)] \in \mathit{top}(L(s))$: if $\psi \in L(s)$, then $\mathbf{P}_{\rhd' r'}[(\phi)\ \mathbf{U}\ (\psi)] \notin L(t)$, for all r', $\rhd'$, and $t \in \mathit{post}(s)$.

(MH4) For all $\mathbf{P}_{\rhd r}[(\phi)\ \mathbf{R}\ (\psi)] \in \mathit{top}(L(s))$: if $\phi \wedge \psi \in L(s)$, then $\mathbf{P}_{\rhd' r'}[(\phi)\ \mathbf{R}\ (\psi)] \notin L(t)$, for r', $\rhd'$, and $t \in \mathit{post}(s)$.

(MH5) For all $\mathbf{P}_{\rhd r}[(\phi)\ \mathbf{U}\ (\psi)] \in L(s)$: If $\mathit{sub}(\psi) \cap L(s) \neq \emptyset$, then $\psi \in L(s)$.

The definition of minimal Hintikka chains is essentially the reason why we introduced Hintikka chains at all. They utilize the freedom that Hintikka chains provide in order to get rid of unnecessary formulae. For this, we first need to specify what unnecessary actually means. Therefor, we need to specify some $\phi \in L(s_0)$ which we are interested in. This ϕ is to be satisfied—all the other formulae are only interesting if they are required to satisfy ϕ. Otherwise, they can be omitted from the labels.

(MH1) states that we do not need any formulae in the labels that do not occur as subformulae of ϕ. (MH2) states that successors only need to satisfy formulae that might have been propagated by their (unique) predecessor. Due to (MH3), we can omit **U**-formulae after having satisfied their second parameter. Similarly, (MH4) allows us to omit already satisfied **R**-formulae from the successors. We will refer to formulae that do not need to be propagated to their successors as *terminating* formulae. Accordingly, non-terminating formulae will be referred to as *propagating*. Finally, (MH5) allows us to remove subformulae of **U**-formulae, if they do not contribute to the satisfaction of the respective **U**-formula. Recall that we consider sub, sub^*, and L to be multi-sets. Therefore, if a formula occurs multiple times and one of the conditions forces it to be removed, not all instances might be affected. This is particularly important for (MH5). For instance, if a formula is a subformula of the second argument of a **U**-formula and at the same time a top formula of its own, then removing it might violate the formula of interest—namely, ϕ. Hence, it is important to keep it in the labels. We handle this case by considering multi-sets. In fact, we could have instead made a case distinction in the definition. On the other hand, multi-sets are no real overhead, so we preferred to keep the definition simple.

The following theorem makes the ideas of (minimal) Hintikka chains more explicit and proves the vague claims that were made to justify the definitions.

Theorem 4.3. *Let $\phi \in \mathcal{F}_s$. The following statements are equivalent*

1. *There is a model for ϕ.*
2. *There is a Hintikka chain for ϕ.*
3. *There is a minimal Hintikka chain for ϕ.*

Proof. We will show two equivalences: Firstly, we will show that models and Hintikka chains are equivalent. Secondly, we will show that Hintikka chains and minimal Hintikka chains are equivalent. For the latter, we basically have to show that we can minimize every Hintikka chain without affecting the Hintikka properties.

1 implies 2 Here, we will show that every model is a Hintikka chain. For this, we have to show that every condition for Hintikka chains is met by models. Let M be a model, $s \in S$, and $\psi \in L(s)$. We will show that the Hintikka conditions hold for ψ.

I $\psi = a$ or $\psi = \neg a$. In that case, only conditions (H1) and (H2) might be violated. Assume that both $a \in L(s)$ and $\neg a \in L(s)$. Then, from (MS1) and (MS2) it follows that $M, s \models a$ and $M, s \not\models a$, which is a contradiction. Hence, both conditions are met.

II $\psi = \xi \wedge \zeta$. From (MS3) it follows that $M, s \models \xi$ and $M, s \models \zeta$. From the definition of models we know that $\xi \in L(s)$ and $\zeta \in L(s)$. Hence, (H3) is met.

III $\psi = \xi \vee \zeta$. $\xi \vee \zeta \equiv \neg(\neg\xi \wedge \neg\zeta)$. Thus, $\neg\xi \wedge \neg\zeta \notin L(s)$. That means that $\xi \in L(s)$ or $\zeta \in L(s)$. So, condition (H4) is met.

IV $\psi = \mathbf{P}_{\rhd r}[\mathbf{X}\ (\xi)]$. Then, $Pr\{\pi \in Cyl(s) \mid \pi \models_p \mathbf{X}\ (\xi)\}) \rhd r$. Hence, there must be successors $T \subseteq post(s)$, such that $\xi \in L(t)$ for all $t \in T$, and $\sum_{t \in T} P(s,t) \rhd r$. This is exactly condition (H5).

V $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{U}\ (\zeta)]$. From (MS4) it immediately follows that (H8) is met. Moreover, it must either be the case that $\zeta \in L(s)$ already, or some of the successors must also satisfy $\mathbf{P}_{\rhd' r'}[(\xi)\ \mathbf{U}\ (\zeta)]$ for some $\rhd'$, and r'. In fact, one can easily see that it is exactly condition (H6) that has to be satisfied.

VI $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{R}\ (\zeta)]$. Since $(\xi)\ \mathbf{R}\ (\zeta) \equiv \neg((\neg\xi)\ \mathbf{U}\ (\neg\zeta))$, in order to satisfy $(\xi)\ \mathbf{R}\ (\zeta)$, a path must not satisfy $(\neg\xi)\ \mathbf{U}\ (\neg\zeta)$. For this, it must either be the case that ζ is always satisfied, or else $\neg\xi$ must be violated before $\neg\zeta$ has been satisfied. This means that $\xi \wedge \zeta$ must hold at some point and ζ must hold before. From this, it follows that $(\xi)\ \mathbf{R}\ (\zeta) \equiv (\zeta)\ \mathbf{U}\ (\xi \wedge \zeta) \vee \mathbf{G}\ (\zeta)$. From a similar discussion as in the above case follows that (H7) must hold.

2 implies 1 Let M be a Hintikka chain. We will show that we can extend the labeling to obtain a model for ϕ. Let $s \in S$, and $\psi \in L(s)$. We apply induction over ψ, in order to show that $M, s \models \psi$.

I $\psi = a$.
Then, due to (MS1), $M, s \models a$.

II $\psi = \neg a$.
Then, due to (H2), $a \notin L(s)$. Hence, because of (MS1) $M, s \not\models a$, and due to (MS2) $M, s \models \neg a$.

III $\psi = \xi \wedge \zeta$.
Then, (H3) implies $\xi \in L(s)$ and $\zeta \in L(s)$. From the induction hypothesis follows that $M, s \models \xi$ and $M, s \models \zeta$, thus $M, s \models \xi \wedge \zeta$.

IV $\psi = \xi \vee \zeta$.
Due to (H4), $\xi \in L(s)$ or $\zeta \in L(s)$. Induction hypothesis yields $M, s \models \xi$ or $M, s \models \zeta$. Thus $M, s \not\models \neg\xi \wedge \neg\zeta$, and that means $M, s \models \neg(\neg\xi \wedge \neg\zeta) = \xi \vee \zeta$.

V $\psi = \mathbf{P}_{\rhd r}[\mathbf{X}\ (\xi)]$.
Let $T := \{t \in post(s) \mid \xi \in L(t)\}$. From (H5) follows that $\sum_{t \in T} P(s,t) \rhd r$. From the induction hypothesis follows that for all $t \in T$, $M, t \models \xi$, and therefore $M, s \models \mathbf{P}_{\rhd r}[\mathbf{X}\ (\xi)]$.

VI $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{U}\ (\zeta)]$.
Let $\mathcal{B} := \{\pi \in Cyl(s) \mid \exists i.(\zeta \in L(\pi[i]) \wedge \forall j < i.\xi \in L(\pi[j]))\}$. From (H8) follows that $Pr(\mathcal{B}) \rhd r$. Induction hypothesis yields that for all states $t \in S$, $\zeta \in L(t)$ implies $M, t \models \zeta$, and similarly $\xi \in L(t)$ implies $M, t \models \xi$. Finally, that means $M, s \models \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{U}\ (\zeta)]$.

VII $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{R}\ (\zeta)]$.
Recall that $(\xi)\ \mathbf{R}\ (\zeta) \equiv (\zeta)\ \mathbf{U}\ (\xi \wedge \zeta) \vee \mathbf{G}\ (\zeta)$. (H7) guarantees that either $\xi \wedge \zeta \in L(s)$, and thus every path $\pi \in Cyl(s)$ models $(\zeta)\ \mathbf{U}\ (\xi \wedge \zeta)$. Otherwise, the condition ensures that $(\xi)\ \mathbf{R}\ (\zeta)$ is propagated properly to its successors.

Now, in order to obtain a model, we simply have to add all formulae that are satisfied to the labels.

2 iff 3 Since a minimal Hintikka chain is a Hintikka chain by definition, it only remains to show that we can always minimize a Hintikka chain for ϕ while preserving the Hintikka conditions. The minimization procedure is pretty much straight forward and thus omitted here, for the sake of brevity. However, it can be found in the appendix—algorithm 1.

What we will show here is that none of the minimal Hintikka conditions contradicts the Hintikka conditions. For a Hintikka chain M, we consider the unfolding $T_M := (S', P', L')$. Recall that the definition of minimal Hintikka chains requires trees. It is clear that T_M is also a Hintikka chain.

(MH1) First, note that for some formula ψ, all Hintikka conditions require only subformulae of ψ to be satisfied at certain states. Therefore, if we remove all formulae from the labels that are not subformulae of ϕ, then we can certainly not violate any of the Hintikka conditions for any of the subformulae of ϕ.

(MH2) Also note that for a state t, no Hintikka condition requires a successor of t to satisfy some ψ, which is not a subformula of any $\xi \in L'(t)$. Therefore, it is clear that removing all formulae from labels that are not propagated by the predecessor, cannot violate the Hintikka conditions. Since T_M is a tree, we know that there is always a unique predecessor, except for the root—say s_0—which has no predecessor. The latter is important in order to preserve that $\phi \in L'(s_0)$.

(MH3) Condition (H6) requires that for some $\mathbf{P}_{\triangleright r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s)$, either $\xi \in L'(s)$, or $(\psi)\ \mathbf{U}\ (\xi)$ is propagated to the successors. Hence, if $\xi \in L'(s)$, we can safely remove $\mathbf{P}_{\triangleright' r'}[(\psi)\ \mathbf{U}\ (\xi)]$ from the successors without violating (H6) for this particular formula. However, if the formula is a subformula of another propagating formula, then we might violate Hintikka conditions. The requirement that $\mathbf{P}_{\triangleright r}[(\psi)\ \mathbf{U}\ (\xi)] \in top(L'(s))$ handles this case. Note that we need the fact that every successor has a unique predecessor, again. Otherwise, this condition might remove formulae from a state which are required in order to satisfy the propagating formulae of another predecessor. As there is only one, this cannot happen.

Since we do not remove a $\mathbf{U}$-formula unless it has been terminated already, (H8) also holds. Finally, we have to argue that the other conditions can also be met. For instance, by removing a $\mathbf{U}$-formula—even if it is in $top(L'(s))$—we might violate the conditions (H3) and (H4). Note that those cannot be subformulae of propagating ones because of the definition of $top(L'(s))$. Therefore, they cannot be required to be propagated to the successors and can safely be removed. For the other conditions, we can apply similar arguments.

(MH4) The exact same arguments as in the above case can be applied here, as well.

(MH5) Assume that some $\psi \in L'(s)$ has to be removed due to this condition. Then, there is a $\mathbf{P}_{\triangleright r}[(\xi)\ \mathbf{U}\ (\zeta)] \in L'(s)$, with $\psi \in sub^*(\zeta)$ and $\zeta \notin L'(s)$. Then, $\mathbf{P}_{\triangleright r}[(\xi)\ \mathbf{U}\ (\zeta)]$ has to be propagated anyways. Therefore, even if ψ is omitted, $\mathbf{P}_{\triangleright r}[(\xi)\ \mathbf{U}\ (\zeta)]$ can still be satisfied.

We also have to take care of the other Hintikka conditions. If omitting ψ violates any Hintikka condition for some other formula, then this formula must also be a subformula of ζ and can, thus, as well be omitted. The reason for this is that $L'(s)$ is a multi-set. Therefore, if ψ occurs as a subformula of some formula which is not itself a subformula of ζ, then ψ is considered to be a different element of the multi-set $L'(s)$ and therefore not necessarily omitted.

□

As already mentioned, Hintikka chains are sometimes easier to handle. On the other hand, we will also see proofs, where we will prefer to deal with regular models. The above result, will allow us to use the notions almost interchangeably.

4.2 General Collapsing Methods

The aim of the previous section was to improve our tools for proofs. In this part, we are going to explore methods to simplify the shapes of models for almost general formulae. By almost general formulae, we mean formulae of the following kind

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[(\Phi)\ \mathbf{U}\ (\Phi)] \mid \mathbf{P}_{\rhd r}[(\Phi)\ \mathbf{R}\ (\Phi)].$$

That is, we do not allow **X**-formulae anymore. The reason is that they might enforce rather complicated shaped models. Abstractly, the proofs in this section will read somewhat like: *Assume that we have a model or Hintikka chain. We can transform it into a simpler model or Hintikka chain that does essentially the same*. First, we will show how we can get rid of certain successors of a state. We might refer to such techniques as *horizontal* collapse methods, for they reduce the branching degree. In the second part, we will introduce the notions of *selections* and *reductions* which will enable us to reduce the height of the unfolded tree. We can, therefore, refer to this as *vertically* collapsing the model. In order to prove that a PCTL-fragment has the small model property, we will have to apply both, horizontal and vertical collapse.

4.2.1 Horizontal Collapse

Horizontal collapse is a family of methods that can be applied in order to cut off complete branches. One such method can be found in (Brázdil, Forejt, Křetínský, and Kucera, 2008) in the form of the following theorem:

Theorem 4.4. *Let $\phi \in \mathcal{F}_s$ be a satisfiable formula. Then, there is a model for ϕ, such that every state has at most $|\phi| + 2$ successors.*

A proof for this theorem is given in (Brázdil, Forejt, Křetínský, and Kucera, 2008). We will use this fact in order to show the small model property of certain fragments. Another horizontal collapse method is provided by theorem 4.5. Intuitively, it states that we do not need successors, which satisfy exactly the same formulae with the same probabilities. An obvious implication is that we do not need self loops—except if there are no other successors.

Theorem 4.5 (Collapsing by L)**.** *Let M be a model, $s \in S$ and $\phi \in L(s)$. Moreover, let*

$$post'(s) := \{t \in post(s) \mid L(t) \neq L(s)\}$$

1. *We can construct a model M', such that for all $s' \in S'$, either $|post'_{M'}(s')| = 0$ or $|post_{M'}(s') \setminus post'_{M'}(s')| = 0$, and $\phi \in L'(s')$.*
2. *We can construct a model M', such that for all $s' \in S'$, and for all $t, t' \in post_{M'}(s')$, $L'(t) \neq L'(t')$, and $\phi \in L'(s')$.*

Proof. First, we assume that there are no propagating formulae in $L(s)$—i.e. there are no **U**-formulae whose second argument is not in $L(s)$. If this is the case, then we can self loop on s with probability 1 and still satisfy $L(s)$. Obviously, both claims hold for s, then. Hence, we can assume that there is a propagating $\mathbf{P}_{\rhd r}[\varphi] \in L(s)$. We will use the following conventions throughout the proof. For a state $t \in S$, we will abbreviate $p_t := P(s,t)$ and $r_t^{\varphi} := Pr\{\pi \in Cyl(t) \mid \pi \models \varphi\})$.

