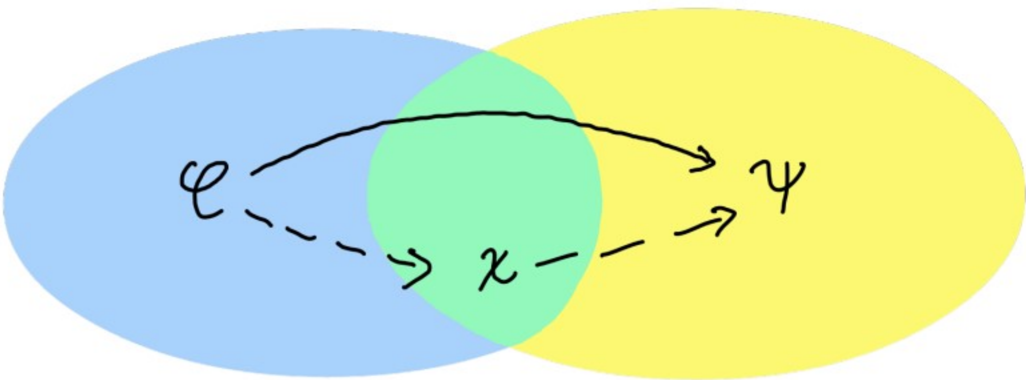
Interpolation through the Lens of Proof Theory

Iris van der Giessen

Lecture notes for Logic Summer School @ANU 2024
Canberra, Australia

(Version 20-12-2024)



Institute of Logic, Language and Computation
University of Amsterdam

Abstract

Craig interpolation is a fundamental concept in mathematical logic and computer science. Craig interpolants are formulas in a specified vocabulary that, intuitively speaking, explain why one formula entails the other. The existence of Craig interpolants is a useful property serving in many applications. For example, in knowledge representation, interpolants are used to enlarge knowledge bases by learning new concepts. In proof complexity, the feasible extraction of interpolants from proofs relates to the NP vs co-NP problem.

The goal of the course is to introduce theory and practice of interpolation through the lens of proof theory. Proof-theoretic techniques allow to explicitly construct interpolants which is useful in computations. We will discuss methods based on sequent calculi. We will discuss uniform interpolation, a strengthening of Craig's interpolation. We illustrate the applications of interpolation in the fields of universal proof theory, knowledge representation, and proof complexity.

For this course it is useful to have some prior knowledge on propositional logic, modal logic and sequent calculi.

Acknowledgements

I am very grateful to the organisers of the Logic Summer School @ANU 2024 for giving me the opportunity to offer this course. I thank Tom de Jong for the template to write these lecture notes in.

I would like to thank Rosalie Iemhoff, Raheleh Jalali, Roman Kuznets, Hugo Férée, Sam van Gool, and Ian Shillito for all good discussions in the last years which enables me to collect my best explanations on interpolation in proof theory in the first four chapters of these course notes. I thank Frank Wolter, Patrick Koopmann and Balder ten Cate for encouraging me to study interpolation in knowledge representation on which Chapter 5 is based. I especially thank Raheleh Jalali for her great course on Proof Complexity in the Proof Society School 2022 in Utrecht. From her I learned the use of interpolation in proof complexity on which the final chapter of these lecture notes is based.

These notes are written as past of the project *Finding Interpolants: Proofs in Action* with file number VI.Veni.232.369 of the research programme Veni financed by the Dutch Research Council (NWO).

If you find an inaccuracy of any kind, write to me at `i.vandergiessen@uva.nl`.

Contents

Chapter 1

Introduction

The study of interpolation in logic finds its roots in Craig's famous interpolation theorem for first order logic [Cra57]. A logic has *Craig interpolation* if for any provable implication $\varphi \to \psi$ there is an interpolant θ with non-logical symbols that occur in both φ and ψ such that the implications $\varphi \to \theta$ and $\theta \to \varphi$ are provable. One could say that the purpose of the interpolant is to state the reason why ψ is implied by φ by using the common language of the two. The theorem represents the 'last significant property of first-order logic that has come to light' [vBen08].

The significance of the Craig interpolation property and versions of it (such as *uniform interpolation*) stretch out over theory and applications. Let us list some examples.

- *Beth's definability theorem* [Bet53] follows from Craig interpolation and imposes a good theoretical balance between syntax and semantics.
- In *knowledge representation*, Beth's result is used to enlarge knowledge bases and uniform interpolation can be used to hide sensitive data from a knowledge base while preserving the knowledge base's integrity. (See *e.g.* [AJM+23; EK19].)
- In *automated deduction*, uniform interpolation is linked to *quantifier elimination* that reduces statements with quantifiers to equivalent statements without quantifiers that are easier to solve. (See *e.g.* [GSS08].)
- In *software verification*, it is used to simplify reasoning in model checking [McM03].
- In *model theory*, interpolation is linked to *Robinson's joint consistency theorem* [Rob56] enabling the elegant combination of theories.
- In *proof theory*, Craig interpolation features in a subfield called *universal proof theory* that solves question about the existence of sequent calculi for a given logic. (See *e.g.* [Iem19; AJ18a].)
- In *complexity theory*, the feasible extraction of interpolants from proofs relates to the NP vs coNP problem. (See *e.g.* [Kra19].)
- ...

1.1 Roadmap of the course

In this course we dive into the proof-theoretic methods to prove interpolation properties. Proof-theoretic techniques allow to explicitly construct interpolants, in contrast to many semantic methods that only state the existence of interpolants. We concentrate on propositional and modal logics and we focus on the sequent calculus. We illustrate the importance of Craig interpolation in three ways: in *universal proof theory*, *knowledge representation*, and *proof complexity*.

The course is outlined as follows:

- Chapter 2 introduces the basics of propositional logic and modal logic. We only provide the necessary definitions about axiomatisation, sequent calculi and semantics.
- Chapter 3 introduces the definition of Craig interpolation. We explain *Maehara's method* which is the first proof-theoretic proof of Craig interpolation [Mae61] and we discuss various extensions of Maehara's method. An important generalization is used in *universal proof theory*, a recent subfield in proof theory that aims to characterize and identify classes of proof systems in a uniform manner.
- Chapter 4 discusses a strengthening of Craig interpolation: *uniform interpolation*. We discuss a proof-theoretic method introduced by Pitts [Pit92].
- In Chapter 5 we deviate from proof theory and discuss applications of Craig and uniform interpolation in *description logics* used in *knowledge representation*. We introduce *description logics* which can be seen as variant of modal logic introduced in Chapter 2.
- In Chapter 6 we look at a useful application of Craig interpolation in the intersection of proof theory and complexity theory, namely in *proof complexity*. We will see the link between Craig interpolation and complexity problems.

1.2 Extra reading

The following chapters and papers form a good introduction to proof-theoretic techniques for interpolation. For explanations of Maehara's method we refer to [Ono98] and Chapter 1 in [Tak87]. For Pitts's method we recommend Pitts's paper itself [Pit92] and an easier variant for classical modal logic in [Bíl06]. For results in universal proof theory see [Iem19; AJ18a; AJ18b]. To the best of my knowledge, there is no textbook covering all these proof-theoretic techniques for interpolation. However, [GM05] presents many results on interpolation properties in propositional and modal logic using algebraic methods. For an introduction on description logic we recommend [BHLS17]. For applications of interpolation in description logic see *e.g.* [AJM+23; EK19]. For interpolation in proof complexity we refer to [Kra19] and the slides of Raheleh Jalali of the Proof Society School in Utrecht, 2022.

Chapter 2

Propositional and modal logics

In these lecture notes we restrict ourselves to the study of interpolation properties in propositional logics, intermediate logics, and modal logics. Interpolation plays also an important in first-order logic, but this will fall outside the scope of these lectures.

2.1 Axiomatization

We assume familiarity with propositional logic. We quickly recall definitions.

Fix a countable set of propositions variables Prop $= \{p, q, \ldots\}$. For propositional logic we work with the following grammar:

$$\varphi, \psi \quad ::= \quad \top \quad | \quad \bot \quad | \quad p \in \mathsf{Prop} \quad | \quad \varphi \to \psi \quad | \quad \varphi \vee \psi \quad | \quad \varphi \wedge \psi$$

We use the standard abbreviation $\neg\varphi := \varphi \to \bot$. The set of all formulas is denoted by Form. We assume that the reader is familiar with the axiomatization of *classical propositional logic* CPC and *intuitionistic propositional logic* IPC. Recall that both feature the rule modus ponens:

$$\frac{\varphi \to \psi \quad \varphi}{\psi}$$

An **intermediate logic** is an extension of IPC with extra axioms and is closed under the rule modus ponens. For example Gödel-Dummett logic G is defined as G $:=$ IPC $+ (\varphi \to \psi) \vee (\psi \to \varphi)$ where everything becomes linear. We will only consider finitely axiomatized logics. See [TvD88] for introductions on propositional logic. For an intermediate logic L, we write $\varphi \in$ L if φ follows from the axiomatization.

For **modal logic** we define the basic definitions necessary for this course. For a full introduction we refer to [BRV01]. We work with the grammar:

$$\varphi, \psi \quad ::= \quad \top \quad | \quad \bot \quad | \quad p \in \mathsf{Prop} \quad | \quad \varphi \to \psi \quad | \quad \varphi \vee \psi \quad | \quad \varphi \wedge \psi \quad | \quad \Box\varphi$$

The dual $\Diamond$ of the modality $\Box$ is defined as usual by $\Diamond\varphi := \neg\Box\neg\varphi$. This is the basic modal language and is flexibly used for many applications. For example, *alethic* modalities express $\Box\varphi$ as 'it is necessary that φ' (dually $\Diamond\varphi$ as 'it is possible that φ'), *epistemic* modalities modeling $\Box\varphi$ as 'it is known that φ'. Other examples are *temporal* modalities modeling truth over time useful in formal verification, and *provability* modalities expressing provability in arithmetical theories.

Figure 2.1 states common modal axioms. Figure 2.2 presents basic modal logics. Each classical modal logic should be understood as closed under modus ponens and the necessitation rule.

(k)	$\Box(p \to q) \to (\Box p \to \Box q)$	*normality axiom*
(t)	$\Box p \to p$	*reflection axiom*
(4)	$\Box p \to \Box\Box p$	*transitivity axiom*
(5)	$\neg\Box p \to \Box\neg\Box p$	*Euclidean axiom*
(wlob)	$\Box(\Box p \to p) \to \Box p$	*weak Löb axiom*
(N)	$\dfrac{\varphi}{\Box\varphi}$	*necessitation rule*

Figure 2.1: Modal axioms and rules. For those who are familiar with semantics of modal logics: the names of the axioms come from their corresponding properties in relational semantics from Section 2.2.

$\mathsf{K} := \mathsf{CPC} + (\mathsf{k})$	alethic logic
$\mathsf{T} := \mathsf{K} + (\mathsf{t})$	
$\mathsf{K4} := \mathsf{K} + (4)$	
$\mathsf{S4} := \mathsf{K} + (\mathsf{t}) + (4)$	epistemic logic
$\mathsf{S5} := \mathsf{K} + (\mathsf{t}) + (5)$	epistemic logic
$\mathsf{GL} := \mathsf{K} + (\mathsf{wlob})$	provability logic

Figure 2.2: Classical modal logics. Each logic is closed under modus ponens and the necessitation rule.

In Chapter 5 we will introduce *description logics* which are a form of modal logics used in knowledge representation.

2.2 Semantics

We assume that the reader is familiar with the truth table semantics of classical propositional logic. This can be written as follows.

Definition 2.1. Let $V \subseteq \mathsf{Prop}$ be a subset of propositional variables, called a **valuation**. The **satisfaction relation** $\models \subseteq \mathcal{P}(\mathsf{Prop}) \times \mathsf{Form}$ is defined inductively as follows.

$$
\begin{aligned}
&V \models p && \text{iff } p \in V \\
&V \models \top && \\
&V \not\models \bot && \\
&V \models \varphi \to \psi && \text{iff } V \not\models \varphi \text{ or } V \models \psi \\
&V \models \varphi \vee \psi && \text{iff } V \models \varphi \text{ or } V \models \psi \\
&V \models \varphi \wedge \psi && \text{iff } V \models \varphi \text{ and } V \models \psi.
\end{aligned}
$$

We say that φ is **classically valid** if $V \models \varphi$ for all valuations V.

Theorem 2.2. *$\varphi \in \mathsf{CPC}$ iff φ is classically valid.*

The semantics of modal logic can be seen as an extension of the classical propositional semantics. Now we evaluate formulas in a relational structure with so-called *possible worlds.* A modalized formula $\Box\varphi$ is true at a world if φ holds in all its accessible worlds. See [BRV01] for a full introduction on modal semantics.