Part one Let $s \in S$ be a state, where $|post'_M(s)| > 0$ and $|post_M(s) \setminus post'_M(s)| > 0$. We can assume that such a state exists. Otherwise, there is nothing to show. Let $q := \sum_{t \in post_M(s) \setminus post'_M(s)} p_t$. Note that for all $t \in post_M(s) \setminus post'_M(s)$, by definition $L(t) = L(s)$, hence $r_t^\varphi = r_s^\varphi$. Since $\mathbf{P}_{\geq r_s^\varphi}[\varphi] \in L(s)$ is a propagating formula, $r_s^\varphi = \sum_{t \in post_M(s)} p_t r_t^\varphi$. Therefore, we can compute and simplify r_s^φ as follows

$$\begin{aligned}
\sum_{t \in post'_M(s)} p_t r_t^\varphi + \sum_{t \in post_M(s) \setminus post'_M(s)} p_t r_s^\varphi &= r_s^\varphi \\
\sum_{t \in post'_M(s)} p_t r_t^\varphi + r_s^\varphi \sum_{t \in post_M(s) \setminus post'_M(s)} p_t &= r_s^\varphi \\
\sum_{t \in post'_M(s)} p_t r_t^\varphi + r_s^\varphi q &= r_s^\varphi \\
\sum_{t \in post'_M(s)} p_t r_t^\varphi &= (1-q) r_s^\varphi .
\end{aligned}$$

Besides, from the definition of Markov chains, we know that

$$\sum_{t \in post'_M(s)} p_t = 1 - q.$$

Now, our aim is to construct a model $M' := (S, P', L')$ such that $|post_{M'}(s) \setminus post'_{M'}(s)| = 0$ while $L'(s) \supseteq L(s)$. For this, we will redistribute the probabilities p_t by finding p'_t that solve the equations

$$\begin{aligned}
\sum_{t \in post'_M(s)} p'_t r_t^\varphi &= r_s^\varphi \\
\sum_{t \in post'_M(s)} p'_t &= 1.
\end{aligned}$$

We can set $p'_t := p_t/(1-q)$, and then simplify

$$\begin{aligned}
\sum_{t \in post'_M(s)} p_t \frac{1}{1-q} r_t^\varphi &= \frac{1}{1-q} \sum_{t \in post'_M(s)} p_t r_t^\varphi \\
&= \frac{1}{1-q} (1-q) r_s^\varphi \\
&= r_s^\varphi .
\end{aligned}$$

And similarly

$$\begin{aligned}
\sum_{t \in post'_M(s)} p_t \frac{1}{1-q} &= \frac{1}{1-q} \sum_{t \in post'_M(s)} p_t \\
&= \frac{1}{1-q} (1-q) \\
&= 1.
\end{aligned}$$

From this, we can immediately construct P':

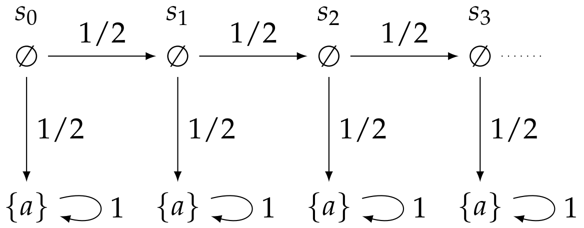

FIGURE 4.1: Example of a simple infinite model

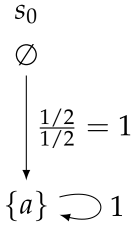

FIGURE 4.2: Reduced version of the model in figure 4.1

$$P'(s',s'') := \begin{cases} P(s',s'') & \text{if } s' \neq s \\ 0 & \text{if } s' = s \text{ and } s'' \in post_M(s) \setminus post'_M(s) \\ p_t/(1-q) & \text{if } s' = s \text{ and } s'' \in post'_M(s). \end{cases}$$

This construction guarantees that $\mathbf{P}_{\rhd r}[\varphi] \in L(s)$ implies $\mathbf{P}_{\rhd r}[\varphi] \in L'(s)$; thus $L'(s) \supseteq L(s)$. We can repeat this procedure until the desired property is satisfied.

Part two Let $s \in S$, and $t', t'' \in post_M(s)$, such that $L(t') = L(t'')$. Then, $r^\varphi_{t'} = r^\varphi_{t''}$, and thus

$$\sum_{t \in post_M(s) \setminus \{t',t''\}} p_t r^\varphi_t + p_{t'} r^\varphi_{t'} + p_{t''} r^\varphi_{t'} = \sum_{t \in post_M(s) \setminus \{t',t''\}} p_t r^\varphi_t + r^\varphi_{t'}(p_{t'} + p_{t''}).$$

P' can therefore be constructed as follows

$$P'(s',s'') := \begin{cases} P(s',s'') & \text{if } s' \neq s \text{ or } s'' \notin \{t',t''\} \\ 0 & \text{if } s' = s \text{ and } s'' = t'' \\ p_{t'} + p_{t''} & \text{if } s' = s \text{ and } s'' = t'. \end{cases}$$

Again, this procedure can be repeated to obtain a model with the desired properties while preserving satisfaction of ϕ. □

Unlike theorem 4.4, this result does not yield that the branching degree is limited in any way—not even that it is finite. Therefore, we will not use it in our proofs for small model properties. However, it might still be interesting if it comes to concrete algorithms and practical applications. In certain cases, one could even obtain a finite model from an infinite one by applying only this theorem.

Example 4.6. Consider the model in figure 4.1. It is clear that all s_i satisfy exactly the same formulae. Therefore, we can apply theorem 4.5, in order to obtain the model in figure 4.2.

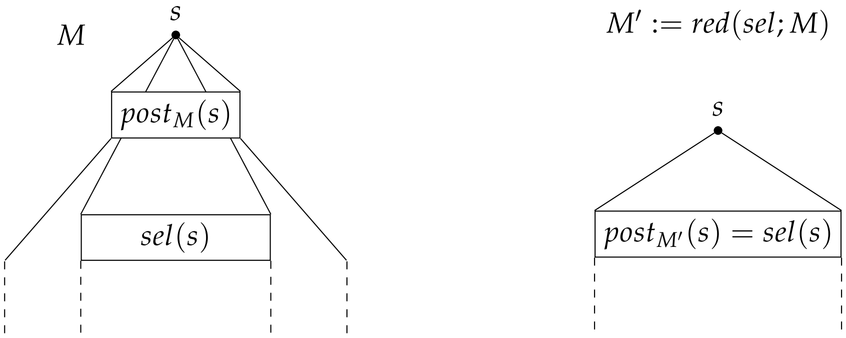

FIGURE 4.3: Illustration of reductions

4.2.2 Vertical Collapse

In this section, we are going to explore one method to reduce the height of a model. The intuitive idea behind this method is that there is no use in successors that do not terminate at least one propagating formula. Actually, the statement might sound similar to the one of theorem 4.5, though it is not quite the same. A successor might have the same propagating formulae but with different probabilities. Thus, theorem 4.5 could not be applied. Theorem 4.10 can handle this case. Instead of simply pruning the respective branch, we will rather squeeze the model vertically, in a sense. Definition 4.7 formalizes this idea of squeezing. In this entire section, we will always consider trees. On the other hand, some theorems need properties of finite chains, which trees are not. In such cases, we will assume that the tree is the unfolding of a finite chain.

Definition 4.7 (Selections and Reductions)**.** Let M be a tree, and $sel : S \to 2^S$. We call sel a selection, if for all $s \in S$, $sel(s) \subseteq post^*(s)$, and there are no $t, t' \in sel(s)$, such that $t \in pre^*(t')$ or $t' \in pre^*(t)$. If in addition $p_s := \sum_{t \in sel(s)} P^*(s,t) = 1$, then we call sel a complete selection. Given a selection sel, and a Markov chain M, we define a reduction function $red(sel; M) := M'$, where

$$P'(s,t) := \begin{cases} P^*(s,t)/p_s & \text{if } t \in sel(s) \\ 0 & \text{otherwise} \end{cases}$$

$S' := S \cap post^*_{M'}(s_0)$, and $L' := L|_{S'}$.

Intuitively, a selection can be thought of as drawing borders around fragments of a Markov chain. Then, the according reduction connects such borders directly while omitting everything in between. Figure 4.3 illustrates the procedure.

It is easy to verify that $red(sel; M)$ is a Markov chain. For a Markov chain, $\sum_{t \in post(s)} P(s,t) = 1$ must hold for all $s \in S$. This is true for $red(sel; M)$:

$$\sum_{t \in post(s)} P'(s,t) = \sum_{t \in sel(s)} P^*(s,t)/p_s = 1/p_s \cdot p_s = 1$$

Obviously, this construction does not necessarily preserve model or Hintikka properties. What it does preserve in a certain sense, are reachability probabilities.

Lemma 4.8 (Conservation of Probabilities)**.** *Let M be a Markov chain, sel a selection over M, $M' := red(sel; M)$, $s \in S'$, and $t \in post^*_{M'}(s)$. Then, $P'^*(s,t) \geq P^*(s,t)$. If the selection is complete, then $P'^*(s,t) = P^*(s,t)$.*

Proof. Let $\rho \in paths_{M'}(s) \subseteq paths_M(s)$ be the path leading from s to t. Note that we can assume that ρ is unique, since M is a tree and selections preserve this property. We will show the claim by induction over ρ.

I $\rho = st$. Then, $P'^*(s,t) = P'(s,t) \overset{def.}{=} P^*(s,t)/p_s \geq P^*(s,t)$. The last inequality follows from the fact that $p_s \in [0,1]$.

II $\rho = s\rho' t$, where $len(\rho') > 0$. Let $s' := \rho'[0]$.

$$\begin{aligned} P'^*(s,t) &= P'^*(s,s') \cdot P'^*(s',t) \\ &= P'(s,s') \cdot P'^*(s',t) \\ &\overset{def.}{=} P^*(s,s')/p_s \cdot P'^*(s',t) \\ &\geq P^*(s,s') \cdot P'^*(s',t) \\ &\overset{I.H.}{\geq} P^*(s,s') \cdot P^*(s',t) \\ &= P^*(s,t) \end{aligned}$$

If sel is a complete selection, then $p_s = 1$ for all s. Then, it is easy to see that all inequalities in the above calculations can be replaced by equalities. □

As mentioned before, reductions do not necessarily create models from models. Since this is our aim, we will now define a canonical selection, such that the reduction does preserve model properties. Let M be a model. Then, the canonical selection can be defined as follows:

$$\begin{aligned} \overline{sel}_M(s) := \{ & t \in post^*(s) \mid \\ & \text{There is a } \mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s) \text{, such that } \xi \in L(t) \\ & \text{or } \mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{U}\ (\xi)] \notin L(t) \text{, for any } \rhd' \text{ and } r', \\ & \text{and for all } t \in pre^*(t) \cap post^*(s) \text{, the above condition is violated} \} \end{aligned}$$

$$sel_M(s) := \begin{cases} \overline{sel}_M(s) & \text{if there is a propagating } \mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s) \\ post(s) & \text{otherwise} \end{cases}$$

Once again, recall the notion of propagating formulae: a $\mathbf{U}$-formula in a state is propagating if its second argument is not satisfied by that state. First, we will prove that for unfoldings of finite models, sel_M is a complete selection.

Lemma 4.9. *For the unfolding M of a finite model, sel_M is a complete selection.*

Proof. It follows immediately from the definition that $sel_M(s) \subseteq post^*(s)$, and that there are no $t, t' \in S'$, where one is the predecessor of the other. Hence, we only need to show that $p_s = 1$. If there is no propagating formula $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s)$ then there is again nothing to show, since then $sel_M(s) = post_M(s)$. Therefore, we can assume that there is a $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s)$, and $\xi \notin L(s)$. We will show the claim in two steps. First, we show that $p_s \leq 1$, and then that $p_s \geq 1$.

$p_s \leq 1$ Let $\rho_{st} \in \mathit{paths}_M(s)$ be the unique path leading from s to t. $p_s > 1$ is only possible, if there are two states $t, t' \in \mathit{sel}_M(s)$, where $\mathit{Cyl}(\rho_{st}) \cap \mathit{Cyl}(\rho_{st'}) \neq \emptyset$. This is only possible, if $t \in \mathit{pre}^*(t')$ or $t' \in \mathit{pre}^*(t)$. However, this violates the conditions for selections, and we have already argued that this condition follows from the definition. Hence, $p_s \leq 1$.

$p_s \geq 1$ Since we are talking about the unfolding of a finite model, every path ends up in the unfolding of a BSCC. In a BSCC—and so in its unfolding—every state is reached almost surely. Therefore, in order for $p_s < 1$ to hold, there must be a BSCC T that is reachable with positive probability without passing through $\mathit{sel}_M(s)$, such that $T \cap \mathit{sel}_M(s) = \emptyset$. But then, by definition of $\mathit{sel}_M(s)$, for all $t \in T$, $\mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{U}\ (\xi)] \in L(t)$, for appropriate r' and $\rhd'$. On the other hand, there is no state $t' \in T$ with $\xi \in L(t')$ for otherwise $t' \in \mathit{sel}_M(s)$. But then, $\mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{U}\ (\xi)]$ cannot be satisfied and thus M cannot be a model, which contradicts our assumption. Therefore $p_s \geq 1$. □

Note that we had to assume that the unfolding was derived from a finite models. For infinite models, not all runs must end up in BSCCs, and therefore our argument for $p_s \geq 1$ cannot be applied to those. It is easy to find an example, which shows that the lemma is indeed not true for arbitrary models; e.g. consider the model given in figure 4.6. Now, we can proceed to the important result about canonical reductions which will allow us to limit the size of certain fragments.

Theorem 4.10 (Collapsing by sel_M)**.** *For the unfolding M of a finite model, $M' := \mathit{red}(\mathit{sel}_M; M)$ is also a model, and for all $s \in S'$, $L'(s) = L(s)$.*

Proof. Let $s \in S'$, and $\psi \in L(s)$. We have to prove that either $M', s \models \psi$ or that the Hintikka conditions hold for ψ. Depending on the case, we will prefer one or the other. As we already know, this is equivalent. We apply induction over ψ.

I $\psi = a$, $\psi = \neg a$, $\psi = \xi \wedge \zeta$, or $\psi = \xi \vee \zeta$. In all of those cases, the Hintikka conditions can only be violated if $L'(s) \neq L(s)$. From definition 4.7 follows that the labels in M' are the same as in M. The rest follows from the induction hypothesis.

II $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{U}\ (\zeta)]$. Here, it is easier to prove that $M', s \models \psi$. If $\zeta \in L(s)$, then $\zeta \in L'(s)$ and we are done. Assume that $\zeta \notin L(s)$. Let $T \subseteq \mathit{post}^*_M(s)$ be the set of states that satisfy ζ and are reached from s through states that satisfy ξ. Since every state in S' is reached with the same probability as it was in M (by lemma 4.8), all we have to show is that $T \subseteq S'$. However, this follows immediately from the definition of sel_M: Since $\zeta \notin L(s)$, and for all $t \in T$, $\zeta \in L(t)$, $T \subseteq \mathit{sel}_M(s)$. Since no labels are changed and due to the induction hypothesis, all states in $\mathit{pre}^*_M(T)$, must still satisfy ξ, and all states in T must satisfy ζ.

III $\psi = \mathbf{P}_{\rhd r}[(\xi)\ \mathbf{R}\ (\zeta)]$. Again, we will prove that $M', s \models \psi$. Keep in mind that both, M and M' are trees, and that M was derived from a finite model. Thus, whenever we mention BSCCs, we actually mean the unfoldings of BSCCs. We can make some observations about BSCCs in M'. Firstly, if a state was in a BSCC in M, it can only reach other states from the same BSCC in M'. This follows immediately from the definition of selections. From lemma 4.8, we can see that the states from a BSCC in M that are included in S' are reached with the probability that this BSCC was reached with in M. Finally, we can see that for each BSCC in M, there is at least one state in S'. Otherwise, one of the other

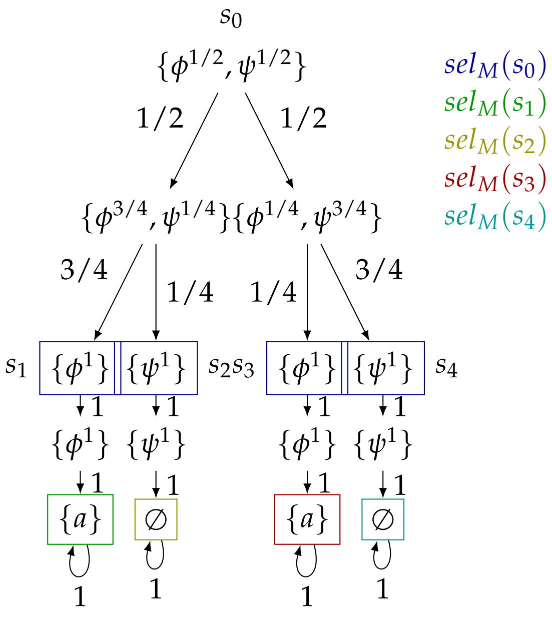

FIGURE 4.4: Example of a finite model

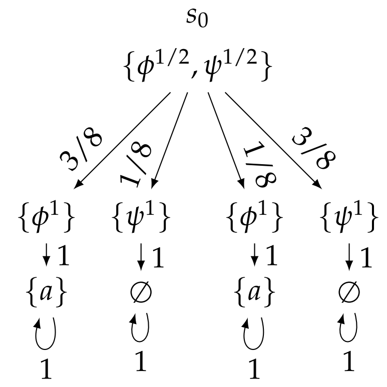

FIGURE 4.5: Collapsed version of the model in figure 4.4

BSCCs would be reached with greater probability than it was reached with in M, which contradicts our above observation.

Now, recall that (ξ) **R** $(\zeta) \equiv (\zeta)$ **U** $(\xi \wedge \zeta) \vee$ **G** (ζ). Therefore, we have to show that if $M, s \models \mathbf{P}_{\trianglerighteq_1 r_1}[(\zeta)\ \mathbf{U}\ (\xi \wedge \zeta)]$, the same holds for M' and similarly for $\mathbf{P}_{\trianglerighteq_2 r_2}[\mathbf{G}\ (\zeta)]$. The former is covered by the above cases. The latter follows from our observations on BSCCs. Finally, we conclude $M', s \models \psi$.

□

Example 4.11. Let $\phi^p := \mathbf{P}_{\geq p}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (a)])]$, and $\psi^p := \mathbf{P}_{\geq p}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\neg a)])]$. The Markov chain in figure 4.4 is a model for $\phi^{1/2} \wedge \psi^{1/2}$. The colored boxes visualize the respective selections. Figure 4.5 shows the reduced model according those selections.

This theorem alone is insufficient to limit the size of models in any way. The reason is that **U**-formulae might repeat indefinitely and thus the height of the tree can be arbitrary. If such **U**-formulae are not nested, we can easily get around that problem by minimizing the Hintikka chain according to theorem 4.3. If, however,

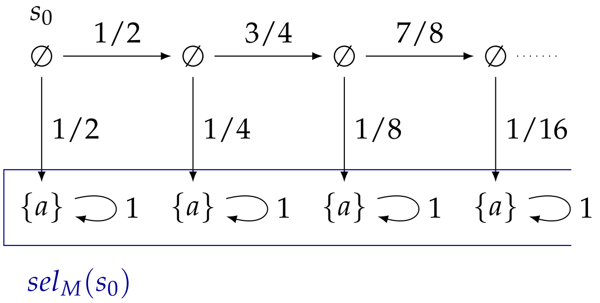

FIGURE 4.6: Example of a selection for an infinite model

such formulae are nested in **R**-formulae or **U**-formulae, this minimization will not help. One example for a model, which cannot be properly minimized that way, is given in figure 5.8. In the sections to come, we will deal with various fragments. In order to show the small model properties, we will tackle this problem of repeated **U**-formulae in different ways. Basically, we will embed the above theorem in more complex procedures in order to limit the size while preserving model properties.

Note that the only case where we had to use BSCCs was the last one. Therefore, we can extend this theorem to arbitrary models—not only finite ones—if we restrict **R**-formulae. Consider the following fragment

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[(\Phi)\ \mathbf{U}\ (\Phi)] \mid \mathbf{P}_{=1}[\mathbf{G}\ (\Phi)].$$

In this fragment we can state:

Theorem 4.12. *For the unfolding M of a model, $M' := red(sel_M; M)$ is also a model, and $L'(s) = L(s)$ for all $s \in S$.*

Proof. Again, we apply induction over the structure of $\psi \in L'(s)$, to show that $M', s \models \psi$. All of the cases are mostly identical to those in the proof for theorem 4.10, except for the case where $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. Therefore, we will only cover this case, here. Since for all $s \in S$, $sel_M(s) \subseteq post^*_M(s)$, it is clear that $post^*_{M'}(s) \subseteq post^*_M(s)$. Because M is a model, for all $t \in post^*_M(s)$, $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in L(t)$. Therefore, for all $t \in post^*_{M'}(s)$, the same is true. Moreover, since $L'(s) = L(s)$, for all $s \in S'$, and since M is a model, $\xi \in L'(s)$. Then, it follows from the induction hypothesis that $M', s \models \xi$. Finally, it follows that $M', s \models \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. □

Example 4.13. Figures 4.6 and 4.7 show an example of a selection in an infinite model and the respective reduction. In the reduction, the probabilities p_i sum up to 1. Those figures also demonstrate why we had to exclude general **R**-formulae—and thereby general **G**-formulae. As was pointed out in (Brázdil, Forejt, Křetínský, and Kucera, 2008), the chain in figure 4.6 is a model for $\phi := \mathbf{P}_{>0}[\mathbf{G}\ (\mathbf{P}_{>0}[\mathbf{F}\ (a)] \wedge \neg a)]$. However, the chain in 4.7 does not satisfy ϕ.

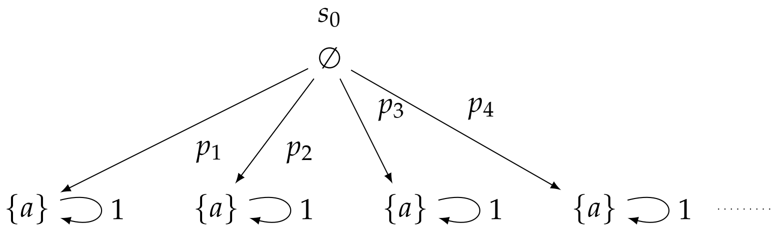

FIGURE 4.7: Reduction of the model in figure 4.7

5 PCTL Fragments

In this section, we will approach the satisfiability problem for PCTL. Our strategy will typically read as follows: *Assume that for some formula, we have an arbitrary model. Then, we can use this model to construct a model of certain shape and size.* Thus, when searching for a model of a formula, it suffices to consider only such simple models. If the size is bounded by some computable number, the satisfiability problem is solved, due to (Bertrand, Fearnley, and Schewe, 2012).

However, what if it is not possible to obtain simple models for certain formulae? What if the satisfiability problem is not even decidable for general PCTL? Even if it is, it might be a rather challenging task to find a construction that simplifies the model while preserving the model properties. In this thesis, we will focus only on few specific fragments of PCTL and solve the satisfiability problem for those. We will also present some obstacles for other fragments which one should consider when searching for solutions.

5.1 Conjunctive $\mathbf{F}_q\mathbf{G}_1$-fragment

This fragment limits PCTL in various ways. Firstly, we only allow **G**- and **F**-formulae. Secondly, only **F**-formulae are allowed to have arbitrary bounds, while **G**-formulae can only appear with probability 1. Finally, we forbid disjunctions.

Definition 5.1 (Conjunctive $\mathbf{F}_q\mathbf{G}_1$-fragment)**.** The conjunctive $\mathbf{F}_q\mathbf{G}_1$-fragment conforms to the following grammar

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \mathbf{P}_{\rhd r}[\mathbf{F}\ (\Phi)] \mid \mathbf{P}_{=1}[\mathbf{G}\ (\Phi)]$$

In the previous section, we mentioned that it might be difficult to deal with repeated **U**-formulae. In this fragment, although **F**-formulae are allowed inside of **G**-formulae, we will see that this is not a problem. Intuitively, the reason is that **F**-formulae within **G**s can be replaced by qualitative ones. This simplifies the problem considerably, as we shall see soon.

5.1.1 Solution for G-formulae

In this section, we will formalize the vague idea that was mentioned above. We will show that **G**-formulae can be transformed into a flat normal form. Concretely, we will prove the following theorem.

Theorem 5.2. *Let ϕ be a conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula. Then, the following equality holds*

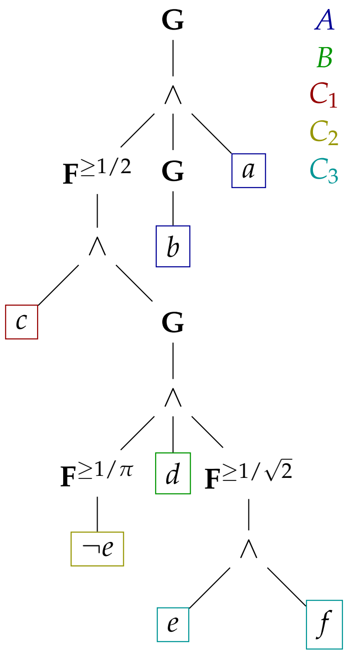

FIGURE 5.1: Example of a nested **G**-formula

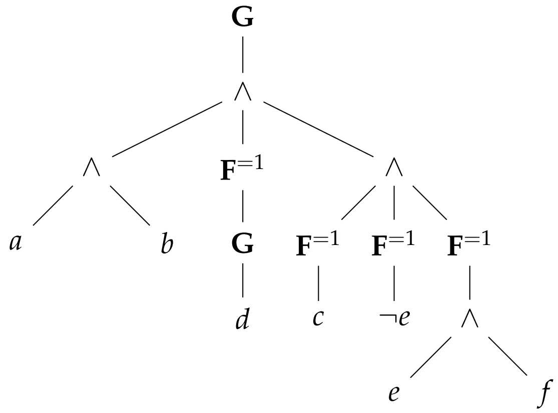

FIGURE 5.2: Normalized version of the formula in figure 5.1

$$\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \equiv_{fin} \mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l\in A} l \wedge \mathbf{P}_{=1}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l\in B} l)])] \wedge \bigwedge_{i\in I} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l\in C_i} l)])]$$

for appropriate $I \subset \mathbb{N}$, and $A, B, C_i \subset \mathcal{L}$.

Along the way, we will prove some other interesting results about **G**-formulae. The most interesting one is the fact that the finite satisfiability problem is the same as the general satisfiability problem, for those.

Example 5.3. Before we prove the theorem, we will first have a look at an example, which shall demonstrate our construction. Consider the syntactic tree in figure 5.1. The colored boxes illustrate the sets A, B, and C_i, respectively. In figure 5.2 you can see the normalized syntactic tree. Later on, we will show how to construct those sets in general.

In order to obtain a normal form, we will flatten the formulae. For this, we will consider paths in the syntactic tree. Recall that $\psi \prec \xi$, if $\psi \in sub(\xi)$ and $\psi \neq \xi$. For $n \in \mathbb{N}$, let

$$\begin{aligned} \mathfrak{P}_n :=& \{\psi_1 \dots \psi_n \mid \text{for all i } \in \{1, \dots, n-1\}. \\ & (\psi_{i+1} \prec \psi_i \text{ and } \text{ there is no } \xi.(\psi_{i+1} \prec \xi \prec \psi_i))\} \\ \mathfrak{P} :=& \bigcup_{n \in \mathbb{N}} \mathfrak{P}_n. \end{aligned}$$

Intuitively, $\mathfrak{P}$ denotes the set of all possible paths in all possible syntactic trees. In the subsequent proofs, we will apply induction over elements of this set—i.e. over the depth of a given formula. The following theorem shows a fundamental property of this fragment and is important for the solution thereof.

Theorem 5.4. *Let M be a model, ϕ a conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula, and $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$, for some $s_0 \in S$. Then, for every $\psi \in sub(\phi)$, and $s \in S$, there is a state $t \in post^*(s)$, such that $\psi \in L(t)$.*

Proof. Let $\psi_1 \dots \psi_n \in \mathfrak{P}$, such that $\psi_1 = \phi$ and $\psi_n = \psi$. We apply induction over n.

I $n = 1$. Then, $\phi = \psi$ and thus for all $t \in post^*(s_0)$, $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \in L(t)$. Therefore $\psi \in L(t)$.

II $n = n' + 1$. By the induction hypothesis, there is a state $t \in post^*(s)$, such that $\psi_{n'} \in L(t)$. We have to show that there is a state $t' \in post^*(s)$, with $\psi = \psi_n \in L(t')$. Consider the following cases:

(a) $\psi_{n'} = \psi_n \wedge \xi$. Then, $\psi_n \in L(t)$.

(b) $\psi_{n'} = \mathbf{P}_{=1}[\mathbf{G}\ (\psi_n)]$. Then, $\psi_n \in L(t)$.

(c) $\psi_{n'} = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi_n)]$. Then, there must be a state $t' \in post^*(t)$, such that $\psi_n \in L(t')$.

□

From this theorem, we can immediately derive two interesting corollaries.

Corollary 5.5. *Let ϕ be a $\mathbf{F}_q\mathbf{G}_1$-formula, and M a model with $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$, for some $s_0 \in S$. Moreover, let $G := \{\psi \in sub(\phi) \mid \psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$ for some $\xi\}$. Then, there is a state, $s \in S$, such that $G \subseteq L(s)$.*

Proof. Let $s \in S$. A straight forward induction over $n := |G \setminus L(s)|$ yields the claim.

I $n = 0$. Then, we are done.

II $n = n' + 1$. Let $\psi \in G \setminus L(s)$. Due to theorem 5.4, there is a state $t \in post^*(s)$, with $\psi \in L(t)$. Since all formulae in G are $\mathbf{G}$-formulae, $G \setminus L(t) \subset G \setminus L(s)$, hence $|G \setminus L(t)| < |G \setminus L(s)|$. Now, the claim follows from the induction hypothesis.

□

That means there is a state which satisfies all $\mathbf{G}$-formulae. This fact will enable us to prove that all satisfiable $\mathbf{G}$-formulae in this fragment are finitely satisfiable. The next corollary is important for the proof of theorem 5.2.

Corollary 5.6. *Let M be finite a model, ϕ a conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula, and $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$ for some $s_0 \in S$. Then, for every BSCC $T \subseteq S$, the following holds*

1. *For all $\psi \in sub(\phi)$, there is a state $t \in T$, such that $\psi \in L(t)$.*
2. *For all $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \in sub(\phi)$, and for all states $t \in T$, $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \in L(t)$.*

Proof. Let $\psi \in sub(\phi)$, $T \subseteq S$ be a BSCC, and $t \in T$. Theorem 5.4 states that there is a $t' \in post^*(t) = T$, such that $\psi \in L(t')$. If $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$, then it is clear that for all $t' \in T$, $\psi \in L(t')$. □

This result can be reformulated as follows: Whenever we have a formula nested within a **G**, it will appear in every BSCC. The obvious implication for **G**-formulae nested within **G**s is that they will hold in every state of every BSCC. Earlier, we mentioned that **F**-formulae nested within **G**s can be replaced by qualitative ones. Corollary 5.6 justifies this claim. However, theorem 5.2 states that we can simplify **G**-formulae even more. For this, we need some more lemmas. A rather basic one is the distributivity of **G**-formulae over conjunctions, i.e.

Lemma 5.7. *For arbitrary formulae $\phi, \psi \in \mathcal{F}_s$, $\mathbf{P}_{=1}[\mathbf{G}\ (\phi \wedge \psi)] \equiv \mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \wedge \mathbf{P}_{=1}[\mathbf{G}\ (\psi)]$.*

A proof for this is provided in the appendix—see lemma A.2, equality (A.7). Now, we will show how one can construct the **G**-normal form. For this, we first define maps $A, B, C : \mathcal{F}_s \to 2^{\mathcal{L}}$.

$$\begin{aligned}
A(\psi) := \{l\ |\exists \psi_1 \dots \psi_n \in \mathfrak{P}.(&\psi_1 = \psi \text{ and } \psi_n = l \text{ and}\\
&\nexists i \in \{1, \dots, n-1\}.(\psi_i = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi_{i+1})]))\}\\
B(\psi) := \{l\ |\exists \psi_1 \dots \psi_n \in \mathfrak{P}.(&\psi_1 = \psi \text{ and } \psi_n = l \text{ and}\\
&\exists i \in \{1, \dots, n-1\}.(\psi_i = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi_{i+1})]) \text{ and}\\
&\exists i \in \{1, \dots, n-1\}.(\psi_i = \mathbf{P}_{=1}[\mathbf{G}\ (\psi_{i+1})] \text{ and}\\
&\nexists j > i.(\psi_j = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi_{j+1})]))))\}\\
C(\psi) := \{l\ |\exists \psi_1 \dots \psi_n \in \mathfrak{P}.(&\psi_1 = \psi \text{ and } \psi_n = l \text{ and}\\
&\nexists i \in \{1, \dots, n-1\}.(\psi_i = \mathbf{P}_{=1}[\mathbf{G}\ (\psi_{i+1})]) \text{ and}\\
&\nexists i \in \{1, \dots, n-1\}.(\psi_i = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi_{i+1})]))\}.
\end{aligned}$$

Moreover, let $F(\psi) := \{\xi \in sub(\psi) \mid \xi = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\zeta)]\}$. Finally, we can define a normalization map $\mathcal{G}$ as follows:

$$\mathcal{G}(\psi) := \mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in A(\psi)} l \wedge \mathbf{P}_{=1}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B(\psi)} l)])] \wedge \bigwedge_{\xi \in F(\psi)} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l \in C(\xi)} l)])].$$

We will prove theorem 5.2 by showing the equality $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \equiv_{fin} \mathcal{G}(\phi)$. Before we can proceed, we have to look at some properties of $\mathcal{G}$ and models thereof. First, we will show that models for $\mathcal{G}(\phi)$ have a rather regular structure.