Definition 2.3. Let $\mathcal{M} = (W, R, V)$ be a triple with a non-empty set W where its elements are called **worlds**, a binary relation $R \subseteq W \times W$ called the **accessibility relation** and a function $V : W \to \mathcal{P}(\mathsf{Prop})$ called a **valuation**. We call $\mathcal{M}$ a **model**. We define the **modal satisfaction relation** $\models$ inductively as follows where $\mathcal{M} = (W, R, V)$ is a model and $w \in W$:

$$
\begin{aligned}
&\mathcal{M}, w \models p && \text{iff } p \in V(w) \\
&\mathcal{M}, w \models \top && \\
&\mathcal{M}, w \not\models \bot && \\
&\mathcal{M}, w \models \varphi \to \psi && \text{iff } \mathcal{M}, w \not\models \varphi \text{ or } \mathcal{M}, w \models \psi \\
&\mathcal{M}, w \models \varphi \vee \psi && \text{iff } \mathcal{M}, w \models \varphi \text{ or } \mathcal{M}, w \models \psi \\
&\mathcal{M}, w \models \varphi \wedge \psi && \text{iff } \mathcal{M}, w \models \varphi \text{ and } \mathcal{M}, w \models \psi. \\
&\mathcal{M}, w \models \Box\varphi && \text{iff for all } v \text{ such that } wRv, \mathcal{M}, w \models \varphi \\
&\mathcal{M}, w \models \Diamond\varphi && \text{iff there exists } v \text{ such that } wRv \text{ and } \mathcal{M}, w \models \varphi.
\end{aligned}
$$

We say that φ is **valid in** $\mathcal{M} = (W, R, V)$ if $\mathcal{M}, w \models \varphi$ for all worlds $w \in W$.

Soundness and completeness results for the different modal logics in Figure 2.2 depend on restrictions on the accessibility relation in the models, such as *transitivity*, *reflexivity*, etc. We only state soundness and completeness without proof.

Theorem 2.4 (Soundness and completeness)**.**
- *$\varphi \in \mathsf{K}$ iff φ is valid in all relational models.*
- *$\varphi \in \mathsf{T}$ iff φ is valid in all reflexive models.*
- *$\varphi \in \mathsf{K4}$ iff φ is valid in all transitive models.*

- *$\varphi \in \mathsf{S4}$ iff φ is valid in all reflexive and transitive models.*
- *$\varphi \in \mathsf{S5}$ iff φ is valid in all total models (every world is related to every other world including itself).*
- *$\varphi \in \mathsf{GL}$ iff φ is valid in all transitive and conversely well-founded models (there are no infinite R-paths).*

For convenience later, we call a total model an S5-model.

2.3 Sequent calculi

Proof systems contain inference rules that provide a transparent step-by-step way to determine the valid principles of a given logic. In these lecture notes we concentrate on sequent calculi that originate from Gentzen in 1935. The analysis of sequent calculi can reveal many important properties of the logic at hand such as consistency, decidability, and Craig interpolation!

A **sequent** is an expression of the form $\Gamma \Rightarrow \Delta$ where Γ and Δ are finite multisets of formulas. Γ is called the **antecedent** and Δ is called its **succedent**. They are both referred to as **cedents**.

The intended meaning of a sequent $\varphi_1, \dots, \varphi_m \Rightarrow \psi_1, \dots, \psi_n$ is the formula

$$\bigwedge_{i=1}^{m} \varphi_i \supset \bigvee_{j=1}^{n} \psi_j,$$

also called the **formula interpretation** of the sequent. We adopt the convention that an empty conjunction (say, when $m = 0$ above) is $\top$ and an empty disjunction (say, when $n = 0$ above) is $\bot$.

For convenience, we work with standard multiset sequent calculi in which contraction and weakening are built in into the rules following the tradition of [TS00; NvPR01]. Figure 2.3 presents the sequent calculus G3pc for classical logic CPC. Figure 2.4 presents calculus G3pi for intuitionistic logic IPC in which each sequent obeys the restriction that the succedent has at most one formula.

For modal logics, one can enrich the propositional calculi by modal rules. Figure 2.5 presents some well-known classical modal sequent rules. We write $\Box\Gamma := \{\Box\varphi \mid \varphi \in \Gamma\}$. Calculus G3pi can be enriched by modal rules yielding a certain class of intuitionistic modal logics, but these fall outside the scope of these lecture notes (see [Gie22] for details).

Let us fix some terminology. Each inference rule should be understood as a rule scheme in which any context and formula of the right shape can be used. The upper sequents of a rule are called **premisse(s)** and the lower sequent is called the **conclusion**. A rule with no premisses is called an **axiom**. The distinguished formula in the conclusion is called the **principal formula**. The cedents like Γ, Δ, etc are called the **context**. The intended reading is from top to bottom *viz.* assuming the premisses, the conclusion is true. A **proof** in a given sequent calculus SC is a rooted tree, in which the nodes are sequents, generated inductively from *inference rules* of SC. The root of the tree is called the **endsequent** and is the sequent proved by the proof. Subtrees of a proof are called **subproofs**. We write $\vdash_{\mathsf{SC}} \Gamma \Rightarrow \Delta$ if there is a proof in sequent calculus SC for $\Gamma \Rightarrow \Delta$.

Soundness and completeness theorems make it formal that the considered sequent calculi indeed represent their corresponding logic. We present the theorems without proof.

Theorem 2.5 (Soundness and completeness)**.**
- $\varphi \in \mathsf{IPC}$ *iff* $\vdash_{\mathsf{G3pi}} \Rightarrow \varphi$,
- $\varphi \in \mathsf{CPC}$ *iff* $\vdash_{\mathsf{G3pc}} \Rightarrow \varphi$,
- *For any* $\mathsf{L} \in \{\mathsf{K}, \mathsf{T}, \mathsf{K4}, \mathsf{S4}, \mathsf{GL}\}$, $\varphi \in \mathsf{L}$ *iff* $\vdash_{\mathsf{G3L}} \Rightarrow \varphi$.

Below we present some important rules. These rules are admissible in the considered proof systems. This means that the addition of these rules to one of our calculi does not yield new sequents.

$$\text{form-init}\ \frac{}{\varphi, \Gamma \Rightarrow \Delta, \varphi}$$

$$\text{w}_l\ \frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \qquad \text{w}_r\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi} \qquad \text{c}_l\ \frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \qquad \text{c}_r\ \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}$$

$$\text{cut}\ \frac{\Gamma \Rightarrow \Delta, \varphi \qquad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Rule form-init is an extended version of init where we allow for formulas and is sometimes called **axiom expansion**.

Weakening and **contraction** rules are structural rules and are the equivalent of resource management in programs. Contraction allows one to duplicate resources, and weakening allows one to discard resources. As mentioned before, weakening and contraction rules are admissible in all considered calculi (modulo the single-succedent condition for intuitionistic calculus G3pi).

The **cut rule** has a special status in proof theory. It tells us that we can reuse lemma's in proofs once we have proved the lemma. It features prominently in completeness results. More important to note is that the cut rule is admissible in all considered calculi. The famous cut-elimination theorem by Gentzen has far reaching applications such as consistency and decidability results. In the next chapter we see its upmost importance for the first proof-theoretic proof of Craig interpolation.

Identity rule:

$$\text{init}\ \frac{}{p, \Gamma \Rightarrow \Delta, p}$$

Left rules:

$$\bot_l\ \frac{}{\bot, \Gamma \Rightarrow \Delta} \qquad \to_l\ \frac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta} \qquad \vee_l\ \frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \qquad \wedge_l\ \frac{\varphi, \psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}$$

Right rules:

$$\top_r\ \frac{}{\Gamma \Rightarrow \Delta, \top} \qquad \to_r\ \frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \to \psi} \qquad \vee_r\ \frac{\Gamma \Rightarrow \Delta, \varphi, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \qquad \wedge_r\ \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}$$

Figure 2.3: Inference rules of G3pc

Identity rule:

$$\text{init}\ \frac{}{p, \Gamma \Rightarrow p}$$

Left rules:

$$\bot_l\ \frac{}{\bot, \Gamma \Rightarrow \Delta} \qquad \to_l\ \frac{\varphi \to \psi, \Gamma \Rightarrow \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta} \qquad \vee_l\ \frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \qquad \wedge_l\ \frac{\varphi, \psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}$$

Right rules:

$$\top_r\ \frac{}{\Gamma \Rightarrow \top} \qquad \to_r\ \frac{\varphi, \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \to \psi} \qquad \vee_r^i\ \frac{\Gamma \Rightarrow \varphi_i}{\Gamma \Rightarrow \varphi_0 \vee \varphi_1}\ i = 0, 1 \qquad \wedge_r\ \frac{\Gamma \Rightarrow \varphi \quad \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \wedge \psi}$$

Figure 2.4: Inference rules of G3pi. Δ consists of at most one formula.

Modal rules:

$$K\ \frac{\Gamma \Rightarrow \varphi}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Delta} \qquad 4\ \frac{\Box\Gamma, \Gamma \Rightarrow \varphi}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Delta} \qquad S4\ \frac{\Box\Gamma \Rightarrow \varphi}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Delta}$$

$$T\ \frac{\Box\varphi, \varphi, \Gamma \Rightarrow \Delta}{\Box\varphi, \Gamma \Rightarrow \Delta} \qquad GL\ \frac{\Box\Gamma, \Gamma, \Box\varphi \Rightarrow \varphi}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Delta}$$

Modal sequent calculi:

$$\begin{aligned} \text{G3K} &:= \text{G3pc} + K \\ \text{G3T} &:= \text{G3K} + T \\ \text{G3K4} &:= \text{G3pc} + 4 \\ \text{G3S4} &:= \text{G3pc} + S4 + T \\ \text{G3GL} &:= \text{G3pc} + GL \end{aligned}$$

Figure 2.5: Modal rules and modal sequent calculi. Logic $\mathsf{L} \in \{\mathsf{K}, \mathsf{T}, \mathsf{K4}, \mathsf{S4}, \mathsf{GL}\}$ is sound and complete w.r.t. sequent calculus G3L.

2.4 Hypersequent calculi

I did not discuss this section in the lectures.

Not all logics can be described by a cut-free sequent calculus. Examples are intermediate Gödel-Dummett logic G and modal logic S5. The informal reason for that is that the sequent calculus does not provide enough structure to reason in these logics. The sequent arrow $\Rightarrow$ provides structural reasoning for $\to$. Informally speaking, for G one needs to be able to reason under the $\vee$ to break down axiom $(\varphi \to \psi) \vee (\psi \to \varphi)$, and for modal logic S5 one needs to be able to reason under the $\Box$ to handle symmetry of the models.

There are multiple ways to add structure to sequents which has led to different variants like *nested sequents*, *hypersequents*, and *labelled sequents*. Here we only introduce hypersequents to get an impression of what such generalizations of standard sequents can look like. After that we present a cut-free hypersequent for S5.

A **hypersequent** is a multiset of sequents $\Gamma_i \Rightarrow \Delta_i$ which we write in the following notation:

$$\Gamma_1 \Rightarrow \Delta_1 \mid \cdots \mid \Gamma_n \Rightarrow \Delta_n.$$

We use letter $\mathcal{G}$ to denote hypersequents. For $\mathcal{G}$ as in the form above, we call each $\Gamma_i \Rightarrow \Delta_i$ a **sequent component** of $\mathcal{G}$ and we say that the **length** of $\mathcal{G}$ is n.

In modal logic, the **formula interpretation** of hypersequent $\Gamma_1 \Rightarrow \Delta_1 \mid \cdots \mid \Gamma_n \Rightarrow \Delta_n$ is the formula

$$\Box(\bigwedge \Gamma_1 \to \bigvee \Delta_1) \vee \cdots \vee \Box(\bigwedge \Gamma_n \to \bigvee \Delta_n).$$

Figure 2.6 presents a hypersequent calculus for S5 that we call HS5 (the first hypersequent calculi for S5 were independently defined in [Min68; Pot83; Avr96]). The left and right propositional rules are almost the same as the usual sequent rules in the sense that they only modify one sequent component. The modal rules $\Box_l$ and $\Box_r$ are more important, because these modify the hypersequent. Rule $\Box_r$ introduces a new sequent component in the premise. Rule $\Box_l$ affects a sequent component that is different from the component in which the principal formula occurs.