Lemma 5.8. *A finite Markov chain M is a model for*

$$\psi := \mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in A} l \wedge \mathbf{P}_{=1}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B} l)])] \wedge \bigwedge_{i \in I} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l \in C_i} l)])]$$

iff for some state $s_0 \in S$, the following conditions hold

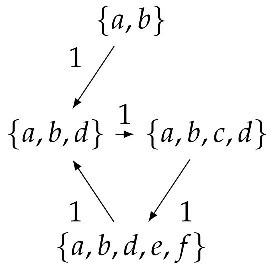

FIGURE 5.3: Model for the formula in figure 5.2

1. *For all $l \in A$, $l \in L(s_0)$ and for all $t \in post^*(s_0)$, $l \in L(t)$.*
2. *For all $l \in B$, all BSCCs T, and all $t \in T$, $l \in L(t)$.*
3. *For all $i \in I$ and all BSCCs T, there is a state $t \in T$, such that for all $l \in C_i$, $l \in L(t)$.*

Proof. We have to show two things. If all the conditions hold for some Markov chain, then the chain is a model. Otherwise, it is not.

The three conditions hold The first condition guarantees that $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in A} l)] \in L(s_0)$. Since the second condition assures that every BSCC T satisfies $l \in B$ in every state $t \in T$ it follows that $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B} l)] \in L(t)$. Since some BSCC is eventually reached almost surely, this implies that $\mathbf{P}_{=1}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B} l)])] \in L(s_0)$. The last condition assures that in every state $t \in T$ for every BSCC T it holds that $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{i \in I} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l \in C_i} l)])] \in L(t)$. Again, this implies that $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{i \in I} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l \in C_i} l)])] \in L(t)$. From lemma 5.7 it follows that $\psi \in L(s_0)$.

One of the conditions does not hold We will show that each of the conditions is required for models. For this, we will assume that one is violated and deduce that the Markov chain cannot be a model then.

Condition 1 is violated That means there is a state $s \in post^*(s_0)$, such that for some $l \in A$, $l \notin L(s)$. But then $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in A} l)] \notin L(s_0)$, and therefore $\psi \notin L(s_0)$ (which again follows from lemma 5.7).

Condition 2 is violated In that case there must exist a BSCC T reachable from s_0, such that there is a state $t \in T$, with $l \notin L(t)$ for some $l \in B$. Since every state in a BSCC is reached infinitely often once the BSCC is reached, $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B} l)] \notin L(t')$, for any state $t' \in T$, and therefore $\mathbf{P}_{=1}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{l \in B} l)])] \notin L(s_0)$. Hence, due to lemma 5.7, $\psi \notin L(s_0)$.

Condition 3 is violated If for some BSCC T, there is a C_i, such that for all $t \in T$, there is a $l \in C_i$, such that $l \notin L(t)$, then once this BSCC is reached $\bigwedge_{l \in C_i} l$ will never hold. Therefore, $\mathbf{P}_{=1}[\mathbf{G}\ (\bigwedge_{i \in I} \mathbf{P}_{=1}[\mathbf{F}\ (\bigwedge_{l \in C_i} l)])] \notin L(s_0)$ and then, due to lemma 5.7, $\psi \notin L(s_0)$. □

Example 5.9. Consider our previous example in figure 5.2. Figure 5.3 shows a model for this formula. One can see how the states reflect the sets A, B, and C_i.

This lemma and corollary 5.6 enable us to easily prove $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \Rightarrow_{fin} \mathcal{G}(\phi)$. Moreover, it is useful for the proof of the following lemma, which will be required for the opposite implication.

Lemma 5.10. *For conjunctive* $\mathbf{F}_q\mathbf{G}_1$*-formulae* ψ *and* ξ*,* $\mathcal{G}(\psi) \wedge \mathcal{G}(\xi) \equiv_{fin} \mathcal{G}(\psi \wedge \xi)$*.*

Proof. It is easy to see that $A(\psi \wedge \xi) = A(\psi) \cup A(\xi)$, $B(\psi \wedge \xi) = B(\psi) \cup B(\xi)$, and $F(\psi \wedge \xi) = F(\psi) \cup F(\xi)$. Therefore and due to lemma 5.8, a model for $\mathcal{G}(\psi \wedge \xi)$ must satisfy $A(\psi)$ and $A(\xi)$ everywhere, satisfy $B(\psi)$ and $B(\xi)$ in every BSCC, and for every $\zeta \in F(\psi) \cup F(\xi)$, satisfy $C(\zeta)$ in at least one state in every BSCC. It immediately follows that $\mathcal{G}(\psi \wedge \xi) \Rightarrow \mathcal{G}(\psi) \wedge \mathcal{G}(\xi)$.

Similarly, from $\mathcal{G}(\psi)$ and $\mathcal{G}(\xi)$ follows that $A(\psi)$ and $A(\xi)$, respectively, must be satisfied everywhere. Therefore, $A(\psi) \cup A(\xi)$ holds everywhere. The same argument can be applied to B and F, and from lemma 5.8 follows that $\mathcal{G}(\psi) \wedge \mathcal{G}(\xi) \Rightarrow \mathcal{G}(\psi \wedge \xi)$. □

Finally, we can prove theorem 5.2.

Proof. We will show that for a conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula ϕ, $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \equiv_{fin} \mathcal{G}(\phi)$.

$\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \Rightarrow_{fin} \mathcal{G}(\phi)$ Let M be a model and $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$ for some $s_0 \in S$. We will show that the conditions of lemma 5.8 hold.

Condition 1 Let $l \in A(\phi)$. Then, there must be $\psi_1 \dots \psi_n \in \mathfrak{P}$, such that $\psi_1 = \phi$ and $\psi_n = l$. We apply induction over n to show that for all ψ_i, $\psi_i \in L(s_0)$ and for all $t \in post^*(s_0)$, $\psi_i \in L(t)$. First, note that $\phi \in L(s_0)$, and $\phi \in L(t)$, for all $t \in post^*(s_0)$, since $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$.

Now, we show that if the claim holds for ψ_i, then it does so for ψ_{i+1}. Consider the following possibilities for ψ_i.

1. $\psi_i = l$. Then, there is nothing to show since there is no ψ_{i+1}.
2. $\psi_i = \psi_{i+1} \wedge \xi$. Then, $\psi_{i+1}, \xi \in L(s_0)$. Moreover, since $\psi_i \in L(t)$, for all $t \in post^*(s_0)$, the same holds for ψ_{i+1}.
3. $\psi_i = \mathbf{P}_{=1}[\mathbf{G}\ (\psi_{i+1})]$. Then, $\psi_{i+1} \in L(s_0)$, and $\psi_{i+1} \in L(t)$, for all $t \in post^*(s_0)$.

Condition 2 We have to show that $l \in B(\phi)$ is satisfied in every state of every BSCC. Let $\psi_1 \dots \psi_n \in \mathfrak{P}$, with $\psi_1 = \phi$, and $\psi_n = l$. Moreover, let $\psi_k = \mathbf{P}_{=1}[\mathbf{G}\ (\psi_{k+1})]$, such that no $k' > k$ exists of that form —i.e. ψ_k is the deepest $\mathbf{G}$-formula with $l \prec \psi_k$. Then, from the definition of B, we know that all subformulae of ψ_k are conjunctions or literals. From corollary 5.6, we know that for every BSCC T, there is a state $t \in T$, such that $\psi_k \in L(t)$. But because of the shape of ψ_k, every subformula of ψ_k must be satisfied wherever ψ_k is satisfied. Thus, $l \in L(t)$.

Condition 3 We have to show that for every $\xi \in F(\phi)$ and every BSCC T, there is a state $t \in T$, such that for all $l \in C(\xi)$, $l \in L(t)$. According to the definition of C, the literals within $C(\xi)$ are connected with conjunctions. Let $\zeta := \bigwedge_{l \in C(\xi)} l$. Corollary 5.6 implies that there is a state $t \in T$, such that $\zeta \in L(t)$. Therefore, for every $l \in C(\xi)$, $l \in L(t)$.

$\mathcal{G}(\phi) \Rightarrow_{fin} \mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$ Let M be a model, and $\mathcal{G}(\phi) \in L(s_0)$, for some $s_0 \in S$. We apply induction over ϕ.

I $\phi = a$. Then, $\mathcal{G}(\phi) = \mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$.

II $\phi = \psi \wedge \xi$. From lemma 5.10, we know that $\mathcal{G}(\psi \wedge \xi) \equiv_{fin} \mathcal{G}(\psi) \wedge \mathcal{G}(\xi)$. By the induction hypothesis follows that $\mathcal{G}(\psi) \wedge \mathcal{G}(\xi) \Rightarrow_{fin} \mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \wedge \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$, and finally, lemma 5.7 yields $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \wedge \mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \equiv \mathbf{P}_{=1}[\mathbf{G}\ (\psi \wedge \xi)]$.

III $\phi = \mathbf{P}_{=1}[\mathbf{G}\ (\psi)]$. It is clear from the definitions that $\mathcal{G}(\mathbf{P}_{=1}[\mathbf{G}\ (\psi)]) = \mathcal{G}(\psi)$. By the induction hypothesis it follows that $\mathcal{G}(\psi) \Rightarrow_{fin} \mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \equiv \mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\psi)])]$. The last equality follows from lemma A.1, which can be found in the appendix.

IV $\phi = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi)]$. It suffices to show that for every BSCC T, there is a state $t \in T$, such that $\psi \in L(t)$. We will apply induction over ψ. However, the current claim is too weak in order to cover the case $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. For this, we have to make the claim stronger in the following way: 1) For every $\mathbf{P}_{\rhd' r'}[\mathbf{F}\ (\xi)] \in sub(\psi)$, and for every BSCC T, there is a state $t \in T$, such that $\xi \in L(t)$. 2) For every $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in sub(\psi)$, BSCC T, and state $t \in T$, $\xi \in L(t)$. Now we can apply the induction.

(a) $\psi = l$. Then, by construction $l \in C(\phi)$, and therefore the claim holds.

(b) $\psi = \xi \wedge \zeta$. There are different subcases to consider.

i. $\xi = l_1$, and $\zeta = l_2$. In that case, both $l_1, l_2 \in C(\phi)$, by construction. Hence, there is a state that satisfies both.

ii. $\xi = \mathbf{P}_{=1}[\mathbf{G}\ (\vartheta)]$. Then, by the induction hypothesis follows that every state of every BSCC satisfies ξ. Moreover, from the induction hypothesis follows that in every BSCC, there is a state that satisfies ζ. Then, this state satisfies ψ.

iii. $\xi = \mathbf{P}_{\rhd' r'}[\mathbf{F}\ (\vartheta)]$. By the induction hypothesis, there is a state in every BSCC that satisfies ξ. But this means that there is a state in every BSCC that satisfies ϑ. Due to the BSCC properties, this state is reached almost surely from every other state within the same BSCC, and therefore every state in a BSCC satisfies ξ. Again, from the induction hypothesis it follows that there is a state that satisfies ζ. This state satisfies ψ.

(c) $\psi = \mathbf{P}_{\rhd' r'}[\mathbf{F}\ (\xi)]$. Then, by the induction hypothesis, there is a state for each BSCC that satisfies ξ, and thereby ψ.

(d) $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. Here, we need to distinguish several subcases again.

i. $\xi = l$. Then, by construction $l \in B(\phi)$, and thus the claim holds.

ii. $\xi = \zeta \wedge \vartheta$. By lemma 5.7 $\mathbf{P}_{=1}[\mathbf{G}\ (\zeta \wedge \vartheta)] \equiv \mathbf{P}_{=1}[\mathbf{G}\ (\zeta)] \wedge \mathbf{P}_{=1}[\mathbf{G}\ (\vartheta)]$. Then, by the induction hypothesis, the claim holds for both conjuncts, and hence for the conjunction.

iii. $\xi = \mathbf{P}_{=1}[\mathbf{G}\ (\zeta)]$. Then, the claim immediately follows from the induction hypothesis.

iv. $\xi = \mathbf{P}_{\rhd r''}[\mathbf{F}\ (\zeta)]$. By the induction hypothesis, for every BSCC, there is a state that satisfies ζ. The properties of BSCCs provide that ξ holds in every state of such a BSCC.

□

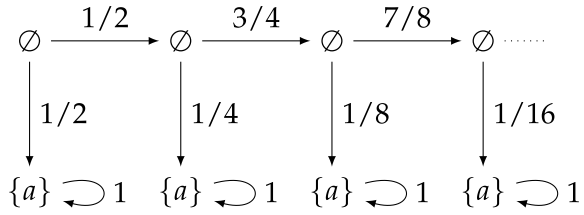

FIGURE 5.4: Counterexample for equality (5.1)

From theorem 5.2 we can derive a method for the construction of models for **G**-formulae. Let ϕ be a **G**-formula and M, with $S := \{s_\psi \mid \psi \in F(\phi)\}$, and $L(s_\psi) := A(\phi) \cup B(\phi) \cup C(\psi)$. Moreover, let P be an arbitrary transition function that generates a BSCC from S; e.g. P might create a circle out of all states.

Corollary 5.11. *If L is a valid labeling, then M can be extended to a model for ϕ. Otherwise ϕ is unsatisfiable.*

Proof. From theorem 5.2 follows that $\phi \equiv \mathcal{G}(\phi)$. Lemma 5.8 yields that all BSCCs in models for ϕ must be of the form of M. Therefore, if L is not a valid labeling, there cannot be a model for ϕ. If it is a valid labeling, then M satisfies the conditions in lemma 5.8 and therefore can be transformed into a model for ϕ by adding the missing labels. □

There are some interesting facts about the normal form. We have proven that a **G**-formula is *finitely* equivalent to its normal form. We heavily relied on the properties of finite models—namely, that they always end up in BSCCs. Now, one might wonder, if it was really necessary to do this. Would it not have been possible to prove general equality with a more sophisticated technique? From the above proof, it is not obvious whether or not we could do this. In the appendix, we provide an alternative proof for the normal form which shows the equivalence in a more straight forward—yet also more technical—way. Along with various general equalities, we also provide a proof for the following finite equality

$$\mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi)])] \equiv_{fin} \mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (\psi)])]$$

For the proof, we again use BSCCs. In this case, we can give a concrete counterexample for the general equality

$$\mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi)])] \equiv \mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (\psi)])] \tag{5.1}$$

The infinite Markov chain given in figure 5.4 is a model for $\mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{>0}[\mathbf{F}\ (a)])]$, yet it does not model $\mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (a)])]$. Therefore, this model is also a counterexample for the general equality for the normal form. This chain is also a possible model for a satisfiable PCTL formula, which is not finitely satisfiable (Brázdil, Forejt, Křetínský, and Kucera, 2008). However, it is obvious that the above formulae are both finitely satisfiable. In fact, we will show that all satisfiable **G**-formulae in this fragment are finitely satisfiable.

Theorem 5.12. *Let ϕ be a $\mathbf{F}_q\mathbf{G}_1$-formulae, and M a model with $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$ for some $s_0 \in S$. Then, there is a finite model for $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$.*

Proof. Corollary 5.5 yields a state $s \in S$ which satisfies all **G**-subformulae of ϕ. Let $S' := \{s_\psi \in post^*_M(s) \mid \mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi)] \in sub(\phi) \text{ and } \psi \in L(s_\psi)\}$. Then, we construct a new Markov chain M' where $L' := L|_{S'}$ and P' generates a BSCC from S'. Obviously,

M' is finite. So, all we have to show is that $M', t_0 \models \mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$ for some $t_0 \in S'$. Let $\psi \in sub(\phi)$, and $t \in S'$, with $\psi \in L(t)$. We apply induction over the structure of ψ and show that $M', t \models \psi$.

I $\psi = a$ or $\psi = \neg a$. Nothing to show.

II $\psi = \xi \wedge \zeta$. Then, $\xi, \zeta \in L(t) = L'(t)$. Therefore, by the induction hypothesis, $M', t \models \xi$ and $M', t \models \zeta$, thus $M', t \models \xi \wedge \zeta$.

III $\psi = \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\xi)]$. Then, by the definition of S', there is a $s_\xi \in S'$, such that $\xi \in L(s_\xi)$. By the induction hypothesis, $M', s_\xi \models \xi$. Moreover, since S' is a BSCC, s_ξ is reached almost surely from t, and therefore $M', t \models \mathbf{P}_{=1}[\mathbf{F}\ (\xi)] \Rightarrow \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\xi)]$.

IV $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. Since $t \in post^*_M(s)$ by definition, and s satisfies all $\mathbf{G}$-subformulae, the same is true for all of its successors, and thus for all $t' \in post^*_{M'}(t) = S'$, $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in L'(t')$, and therefore $\xi \in L'(t')$. Then, by induction hypothesis, $M', t' \models \xi$. Finally, $M', t \models \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$.

□

There is an interesting reason why this proof works. Normally, when we have an infinite model, we cannot reason about BSCCs for they might not even exist. There exist formulae which require paths that do not end up in BSCCs. In this fragment, however, corollary 5.5 enables us to determine a state which behaves quite similar to a BSCC in that it satisfies all **G**-subformulae. By filtering out only the interesting states, we have indeed been able to obtain a BSCC from this state's subtree.