Example 2.6. Formula $\Box\neg\Box p \vee p$ is true in S5. Here we provide a hypersequent proof for it.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \Rightarrow \Box\neg\Box p, p \mid \Box p \Rightarrow \bot}\ \text{init}}{\Rightarrow \Box\neg\Box p, p \mid \Box p \Rightarrow \bot}\ \Box_l}{\Rightarrow \Box\neg\Box p, p \mid \Rightarrow \neg\Box p}\ \to_r}{\Rightarrow \Box\neg\Box p, p}\ \Box_r}{\Rightarrow \Box\neg\Box p \vee p}\ \vee_r$$

Identity rule:

$$\text{init}\ \frac{}{\mathcal{G} \mid p, \Gamma \Rightarrow \Delta, p}$$

Left rules:

$$\bot_l\ \frac{}{\mathcal{G} \mid \bot, \Gamma \Rightarrow \Delta} \qquad \to_l\ \frac{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi \quad \mathcal{G} \mid \psi, \Gamma \Rightarrow \Delta}{\mathcal{G} \mid \varphi \to \psi, \Gamma \Rightarrow \Delta}$$

$$\vee_l\ \frac{\mathcal{G} \mid \varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\mathcal{G} \mid \varphi \vee \psi, \Gamma \Rightarrow \Delta} \qquad \wedge_l\ \frac{\mathcal{G} \mid \varphi, \Gamma \Rightarrow \Delta}{\mathcal{G} \mid \varphi \wedge \psi, \Gamma \Rightarrow \Delta}$$

Right rules:

$$\top_r\ \frac{}{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \top} \qquad \to_r\ \frac{\mathcal{G} \mid \varphi, \Gamma \Rightarrow \Delta, \psi}{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi \to \psi}$$

$$\vee_r\ \frac{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi, \psi}{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi \vee \psi} \qquad \wedge_r\ \frac{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi \quad \mathcal{G} \mid \Gamma \Rightarrow \Delta, \psi}{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi \wedge \psi}$$

Modal rules:

$$\Box_r\ \frac{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \Box\varphi \mid \Rightarrow \varphi}{\mathcal{G} \mid \Gamma \Rightarrow \Delta, \Box\varphi} \qquad \Box_l\ \frac{\mathcal{G} \mid \Box\varphi\Gamma \Rightarrow \Delta \mid \varphi, \Gamma' \Rightarrow \Delta'}{\mathcal{G} \mid \Box\varphi\Gamma \Rightarrow \Delta \mid \Gamma' \Rightarrow \Delta'} \qquad T\ \frac{\mathcal{G} \mid \Box\varphi, \varphi, \Gamma \Rightarrow \Delta, \varphi, \psi}{\mathcal{G} \mid \Box\varphi\Gamma \Rightarrow \Delta}$$

Figure 2.6: Inference rules of hypersequent calculus HS5

Theorem 2.7 (Soundness and completeness). *Hypersequent* $\Gamma_1 \Rightarrow \Delta_1 \mid \cdots \mid \Gamma_n \Rightarrow \Delta_n$ *is provable in* HS5 *if and only if its formula interpretation* $\Box(\bigwedge \Gamma_1 \to \bigvee \Delta_1) \vee \cdots \vee \Box(\bigwedge \Gamma_n \to \bigvee \Delta_n)$ *is true in* S5.

We state the soundness and completeness theorem without proof. The idea is that each sequent component of the hypersequent represents reasoning in a different world of a relational model.

Instead of using the formula interpretation, there is also another way to interpret hypersequents in a relational model. This is a componentwise approach.

Definition 2.8. Let $\mathcal{M}$ be an S5-model and let $\overline{w} = w_1, \ldots, w_n$ be a tuple of n worlds in $\mathcal{M}$. Let $\mathcal{G} = \Gamma_1 \Rightarrow \Delta_1 \mid \cdots \mid \Gamma_n \Rightarrow \Delta_n$ be a hypersequent. We define

$$\mathcal{M}, \overline{w} \models \mathcal{G} \quad \text{iff} \quad \mathcal{M}, w_i \models \bigwedge \Gamma_i \to \bigwedge \Delta_i \text{ for some } i.$$

We say that hypersequent $\mathcal{G}$ of length n is **componentwise valid** in S5 if $\mathcal{M}, \overline{w} \models \mathcal{G}$ for any S5-model $\mathcal{M}$ and any tuple $\overline{w}$ of n worlds in $\mathcal{M}$.

Theorem 2.9 (Componentwise soundness and completeness). *Hypersequent* $\mathcal{G}$ *is provable in* HS5 *if and only if* $\mathcal{G}$ *is componentwise valid in* S5.

Chapter 3

Craig interpolation via proof theory

3.1 Craig interpolation

The beauty of Craig's interpolation theorem lies in its simple formulation with its far reaching applications as mentioned in the Introduction. Intuitively, Craig interpolants are formulas in a specified vocabulary that *explain* why one formula entails the other. This is a very natural property to wish for, but it turns out that Craig interpolation is quite rare among intermediate and modal logics!

Definition 3.1. The **vocabulary** of a formula φ, denoted $\mathsf{Voc}(\varphi)$, is the set of propositional variables in φ. For a cedent Γ, $\mathsf{Voc}(\Gamma) = \bigcup_{\varphi\in\Gamma} \mathsf{Voc}(\varphi)$.

Remark 3.2. If one would like to consider first-order logic, the vocabulary consists of relational and function symbols occurring in a first-order formula φ. As mentioned before, these lecture notes do not treat first-order logic.

Definition 3.3 (Craig's interpolation)**.** A logic L has the **Craig interpolation property**, if whenever $\vdash_{\mathsf{L}} \varphi \to \psi$, there is a formula θ such that:

1. $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi)$,
2. $\vdash_{\mathsf{L}} \varphi \to \theta$ and $\vdash_{\mathsf{L}} \theta \to \psi$.

The formula θ is called an **interpolant** of $\varphi \to \psi$.

Craig interpolation can be visualized as in Figure 3.1.

Remark 3.4. The Craig interpolation property presented in Definition3.3 is also known as the *local* Craig interpolation property. The reason is that it interpolates the local symbol $\to$ corresponding to what is called the *local consequence relation*. One can also interpolate the *global consequence relation* $\models$ as we will discuss in Chapter 5.

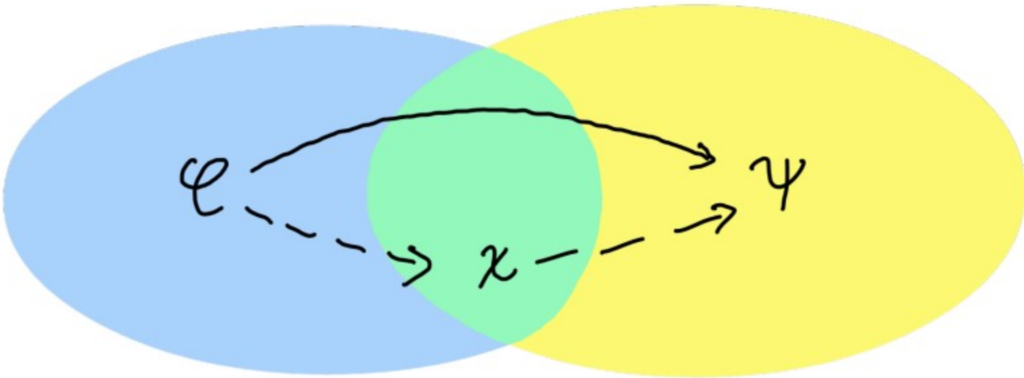


Figure 3.1: χ is a Craig interpolant for $\varphi \to \psi$. Blue indicates the set of formulas in $\mathsf{Voc}(\varphi)$ and yellow the formulas in $\mathsf{Voc}(\psi)$.

Example 3.5 (Interpolants are not necessarily unique)**.** Let $\varphi = (p_1 \wedge p_2) \vee (\neg p_3 \wedge q)$ and $\psi = r \vee p_1 \vee p_2 \vee \neg p_3$. We have $\vdash_{\mathsf{CPC}} \varphi \to \psi$ and that $\mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi) = \{p_1, p_2, p_3\}$. There are multiple interpolants *viz.* $(p_1 \wedge p_2) \vee \neg p_3$, $p_1 \vee \neg p_3$, $p_2 \vee \neg p_3$, and $p_1 \vee p_2 \vee \neg p_3$.

Exercise 3.6 (The space of interpolants)**.** Let $C(\varphi, \psi)$ be the set of Craig interpolants of $\vdash \varphi \to \psi$. Prove the following properties.

1. $C(\varphi, \psi)$ is closed under conjunction, *i.e.* if $\theta_1, \theta_2 \in C(\varphi, \psi)$, then $\theta_1 \wedge \theta_2 \in C(\varphi, \psi)$.
2. $C(\varphi, \psi)$ is closed under disjunction, *i.e.* if $\theta_1, \theta_2 \in C(\varphi, \psi)$, then $\theta_1 \vee \theta_2 \in C(\varphi, \psi)$.

Example 3.7. The logics CPC, IPC, K, K4, S4, S5, and GL all have the Craig interpolation property. This can be shown in various ways using semantics, algebra, or proof theory. Throughout these lecture notes we will discuss the proof-theoretic approach.

Surprisingly, there are many intermediate and modal logics that do not admit Craig interpolation. These theorems are shown by *algebraic* methods.

Theorem 3.8 ([Mak77])**.** *Only 7 consistent intermediate logics have Craig interpolation. Among them are* IPC *and* CPC*.*

Theorem 3.9 ([Mak79; CZ97])**.** *At most 37 modal logics extending* S4 *enjoy Craig interpolation. For* GL*, there is a continuum of extensions with Craig interpolation, but also a continuum without Craig interpolation.*

3.2 Maehara's method

Theorem 3.10. *Classical propostional logic* CPC *has the Craig interpolation property.*

Several proofs of interpolation are known in the literature for various logics. We will focus on a proof-theoretic technique known as **Maehara's method**. The idea is to formulate a sequent-based interpolation property that is at least as strong as the Craig interpolation property. To do this, we will set up some notation.

Definition 3.11. Let SC be a sequent calculus. Let Γ, Γ', Δ, and Δ' be cedents and θ be a formula such that $\mathrm{Voc}(\theta) \subseteq \mathrm{Voc}(\Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta')$, $\vdash_{\mathrm{SC}} \Gamma \Rightarrow \Delta, \theta$, and $\vdash_{\mathrm{SC}} \theta, \Gamma' \Rightarrow \Delta'$. We write these properties in short by $\vdash_{\mathrm{SC}} \Gamma; \Gamma' \overset{\theta}{\Rightarrow} \Delta; \Delta'$. We call $\Gamma; \Gamma' \Rightarrow \Delta; \Delta'$ a **split sequent**.

Maehara's method uses the following sequent formulation of Craig interpolation.

Lemma 3.12 (Maehara's method)**.** *Suppose* $\vdash_{\mathrm{G3pc}} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$. *Then, there exists* $\theta \in \mathsf{Form}$ *such that* $\vdash_{\mathrm{G3pc}} \Gamma; \Gamma' \overset{\theta}{\Rightarrow} \Delta; \Delta'$.

Theorem 3.10 follows immediately from Lemma 3.12.

Proof of Theorem 3.10. Since G3pc forms a sequent calculus for CPC we have that $\vdash_{\mathrm{G3pc}} \varphi \Rightarrow \psi$. Plugging $\Gamma = \varphi$, $\Gamma' = \varnothing$, $\Delta = \varnothing$, and $\Delta' = \psi$ in Lemma 3.12, we have that there exists θ such that $\varphi; \varnothing \overset{\theta}{\Rightarrow} \varnothing; \psi$. These form exactly the properties of Craig's interpolation. □

Proof of Lemma 3.12. Suppose $\vdash_{\mathrm{G3pc}} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$. Let π be a proof of $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$. We will construct an interpolant θ by induction on the structure of π. In other words, starting from the axioms of π, we recursively define the interpolants from premises to conclusion for each rule in the proof.

The base case is an application of the init, $\top_r$, or $\bot_l$ rule. However, since we have split sequents we have several cases, depending on which side of the *split* the formulas are. We will treat one salient case:

$$\pi = \mathsf{init}\ \frac{}{\Gamma; \Gamma', p \Rightarrow \Delta; \Delta', p}$$

We claim that $\theta = \top$. Indeed, $\mathrm{Voc}(\top) = \varnothing \subseteq \mathrm{Voc}(\Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta', p)$, $\vdash_{\mathrm{G3pc}} \Gamma \Rightarrow \Delta, \top$ and $\vdash_{\mathrm{G3pc}} \Gamma', p \Rightarrow \Delta', p$.

For the induction step, there are several subcases based on the bottommost rule of π. Again, the cases are doubled because of the split sequents. We will treat two cases.

- The bottom-most rule is an instance of $\to_l$ of the following form. Note that the split in the conclusion is fixed, but that we have chosen appropriate splits in the premisses.

$$\pi = \quad \to_l \frac{\overset{\pi_1}{\Gamma'; \Gamma \Rightarrow \Delta'; \Delta, \varphi} \qquad \overset{\pi_2}{\psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}}{\varphi \to \psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}$$

By applying the induction hypothesis on π_1 and π_2, there are interpolants θ_1 and θ_2 such that $\Gamma'; \Gamma \overset{\theta_1}{\Longrightarrow} \Delta'; \Delta, \varphi$ and $\psi, \Gamma; \Gamma' \overset{\theta_2}{\Longrightarrow} \Delta; \Delta'$. Note that we have chosen the split in the left premise such that Γ' and Δ' are on the left side of the split and Γ, Δ, and φ are on the right side of the split. This enables as to prove that $\theta = \theta_1 \to \theta_2$ is the desired interpolant. Indeed,

$$\begin{aligned}
\mathsf{Voc}(\theta) &= \mathsf{Voc}(\theta_1) \cup \mathsf{Voc}(\theta_2) \\
&\subseteq (\mathsf{Voc}(\Gamma', \Delta') \cap \mathsf{Voc}(\Gamma, \Delta, \varphi)) \cup (\mathsf{Voc}(\psi, \Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')) \quad (*) \\
&= (\mathsf{Voc}(\varphi, \Gamma, \Delta) \cup \mathsf{Voc}(\psi, \Gamma, \Delta)) \cap \mathsf{Voc}(\Gamma', \Delta') \\
&= \mathsf{Voc}(\varphi \to \psi, \Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')
\end{aligned}$$

Line $(*)$ follows by induction. It remains to check that $\vdash_{\mathsf{G3pc}} \varphi \to \psi, \Gamma \Rightarrow \Delta, \theta_1 \to \theta_2$ and $\vdash_{\mathsf{G3pc}} \theta_1 \to \theta_2, \Gamma' \Rightarrow \Delta'$ by the following derivations. Note that rule weakening w is admissible in the calculus.