5.1.2 General Solution

Theorem 5.2 enables us to create simple models for finitely satisfiable **G**-formulae in the conjunctive $\mathbf{F}_q\mathbf{G}_1$-fragment, as we have shown in corollary 5.11. With theorem 5.12 we can, therefore, construct models for general, satisfiable **G**-formulae. In this section, we will see how those two theorems can help us to solve the satisfiability problem for general formulae of the considered fragment.

Theorem 5.13. *A satisfiable, conjunctive* $\mathbf{F}_q\mathbf{G}_1$*-formula* ϕ *has a model of size* $f(|\phi|)$*, for some computable function* f*.*

Proof. Let ϕ be a satisfiable, conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula. For a formula ψ, let

$$\hat{\psi} := \begin{cases} a & \text{if } \psi = a \\ \hat{\xi} \wedge \hat{\zeta} & \text{if } \psi = \xi \wedge \zeta \\ \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\hat{\xi})] & \text{if } \psi = \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\xi)] \\ \mathbf{P}_{=1}[\mathbf{G}\ (\overline{\xi})] & \text{if } \psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \end{cases}$$

$$\overline{\psi} := \begin{cases} a & \text{if } \psi = a \\ \overline{\xi} \wedge \overline{\zeta} & \text{if } \psi = \xi \wedge \zeta \\ a_\psi & \text{if } \psi = \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\xi)] \\ \mathbf{P}_{=1}[\mathbf{G}\ (\overline{\xi})] & \text{if } \psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \end{cases}$$

where $a_\psi \in \mathcal{A}$; that is, we replace all **F**-formulae within **G**-formulae by atomic propositions. Let M be a minimal Hintikka chain, and $\phi \in L(s_0)$, for some $s_0 \in S$. We construct $\hat{M} := (S, P, \hat{L})$ where $\hat{L}(s) := \{\hat{\psi} \mid \psi \in L(s)\}$ for all $s \in S$. Therefore,

$\hat{\phi} \in \hat{L}(s_0)$. It is easy to see that $\hat{M}$ is a Hintikka chain. Now, let $M' := red(sel_{\hat{M}}; \hat{M})$. From theorem 4.10, we know that M' is a Hintikka chain for $\hat{\phi}$. We can assume that it is minimal. We will now show how we can construct a model of limited size for ϕ out of M'.

Limited size From theorem 4.4, we know that we can always bound the branching degree to $|\phi| + 2$. We can consider states without **F**-formulae in their labels as leaves of the tree. They only have to satisfy **G**-formulae, which do not contain any **F**-formulae, by the definition of $\hat{\phi}$. Therefore, a single state suffices to satisfy those. We will now show that the height of the tree M' is bounded. For this, we will apply induction over $n := |\{\psi \in L(s) \mid \psi = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\xi)]\}|$, where $s \in S'$.

I $n = 0$. In that case, s is a leaf.

II $n = n' + 1$. By the construction of *red*, for every $t \in post_{M'}(s)$, there is a $\mathbf{P}_{\rhd r}[\mathbf{F}\ (\psi)] \in L(s)$, such that $\psi \in L(t)$. Since M' is a minimal Hintikka chain, $\mathbf{P}_{\rhd' r'}[\mathbf{F}\ (\psi)] \notin L(t')$, for any $\rhd', r'$, and $t' \in post^*_{\hat{M}}(t)$. Hence, every immediate successor of t has less **F**-formulae to satisfy —i.e. at most n'. By the induction hypothesis, the height from the immediate successors of t is therefore bounded, and so it is from t, and thus from s.

Construct a Hintikka chain for ϕ We can construct a Hintikka chain for ϕ by constructing models for the leaves of M', i.e. all states that do not contain **F**-formulae. We will refer to the resulting model as $\tilde{M}$. We construct it by first expanding every formula to its original form. Now, we construct models for every leaf by applying corollary 5.11. This is possible because M' has been constructed from a model for ϕ. Thus, every **G**-formula in the leaves is satisfiable. Theorem 5.12 yields that they are finitely satisfiable, and then due to theorem 5.2 we can normalize them.

Now, we still have to prove that the expanded **F**-formulae hold. Let $s \in \tilde{S}$, $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)] \in L(s)$, and $\mathbf{P}_{=1}[\mathbf{F}\ (\xi)] \in sub(\psi)$. We can safely limit our attention to such formulae due to theorem 5.2. $\mathbf{P}_{=1}[\mathbf{G}\ (\psi)]$ is satisfied in every BSCC reachable from s. Thus, so is $\mathbf{P}_{=1}[\mathbf{F}\ (\xi)]$. Because some BSCC is reached from s almost surely, $\mathbf{P}_{=1}[\mathbf{F}\ (\xi)]$ is satisfied at s.

Note that we started from a minimal Hintikka chain, which is by definition a tree, and thus infinite. What we called leaves, where in fact still infinite chains. However, corollary 5.11 enabled us to replace those by BSCCs, and thus obtain a finite model, in the end. □

The reduction procedure described in the proof is illustrated in figure 5.5. For a concrete example refer to example 4.11

5.2 Finite satisfiability for G-formulae within the $\mathbf{F}_q\mathbf{G}_q$-Fragment

In section 5.1.1, we have seen how one can create finite models for **G**-formulae within the conjunctive $\mathbf{F}_q\mathbf{G}_1$-Fragment. In this section, we will extend this idea to the general $\mathbf{F}_q\mathbf{G}_q$-Fragment which is defined as follows

Definition 5.14. Formulae conforming to the grammar

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[\mathbf{F}\ (\Phi)] \mid \mathbf{P}_{\rhd r}[\mathbf{G}\ (\Phi)]$$

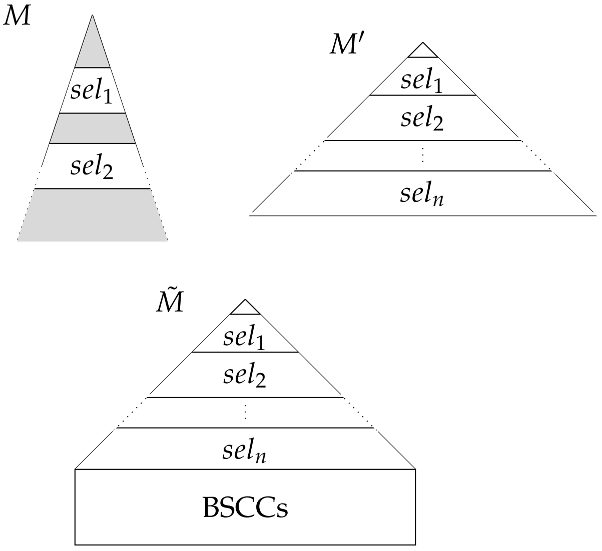

FIGURE 5.5: Reduction of models for conjunctive $\mathbf{F}_q\mathbf{G}_1$-formulae

are called $\mathbf{F}_q\mathbf{G}_q$-formulae.

Basically, we will see that the properties of BSCCs can help us to obtain a simple normal form and then simple models for **G**-formulae within this fragment. However, our results will only yield equisatisfiability, not equivalence. There is a fundamental difference between those notions: If two formulae are equivalent, then we can indeed replace one by the other within more complex formulae. For equisatisfiable formulae this is not the case. Therefore, we were not able to solve the complete $\mathbf{F}_q\mathbf{G}_q$-Fragment in the same way, as we did for the conjunctive $\mathbf{F}_q\mathbf{G}_1$-Fragment. However, in section 5.3, we will see, how this result can still help to solve formulae other than pure **G**-formulae. The following lemma formalizes the normal form.

Theorem 5.15. *Let ψ be a $\mathbf{F}_q\mathbf{G}_q$-formula. Then, $\phi := \mathbf{P}_{\triangleright r}[\mathbf{G}\ (\psi)]$ is finitely equisatisfiable to a $\mathbf{F}_1\mathbf{G}_1$-formula ϕ', such that $\phi' \Rightarrow \phi$.*

Proof. Let M be a finite model, and $\phi \in L(s_0)$, for some $s_0 \in S$. Then, there must be at least one BSCC T, and a state $t \in T$, such that $\mathbf{P}_{\triangleright' r'}[\mathbf{G}\ (\psi)] \in L(t)$. For a formula ξ, we define $\hat{\xi}$ recursively as follows

$$\hat{\xi} := \begin{cases} a & \text{if } \xi = a \\ \hat{\zeta} \wedge \hat{\vartheta} & \text{if } \xi = \zeta \wedge \vartheta \\ \hat{\zeta} \vee \hat{\vartheta} & \text{if } \xi = \zeta \vee \vartheta \\ \mathbf{P}_{=1}[\mathbf{F}\ (\hat{\zeta})] & \text{if } \xi = \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\zeta)] \\ \mathbf{P}_{=1}[\mathbf{G}\ (\hat{\zeta})] & \text{if } \xi = \mathbf{P}_{\triangleright r}[\mathbf{G}\ (\zeta)]. \end{cases}$$

Let $t \in T$, and $\xi \in L(t)$. We will show that $\hat{\xi} \in L(t)$.

I $\xi = a$. Then, $\hat{\xi} = a = \xi$, and thus there is nothing to show.

II $\xi = \zeta \wedge \vartheta$. Then, $\zeta, \vartheta \in L(t)$. By the induction hypothesis it follows that $\hat{\zeta}, \hat{\vartheta} \in L(t)$, and hence $\hat{\zeta} \wedge \hat{\vartheta} = \hat{\xi} \in L(t)$.

III $\xi = \zeta \vee \vartheta$. Then, $\zeta \in L(t)$, or $\vartheta \in L(t)$. By the induction hypothesis it follows that $\hat{\zeta} \in L(t)$, or $\hat{\vartheta} \in L(t)$, and hence $\hat{\zeta} \vee \hat{\vartheta} = \hat{\xi} \in L(t)$.

IV $\xi = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\zeta)]$. Then, there is a state $t' \in T$, such that $\zeta \in L(t')$. By the induction hypothesis, $\hat{\zeta} \in L(t')$. Since T is a BSCC, t' is reached almost surely. Therefore, $\mathbf{P}_{=1}[\mathbf{F}\ (\hat{\zeta})] = \hat{\xi} \in L(t)$.

V $\xi = \mathbf{P}_{\rhd r}[\mathbf{G}\ (\zeta)]$. Assume there was a state $t' \in T$, such that $\zeta \notin L(t')$. Since T is a BSCC, t' is reached almost surely, and therefore $\mathbf{P}_{\rhd r}[\mathbf{G}\ (\zeta)] \notin L(t)$, which is a contradiction. Hence, $\zeta \in L(t')$, for all $t' \in T$. By the induction hypothesis, $\hat{\zeta} \in L(t')$, for all $t' \in T$. Finally, this implies that $\mathbf{P}_{=1}[\mathbf{G}\ (\hat{\zeta})] = \hat{\xi} \in L(t)$.

We have now shown that if ϕ is satisfiable, then so is $\hat{\phi}$. Moreover, it is obvious that $\hat{\phi} \Rightarrow \phi$. The other direction follows immediately from this fact. Hence, ϕ is equisatisfiable to $\hat{\phi}$. □

In section 5.3 we will give a formula which makes the finite satisfiability problem particularly challenging for a certain fragment. This formula also shows that we cannot extend the above theorem to be a statement about equality rather than equisatisfiability. However, if we consider only **G**-formulae, theorem 5.15 motivates a simple construction for models of those.

Corollary 5.16. *Let $\phi := \mathbf{P}_{\rhd r}[\mathbf{G}\ (\psi)]$ be a finitely satisfiable $\mathbf{F}_q\mathbf{G}_q$-formula. Then, there is a model of size linear in $|\phi|$.*

Proof. By theorem 5.15 we can consider $\hat{\phi}$ instead of ϕ. Let M be a model, and $\hat{\phi} \in L(s_0)$, for some $s_0 \in S$. We define a new Markov chain M', such that $S' := \{s_\psi \in S \mid \mathbf{P}_{=1}[\mathbf{F}\ (\psi)] \in sub(\hat{\phi}) \text{ and } \psi \in L(s_\psi)\}$, $L' := L|_{S'}$, and P' generating a BSCC from S'. Now, we will prove that for $s \in S'$, and $\xi \in L'(s)$, $M', s \models \xi$.

I $\xi = a$. There is nothing to show.

II $\xi = \zeta \wedge \vartheta$. Since M is a model, $\zeta, \vartheta \in L(s)$, and therefore $\zeta, \vartheta \in L'(s)$. By the induction hypothesis, $M', s \models \zeta$, and $M', s \models \vartheta$. Thus, $M', s \models \zeta \wedge \vartheta$.

III $\xi = \zeta \vee \vartheta$. Since M is a model, $\zeta \in L(s) = L'(s)$, or $\vartheta \in L(s) = L'(s)$. By the induction hypothesis, $M', s \models \zeta$, or $M', s \models \vartheta$. Thus, $M', s \models \zeta \vee \vartheta$.

IV $\xi = \mathbf{P}_{=1}[\mathbf{F}\ (\zeta)]$. By construction, S' is a BSCC. Thus, s_ζ is reached almost surely. By the induction hypothesis, $M', s_\zeta \models \zeta$. Therefore, $M', s \models \mathbf{P}_{=1}[\mathbf{F}\ (\zeta)]$.

V $\xi = \mathbf{P}_{=1}[\mathbf{G}\ (\zeta)]$. Since M is a model, for all $s' \in S$, $\zeta \in L(s')$, and thus for all $s' \in S'$, $\zeta \in L'(s')$. By the induction hypothesis, for all $s' \in S'$, $M', s' \models \zeta$. Hence, $M', s \models \mathbf{P}_{=1}[\mathbf{G}\ (\zeta)]$.

□

Example 5.17. Consider $\phi := \mathbf{P}_{\geq 1/2}[\mathbf{G}\ (\mathbf{P}_{\geq 1/3}[\mathbf{F}\ (a)] \wedge \mathbf{P}_{\geq 1/3}[\mathbf{F}\ (\neg a)])]$. The chain in figure 5.6 models ϕ. Unlabeled arcs indicate a uniform distribution over all successors. It is clear that the model is unnecessarily complicated. The chain in figure 5.7 is a simplified version thereof.

Note that we made frequent use of the BSCC properties for the proofs of this section. This normal form that we created was also based on the fact that some BSCC is reached almost surely. Since this is only the case for finite Markov chains, we had to assume that the formula is finitely satisfiable. If we considered the general satisfiability problem, then both of the claims here would not be true. E.g. the formula

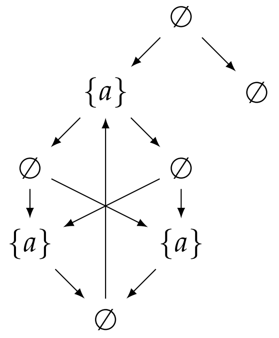

FIGURE 5.6: Large finite model for a $\mathbf{F}_q\mathbf{G}_q$-formula

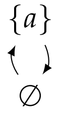

FIGURE 5.7: Simplified version of the model in figure 5.6

$$\phi := \mathbf{P}_{>0}[\mathbf{G}\ (\mathbf{P}_{>0}[\mathbf{F}\ (a)] \wedge \neg a)]$$

is satisfiable, but requires infinite models, as was pointed out in (Brázdil, Forejt, Křetínský, and Kucera, 2008). One such model is given in figure 5.4. Now consider

$$\hat{\phi} := \mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (a)] \wedge \neg a)]$$

Obviously, this is unsatisfiable. Hence, in this case ϕ is not equisatisfiable to $\hat{\phi}$.

5.3 General $\mathbf{F}_q\mathbf{G}_1$-Fragment

The general $\mathbf{F}_q\mathbf{G}_1$-Fragment extends the conjunctive $\mathbf{F}_q\mathbf{G}_1$-Fragment by disjunctions. That is

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[\mathbf{F}\ (\Phi)] \mid \mathbf{P}_{=1}[\mathbf{G}\ (\Phi)]$$

It might seem that this extension does not make the problem much more complicated than it was for the conjunctive fragment. However, we will see that there are some complications with this fragment, which make the satisfiability problem much harder to solve. First, we shall recap what the essence of our solution for the conjunctive fragment was. We were able to deal with the problem of repeated **F**-formulae by simply postponing them until the BSCCs. This strategy was perfectly legitimate because the **G**-formulae could be transformed into a normal form, where every **F**-formula appeared only qualitatively. Moreover, the conjunctions enforced such formulae to hold in every BSCC.