$$\dfrac{\dfrac{\dfrac{\dfrac{IH}{\Gamma, \theta_1 \Rightarrow \Delta, \varphi}}{\Gamma, \theta_1 \Rightarrow \Delta, \theta_2, \varphi}\,\mathsf{w} \qquad \dfrac{\dfrac{IH}{\psi, \Gamma \Rightarrow \Delta, \theta_2}}{\psi, \Gamma, \theta_1 \Rightarrow \Delta, \theta_2}\,\mathsf{w}}{\varphi \to \psi, \Gamma, \theta_1 \Rightarrow \Delta, \theta_2}\,\to_l}{\varphi \to \psi, \Gamma \Rightarrow \Delta, \theta}\,\to_r \qquad \dfrac{\dfrac{IH}{\Gamma' \Rightarrow \Delta', \theta_1} \qquad \dfrac{IH}{\theta_2, \Gamma' \Rightarrow \Delta'}}{\theta_1 \to \theta_2, \Gamma' \Rightarrow \Delta'}\,\to_l$$

- The bottom-most rule is an instance of $\vee_l$ of the following form.

$$\pi = \dfrac{\dfrac{\pi_1}{\varphi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'} \qquad \dfrac{\pi_2}{\psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}}{\varphi \vee \psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}\,\vee_l$$

By applying induction hypothesis on π_1 and π_2, we have $\varphi, \Gamma; \Gamma' \overset{\theta_1}{\Longrightarrow} \Delta; \Delta'$ and $\psi, \Gamma; \Gamma' \overset{\theta_2}{\Longrightarrow} \Delta; \Delta'$ for some θ_1, θ_2. We claim that $\theta = \theta_1 \vee \theta_2$.

$$\begin{aligned}
\mathsf{Voc}(\theta) &= \mathsf{Voc}(\theta_1) \cup \mathsf{Voc}(\theta_2) \\
&\subseteq (\mathsf{Voc}(\varphi, \Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')) \cup (\mathsf{Voc}(\psi, \Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')) \quad (**) \\
&= (\mathsf{Voc}(\varphi, \Gamma, \Delta) \cup \mathsf{Voc}(\psi, \Gamma, \Delta)) \cap \mathsf{Voc}(\Gamma', \Delta') \\
&= \mathsf{Voc}(\varphi \vee \psi, \Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')
\end{aligned}$$

Line $(**)$ holds by induction. We have $\vdash_{\mathsf{PK}} \varphi \vee \psi, \Gamma \Rightarrow \Delta, \theta$ and $\vdash_{\mathsf{PK}} \theta, \Gamma' \Rightarrow \Delta'$ as follows.

$$\dfrac{\dfrac{\dfrac{IH}{\varphi, \Gamma \Rightarrow \Delta, \theta_1}}{\varphi, \Gamma \Rightarrow \Delta, \theta}\,\vee_r^0 \qquad \dfrac{\dfrac{IH}{\varphi, \Gamma \Rightarrow \Delta, \theta_2}}{\psi, \Gamma \Rightarrow \Delta, \theta}\,\vee_r^1}{\varphi \vee \psi, \Gamma \Rightarrow \Delta, \theta}\,\vee_l \qquad \dfrac{\dfrac{IH}{\theta_1, \Gamma' \Rightarrow \Delta'} \qquad \dfrac{IH}{\theta_2, \Gamma' \Rightarrow \Delta'}}{\theta, \Gamma' \Rightarrow \Delta'}\,\vee_l$$

The interpolant construction for each case is summarized in Figure 3.2. The reader is encouraged to verify them. □

Remark 3.13 (Splits are necessary). In classical logic, the split in Maehara's sequents represents the implication that we interpolate shown by De Morgan's laws:

$$\Gamma;\Gamma' \Rightarrow \Delta;\Delta' \text{ corresponds to } \bigwedge \Gamma \wedge \bigwedge \neg\Delta' \to \bigvee \Delta \vee \bigvee \neg\Gamma'.$$

One might wonder why we cannot use normal sequents since these also represents an implication, *i.e.* sequent $\Gamma \Rightarrow \Delta$ is interpreted as $\bigwedge \Gamma \to \bigvee \Delta$. However, the split in Maehara's method is necessary because of the presence of *non-monotone* connective $\to$. Consider rule $\to_r$ with Γ on the left and Δ and $\varphi \to \psi$ on the right.

$$\to_r \frac{\Gamma, \varphi \overset{\theta}{\Rightarrow} \Delta, \psi}{\Gamma \overset{?}{\Rightarrow} \Delta, \varphi \to \psi}$$

In this situation, the induction hypothesis applied to the premise gives us $\mathrm{Voc}(\theta) \subseteq \mathrm{Voc}(\Gamma, \varphi) \cap \mathrm{Voc}(\Delta, \psi)$. Since φ in the premisse 'swaps' sides, it is not possible to find a guaranteed interpolant, say θ', such that $\mathrm{Voc}(\theta') \subseteq \mathrm{Voc}(\Gamma) \cap \mathrm{Voc}(\Delta, \varphi \to \psi)$. In Figure 3.2 one can see that the split makes it possible to keep φ on the 'right' side.

Remark 3.14. Cut-freeness seems crucial for the proof since it is not clear how to obtain an interpolant for the conclusion of an instance of the cut from the interpolants of the premisses. However, one might use restricted forms of cut as discussed in the next section.

Remark 3.15. Note that our proof is *constructive* and it gives a *non-deterministic* algorithm to construct interpolants. However, it has been shown that it is not possible to use this algorithm to generate all possible interpolants! [HJ24]

Exercise 3.16. Verify Example 3.5 using Maehara's method in the proof of Lemma 3.12. Which interpolant do you find? Can you find another interpolant by Maehara's method? Can you find all interpolants by Maehara's method?

Maehara's method is flexible and has been applied to IPC and many modal logics.

Example 3.17. All logics discussed so far have the Craig interpolation property. For logics IPC, K, T, K4, S4, and GL one can use Maehara's method using the calculi displayed in Figures 2.3, 2.4 and 2.5. Logic S5 does not have a suitable *cut-free* sequent calculus. For this we need a more powerful calculus as discussed in Section 2.4.

Exercise 3.18. Perform the modal cases for Maehara's method that prove the Craig interpolation property for logic K using sequent calculus G3K.

Initial rule:

$$\text{init}\,\frac{}{\Gamma;\Gamma',p \xRightarrow{\top} \Delta;\Delta',p} \qquad \text{init}\,\frac{}{p,\Gamma;\Gamma' \xRightarrow{p} \Delta;\Delta',p} \qquad \text{init}\,\frac{}{\Gamma;\Gamma',p \xRightarrow{\neg p} p,\Delta;\Delta'} \qquad \text{init}\,\frac{}{p,\Gamma;\Gamma' \xRightarrow{\bot} p,\Delta;\Delta'}$$

Boolean rules:

$$\bot_l\,\frac{}{\Gamma;\Gamma',\bot \xRightarrow{\top} \Delta;\Delta'} \qquad \bot_l\,\frac{}{\bot,\Gamma;\Gamma' \xRightarrow{\bot} \Delta;\Delta'} \qquad \top_r\,\frac{}{\Gamma;\Gamma' \xRightarrow{\top} \Delta;\Delta',\top} \qquad \top_r\,\frac{}{\Gamma;\Gamma' \xRightarrow{\bot} \top,\Delta;\Delta'}$$

Disjunction rules:

$$\vee_l\,\frac{\varphi,\Gamma;\Gamma' \xRightarrow{\theta_1} \Delta;\Delta' \quad \psi,\Gamma;\Gamma' \xRightarrow{\theta_2} \Delta;\Delta'}{\varphi\vee\psi,\Gamma;\Gamma' \xRightarrow{\theta_1\vee\theta_2} \Delta;\Delta'} \qquad \vee_l\,\frac{\Gamma;\Gamma',\varphi \xRightarrow{\theta_1} \Delta;\Delta' \quad \Gamma,;\Gamma',\psi \xRightarrow{\theta_2} \Delta;\Delta'}{\Gamma;\Gamma',\varphi\vee\psi \xRightarrow{\theta_1\wedge\theta_2} \Delta;\Delta'}$$

$$\vee_r\,\frac{\Gamma,\Gamma' \xRightarrow{\theta} \varphi,\psi,\Delta;\Delta'}{\Gamma,\Gamma' \xRightarrow{\theta} \varphi\vee\psi,\Delta;\Delta'} \qquad \vee_r\,\frac{\Gamma,\Gamma' \xRightarrow{\theta} \Delta;\Delta',\varphi,\psi}{\Gamma,\Gamma' \xRightarrow{\theta} \Delta;\Delta',\varphi\vee\psi}$$

Conjunction rules:

$$\wedge_l\,\frac{\varphi,\Gamma;\Gamma' \xRightarrow{\theta} \Delta;\Delta'}{\varphi\wedge\psi,\Gamma;\Gamma' \xRightarrow{\theta} \Delta;\Delta'} \qquad \wedge_l\,\frac{\Gamma;\Gamma',\varphi \xRightarrow{\theta} \Delta;\Delta'}{\Gamma;\Gamma',\varphi\wedge\psi \xRightarrow{\theta} \Delta;\Delta'}$$

$$\wedge_r\,\frac{\Gamma;\Gamma' \xRightarrow{\theta_1} \varphi,\Delta;\Delta' \quad \Gamma;\Gamma' \xRightarrow{\theta_2} \psi,\Delta;\Delta'}{\Gamma;\Gamma' \xRightarrow{\theta_1\vee\theta_2} \varphi\wedge\psi,\Delta;\Delta'} \qquad \wedge_r\,\frac{\Gamma;\Gamma' \xRightarrow{\theta_1} \Delta;\Delta',\varphi \quad \Gamma;\Gamma' \xRightarrow{\theta_2} \Delta;\Delta',\psi}{\Gamma;\Gamma' \xRightarrow{\theta_1\wedge\theta_2} \Delta;\Delta',\varphi\wedge\psi}$$

Implication rules:

$$\to_l\,\frac{\Gamma';\Gamma \xRightarrow{\theta_1} \Delta';\Delta,\varphi \quad \psi,\Gamma;\Gamma' \xRightarrow{\theta_2} \Delta;\Delta'}{\varphi\to\psi,\Gamma;\Gamma' \xRightarrow{\theta_1\to\theta_2} \Delta;\Delta'} \qquad \to_l\,\frac{\Gamma;\Gamma' \xRightarrow{\theta_1} \Delta;\Delta',\varphi \quad \Gamma;\Gamma',\psi \xRightarrow{\theta_2} \Delta;\Delta'}{\Gamma;\Gamma',\varphi\to\psi \xRightarrow{\theta_1\wedge\theta_2} \Delta;\Delta'}$$

$$\to_r\,\frac{\varphi,\Gamma;\Gamma' \xRightarrow{\theta} \psi,\Delta;\Delta'}{\Gamma;\Gamma' \xRightarrow{\theta} \varphi\to\psi,\Delta;\Delta'} \qquad \to_r\,\frac{\Gamma;\Gamma',\varphi \xRightarrow{\theta} \Delta;\Delta',\psi}{\Gamma;\Gamma' \xRightarrow{\theta} \Delta;\Delta',\varphi\to\psi}$$

Figure 3.2: Construction of interpolants using split sequents in G3pc.

Remark 3.19 (Maehara as cut-introduction). We have seen the importance of cut-free sequent systems. Cut-freeness can be obtained by the famous *cut-elimination* theorem by Gentzen. It is interesting that Maehara's method can be seen as *cut-introduction* in the following sense. If π is a cut-free sequent proof of $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$, then Maehara's method provides an interpolant θ and proofs π_1 and π_2 of $\Gamma \Rightarrow \Delta, \theta$ and $\theta, \Gamma' \Rightarrow \Delta'$ respectively such that the following holds (see [Sau24] for all details in *linear logic*):

$$\text{cut}\,\frac{\begin{array}{c}\pi_1\\ \Gamma \Rightarrow \Delta, \theta\end{array} \quad \begin{array}{c}\pi_2\\ \theta, \Gamma' \Rightarrow \Delta\end{array}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \qquad \text{cut-reduces to} \qquad \begin{array}{c}\pi\\ \Gamma, \Gamma' \Rightarrow \Delta, \Delta'\end{array}$$

3.3 Extending Maehara: cut-restriction

The original method by Maehara relies on cut-free sequent calculi. In this section we will see that we can stretch the cut-freeness condition and that we can allow for a certain type of the cut rule in a proof-theoretic proof of Craig interpolation.

The restricted type of cut that we consider is the **analytic cut rule**. In this rule the cut formula can only be a subformula of a formula occurring in the conclusion. Formally, let us write $\mathsf{Sub}(\varphi)$ for the set of all subformulas occurring in formula φ and $\mathsf{Sub}(\Gamma) := \bigcup_{\varphi \in \Gamma} \mathsf{Sub}(\varphi)$. The analytic cut rule is:

$$\text{an-cut}\,\frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\ \varphi \in \mathsf{Sub}(\Gamma, \Gamma', \Delta, \Delta')$$

Example 3.20. The following is an example of an instance of the analytic cut rule

$$\frac{(\varphi \wedge \psi) \to \chi \Rightarrow \varphi \wedge \psi \quad \varphi \wedge \psi \Rightarrow \varphi \vee \chi}{(\varphi \wedge \psi) \to \chi \Rightarrow \varphi \vee \chi}$$

where the cut formula $\varphi \wedge \psi$ is a subformula of the conclusion.