If we allow disjunctions, the situation is rather different. If a **F**-formula appears as part of a disjunction within a **G**, we cannot guarantee that it will hold in every BSCC. It might as well happen that one of the other disjuncts is satisfied in some of the BSCCs. This discussion should have given the reader some intuition on the nature of the general $\mathbf{F}_q\mathbf{G}_1$-Fragment. Since our arguments were rather abstract, one might wonder, whether there are formulae, which really require such complex models. It might also be possible that we could somehow still obtain simple models

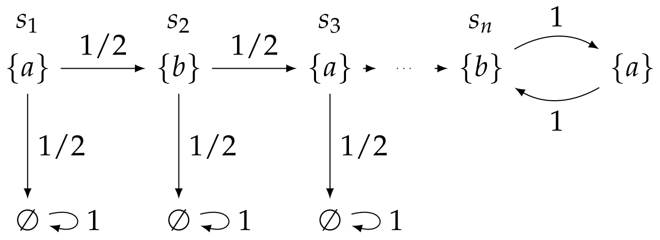

FIGURE 5.8: Large model for (5.2)

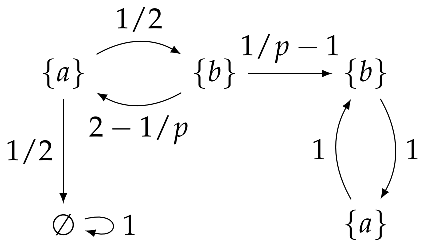

FIGURE 5.9: Small model for (5.2)

similar to those of the conjunctive version. The following formula demonstrates that this is not the case:

$$\begin{aligned}&\mathbf{P}_{=1}[\mathbf{G}\ ((\mathbf{P}_{\geq 1/2}[\mathbf{F}\ (a)] \wedge \neg a) \vee (\mathbf{P}_{\geq 1/2}[\mathbf{F}\ (b)] \wedge \neg b) \vee \mathbf{P}_{=1}[\mathbf{G}\ (\neg a \wedge \neg b)])]\\ &\wedge \mathbf{P}_{\geq p}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\neg a \wedge \neg b)])]\\ &\wedge \mathbf{P}_{\geq 1-p}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (a)] \wedge \mathbf{P}_{=1}[\mathbf{F}\ (b)])])]\end{aligned} \tag{5.2}$$

Intuitively, models for this formula must either be of tree shape with a height that depends on p or contain a SCC, which is not bottom. Figure 5.8 shows a model for (5.2) which is almost a tree in the sense that the only SCCs are BSCCs. We can enforce arbitrarily high values for n, by increasing p. Figure 5.9 shows a model whose size is independent of p. However, we need a not bottom SCC. Our approach for the conjunctive fragment did not consider any of those cases. Therefore, we would have to adapt the procedure in a way that could handle such things. Unfortunately, we have not been able to find a solution for this problem. However, we did find a solution for a simplified fragment that includes disjunctions, which we will present in a subsequent section. But first, we will prove an interesting result about **G**-formulae in this fragment.

Theorem 5.18. *Let ϕ be a $\mathbf{F}_q\mathbf{G}_1$-formula, M a model, and $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)] \in L(s_0)$, for some $s_0 \in S$. Then, there is a finite model for $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$.*

Proof. Let $G := \{\psi \in sub(\phi) \mid \psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$ for some $\xi\}$, and $s \in S$, such that $|G \setminus L(s)| = min_{t \in S}(|G \setminus L(t)|)$. Now, let M' be a Markov chain, with $S' := \{s_\psi \in post^*_M(s) \mid \mathbf{P}_{\triangleright r}[\mathbf{F}\ (\psi)] \in sub(\phi)$ and $\psi \in L(s_\psi)\}$, $L' := L|_{S'}$, and P' generating a BSCC from S'. We claim that M' is model for $\mathbf{P}_{=1}[\mathbf{G}\ (\phi)]$. Let $t \in S'$, and $\psi \in L(t)$. We apply induction over the structure of ψ in order to show that $M', t \models \psi$.

I $\psi = a$ or $\psi = \neg a$. Nothing to show.

II $\psi = \xi \wedge \zeta$. Then, $\xi, \zeta \in L(t) = L'(t)$. From the induction hypothesis follows that $M', t \models \xi$, and $M', t \models \zeta$. Therefore, $M', t \models \xi \wedge \zeta$.

III $\psi = \xi \vee \zeta$. Analogous to the previous case.

IV $\psi = \mathbf{P}_{\rhd r}[\mathbf{F}\ (\xi)]$. By the construction of S', there is a state $s_\xi \in S'$ with $\xi \in L'(s_\xi)$. By the induction hypothesis, $M', s_\xi \models \xi$. Moreover, since S' is a BSCC, s_ξ is reached from t almost surely, and therefore $M', t \models \mathbf{P}_{=1}[\mathbf{F}\ (\xi)] \Rightarrow \mathbf{P}_{\rhd r}[\mathbf{F}\ (\xi)]$.

V $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. By construction, there is no state in $post^*_M(s)$ which satisfies a **G**-formula that is not satisfied by s. Since $S' \subseteq post^*_M(s)$, the same **G**-formulae must be satisfied by all states in S'. Thus, for all $t' \in post^*_M(t) = S'$, $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in L'(t')$, and hence $\xi \in L'(t')$. Induction hypothesis yields $M', t' \models \xi$. Finally, we conclude $M', t \models \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$.

□

5.3.1 $\mathbf{F}_q\mathbf{G}_1$-Fragment with qualitative Fs in Gs

We have already shown that it is not possible to obtain a similar normal form for **G**-formulae as we did for the conjunctive fragment. In order to approach the satisfiability problem for this fragment, we can simply enforce a certain normal form and simplify the fragment that way. The properties that made the **G** normal form so useful were qualitative **F**s as well as the fact that they appeared only in conjunctions. Hence, there are two possibilities how we can reduce the complexity of the general $\mathbf{F}_q\mathbf{G}_1$-Fragment. Firstly, we can allow disjunctions only outside of **G**s. However, this fragment is trivial to solve, since it is not more expressive than the conjunctive one—for every disjunction, there must be at least one disjunct that can be satisfied. We can try all possible selections of disjuncts and forget about the disjunction completely.

Therefore, we shall rather try another restriction; i.e. we allow disjunctions everywhere, but all **F**-formulae within **G**s must be qualitative. Then, we still have to deal with the mentioned problem that some **F**-formulae might not appear in all (or any) BSCCs. However, their qualitative nature simplifies the solution a lot. The considered fragment is the following:

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[\mathbf{F}\ (\Phi)] \mid \mathbf{P}_{=1}[\mathbf{G}\ (\Psi)]$$
$$\Psi ::= a \mid \neg a \mid \Psi \wedge \Psi \mid \Psi \vee \Psi \mid \mathbf{P}_{=1}[\mathbf{F}\ (\Psi)] \mid \mathbf{P}_{=1}[\mathbf{G}\ (\Psi)]$$

In this fragment, we can make the following statement: *If a **F**-formula appears within a **G**-formula, it will be satisfied almost surely.* This gives rise to an intuitive idea: Just like we postponed the **F**-formulae in the conjunctive fragment until the BSCCs, we can postpone the **F**-formulae until a certain moment. Probably, there are various options, when to terminate the **F**-formulae. We will go into the details of our decision in a moment. Merely postponing **F**-formulae might not be enough, though. We have to ensure that the height cannot grow arbitrarily. For this, we need to fix certain equivalence classes for states. In this case, we will consider states as equivalent if they terminate the same **F**-formulae. We will see that this is sufficient to preserve model properties. Now, we can formalize our ideas.

Construction of reduced models For a formula ψ, let $\hat{\psi}$ be defined as in the proof for theorem 5.13; that is, we replace all nested **F**-formulae by atomic propositions. Then, for a tree model M for ϕ, we define $\hat{M} := (S, P, \hat{L})$, with $\hat{L}(s) := \{\hat{\psi} \mid \psi \in L(s)\}$. From this, we can construct the canonical reduction $red(sel_{\hat{M}}, \hat{M}) =: (S', P', \hat{L}') =: \hat{M}'$. Finally, we create $M' := (S', P', L')$, with $L' := L|_{S'}$. So far, the procedure is exactly the same as in the proof for theorem 5.13. However, we now have to deal with the yet unsatisfied **F**-formulae. For this, we will use M, in order to expand M', such that M' models ϕ. In a sense, we will learn from the states that we omitted in M'. Let $s \in S$, and $t \in post_{M'}(s)$. Further, we denote ρ^M_{st} for the unique path leading from s to t in M. Slightly abusing notation, we denote

$$\rho^M_{st}[\psi] := \begin{cases} \rho^M_{st}[i] & \text{if } \psi \in L(\rho^M_{st}[i]) \text{ and } \nexists j > i.\psi \in L(\rho^M_{st}[j]) \\ \texttt{undefined} & \text{otherwise} \end{cases}$$

for the last state on ρ^M_{st} that satisfies ψ. Using this, we can determine which states we need to add to M' in order to obtain a model, namely:

$$T(\rho^M_{st}) := \{\rho^M_{st}[\psi] \mid \exists \mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in sub(\phi).(\mathbf{P}_{=1}[\mathbf{F}\ (\psi)] \in sub(\xi))\}$$

Now, we can define our model $\tilde{M}$, with

$$\tilde{S} := S' \cup \bigcup_{\substack{s \in S' \\ t \in post_{M'}(s)}} T(\rho^M_{st})$$

$$\tilde{L} := L|_{\tilde{S}}$$

$$\tilde{P}(s,t) := \begin{cases} P'(s,t) & \text{if } s,t \in S' \text{ and } T(\rho^M_{st}) = \emptyset \\ P'(s,t') & \text{if } t \in T(\rho^M_{st'}) \text{ and } T(\rho^M_{st'}) \cap pre^*_M(t) = \emptyset \\ 1 & \text{if } s,t \in T(\rho^M_{s't'}), s \in pre^*_M(t) \text{ and} \\ & T(\rho^M_{s't'}) \cap post^*_M(s) \cap pre^*_M(t) = \emptyset \\ 1 & \text{if } s \in T(\rho^M_{s't}) \text{ and } T(\rho^M_{s't}) \cap post^*_M(s) = \emptyset \\ 0 & \text{otherwise} \end{cases}$$

$\tilde{M}$ extends M' by simple chains of states that terminate **F**-formulae. Figure 5.10 illustrates this. sel_1 and sel_2 are the selections. In the conjunctive $\mathbf{F}_q\mathbf{G}_1$-fragment, we directly connected those sets. Here, we insert simple chains between the selections. The construction guarantees that we have at most one state per **F**-formula to terminate. This is obtained by postponing the termination until the last possible moment before $sel_{\tilde{M}}(s)$. In fact, one could probably postpone it even further. However, we think that this way it is easier to formalize and as it still yields the desired result, we prefer this version. The construction of $\tilde{P}$ preserves the probabilities in a certain sense, as the following lemma states.

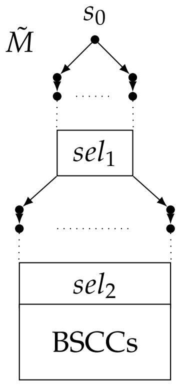

FIGURE 5.10: Reduction of models for $\mathbf{F}_q\mathbf{G}_1$-formulae with qualitative **F**s in **G**s. Note that the BSCCs will be added later. See proof for theorem 5.20

Lemma 5.19. *Let $\rho^{\tilde{M}}, \rho^{M'}$ be two finite paths in $\tilde{M}$ and M', respectively, such that $\rho^{\tilde{M}}[0] = \rho^{M'}[0]$, and $\rho^{\tilde{M}}[n] = \rho^{M'}[m]$ where $n := len(\rho^{\tilde{M}})$ and $m := len(\rho^{M'})$. Then, $\tilde{P}^*(\rho^{\tilde{M}}[0], \rho^{\tilde{M}}[n]) = P'^*(\rho^{M'}[0], \rho^{M'}[m])$.*

Proof. Let $\rho^{\tilde{M}}, \rho^{M'}$ be such paths. From the construction of $\tilde{P}$, we can see that $\rho^{\tilde{M}} \neq \rho^{M'}$ is only possible if there are $s := \rho^{M'}[k], t := \rho^{M'}[k+1]$ with $T(\rho^{M}_{st}) \neq \emptyset$. We will now show that $P'^{*}(s,t) = P'(s,t) = \tilde{P}^{*}(s,t)$.

The first equality is straight forward since t is defined as the successor of s in M'. Now, let $t' \in post_{\tilde{M}}(s)$ (and t' occurs on $\rho^{\tilde{M}}$). We can assume that $t' \neq t$ and therefore $t' \in T(\rho^{M}_{st})$, and there is no $t'' \in T(\rho^{M}_{st}) \cap pre^{*}_{M}(t')$. Then, by definition, $\tilde{P}(s,t') = P'(s,t)$. Moreover, for $u, v \in T(\rho^{M}_{st})$, with $v \in post_{\tilde{M}}(u)$, and $\tilde{P}(u,v) = 1$. Therefore, $\tilde{P}^{*}(t',t) = 1$, and then $\tilde{P}^{*}(s,t) = P'(s,t)$. Now, we can repeat this argument for every fragment on the paths that differ and obtain the equality in the claim. □

This result essentially implies that the **F**-formulae that are not nested in **G**s are still satisfied in $\tilde{M}$. The proof of the following theorem demonstrates how to obtain a model for ϕ from $\tilde{M}$.

Theorem 5.20. *For a satisfiable $\mathbf{F}_q\mathbf{G}_1$-formula ϕ, with only qualitative* **F***s in* **G***s, there is a model of size $f(|\phi|)$, where f is a computable function.*

Proof. $\tilde{M}$ can be extended to such a model. As in the proof for theorem 5.13, we can see that the size of M' is bounded, and it has leaves that have to satisfy only **G**-formulae. Again, when we say leaves, we actually mean infinite chains without **F**-formulae in the labels. We can, therefore, easily see that $\tilde{M}$ is bounded, as well. However, $\tilde{M}$ might not be a model yet, since the formulae in the leaves might not be satisfied. Yet, we can create models of bounded size for those due to theorem 5.18 and corollary 5.16. In order to avoid the introduction of another name for this model, we will use $\tilde{M}$ when we refer to the extended version of our previously defined $\tilde{M}$. Now, we still have to show that our new $\tilde{M}$ indeed models ϕ. For this, we will prove that for all $s \in S'$, and $\psi \in L'(s)$, $\tilde{M}, s \models \psi$.

First, note that it was important to not include all states in $\tilde{S}$ in the claim since this might not be true. Therefore, $\tilde{M}$ is not necessarily a model. However, the claim is sufficient in order to show that $\tilde{M}$ can be transformed into a model for ϕ. We show the claim by induction over ψ. In order for the proof to succeed, we need to additionally prove that for all $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in L'(s)$, all $\zeta \in sub(\xi)$, and all $t \in post^{*}_{\tilde{M}}(s)$, $\zeta \in \tilde{L}(t)$ implies $\tilde{M}, t \models \zeta$; i.e. we need to guarantee that **G**-formulae hold in *all* states of $\tilde{M}$, not only in S'.

I $\psi = a$. There is nothing to show.

II $\psi = \xi \wedge \zeta$. If $\psi \notin sub(\mathbf{P}_{=1}[\mathbf{G}\ (\vartheta)])$, for some ϑ, then we only have to consider states in S'. Since we did not change the labels, $\xi \in L'(s)$, and $\zeta \in L'(s)$. By the induction hypothesis, $\tilde{M}, s \models \xi$, and $\tilde{M}, s \models \zeta$, and therefore $\tilde{M}, s \models \xi \wedge \zeta$. Otherwise, $\xi, \zeta \in sub(\mathbf{P}_{=1}[\mathbf{G}\ (\vartheta)])$. Therefore, if $s \in \tilde{S} \setminus S'$, we can still apply the induction hypothesis and obtain the claim.

III $\psi = \xi \vee \zeta$. Analogous to the previous case.

IV $\psi = \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$. We have to consider all states in $\tilde{S}$. We know that $\xi \in \tilde{L}(s)$, and, therefore, by the induction hypothesis $\tilde{M}, s \models \xi$. The construction of $\tilde{P}$ preserves the order of states; that is, $post^{*}_{\tilde{M}}(s) \subseteq post^{*}_{M}(s)$. Hence, for all $t \in post^{*}_{\tilde{M}}(s)$, $\mathbf{P}_{=1}[\mathbf{G}\ (\xi)] \in \tilde{L}(t)$. Thus $\tilde{M}, s \models \mathbf{P}_{=1}[\mathbf{G}\ (\xi)]$.

V $\psi = \mathbf{P}_{\trianglerighteq r}[\mathbf{F}\ (\xi)]$. If there is no $\mathbf{P}_{=1}[\mathbf{G}\ (\zeta)]$, such that $\psi \in sub(\zeta)$, then we can assume that $s \in S'$. From lemma 5.19 we know that for every finite path in $\tilde{M}$ starting at s, the probability is the same as the corresponding path in M'. From theorem 4.10, we know that $M', s \models \psi$, and therefore $\tilde{M}, s \models \psi$.

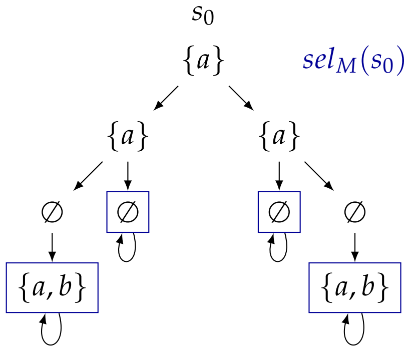

FIGURE 5.11: Example of a model for a $\mathbf{F}_q\mathbf{G}_1$-formula

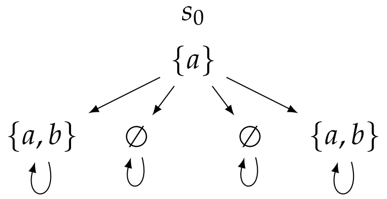

FIGURE 5.12: Reduced version of the model in figure 5.11

Now assume that $\psi \in sub(\mathbf{P}_{=1}[\mathbf{G}\ (\zeta)])$. Then, $\psi = \mathbf{P}_{=1}[\mathbf{F}\ (\xi)]$. If $s \in S'$ is a leaf, then our extension guarantees that $\tilde{M}, s \models \psi$. Therefore, we can assume that s is not a leaf in M' and thus there is a $t \in post_{M'}(s)$ and $t \neq s$. Either, $\psi \in \tilde{L}(t)$, or there is a state $t' \in post^*_M(s) \cap pre^*_M(t)$, with $\xi \in L(t')$. In the latter case, by construction of $\tilde{M}$, $t' \in post^*_{\tilde{M}}(s) \cap pre^*_{\tilde{M}}(t)$. In the other case, we can apply the same argument at a latter point on the path. In any way, whenever there is at least one state on a path that satisfies ξ, at least one will be included. Since such states are reached almost surely in M, the same goes for $\tilde{M}$. If $s \in \tilde{S} \setminus S'$, then similar arguments yields the claim. Therefore, $\tilde{M}, s \models \psi$.

□

The essential idea was to insert simple chains in order to preserve the satisfaction of nested **F**-formulae. This only worked because of the qualitative nature of those. If we allowed for arbitrary **F**-formulae, such simple chains might not suffice anymore. Instead, we might have to preserve not only the order of the inserted states but also (parts of) their subtrees. This, however, might lead to models of arbitrary height. At the beginning of this section, we have already shown that this problem is fundamental, and that there is no easy way around it.

Example 5.21. Consider the formula

$$\phi := \mathbf{P}_{\geq 1/2}[\mathbf{F}\ (\mathbf{P}_{=1}[\mathbf{G}\ (a)])] \wedge \mathbf{P}_{=1}[\mathbf{G}\ (\mathbf{P}_{=1}[\mathbf{F}\ (\neg a)] \vee \mathbf{P}_{=1}[\mathbf{F}\ (b)])].$$

Figure 5.11 shows a model for ϕ. The blue boxes illustrate the canonical selection of s_0. Figure 5.12 shows the corresponding reduced chain. However, it is not a model for ϕ. The reason is that neither states satisfying $\neg a$ nor such that satisfy b are reached almost surely from s_0. By including additional states, the chain in figure 5.13 corrects this, and thereby we obtain a model ϕ.

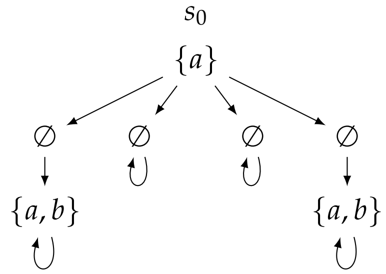

FIGURE 5.13: Corrected version of the model in figure 5.12

5.4 Semi-recursive $\mathbf{U}_q$-Fragment

For now, we have only considered fragments that consisted purely out of **F**s and **G**s. The reason for this is that they are simpler than **U**s and **R**s in the sense that they make sort of qualitative claims—either some formula is satisfied somewhere or not. **U**-formulae can additionally express properties of the path before some formula is satisfied. This makes them much more complicated than **F**s. Therefore, we will consider those in isolation. As in **G**s, we might have to deal with repeated **U**-formulae, if they appear in the first argument to another **U**-formula. Since we were not able to find a solution for that problem in this fragment, we will simply avoid it, and consider what we call the semi-recursive $\mathbf{U}_q$-Fragment.

Definition 5.22 (Semi-recursive $\mathbf{U}_q$-fragment)**.** The semi-recursive $\mathbf{U}_q$-fragment consists of formulae of the form

$$\begin{aligned}\Phi &::= A \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \mathbf{P}_{\rhd r}[(A)\ \mathbf{U}\ (\Phi)] \\ A &::= a \mid \neg a \mid A \wedge A \mid A \vee A\end{aligned}$$

What makes this fragment simple, is the fact that the first argument cannot be a propagating formula. It is, therefore, similar to the pure **F**-Fragment, except that it allows general formulae of propositional logic as the first argument, and not only $\top$. Since we avoid repeating **U**-formulae, we can minimize models of this fragment by simply minimizing the Hintikka chain and applying our canonical reduction.

Theorem 5.23. *A satisfiable, semi-recursive $\mathbf{U}_q$-formula ϕ has a model of size $f(|\phi|)$, where f is a computable function.*

Proof. Let M be a minimal Hintikka chain and $\phi \in L(s_0)$, for some $s_0 \in S$. From theorem 4.10, we already know that $M' := red(sel_M, M)$ is a Hintikka chain and can thus be transformed into a model. We will now show that the size of M' can be limited.

Let $s \in S'$ and $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s)$. Observe that ψ cannot contain any **U**-formulae by definition. First assume that there is a formula $\mathbf{P}_{\rhd' r'}[(\zeta)\ \mathbf{U}\ (\vartheta)]$, with $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in sub(\vartheta)$. Then, due to the minimal Hintikka condition (MH5), $\vartheta \in L(s)$ and then due to (MH3), $\mathbf{P}_{\rhd'' r''}[(\zeta)\ \mathbf{U}\ (\vartheta)] \notin L(t)$, for any $t \in post^*_{M'}(s)$.

Now, assume that no formula ζ exists in $L(s)$, with $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \prec \zeta$. Let $T \subseteq S$, such that for all states $t \in T$, $\xi \in L(t)$. Then, for all successors $t' \in post^*(t)$, $\mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{U}\ (\xi)] \notin L(t')$. Therefore, whenever a **U**-formula is terminated at some state, all successors have less formulae to satisfy. Since in M' at least one **U**-formula is terminated after every step, the height of the tree is limited by $|\phi|$. By this, we

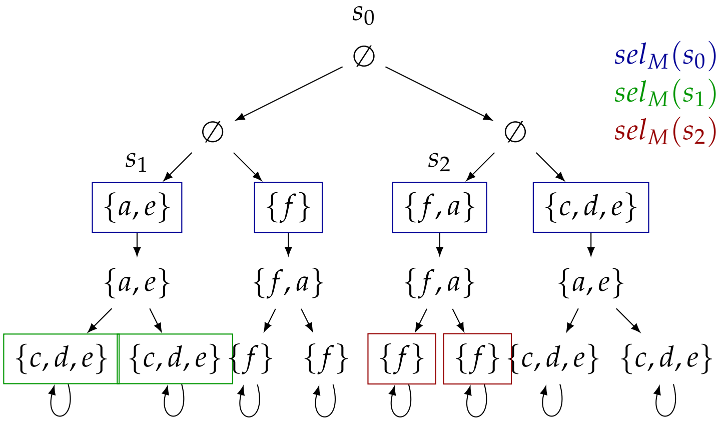

FIGURE 5.14: Example of a model for a semi-recursive $\mathbf{U}_q$-formula

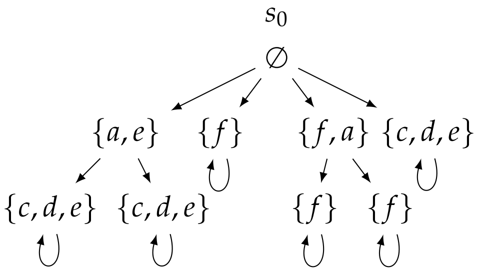

FIGURE 5.15: Reduced version of the model in figure 5.14

mean that after at most $|\phi|$ steps, we reach a state that does not have to satisfy any propagating formulae. We can thus simply self loop with probability 1.

Due to theorem 4.4, we can limit the branching degree by $|\phi| + 2$ and thus the overall model size is limited by $|\phi|^{|\phi|+2}$. □

Example 5.24. Consider the formula

$$\begin{aligned} \phi := & \\ & \mathbf{P}_{\geq 1/2}[(\neg f)\ \mathbf{U}\ (\mathbf{P}_{=1}[(a \wedge e)\ \mathbf{U}\ (c \wedge d \wedge e)])] \wedge \\ & \mathbf{P}_{\geq 1/2}[(\neg e)\ \mathbf{U}\ (\mathbf{P}_{=1}[(\neg c \wedge f)\ \mathbf{U}\ (\neg a \wedge \neg d \wedge f)])]. \end{aligned}$$

The Markov chains in figures 5.14 and 5.15 are both models for ϕ. The latter is the reduced version of the former. This example also illustrates, how the minimization of the Hintikka chain can help reducing the size: After having terminated the **U**-formulae, we self-loop immediately and omit subsequent states.

6 Conclusion and Future Work

In this thesis, we have introduced various techniques to normalize models. We have seen how one can vertically collapse models by applying reductions, and horizontally collapse models by cutting off certain branches. We have shown that those methods are applicable to models of quite general formulae and demonstrated how they can help us to obtain limited models for the semi-recursive $\mathbf{U}_q$q and the restricted $\mathbf{F}_q\mathbf{G}_1$-fragments. For those fragments, we have even shown that the general satisfiability problem is equivalent to the finite satisfiability problem. For the $\mathbf{F}_q\mathbf{G}_q$-fragment, we have solved the finite satisfiability problem for $\mathbf{G}$-formulae, and argued why we cannot easily extend the result to general formulae in this fragment. Furthermore, we discussed the limitations of the developed methods for other fragments and presented a concrete example of a challenging formula in the $\mathbf{F}_q\mathbf{G}_1$-fragment.

Future Work Many open questions still remain. Firstly, we solved the satisfiability problem for quite restrictive fragments. Therefore, it would be interesting to extend the results to more general ones. For instance, considering the full $\mathbf{U}_q$-fragment might be quite interesting. Similarly, overcoming our restriction in the $\mathbf{F}_q\mathbf{G}_1$-fragment is certainly of interest. Of course, we could continue generalizing the fragments until we can capture the whole of PCTL. From this the question arises, whether satisfiability is at all decidable for general formulae—and if it is not, what is the largest decidable fragment? Furthermore, it is certainly interesting to explore the differences between general and finite satisfiability. What do we need to add in order for those to be different problems? As soon as we start considering fragments where those are indeed different, we need to understand which representation of infinite Markov chains is sufficient to capture all possible models for the formulae. One important thing that we have not covered at all, is the complexity of the considered problems.

A Alternative Proof for Theorem 5.2

In the subsequent proofs, we will deal with rather complex formulae. In order to improve readability, we will abbreviate **G**- and **F**-formulae, such that the syntax becomes

$$\Phi := a \mid \neg a \mid \mathbf{F}_{\rhd r}\Phi \mid \mathbf{G}_{=1}\Phi$$

Lemma A.1.

$$\mathbf{G}_{=1}\mathbf{G}_{=1}\psi \equiv \mathbf{G}_{=1}\psi \tag{A.1}$$

$$\mathbf{G}_{=1}\mathbf{F}_{\rhd r}\psi \equiv_{fin} \mathbf{G}_{=1}\mathbf{F}_{=1}\psi \tag{A.2}$$

$$\mathbf{F}_{=1}\mathbf{F}_{\rhd r}\psi \equiv \mathbf{F}_{\rhd r}\psi \tag{A.3}$$

$$\mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \equiv \mathbf{G}_{=1}\mathbf{F}_{=1}\psi \tag{A.4}$$

$$\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \equiv \mathbf{F}_{=1}\mathbf{G}_{=1}\psi \tag{A.5}$$

Proof. Let M be a model. First, observe that $\mathbf{G}_{=1}\psi \in L(s_0)$ implies that $\psi \in L(s_0)$, whereas $\psi \in L(s_0)$ implies that $\mathbf{F}_{=1}\psi \in L(s_0)$.

Equality (A.1) Assume that $\mathbf{G}_{=1}\mathbf{G}_{=1}\psi \in L(s_0)$. Then, due to the above observation, $\mathbf{G}_{=1}\psi \in L(s_0)$. Now assume that $\mathbf{G}_{=1}\psi \in L(s_0)$. Then, $\mathbf{G}_{=1}\psi \in L(s)$, for all $s \in post^*(s_0)$. Therefore, $Pr(\{\pi \in Cyl(s_0) \mid \pi \models \mathbf{G}\ (\mathbf{G}_{=1}\psi)\}) = 1$, which implies $\mathbf{G}_{=1}\mathbf{G}_{=1}\psi \in L(s_0)$.

Equality (A.2) Assume that $\mathbf{G}_{=1}\mathbf{F}_{\rhd r}\psi \in L(s_0)$. Then, for all BSCCs T, and all states $t \in T$, $\mathbf{G}_{=1}\mathbf{F}_{\rhd r}\psi \in L(t)$, and therefore $\mathbf{F}_{\rhd r}\psi \in L(t)$. Hence, there must be a state $t' \in T$, with $\psi \in L(t')$. Since T is a BSCC, t' is reached almost surely from every state in T. Therefore, $\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \in L(t)$. As we are considering finite models only, every run ends up in a BSCC almost surely and thus $\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \in L(s_0)$. The reverse implication is obvious.

Equality (A.3) Assume $\mathbf{F}_{=1}\mathbf{F}_{\rhd r}\psi \in L(s_0)$. Then, there is a set $T \subseteq post^*(s_0)$, such that for all $t \in T$, $\mathbf{F}_{\rhd r}\psi \in L(t)$ and $Pr(\{\pi \in Cyl(s_0) \mid \exists i.\pi[i] \in T\}) = 1$. We can compute the probability to reach ψ as follows

$$Pr(\{\pi \in Cyl(s_0) \mid \pi \models \mathbf{F}\ (\psi)\}) \rhd \sum_{t \in T} P^*(s_0, t) \cdot r = r$$

This means that $\mathbf{F}_{\rhd r}\psi \in L(s_0)$. The converse implication follows immediately from the fact that $\xi \in L(s_0)$ implies $\mathbf{F}_{=1}\xi \in L(s_0)$.

Equality (A.4) Assume $\mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \in L(s_0)$. Then, there is a set $T \subseteq post^*(s)$, where for all $t \in T$, $\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \in L(t)$ and $Pr(\{\pi \in Cyl(s_0) \mid \exists i.\pi[i] \in T\}) = 1$. Thus, for all $t \in T$, $\mathbf{F}_{=1}\psi \in L(t)$. Therefore, $\mathbf{F}_{=1}\mathbf{F}_{=1}\psi \in L(s_0)$. Equality (A.3) yields $\mathbf{F}_{=1}\psi \in L(s_0)$. This argument can be applied to all states in $post^*(s_0) \cap pre^*(T)$. Therefore, for all $s \in post^*(s_0)$, $\mathbf{F}_{=1}\psi \in L(s)$ and then $\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \in L(s_0)$. The converse implication is again due to $\xi \Rightarrow \mathbf{F}_{=1}\xi$.

Equality (A.5) Assume $\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \in L(s_0)$. Then, for every state $s \in post^*(s_0)$, either $\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \in L(s)$ or $\mathbf{G}_{=1}\psi \in L(s)$. In the latter case, however, it also holds that $\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \in L(s_0)$. Therefore, for every state $s \in post^*(s_0)$, $\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \in L(s)$, and thus $\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}\psi \in L(s_0)$. The converse implication follows from $\mathbf{G}_{=1}\psi \Rightarrow \psi$.

□

Lemma A.2 (Distributivity).

$$\mathbf{F}_{=1}(\bigwedge_i \mathbf{F}_{\rhd r_i}\psi_i) \equiv \bigwedge_i \mathbf{F}_{\rhd r_i}\psi_i \tag{A.6}$$

$$\mathbf{G}_{=1}(\bigwedge_i \psi_i) \equiv \bigwedge_i \mathbf{G}_{=1}\psi_i \tag{A.7}$$

$$\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_i \psi_i) \equiv \bigwedge_i \mathbf{F}_{=1}\mathbf{G}_{=1}\psi_i \tag{A.8}$$

$$\mathbf{G}_{=1}\mathbf{F}_{=1}(\psi \wedge \mathbf{F}_{\rhd r}\xi) \equiv_{fin} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\xi) \tag{A.9}$$

$$\mathbf{G}_{=1}\mathbf{F}_{=1}(\psi \wedge \mathbf{G}_{=1}\xi) \equiv \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}\xi) \tag{A.10}$$

Proof. Let M be a model. In general,

$$\mathbf{F}_{=1}\bigwedge_i \psi_i \Rightarrow \bigwedge_i \mathbf{F}_{=1}\psi_i \tag{A.11}$$

Equality (A.6) From the implication (A.11) follows

$$\mathbf{F}_{=1}\bigwedge_i \mathbf{F}_{\rhd r_i}\psi_i \Rightarrow \bigwedge_i \mathbf{F}_{=1}\mathbf{F}_{\rhd r_i}\psi_i \overset{\text{(A.3)}}{\equiv} \bigwedge_i \mathbf{F}_{\rhd r_i}\psi_i$$

The converse implication is clear.