Definition 3.21. A sequent calculus whose only cut rule is the analytic cut rule is said to have the **analytic cut property**.

Complete sequent calculi with the analytic cut property usually have the same benefits as cut-free calculi. An example is the **global subformula property** which says that in any proof each formula occurring in it is a subformula of the end sequent of the proof.

In this section we take modal logic S5 as an example to show that the analytic cut property is also useful to prove Craig interpolation. S5 is not known to have a cut-free sequent calculus, but there is a complete sequent calculus for it with the analytic cut property. The sequent calculus is an extension of G3pc from Figure 2.3 by the rules shown in Figure 2.6. We call this sequent calculus GS5.

$$T\,\frac{\Box\varphi, \varphi, \Gamma \Rightarrow \Delta}{\Box\varphi, \Gamma \Rightarrow \Delta} \qquad 5\,\frac{\Box\Gamma \Rightarrow \varphi, \Box\Delta}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Box\Delta} \qquad \text{an-cut}\,\frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\ \varphi \in \mathsf{Sub}(\Gamma, \Gamma', \Delta, \Delta')$$

Figure 3.3: Extra rules for GS5

Example 3.22. We present an example to show that we indeed need the analytic cut rule for a complete proof system for S5. The formula $\Box\neg\Box p \vee p$ is true in S5. Represented as a sequent, *i.e.* $\Rightarrow \Box\neg\Box p, p$, it is not provable without cut in GS5 as no other rule can be applied to it bottom-up. However, we can use the analytic cut rule to prove it:

$$\text{an-cut}\,\dfrac{5\,\dfrac{\to_r\,\dfrac{\text{form-init}\,\dfrac{}{\Box p \Rightarrow \Box p, \bot}}{\Rightarrow \Box p, \neg\Box p}}{\Rightarrow \Box\neg\Box p, \Box p} \qquad T\,\dfrac{\text{init}\,\dfrac{}{p \Rightarrow p}}{\Box p \Rightarrow p}}{\Rightarrow \Box\neg\Box p, p}$$

Theorem 3.23. *Modal logic* S5 *has the Craig interpolation property.*

Proof. We use calculus GS5 and employ a Maehara style argument such as in the proof of Lemma 3.12. So suppose $\vdash_{S5} \Gamma; \Gamma' \Rightarrow \Delta; \Delta'$ and let π be its proof. We will construct an interpolant θ by induction on the structure of π.

- The cases in which propositional rules from G3pc are used proceed the same as in Lemma 3.12.
- We leave the cases of the modal rules as an exercise to the reader.
- Here we only treat the case of the analytic cut rule. So suppose the bottom-most rule on π is an instance of an-cut with cut formula φ:

$$\pi = \quad \text{an-cut}\,\dfrac{\begin{array}{c}\pi_1\\ \Gamma_1, \Gamma_1' \Rightarrow \Delta_1, \Delta_1', \varphi\end{array} \quad \begin{array}{c}\pi_2\\ \varphi, \Gamma_2, \Gamma_2' \Rightarrow \Delta_2, \Delta_2'\end{array}}{\Gamma_1, \Gamma_2; \Gamma_1', \Gamma_2' \Rightarrow \Delta_1, \Delta_2; \Delta_1', \Delta_2'}$$

  Note that the cut rule itself splits the context over the premisses indicated here by 1 on the left and 2 on the right. We also have to deal with the split of Maehara's method indicated by ; . The split in the conclusion is our starting point, but we haven't yet indicated the splits in the premisses. This depends on two cases:
  - First assume that $\varphi \in \mathsf{Sub}(\Gamma_1, \Gamma_2, \Delta_1, \Delta_2)$, *i.e.* on the left side of Maehara's

split. Then we take the following splits indicated by ; in the premisses:

$$\pi = \quad \text{an-cut}\ \dfrac{\overset{\pi_1}{\vdots}\quad \Gamma_1'; \Gamma_1 \Rightarrow \Delta_1'; \Delta_1, \varphi \qquad \overset{\pi_2}{\vdots}\quad \varphi, \Gamma_2; \Gamma_2' \Rightarrow \Delta_2; \Delta_2'}{\Gamma_1, \Gamma_2; \Gamma_1', \Gamma_2' \Rightarrow \Delta_1, \Delta_2; \Delta_1', \Delta_2'}$$

By induction, we can find an interpolant θ_1 for the first premisse and θ_2 for the second premisse. We claim that $\theta_1 \to \theta_2$ is the required interpolant for the bottom sequent. The variable condition is fulfilled because of the subformula requirement of the analytic cut. We further have to derive the sequents $\Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2, \theta \to \theta_2$ and $\theta_1 \to \theta_2, \Gamma_1', \Gamma_2' \Rightarrow \Delta_1', \Delta_2'$ in GS5. This is done by the following derivations using the induction hypothesis.

$$\to_r \dfrac{\text{an-cut}\ \dfrac{\overset{IH}{\vdots}\quad \theta_1, \Gamma_1 \Rightarrow \Delta_1, \varphi \qquad \overset{IH}{\vdots}\quad \varphi, \Gamma_2 \Rightarrow \Delta_2, \theta_2}{\theta_1, \Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2, \theta_2}}{\Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2, \theta_1 \to \theta_2} \qquad \to_l \dfrac{\overset{IH}{\vdots}\quad \Gamma_1' \Rightarrow \Delta_1', \theta_1 \qquad \overset{IH}{\vdots}\quad \theta_2, \Gamma_2' \Rightarrow \Delta_2'}{\theta_1 \to \theta_2, \Gamma_1', \Gamma_2' \Rightarrow \Delta_1', \Delta_2'}$$

Note that the instance of the analytic cut in the left derivation is valid, because φ admits the subformula requirement by our assumption that $\varphi \in \mathsf{Sub}(\Gamma_1, \Gamma_2, \Delta_1, \Delta_2)$.

- Now assume $\varphi \in \mathsf{Sub}(\Gamma_1', \Gamma_2', \Delta_1', \Delta_2')$, *i.e.* on the right side of Maehara's split. Then we take the following splits in the premisses:

$$\pi = \quad \text{an-cut}\ \dfrac{\overset{\pi_1}{\vdots}\quad \Gamma_1; \Gamma_1' \Rightarrow \Delta_1; \Delta_1', \varphi \qquad \overset{\pi_2}{\vdots}\quad \Gamma_2; \Gamma_2', \varphi \Rightarrow \Delta_2; \Delta_2'}{\Gamma_1, \Gamma_2; \Gamma_1', \Gamma_2' \Rightarrow \Delta_1, \Delta_2; \Delta_1', \Delta_2'}$$

By induction, there exist interpolants θ_1 and θ_2 for the left and right premisse, respectively. One can verify that $\theta_1 \wedge \theta_2$ is the desired interpolant in this case. We leave this as an exercise for the reader.

□

Exercise 3.24. Check the final details in the proof of Theorem 3.23. Why does this argument not work for the usual unrestricted cut rule?

3.4 Universal proof theory

We have seen that Maehara's method is a flexible method to construct Craig interpolants. But how far can we stretch Maehara's method? What type of rules do align well with Maehara's method?

In [AJ18a], the authors explore a very general form of sequent rules and axioms, called **semi-analytic rules** and **focused axioms**. Where the analytic cut rule puts a subformula restriction on the rule, semi-analytic rules adopt a more relaxed condition saying that every formula in the premisses 'coming' from the principal formula must only contain propositional variables occurring in the principal formula.

Definition 3.25. An axiom is **focused** if it is of the form:

$$(\Gamma, \varphi \Rightarrow \varphi, \Delta),\ (\Gamma \Rightarrow \varphi, \Delta),\ \text{or } (\Gamma, \varphi \Rightarrow \Delta)$$

A rule is **left semi-analytic** if it is of the form

$$\frac{\{\Gamma^i, \psi^i_1, \ldots, \psi^i_{m_i} \Rightarrow \chi^i_1, \ldots, \chi^i_{n_i}, \Delta^i \mid i = 1, \ldots, k\}}{\Gamma, \varphi \Rightarrow \Delta}$$

and a rule is **right semi-analytic** if it is of the form

$$\frac{\{\Gamma^i, \psi^i_1, \ldots, \psi^i_{m_i} \Rightarrow \chi^i_1, \ldots, \chi^i_{n_i}, \Delta^i \mid i = 1, \ldots, k\}}{\Gamma \Rightarrow \varphi, \Delta}$$

where $\mathsf{Voc}(\psi^i_j) \subseteq \mathsf{Voc}(\varphi)$ for all j and $\mathsf{Voc}(\chi^i_l) \subseteq \mathsf{Voc}(\varphi)$ for all l and for the contexts we have $\bigcup_i \Gamma^i = \Gamma$ and $\bigcup_i \Delta^i = \Delta$.

Example 3.26. All propositional rules in G3pc are semi-analytic. In for example,

$$\vee_r \frac{\Gamma \Rightarrow \Delta, \varphi, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}$$

the propositional variables occurring in φ or ψ also occur in the principal formula $\varphi \vee \psi$.

Example 3.27. The modal rules are not semi-analytic by Definition 3.25. For example,

$$K \frac{\Gamma \Rightarrow \varphi}{\Sigma, \Box\Gamma \Rightarrow \Box\varphi, \Delta}$$

changes the context Γ in the premisse to $\Box\Gamma$ in the conclusion which is not allowed according to Definition 3.25. Semi-analyticity for modal rules needs different treatment and falls outside the scope of these lectures.

Example 3.28. Semi-analytic rules are defined very generally and cover also artificial connectives. The following is a semi-analytic rule for the three-ary artificial connective ☺(·, ·, ·):

$$☺ \frac{\Gamma, p \wedge q \Rightarrow \Delta, r \quad \Gamma, ☺(p,q,r), ☺(q,p,r) \Rightarrow \Delta' \quad \Gamma', ☺(r,r,r) \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', ☺(\varphi, \psi, \chi)}\ p, q, r \in \mathsf{Voc}(\varphi, \psi, \chi)$$

We have the following general theorem (the underlying basis of its proof is again Maehara's method):

Theorem 3.29. *If a logic has a sound and complete sequent calculus only containing focused axioms and semi-analytic rules, then the logic admits the Craig interpolation property.*

Maehara's method uses proof systems as a tool to prove a property of the corresponding logic. We can also turn to the opposite perspective by posing the following question:

Question 3.30. Can we use a property of a logic (*e.g.* interpolation) as a tool to say something about the existence of a 'nice' sequent calculus for that logic?

What a 'nice' calculus is depends on the context. Here we mean semi-analytic. So-called negative results provide an answer to this question. Negative results come from the contraposition of Theorem 3.29: if a certain logic does not have Craig interpolation, then it cannot have a 'nice' sequent calculus.

Such negative results are powerful, because Craig interpolation is a rare property among logics whereas semi-analytic rules define a large class of sequent calculi. In particular, by Theorem 3.8 we have the following negative result:

Theorem 3.31. *Only 7 consistent intermediate logics have a 'nice' (aka semi-analytic) sequent calculus.*

The questions and negative results like Theorem 3.31 fall into the subarea of proof theory called **universal proof theory**. It is a recent research program that aims to study the mathematical properties of proof systems in a uniform manner (analogous to the generic study of algebras in universal algebra). The program consists of three fundamental problems:

1. the *existence problem*, to investigate the existence of certain kinds of proofs systems for a given logic.
2. the *equivalence problem*, to study the natural notions of equivalence of proof systems, and
3. the *characterization problem*, to investigate the possible characterizations of proof systems.

Theorem 3.31 is an example of the existence problem. It shows that Craig interpolation serves as a great tool in universal proof theory.

3.5 Extending Maehara: hypersequents

I did not discuss this section in the lectures. It is meant for those who are familiar with hypersequents to show that we can also use these systems to construct Craig interpolants.

In this section we explore a more advanced proof-theoretic proof of Craig interpolation based on hypersequents. The technique that we will present is inspired by Maehara's method and is first published by R. Kuznets using hypersequents for S5 [Kuz16]. Later, similar methods has been applied to prove Craig interpolation using hypersequents and nested sequents for intermediate logics [KL18]. The method is important for logics that do not have a standard sequent calculus.

We take modal logic S5 as our example. Figure 2.6 present the hypersequent calculus HS5. The challanges are to find a correct formulation of a 'split hypersequent' and a correct hypersequent-based formulation of Craig interpolation.

Definition 3.32. A **split hypersequent** is a hypersequent in which each antecedent and succedent in each sequent component is split into two cedents by a semicolon:

$$\Gamma_1; \Pi_1 \Rightarrow \Delta_1; \Sigma_1 \mid \cdots \mid \Gamma_n; \Pi_n \Rightarrow \Delta_n; \Sigma_n.$$

Given a split sequent $\mathcal{G}$ of the form above, the left side of the split is the hypersequent

$$L\mathcal{G} := \Gamma_1 \Rightarrow \Delta_1 \mid \cdots \mid \Gamma_n \Rightarrow \Delta_n,$$

and the right side of the split is the hypersequent

$$R\mathcal{G} := \Pi_1 \Rightarrow \Sigma_1 \mid \cdots \mid \Pi_n \Rightarrow \Sigma_n.$$

In contrast to the formula interpretation of sequents, the formula interpretation of a hypersequent is *not* an implication. This makes it complicated to find a suitable hypersequent-style formulation of Craig interpolation. The solution is to not work with plain formulas as interpolants (as is done in the sequent-based version of Craig interpolation in Lemma 3.12), but to work with 'hyperformulas' as interpolants for hypersequents. Such formulas are sometimes called multiformulas in the literature and are defined as follows.

Definition 3.33. A **basic multiformula** is a sequence of formulas written in hypersequent notation $\varphi_1 \mid \cdots \mid \varphi_n$ and its **length** is n. **Multiformulas** are then defined using new symbols $\varovee$ and $\varowedge$ as follows. Each basic multiformula is a multiformula. And when A and B are multiformulas of the same length n, then $A \varovee B$ and $A \varowedge B$ are also multiformulas of length n.

Remark 3.34. Note that a multiformula of length 1 can be considered as a normal formula where we replace each occurrence of $\varovee$ by $\vee$ and each occurrence of $\varowedge$ by $\wedge$.

The meaning of multiformulas is defined via semantics.

Definition 3.35. Let $\mathcal{M}$ be an S5-model and let $\overline{w} = w_1, \ldots, w_n$ be a tuple of n worlds in $\mathcal{M}$. If $\varphi_1 \mid \cdots \mid \varphi_n$ is a basic multiformula, we define

$$\mathcal{M}, \overline{w} \models \varphi_1 \mid \cdots \mid \varphi_n \qquad \text{iff} \qquad \mathcal{M}, w_i \models \varphi_i \text{ for some } 1 \leq i \leq n.$$

For arbitrary multiformulas A and B of the same length, we define

$$\mathcal{M}, \overline{w} \models A \varovee B \quad \text{iff} \quad \mathcal{M}, \overline{w} \models A \text{ or } \mathcal{M}, \overline{w} \models B$$
$$\mathcal{M}, \overline{w} \models A \varowedge B \quad \text{iff} \quad \mathcal{M}, \overline{w} \models A \text{ and } \mathcal{M}, \overline{w} \models B.$$

The following theorem provides a suitable hypersequent-based formulation of Craig interpolation.

Theorem 3.36. *Let $\mathcal{G} = \Gamma_1; \Pi_1 \Rightarrow \Delta_1; \Sigma_1 \mid \cdots \mid \Gamma_n; \Pi_n \Rightarrow \Delta_n; \Sigma_n$ be a provable split sequent in* HS5. *Then there exist a multiformula C of length n such that for each* S5*-model $\mathcal{M}$ and each tuple $\overline{w} = w_1, \ldots, w_n$ of worlds in $\mathcal{M}$ it holds that:*

1. $\mathsf{Voc}(C) \subseteq \mathsf{Voc}(L\mathcal{G}) \cap \mathsf{Voc}(R\mathcal{G})$
2. *if $\mathcal{M}, \overline{w} \not\models C$, then $\mathcal{M}, \overline{w} \models L\mathcal{G}$,*
3. *if $\mathcal{M}, \overline{w} \models C$, then $\mathcal{M}, \overline{w} \models R\mathcal{G}$,*

*Multiformula C is called the **multi-interpolant** of $\mathcal{G}$.*

Proof idea. As the proof is very extensive and elaborate, we only provide a proof intuition. Similarly to Maehara's method we construct the multi-interpolant based on a proof π of the split hypersequent $\mathcal{G}$. The recursive construction of the multi-interpolant C depends on the last rule applied in π. We only present one salient case to provide an intuition. It is not our goal to leave the other cases to the reader, because these are more difficult and are not necessary to pursue the idea of Maehara's method in hypersequents.
We look at rule $\to_l$. There are two cases depending on which side of the split the principal formula $\varphi \to \psi$ occurs.

- Suppose the bottom-most rule in π is as follows with principal $\varphi \to \psi$ on the left side of the split:

$$\pi = \quad \to_l \frac{\overset{\pi_1}{\mathcal{G} \mid \Gamma; \Pi \Rightarrow \Delta, \varphi; \Sigma} \qquad \overset{\pi_2}{\mathcal{G} \mid \Gamma, \psi; \Pi \Rightarrow \Delta; \Sigma}}{\mathcal{G} \mid \Gamma, \varphi \to \psi; \Pi \Rightarrow \Delta; \Sigma}$$

  By induction hypothesis there are multi-interpolants C_1 and C_2 for the left and right premisse respectively. If the length of $\mathcal{G}$ is n, then the lengths of the conclusion and the premisses are $n+1$ and so are the lengths of C_1 and C_2. We claim that $C_1 \varovee C_2$ is a multi-interpolant for the conclusion. The variable condition is fulfilled by a standard argument. It remains to check condition (2) and (3) of Definition 3.35. Let $\mathcal{M}$ be an S5-model and $\overline{v}, w = v_1, \ldots, v_n, w$ be $n+1$ worlds in $\mathcal{M}$. For (2), suppose $\mathcal{M}, \overline{v}, w \not\models C_1 \varovee C_2$. We have to show that $\mathcal{M}, \overline{v}, w \models L\mathcal{G} \mid \Gamma, \varphi \to \psi \Rightarrow \Delta$. By $\mathcal{M}, \overline{v}, w \not\models C_1 \varovee C_2$ it follows that $\mathcal{M}, \overline{v}, w \not\models C_1$ and $\mathcal{M}, \overline{v}, w \not\models C_2$. By induction hypotheses, we know that $\mathcal{M}, \overline{v}, w \models L\mathcal{G} \mid \Gamma \Rightarrow \Delta, \varphi$ and $\mathcal{M}, \overline{v}, w \models L\mathcal{G} \mid \Gamma, \psi \Rightarrow \Delta$. By Definition 2.8 we have

$$\mathcal{M}, \overline{v} \models L\mathcal{G} \text{ or } \mathcal{M}, w \models L\mathcal{G} \text{ or } \mathcal{M}, w \models \varphi, \text{ and}$$

$$\mathcal{M}, \overline{v} \models L\mathcal{G} \text{ or } \mathcal{M}, w \models L\mathcal{G} \text{ or } \mathcal{M}, w \not\models \psi$$

This means that $\mathcal{M}, \overline{v} \models L\mathcal{G}$ or $\mathcal{M}, w \models \Gamma \Rightarrow \Delta$ or $\mathcal{M}, w \not\models \varphi \to \psi$. Therefore we may conclude that $\mathcal{M}, \overline{v}, w \models L\mathcal{G} \mid \Gamma, \varphi \to \psi \Rightarrow \Delta$. We leave case (3) for the reader.

- Suppose the bottom-most rule in π is as follows with principal $\varphi \to \psi$ on the right side of the split:

$$\pi = \quad \genfrac{}{}{}{}{\overset{\pi_1}{\mathcal{G} \mid \Gamma; \Pi \Rightarrow \Delta; \Sigma, \varphi} \quad \overset{\pi_2}{\mathcal{G} \mid \Gamma; \Pi, \psi \Rightarrow \Delta; \Sigma}}{\mathcal{G} \mid \Gamma; \Pi, \varphi \to \psi \Rightarrow \Delta; \Sigma} \to_l$$

By induction hypothesis there are multi-interpolants C_1 and C_2 for the left and right premisse respectively. By a similar argument as above one can show that $C_1 \oslash C_2$ is a multi-interpolant for the conclusion. We leave the details for the reader.

□

We state the following theorem without proof.

Theorem 3.37. *If multiformula C of length 1 is a multi-interpolant for split hypersequent $\varphi; \Rightarrow; \psi$, then the formula θ obtained from C as in Remark 3.34 is an interpolant for formula $\varphi \to \psi$.*

This provides another constructive proof of Theorem 3.23 stating that modal logic S5 has the Craig interpolation property.

Chapter 4

Uniform interpolation via proof theory

4.1 Uniform interpolation

Uniform interpolation is a beautiful stronger version of Craig interpolation. In the Introduction we have highlighted its importance across different fields.

Uniform interpolation in a slogan: a Craig interpolant χ for $\varphi \to \psi$ is *uniform* if it *only* relies on φ (or only on ψ). The intuition is that χ is then a Craig interpolant that uniformly works for any provable implication $\varphi \to \psi'$ with ψ' in a specified vocabulary. This is made formal in the following definition and made visual afterwards.

Definition 4.1 (Uniform interpolation)**.** Fix a logic L. Let φ be a formula and let $p \in \mathsf{Prop}$ be a propositional variable. Formula χ is called a **uniform post-interpolant** for φ *wrt* p if the following two properties hold:

1. $\mathsf{Voc}(\chi) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}$,
2. For all p-free formulas ψ (*i.e.* $p \notin \mathsf{Voc}(\psi)$):

$$\text{if } \vdash_{\mathsf{L}} \varphi \to \psi, \text{ then } \vdash_{\mathsf{L}} \varphi \to \chi \text{ and } \vdash_{\mathsf{L}} \chi \to \psi$$

Formula θ is called a **uniform pre-interpolant** for φ *wrt* p if the following dual properties hold:

1. $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}$,
2. For all p-free formulas ψ (*i.e.* $p \notin \mathsf{Voc}(\psi)$):

$$\text{if } \vdash_{\mathsf{L}} \psi \to \varphi, \text{ then } \vdash_{\mathsf{L}} \psi \to \theta \text{ and } \vdash_{\mathsf{L}} \theta \to \varphi$$

Logic L has the **uniform interpolation property** if uniform post- and pre-interpolants exist for all formulas φ and all propositional variables p.

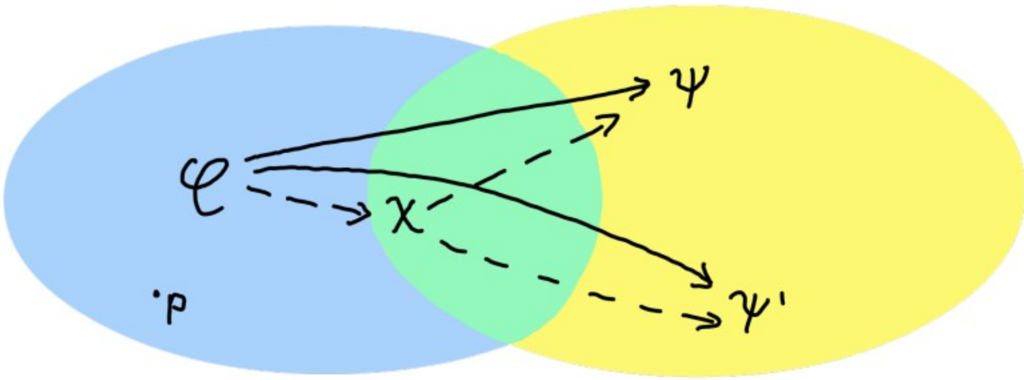


Figure 4.1: Formula χ is a pre-interpolant of φ *wrt* p. Blue indicates the set of formulas in $\mathsf{Voc}(\varphi)$ and yellow indicates the formulas that do not contain p.

Remark 4.2. Uniform interpolation is sometimes called **variable forgetting**, because the uniform interpolant behaves like φ but forgets a variable p.

Remark 4.3. Uniform interpolants encode **propositional quantification**. In the literature, post-interpolant χ in the definition above is often written as $\chi = \exists p\varphi$ and pre-interpolant θ as $\theta = \forall p\varphi$. This does not mean that these formulas contain quantifiers, but it means that they *behave* like propositional quantifiers.

Example 4.4. Let us work in CPC and consider formula $\varphi = (p \wedge q \wedge r)$. We prove that $p \wedge q$ is the uniform post-interpolant for φ *wrt* r.

1. It satisfies the variable condition, *i.e.* $\mathsf{Voc}(p \wedge q) \subseteq \mathsf{Voc}(\varphi) \setminus r$.
2. Suppose ψ is an r-free formula such that $\vdash_{\mathsf{CPC}} (p \wedge q \wedge r) \to \psi$.
   Indeed $\vdash_{\mathsf{CPC}} (p \wedge q \wedge r) \to (p \wedge q)$.
   We have $\vdash_{\mathsf{CPC}} (p \wedge q) \to \psi$ by the following reasoning. Since r does not occur in ψ the truth value of r does not affect the validity of ψ. Therefore, by $\vdash_{\mathsf{CPC}} (p \wedge q \wedge r) \to \psi$ we might try any truth value of r and have

$$\vdash_{\mathsf{CPC}} (p \wedge q \wedge \top) \vee (p \wedge q \wedge \bot) \to \psi.$$

   The antecent equals $p \wedge q$ and therefore $\vdash_{\mathsf{CPC}} (p \wedge q) \to \psi$ as derired.

We state without proof:

Theorem 4.5. *If logic* L *has the uniform interpolation property, then it has the Craig interpolation property.*

Uniform interpolation is stronger than Craig interpolation.

Example 4.6. The logics CPC, IPC, K, S5, and GL have the uniform interpolation property. However, although K4 and S4 admit Craig interpolation, they do not admit uniform interpolation. These facts can be shown in various ways using semantics, algebra, or proof theory. Many results were first proved via semantics which can be found in the book [GZ02]. We focus on proof theory.

In contrast to Craig interpolants, uniform interpolants are unique up to logical equivalence.