Equality (A.7) Assume $\bigwedge_i \mathbf{G}_{=1}\psi_i \in L(s_0)$. Then, for all $s \in post^*(s_0)$, and all i, $\psi_i \in L(s)$. This implies that $\bigwedge_i \psi_i \in L(s)$ and therefore $\mathbf{G}_{=1}\bigwedge_i \psi_i \in L(s_0)$.

If, on the other hand, $\mathbf{G}_{=1}\bigwedge_i \psi_i \in L(s_0)$, then for every $s \in post^*(s_0)$, $\bigwedge_i \psi_i \in L(s)$, and hence, for all i, $\psi_i \in L(s)$. Thus $\bigwedge_i \mathbf{G}_{=1}\psi_i \in L(s_0)$.

Equality (A.8) From equality (A.7) follows that $\mathbf{F}_{=1}\mathbf{G}_{=1}\bigwedge_i \psi_i \equiv \mathbf{F}_{=1}\bigwedge_i \mathbf{G}_{=1}\psi_i$, and from the implication (A.11), $\mathbf{F}_{=1}\bigwedge_i \mathbf{G}_{=1}\psi_i \Rightarrow \bigwedge_i \mathbf{F}_{=1}\mathbf{G}_{=1}\psi_i$.

Now assume that $\bigwedge_i \mathbf{F}_{=1}\mathbf{G}_{=1}\psi_i \in L(s_0)$. Then, for all i, there is a set $T_i \subseteq post^*(s_0)$, where for all $t \in T_i$, $\mathbf{G}_{=1}\psi_i \in L(t)$ and $Pr(\{\pi \in Cyl(s_0) \mid \exists j.\pi[j] \in T_i\}) = 1$. Let $T := \bigcap_i T_i$. Then, for all $t \in T$, and all i, $\mathbf{G}_{=1}\psi_i \in L(t)$. What is left to show is that $Pr(\{\pi \in Cyl(s_0) \mid \exists j.\pi[j] \in T\}) = 1$. Since for all $s \in post^*(s_0)$, either $\mathbf{F}_{=1}\mathbf{G}_{=1}\psi_i \in L(s)$ or $\mathbf{G}_{=1}\psi_i \in L(s)$, the same holds for every $T' \subseteq pre^*(T)$, and in particular for every T_i. Thus, T is reached almost surely.

Equality (A.9) Assume $\mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\xi) \in L(s_0)$. Then, for all states $s \in post^*(s_0)$, $\mathbf{F}_{=1}\psi \in L(s)$ and $\mathbf{F}_{=1}\xi \in L(s)$. Let s' be such that $\psi \in L(s)$. Then, $\mathbf{F}_{=1}\xi \in L(s')$ must also hold, and therefore $\psi \wedge \mathbf{F}_{=1}\xi \in L(s')$. Since this is true for all states that satisfy ψ, and those are reached almost surely from every state, $\mathbf{G}_{=1}(\mathbf{F}_{=1}(\psi \wedge \mathbf{F}_{=1}\xi)) \in L(s_0)$.

For the converse implication, we can apply our proven equalities to obtain

$$\begin{aligned}
\mathbf{G}_{=1}(\mathbf{F}_{=1}(\psi \wedge \mathbf{F}_{\triangleright r}\xi)) &\overset{\text{(A.11)}}{\Rightarrow} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\mathbf{F}_{\triangleright r}\xi) \\
&\overset{\text{(A.3)}}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{\triangleright r}\xi) \\
&\overset{\text{(A.7)}}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi) \wedge \mathbf{G}_{=1}(\mathbf{F}_{\triangleright r}\xi) \\
&\overset{\text{(A.2)}}{\equiv_{fin}} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi) \wedge \mathbf{G}_{=1}(\mathbf{F}_{=1}\xi) \\
&\overset{\text{(A.7)}}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\xi)
\end{aligned}$$

Equality (A.10) Assume $\mathbf{G}_{=1}(\mathbf{F}_{=1}\psi \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}\xi) \in L(s_0)$. Then there is a set $T \subseteq post^*(s_0)$, such that for all $t \in T$, $\mathbf{G}_{=1}\xi \in L(t)$, and $Pr(\{\pi \in Cyl(s_0) \mid \exists i.\pi[i] \in T\}) = 1$. Since all successors of s_0 satisfy $\mathbf{F}_{=1}\psi$, in particular this must be true for all $t \in T$. Hence, there must be $T' \subseteq T$, with all states satisfying ψ and $Pr(\{\pi \in Cyl(s_0) \mid \exists i.\pi[i] \in T'\}) = 1$. Therefore, $\mathbf{F}_{=1}(\psi \wedge \mathbf{G}_{=1}\xi) \in L(s_0)$. This argument can be applied to every successor of s_0, and we therefore conclude that $\mathbf{G}_{=1}\mathbf{F}_{=1}(\psi \wedge \mathbf{G}_{=1}\xi) \in L(s_0)$. The converse implication follows immediately from the implication (A.11). □

Now we can provide an alternative proof for theorem 5.2. Recall the theorem statement.

Theorem A.3. *Let ϕ be a conjunctive $\mathbf{F}_q\mathbf{G}_1$-formula. Then, the following equality holds*

$$\mathbf{G}_{=1}(\phi) \equiv_{fin} \mathbf{G}_{=1}(\bigwedge_{l \in A} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l \in B} l) \wedge \bigwedge_{i \in I} \mathbf{F}_{=1}(\bigwedge_{l \in C_i} l))$$

For appropriate $A, B, C_i \subset \mathcal{L}$.

Proof. We apply induction over ϕ.

Case $\phi = l$ Then $A := \{l\}$ and the claim holds.

Case $\phi \equiv \psi \wedge \xi$

$$\begin{aligned}
&\mathbf{G}_{=1}(\psi \wedge \xi)\\
&\overset{(A.7)}{\equiv} \mathbf{G}_{=1}\psi \wedge \mathbf{G}_{=1}\xi\\
&\overset{I.H}{\equiv}_{fin} \mathbf{G}_{=1}(\bigwedge_{l\in A_\psi} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\psi} l) \wedge \bigwedge_{i\in I_\psi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\psi,i}} l))\\
&\wedge \mathbf{G}_{=1}(\bigwedge_{l\in A_\xi} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\xi} l) \wedge \bigwedge_{i\in I_\xi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\xi,i}} l))\\
&\overset{(A.7)}{\equiv} \mathbf{G}_{=1}(\bigwedge_{l\in A_\psi\cup A_\xi} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\psi} l) \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\xi} l)\\
&\wedge \bigwedge_{i\in I_\psi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\psi,i}} l) \wedge \bigwedge_{i\in I_\xi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\xi,i}} l))\\
&\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\bigwedge_{l\in A_\psi\cup A_\xi} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\psi\cup B_\xi} l)\\
&\wedge \bigwedge_{i\in I_\psi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\psi,i}} l) \wedge \bigwedge_{i\in I_\xi} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\xi,i}} l))
\end{aligned}$$

Case $\phi = \mathbf{G}_{=1}\psi$ Then from equality (A.1) it follows that

$$\mathbf{G}_{=1}\mathbf{G}_{=1}\psi \equiv \mathbf{G}_{=1}\psi$$

and thus the claim holds by induction hypothesis.

Case $\phi = \mathbf{F}_{\rhd r}\psi$ From equality (A.2) it follows

$$\mathbf{G}_{=1}\mathbf{F}_{\rhd r}\psi \equiv_{fin} \mathbf{G}_{=1}\mathbf{F}_{=1}\psi$$

This case will be covered next.

Case $\phi = \mathbf{F}_{=1}\psi$ Now we will show that

$$\mathbf{G}_{=1}\mathbf{F}_{=1}\psi \equiv \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B} l) \wedge \bigwedge_{i\in I} \mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))$$

For this, we will consider several subcases, which results in another induction. In order to distinguish between the hypotheses, we will refer to the inductions as the *inner* and *outer* induction, respectively.

Subcase $\psi = l$ Setting $C := \{l\}$ yields the claim.

Subcase $\psi = \mathbf{F}_{\rhd r}\xi$ Applying Lemma A.1, we get

$$\begin{aligned}
\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{F}_{\rhd r}\xi &\overset{(A.3)}{\equiv} \mathbf{G}_{=1}\mathbf{F}_{\rhd r}\xi\\
&\overset{(A.2)}{\equiv}_{fin} \mathbf{G}_{=1}\mathbf{F}_{=1}\xi
\end{aligned}$$

and the claim holds by inner induction hypothesis.

Subcase $\psi = \mathbf{G}_{=1}\xi$ Applying the outer induction hypothesis and Lemmas A.1 and A.2 yields

$$\begin{aligned}
&\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}\xi\\
&\overset{o.I.H}{\equiv}_{fin} \mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B} l) \wedge \bigwedge_{i\in I}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A} l) \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B} l)\\
&\wedge \bigwedge_{i\in I}\mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{\substack{(A.4)\\(A.5)}}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A} l) \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B} l) \wedge \bigwedge_{i\in I}\mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A\cup B} l) \wedge \bigwedge_{i\in I}\mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{(A.7)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A\cup B} l)) \wedge \mathbf{G}_{=1}\mathbf{G}_{=1}(\bigwedge_{i\in I}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{(A.1)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A\cup B} l)) \wedge \mathbf{G}_{=1}(\bigwedge_{i\in I}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))\\
&\overset{(A.7)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A\cup B} l) \wedge \bigwedge_{i\in I}\mathbf{F}_{=1}(\bigwedge_{l\in C_i} l))
\end{aligned}$$

$\psi \equiv \bigwedge_i \xi_i$ In this case we need to show that although $\mathbf{F}_{=1}$ does not distribute over conjunctions in general, we still can get a formula of the desired form. We can split the conjunction into subformulae like this:

$$\bigwedge_i \xi_i \equiv \bigwedge_{l\in C} l \wedge \bigwedge_i \mathbf{F}_{\rhd r_i}\zeta_i \wedge \bigwedge_i \mathbf{G}_{=1}\vartheta_i \tag{A.12}$$

Then we can apply the induction hypotheses and the lemmas A.1 and A.2 to obtain:

$$\begin{aligned}
&\mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_i \xi_i)\\
&\overset{(A.12)}{\equiv} \mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C} l \wedge \bigwedge_i \mathbf{G}_{=1}\vartheta_i \wedge \bigwedge_i \mathbf{F}_{\rhd r}\zeta_i)\\
&\overset{(A.9)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l \wedge \bigwedge_i \mathbf{G}_{=1}\vartheta_i) \wedge \bigwedge_i \mathbf{F}_{=1}\zeta_i)\\
&\overset{(A.7)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l \wedge \mathbf{G}_{=1}\bigwedge_i \vartheta_i) \wedge \bigwedge_i \mathbf{F}_{=1}\zeta_i)\\
&\overset{(A.10)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_i \vartheta_i) \wedge \bigwedge_i \mathbf{F}_{=1}\zeta_i)
\end{aligned}$$

$$\overset{o.I.H}{\equiv}_{fin} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i} \mathbf{F}_{=1}\zeta_i$$

$$\wedge\, \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta} l \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\vartheta} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l)))$$

$$\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i} \mathbf{F}_{=1}\zeta_i \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta} l)$$

$$\wedge\, \mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\vartheta} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{F}_{=1}\mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

$$\overset{\substack{(A.4)\\(A.5)}}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i} \mathbf{F}_{=1}\zeta_i \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta} l)$$

$$\wedge\, \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_\vartheta} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

$$\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i} \mathbf{F}_{=1}\zeta_i \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta\cup B_\vartheta} l)$$

$$\wedge \bigwedge_{i\in I_\vartheta} \mathbf{G}_{=1}\mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

$$\overset{\substack{(A.7)\\(A.1)}}{\equiv} \mathbf{G}_{=1}(\bigwedge_{i} \mathbf{F}_{=1}\zeta_i \wedge \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta\cup B_\vartheta} l) \wedge \mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

$$\overset{\substack{(A.7)\\i.I.H}}{\equiv} \mathbf{G}_{=1}(\bigwedge_{i} (\mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in B_{\zeta_i}} l) \wedge \bigwedge_{j\in I_{\zeta_i}} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\zeta_i,j}} l))$$

$$\wedge\, \mathbf{F}_{=1}\mathbf{G}_{=1}(\bigwedge_{l\in A_\vartheta\cup B_\vartheta} l) \wedge \mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

$$\overset{(A.8)}{\equiv} \mathbf{G}_{=1}(\mathbf{F}_{=1}\mathbf{G}_{=1}((\bigwedge_{i} \bigwedge_{l\in B_{\zeta_i}} l) \wedge (\bigwedge_{l\in A_\vartheta\cup B_\vartheta} l))\wedge$$

$$\wedge \bigwedge_{i} \bigwedge_{j\in I_{\zeta_i}} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\zeta_i,j}} l) \wedge \mathbf{F}_{=1}(\bigwedge_{l\in C} l) \wedge \bigwedge_{i\in I_\vartheta} \mathbf{F}_{=1}(\bigwedge_{l\in C_{\vartheta,i}} l))$$

□

B Hintikka Minimization Algorithm

Algorithm 1 Minimization

```
MINIMIZE($s_0$)
function MINIMIZE($s$)
    $L(s) := L(s) \cap sub^*(\phi)$                                    ▷ (MH1)
    for $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in L(s)$ do                        ▷ (MH5)
        for $\zeta \in sub^*(\xi) \cap L(s)$ do
            if $\xi \notin L(s)$ then
                $L(s) := L(s) \setminus \{\zeta\}$
            end if
        end for
    end for
    for $t \in post(s)$ do
        $L(t) := L(t) \cap sub^*(L(s))$                                ▷ (MH2)
        for $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{U}\ (\xi)] \in \neg rep(L(s))$ do                ▷ (MH3)
            if $\xi \in L(s)$ then
                for $r' \in [0,1], \rhd' \in \{>, \geq\}$ do
                    $L(t) := L(t) \setminus \{\mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{U}\ (\xi)]\}$
                end for
            end if
        end for
        for $\mathbf{P}_{\rhd r}[(\psi)\ \mathbf{R}\ (\xi)] \in \neg rep(L(s))$ do                ▷ (MH4)
            if $\psi \wedge \xi \in L(s)$ then
                for $r' \in [0,1], \rhd' \in \{>, \geq\}$ do
                    $L(t) := L(t) \setminus \{\mathbf{P}_{\rhd' r'}[(\psi)\ \mathbf{R}\ (\xi)]\}$
                end for
            end if
        end for
        MINIMIZE($t$)
    end for
end function
```

Bibliography

Alur, Rajeev, Costas Courcoubetis, and David Dill (1993). "Model-checking in dense real-time". In: *Information and computation* 104.1, pp. 2–34.

Baier, Christel and Joost-Pieter Katoen (2008). *Principles of model checking*. MIT press.

Bertrand, Nathalie, John Fearnley, and Sven Schewe (2012). "Bounded Satisfiability for PCTL". In: *Computer Science Logic (CSL'12) - 26th International Workshop/21st Annual Conference of the EACSL, CSL 2012, September 3-6, 2012, Fontainebleau, France*, pp. 92–106.

Brázdil, Tomáš, Vojtech Forejt, Jan Křetínskỳ, and Antonín Kucera (2008). "The satisfiability problem for probabilistic CTL". In: *Logic in Computer Science, 2008. LICS'08. 23rd Annual IEEE Symposium on*. IEEE, pp. 391–402.

Chakraborty, Souymodip and Joost-Pieter Katoen (2016). "On the satisfiability of some simple probabilistic logics". In: *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*. ACM, pp. 56–65.

Dimitrova, Rayna, Luis María Ferrer Fioriti, Holger Hermanns, and Rupak Majumdar (2016). "Probabilistic CTL ^{*} : The Deductive Way". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, pp. 280–296.

Emerson, E Allen and Joseph Y Halpern (1982). "Decision procedures and expressiveness in the temporal logic of branching time". In: *Proceedings of the fourteenth annual ACM symposium on Theory of computing*. ACM, pp. 169–180.

Rosenthal, Jeffrey S (2006). *A first look at rigorous probability theory*. World Scientific Publishing Co Inc.