Exercise 4.7 (Uniform interpolants are unique)**.** Let χ_1 and χ_2 both be a post-interpolants for φ *wrt* p in your favorite logic L. Prove that $\vdash_{\mathsf{L}} \chi_1 \to \chi_2$ and $\vdash_{\mathsf{L}} \chi_2 \to \chi_1$.

In fact, uniform interpolants provide *weakest* and *strongest* Craig interpolants. We explain this by the following example.

Example 4.8 (Weakest and strongest interpolants)**.** Let us work in CPC. The following implication is provable in CPC:

$$(p \wedge q \wedge r) \to (p \vee q \vee s).$$

It has four Craig interpolants, namely $p \wedge q$, p, q, and $p \vee q$. We observe:

- $p \wedge q$ is the *strongest* Craig interpolant, *i.e.* it implies all the other Craig interpolants. Recall from Example 4.4 that $(p \wedge q)$ is exactly the post-interpolant of the antecedent $\varphi = (p \wedge q \wedge r)$ *wrt* r. It was computed based on φ by:

$$p \wedge q = (p \wedge q \wedge \top) \vee (p \wedge q \wedge \bot).$$

- Dually, $p \vee q$ is the *weakest* Craig interpolant, *i.e.* it is implied by all other Craig interpolants. One can verify that $(p \vee q)$ is exactly the pre-interpolant of the succedent $\psi = (p \vee q \wedge s)$ *wrt* s. It is computed based on ψ by:

$$p \vee q = (p \vee q \vee \top) \wedge (p \vee q \vee \bot).$$

Exercise 4.9. Recall Example 3.5 where we considered the following provable implication in CPC

$$(p_1 \wedge p_2) \vee (\neg p_3 \wedge q) \to (r \vee p_1 \vee p_2 \vee \neg p_3).$$

We write $\varphi = (p_1 \wedge p_2) \vee (\neg p_3 \wedge q)$ and $\psi = (r \vee p_1 \vee p_2 \vee \neg p_3)$. We have seen four Craig interpolants for $\vdash_{\mathsf{CPC}} \varphi \to \psi$ in Example 3.5. Which of these four interpolants is the strongest one? Which is the weakest one? Which one is the uniform post-interpolant of $\varphi = (p_1 \wedge p_2) \vee (\neg p_3 \wedge q)$ *wrt* q? Which one is the uniform pre-interpolant of $\psi = (r \vee p_1 \vee p_2 \vee \neg p_3)$ *wrt* r?

The observations in the examples can be used to prove the following theorem.

Theorem 4.10. *Logic* CPC *has the uniform interpolation property.*

Proof. Let φ be a formula and let $p \in \text{Prop}$. Let us write $\varphi(p)$ to distinguish the occurrences of p. We write $\varphi(\top)$ for the formula in which each occurrences of p in φ is replaced by $\top$. Similarly for $\varphi(\bot)$ replacing p by $\bot$. We have:

- $\chi := \varphi(\top) \vee \varphi(\bot)$ is the post-interpolant for φ *wrt* p.
- $\theta := \varphi(\top) \wedge \varphi(\bot)$ is the pre-interpolant for φ *wrt* p.

We leave it to the reader to check the details. The proof uses the same idea as used in Example 4.4. ☐

Now we prove uniform interpolation for so-called locally tabular logics.

Definition 4.11. A logic is **locally tabular** if given a fixed finite set of variables there are only finitely many non-equivalent formulas with variables from this set.

Example 4.12. Logics CPC and S5 are locally tabular.

Theorem 4.13. *If a locally tabular logic has Craig interpolation, then it has uniform interpolation.*

Proof. We define:

$$\chi := \bigwedge \{\psi \mid \vdash \varphi \to \psi \text{ and } \mathsf{Voc}(\psi) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}\}$$
$$\theta := \bigvee \{\psi \mid \vdash \psi \to \varphi \text{ and } \mathsf{Voc}(\psi) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}\}$$

We claim that χ is a post-interpolant for φ *wrt* p. It is very important to note that χ is a well-defined formula. This is because the set $\{\psi \mid \vdash \varphi \to \psi \text{ and } \mathsf{Voc}(\psi) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}\}$ can only have finitely many non-equivalent formulas by local tabularity. Let us check the properties from Definition 4.1. Property 1 holds because $\mathsf{Voc}(\chi) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}$. For property 2 suppose that γ is p-free such that $\vdash \varphi \to \gamma$. We have $\vdash \varphi \to \chi$ because χ is a conjunction where each conjunct ψ satisfies $\vdash \varphi \to \psi$. Now we verify $\vdash \chi \to \gamma$. We have assumed that the logic has Craig interpolation, so there exists an interpolant ψ' of $\vdash \varphi \to \gamma$. In particular, $\mathsf{Voc}(\psi') \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}$ and $\vdash \varphi \to \psi'$ and $\vdash \psi' \to \gamma$. Therefore, ψ' is a conjunct of χ and so $\vdash \chi \to \gamma$. ☐

Theorem 4.14. *Logic* S5 *has uniform interpolation.*

4.2 Pitts's method

In the previous section we have seen a proof of uniform interpolation for locally tabular logics. It relies on the fact that the big conjunction and big disjuntion in the proof of Theorem 4.13 are taken over finite sets. These sets are in general *not* finite for many logics like IPC and modal logics. So we must rely on other methods towards uniform interpolation.

We will discuss a proof-theoretic method first invented by Pitts to prove uniform interpolation for IPC [Pit92].

Theorem 4.15. *Logic* IPC *has the uniform interpolation property.*

The core idea of Pitts methods is to extend Maehara's method to a more general setting as follows:

Craig interpolation	**Uniform interpolation**
Maehara's method	Pitts's method
Sequent formulation of Craig interp.	Sequent formulation of uniform interp.
Cut-free sequent calculus	Terminating sequent calculus
Proof of $\varphi \to \psi$	Proof search of φ

Because of technical reasons we will not prove Theorem 4.15, but we will explain Pitts method by providing a proof-theoretic proof of uniform interpolation for K as done by [Bíl06]. We only focus on the construction of pre-interpolants θ from Definition 4.1.

Let us start by explaining the sequent based version of uniform interpolation. A pre-interpolant for φ *wrt* p works almost as a Craig interpolant for all implications $\psi \to \varphi$ where ψ is p-free (almost, because it might violate the Craig interpolation variable condition). So φ on the right is fixed but ψ on the left is flexible. This idea will be present in the split sequents in the following definition, where $\Gamma \Rightarrow \Delta$ is fixed on the right of the split, and the p-free contexts Π and Σ are flexible and always on the left side of the split.

Definition 4.16. A sequent calculus SC has the **sequent style uniform interpolation property** if for any sequent $\Gamma \Rightarrow \Delta$ and $p \in \mathsf{Prop}$, there exists a formula θ such that the following properties hold in SC:

1. $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\Gamma, \Delta) \setminus \{p\}$
2. for any p-free cedents Π and Σ such that $\vdash_{SC} \Pi; \Gamma \Rightarrow \Sigma; \Delta$ it holds that

$$\vdash_{SC} \Pi \Rightarrow \theta, \Sigma \text{ and } \vdash_{SC} \Gamma, \theta \Rightarrow \Delta.$$

Now the question is how to construct θ using the sequent calculus. Where for Maehara's method we are given a *provable* split sequent $\Gamma; \Gamma' \Rightarrow \Delta; \Delta'$, now we are only given a sequent $\Gamma \Rightarrow \Delta$ that might by *unprovable*. So we cannot look at a *proof* of $\Gamma \Rightarrow \Delta$ because there simply might not be one. The trick is to construct the uniform interpolant via a **proof search** of $\Gamma \Rightarrow \Delta$. A proof search of a sequent is a tree in which we bottom-up apply all possible rules of the sequent calculus and try to find a proof. The key feature that we want of this proof search is that it is *finite*. In other words, we want a strongly terminating sequent calculus:

Definition 4.17. A sequent calculus is said to be **strongly terminating** if for each sequent, any order of bottom-up applications of the rules is finite, i.e., it stops with leaves that are either axioms or unprovable sequents to which no rule can be applied.

A finite proof search tree of $\Gamma \Rightarrow \Delta$ guarantees that the algorithm to construct the uniform pre-interpolant terminates. However, in general, a sequent calculus might not be strongly terminating. This is a problem, because then the uniform interpolant algorithm based on it will not terminate.

Example 4.18. Sequent calculus G3K for modal logic K is terminating. The reason is that in all rules, at least one formula in the premisses 'breaks down' into strict subformula(s) of the principal formula, and the context does not get more complicated. One can make this formal by the weight that counts the number of connectives in both the premisse and conclusion. We see for all rules in G3K that the weight of each premisse is smaller than the weight of the conclusion.

Example 4.19. Sequent calculus G3pi is not terminating. The reason for that is rule

$$\to_l \frac{\varphi \to \psi, \Gamma \Rightarrow \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta}$$

in which formula $\varphi \to \psi$ is repeated in the left premise. This makes it possible to infinitely go on in the proof search by repeately applying $\to_l$ bottom-up.

Exercise 4.20. Show that the calculi G3K4 and G3S4 are *not* strongly terminating.

Calculus G3pi is not terminating, but Pitts used a terminating calculus for IPC called G4pi to prove the theorem. Due to time constraints, we do not present this calculus here, but we continue explaining Pitts's idea via the terminating calculus G3K to prove uniform interpolation for K.

Theorem 4.21. *Sequent calculus* G3K *has the sequent style uniform interpolation property: let* $\Gamma \Rightarrow \Delta$ *be a sequent and let* $p \in \mathsf{Prop}$*, then there exists a modal formula* θ *such that the following properties hold in* G3K*:*

1. $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\Gamma, \Delta) \setminus \{p\}$
2. $\vdash_{\mathsf{G3K}} \Gamma, \theta \Rightarrow \Delta$
3. *for any p-free cedents* Π *and* Σ *such that* $\vdash_{\mathsf{G3K}} \Pi, \Gamma \Rightarrow \Delta, \Sigma$ *it holds that* $\vdash_{\mathsf{G3K}} \Pi \Rightarrow \theta, \Sigma$.

Proof idea. We provide the algorithm to construct the pre-interpolant χ for $\Gamma \Rightarrow \Delta$ *wrt* p. We will define formulas $A_p(\Gamma' \Rightarrow \Delta')$ on inputs $\Gamma' \Rightarrow \Delta'$ and define $\theta := A_p(\Gamma \Rightarrow \Delta)$. We will not prove the correctness of this algorithm, *i.e.* we will leave out the proof that the output of the algorithm indeed satisfies all three properties of the theorem.
The algorithm starts a proof search bottom-up for sequent $\Gamma \Rightarrow \Delta$ and collects all possible uniform pre-interpolants of all possible rules that it finds in the bottom-up proof search of $\Gamma \Rightarrow \Delta$. The algorithm follows the steps in the table below according to the shape of $\Gamma \Rightarrow \Delta$. The left column of the table indicates the rule applied in the proof search, the middle column the shape of the conclusion of that rule, and the

right column defines the pre-interpolant using the premisse(s) of that rule. The finite proof search might end in a non-provable sequent in which the uniform interpolant is defined as in the last row of the table.

rule	$\Gamma \Rightarrow \Delta$ *matches*	$A_p(\Gamma \Rightarrow \Delta)$ *equals*
(init), $q \neq p$	$q, \Gamma' \Rightarrow \Delta, q$	$\top$
(init)	$p, \Gamma' \Rightarrow \Delta, p$	$\top$
$(\wedge_l)$	$\Gamma', \psi_1 \wedge \psi_2 \Rightarrow \Delta$	$A_p(\Gamma', \psi_1, \psi_2 \Rightarrow \Delta)$
$(\vee_l)$	$\Gamma', \psi_1 \vee \psi_2 \Rightarrow \Delta$	$A_p(\Gamma', \varphi_1 \Rightarrow \Delta) \wedge A_p(\Gamma, \varphi_2 \Rightarrow \Delta)$
$(\to_l)$	$\Gamma', \psi_1 \to \psi_2 \Rightarrow \Delta$	$A_p(\Gamma' \Rightarrow \Delta, \psi_1) \wedge A_p(\Gamma, \psi_2 \Rightarrow \Delta)$
$(\wedge_r)$	$\Gamma \Rightarrow \Delta', \psi_1 \wedge \psi_2$	$A_p(\Gamma \Rightarrow \Delta', \psi_1) \wedge A_p(\Gamma \Rightarrow \Delta', \psi_2)$
$(\vee_r)$	$\Gamma \Rightarrow \Delta', \psi_1 \vee \psi_2$	$A_p(\Gamma \Rightarrow \Delta', \psi_1, \psi_2)$
$(\to_r)$	$\Gamma \Rightarrow \Delta', \psi_1 \to \psi_2$	$A_p(\Gamma, \psi_1 \Rightarrow \Delta', \psi_2)$
(K) or no rule applies	$\Box\Gamma', \Phi \Rightarrow \Box\Delta', \chi$	$\bigvee \mathcal{A}_p$ with $\mathcal{A}_p = \{q \in \Psi\} \cup \{\neg r \in \chi\}$ $\cup \{\Box A_p(\Gamma' \Rightarrow \psi) \mid \psi \in \Delta'\}$ $\cup \{\Diamond A_p(\Gamma' \Rightarrow \varnothing)\}$

The algorithm terminates, because the sequent calculus G3K terminates. Note that $\bigvee \mathcal{A}_p$ is well-defined, because $\mathcal{A}_p$ is a finite set.
As mentioned before, we will not prove the properties of the theorem. However, it is easy to convince yourself that $A_p(\Gamma \Rightarrow \Delta)$ is p-free. □

The uniform interpolation algorithm has been formalized in the interactive theorem prover Coq. Please see `https://hferee.github.io/UIML/demo.html` and play with uniform interpolants!

Example 4.22. Let us apply the algorithm from the previous proof to formula $\Box p \vee \Box\neg p$. We present it in a proof search where we compute $A_p(\cdot)$ in red in brackets:

$$\dfrac{\dfrac{\Rightarrow p\ \ (\bot) \qquad \dfrac{p \Rightarrow \bot\ \ (\bot)}{\Rightarrow \neg p\ \ (\bot)}\,\to_r}{\Rightarrow \Box p, \Box\neg p\ \ (\Box\bot \vee \Box\bot)}\ \text{Proof search on rule (K)}}{\Rightarrow \Box p \vee \Box\neg p\ \ (\Box\bot \vee \Box\bot)}\,\vee_r$$

For both top sequents of the proof search no rule of G3K applies, so for these the last rule of the above table is used where $\mathcal{A}_p$ is empty resulting in pre-interpolant $\bot$.

Exercise 4.23. Check that $\Box\bot \vee \Box\bot$ is indeed the pre-interpolant of $\Box p \vee \Box\neg p$ *wrt* p by checking the conditions of Definition 4.1.

Theorem 4.24. *Logic* K *has the uniform interpolation property.*

Proof. Let φ be a formula and $p \in \mathsf{Prop}$. We show that the pre-interpolant exists. By Theorem 4.21 there is a formula θ such that $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\varphi) \setminus \{p\}$. Suppose now that ψ is p-free such that $\vdash_{\mathsf{K}} \psi \to \varphi$. By completeness, $\vdash_{\mathsf{G3K}} \psi \Rightarrow \varphi$. By Theorem 4.21 $\vdash_{\mathsf{G3K}} \theta \Rightarrow \varphi$ and $\vdash_{\mathsf{G3K}} \psi \Rightarrow \theta$. By soundness we conclude $\vdash_{\mathsf{K}} \theta \to \varphi$ and $\vdash_{\mathsf{K}} \psi \to \theta$. □

Uniform interpolation is used in the context of universal proof theory similarly as Craig interpolation is as discussed in Chapter 3. To get an intuition we present an informal theorem based on the fact that K4 and S4 do not have uniform interpolation (Example 4.6).

Theorem 4.25 (Informal negative result)**.** *Logics* K4 *and* S4 *do not have a 'nice'* terminating *sequent calculus.*

Chapter 5

Interpolation in knowledge representation

5.1 Description logic

Description logics provide a formalism to reason about *concepts*, their properties in terms of *roles* and the *relationships* between them. For example, Parent could be a concept and hasChild a role. Description logics represent and structure knowledge and are therefore important in the field of knowledge representation.

When reasoning with description logics one usually takes an ontology as a starting point. An **ontology** is a collection of concepts and relations between them that are axiomatically assumed to be true. From there, one can infer other information. Ontologies are more abstract than *databases*, because they might not talk about individuals such as Alice or Bob, but talk about the structure of concepts like Person. Ontologies can be very large. We give two examples:

- SNOMED CT, that stores large-scale medical information with more than 300.000 concepts and is used in more than 50 countries [CM21].
- Gene Ontology GO, used in biology [DŠ17].

There are many variants of description logics, one more expressive than the other. Most of them can be seen as rich fragments of first-order logic. Logic $\mathcal{ALC}$ can be considered as the base description logic which we will introduce here. $\mathcal{ALC}$ stands for 'Attributive Concept Language with Complements'.
(See also *e.g.* [BHLS17] for an introduction on description logic.)

Let N_c and N_r be two disjoint sets of **concept symbols** and **role symbols**. **Concepts** in $\mathcal{ALC}$ are of the following form where $r \in N_r$:

$$C, D \quad ::= \quad \top \mid \bot \mid A \in N_c \mid \neg C \mid C \sqcup D \mid C \sqcap D \mid \exists r.C \mid \forall r.C$$

It is important to note that $\exists r$ and $\forall r$ are *not* the standard quantifiers that we find in first-order logic, because they do not bind variables. In Remark 5.1 we see that they may rather correspond to modalities in modal logic. (Not all description logics correspond to a modal logic.)

An **ontology** (in other terminology called TBox) is a set of inclusions between concepts of the form $C \sqsubseteq D$. We write $C \equiv D$ to mean '$C \sqsubseteq D$ and $C \sqsubseteq D$'. We use letter $\mathcal{O}$ to denote ontologies.

We define logic $\mathcal{ALC}$ via semantics. We present it in its standard first-order manner. An *interpretation* is a pair $\mathcal{I} = (\mathcal{D}^{\mathcal{I}}, (\cdot)^{\mathcal{I}})$ where $\mathcal{D}^{I}$ is a nonempty set called the **domain** and $(\cdot)^{\mathcal{I}}$ is the **interpretation function** that assigns to each concept symbol $A \in N_c$ a subset of $\mathcal{D}^{\mathcal{I}}$ and to each role symbol $r \in N_r$ a relation as subset of $\mathcal{D}^{\mathcal{I}} \times \mathcal{D}^{\mathcal{I}}$. Given the interpretation function, concepts are then evaluated as follows:

$$
\begin{aligned}
(\bot)^{\mathcal{I}} &:= \varnothing \\
(\top)^{\mathcal{I}} &:= \mathcal{D}^{\mathcal{I}} \\
(\neg C)^{\mathcal{I}} &:= \mathcal{D}^{\mathcal{I}} \setminus C^{\mathcal{I}} \\
(C \sqcap D)^{\mathcal{I}} &:= C^{\mathcal{I}} \cap D^{\mathcal{I}} \\
(C \sqcup D)^{\mathcal{I}} &:= C^{\mathcal{I}} \cup D^{\mathcal{I}} \\
(\forall r.C)^{\mathcal{I}} &:= \{x \in \mathcal{D}^{\mathcal{I}} \mid \text{for all } y \text{ such that } (x,y) \in r^{\mathcal{I}} \text{ we have } y \in C^{\mathcal{I}}\} \\
(\exists r.C)^{\mathcal{I}} &:= \{x \in \mathcal{D}^{\mathcal{I}} \mid \text{exists } y \text{ such that } (x,y) \in r^{\mathcal{I}} \text{ and } y \in C^{\mathcal{I}}\}
\end{aligned}
$$

We say that $C \sqsubseteq D$ is **true** in an interpretation $\mathcal{I}$ iff $C^{\mathcal{I}} \subseteq D^{\mathcal{I}}$. We say that $\mathcal{I}$ is a **model** of ontology $\mathcal{O}$ if $C \sqsubseteq D$ is true in $\mathcal{I}$ for every $C \sqsubseteq D \in \mathcal{O}$. We write $\mathcal{O} \models C \sqsubseteq D$ to mean that for every model $\mathcal{I}$ of $\mathcal{O}$ we have $C^{\mathcal{I}} \subseteq D^{\mathcal{I}}$.

Remark 5.1. Logic $\mathcal{ALC}$ is a notational variant of multi-modal logic K. Concepts are formulas, $\sqcap$ is conjunction, $\sqcup$ is disjunction, $\neg$ is negation, and for each role r, $\forall r$ and $\exists r$ are modalities $\Box_r$ and $\Diamond_r$. $C \sqsubseteq D$ translates to implication. The semantics can be seen as a relational structure with multiple binary relations, one relation for each role symbol r.

Example 5.2 ([tCFS13]). We look at the following ontology $\mathcal{O}$.

$$
\begin{aligned}
\mathsf{Parent} &\equiv \exists \mathsf{hasChild}.\top \\
\mathsf{Parent} &\equiv \mathsf{Father} \sqcup \mathsf{Mother} \\
\mathsf{Father} &\sqsubseteq \mathsf{Man} \\
\mathsf{Mother} &\sqsubseteq \mathsf{Woman} \\
\mathsf{Man} &\sqsubseteq \neg \mathsf{Woman}
\end{aligned}
$$

Using the semantics, we may infer that $\mathcal{O} \models \mathsf{Father} \sqsubseteq \neg\mathsf{Mother}$.

Theorem 5.3. *For $\mathcal{ALC}$ the entailment problem is decidable, that is, we can decide whether given ontology $\mathcal{O}$ and inclusion $C \sqsubseteq D$ we have $\mathcal{O} \models C \sqsubseteq D$. For $\mathcal{ALC}$ this is ExpTime-complete.*

The complexity analysis for $\mathcal{ALC}$ can be based on a tableaux system (*aka* sequent calculi) can be found in [DM00].

5.2 Craig interpolation, Beth definability, and separation

There are two forms of Craig interpolation used in description logic. One can interpolate relation $\sqsubseteq$ between two concepts where the interpolant is a concept. Or one can interpolate relation $\models$ between an ontology and a concept implication where the interpolant is an ontology. In logical terms, the former corresponds to local Craig interpolation from Definition 3.3 and the latter corresponds to what is called global Craig interpolation because $\models$ is a *global* consequence relation.

Instead of Voc() in the previous chapters we now use $\mathsf{Sig}(C) \subseteq N_c \cup N_r$ to denote the **signature** of C which is the set of concept symbols *and* role symbols occurring in C. Similarly so for ontologies we write $\mathsf{Sig}(\mathcal{O})$.

Definition 5.4 (Concept Craig interpolation)**.** A description logic $\mathcal{L}$ has the **concept Craig interpolation property** if for any $\mathcal{L}$-ontologies $\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{L}$-concepts C_1, C_2 such that $\mathcal{O}_1 \cup \mathcal{O}_2 \models C_1 \sqsubseteq C_2$ there exists a concept D such that

1. $\mathsf{Sig}(D) \subseteq \mathsf{Sig}(\mathcal{O}_1, C_1) \cap \mathsf{Sig}(\mathcal{O}_2, C_2)$, and
2. $\mathcal{O}_1 \cup \mathcal{O}_2 \models C_1 \sqsubseteq D$ and $\mathcal{O}_1 \cup \mathcal{O}_2 \models D \sqsubseteq C_2$.

Definition 5.5 (Ontology Craig interpolation)**.** A description logic $\mathcal{L}$ has the **ontology Craig interpolation property** if whenever $\mathcal{O} \models C_1 \sqsubseteq C_2$ there exists an ontology $\mathcal{O}'$ such that

1. $\mathsf{Sig}(\mathcal{O}') \subseteq \mathsf{Sig}(\mathcal{O}) \cap \mathsf{Sig}(C_1 \sqsubseteq C_2)$, and
2. $\mathcal{O} \models \mathcal{O}'$ and $\mathcal{O}' \models C_1 \sqsubseteq C_2$.

Ontology Craig interpolation is used in ontology modules and decomposition. It allows for a structured and controlled design of large ontologies by for example multiple developers and enables operations like re-using or resizing ontologies. [KLWW09]. We will use this form of interpolation when discussing the use of uniform interpolation in description logic in Section 5.3.

In this section we focus on concept Craig interpolation.

Theorem 5.6. *$\mathcal{ALC}$ has the concept Craig interpolation property.*

It is quite unique that $\mathcal{ALC}$ has the concept Craig interpolation property. Many description logics do not have Craig interpolation. There are two problems that you can look at when a logic does not have Craig interpolation.

1. Investigate additions of logical connectives to the language of the logic and try to express Craig interpolants in such a more expressive language. This is also known as **interpolation repairing** and was first studied for hybrid logics [ABM01].

2. Investigate the **existence** of Craig interpolants, that is, for which implications $\mathcal{O}_1 \cup \mathcal{O}_2 \models C_1 \sqsubseteq C_2$ does there exist a Craig interpolant in the logic. Note that the exclusion of Craig interpolation of the logic, does not exclude the existence of Craig interpolants for *some* implications.

Especially the decidability question of problem (2) has became an important development in the research of description logic. The question is: given $\mathcal{O}_1 \cup \mathcal{O}_2 \models C_1 \sqsubseteq C_2$ can we *decide* whether there is an interpolant for $C_1 \sqsubseteq C_2$ over $\mathcal{O}_1 \cup \mathcal{O}_2$? It turns out that for many extensions of $\mathcal{ALC}$ this problem is 2ExpTime-complete or coNExpTime-complete and harder then their entailment problem [AJM+23].

We will now discuss two applications of Craig interpolation: Beth definability and separation. We start with **Beth's definability** which was first shown in pure logic [Bet53]. Here we focus on Beth definability in description logic. The notes here are mainly based on [tCFS13].

The Beth definability property provides a good balance between syntax and semantics in the following way. When defining a new concept C from a given ontology using a specified signature Σ there are two ways to do this. *Implicitly* by using the semantics in which the interpretation of C is uniquely determined over the interpretations of the ontology that share the interpretation over Σ. Or *explicitly* by using syntax which provides a definition D such that $\mathcal{O} \models C \equiv D$ where $\mathsf{Sig}(D) \subseteq \Sigma$. Beth definability says that these two coincide. We provide the necessary definitions.

Definition 5.7 (Implicit definition)**.** Let C be a concept, $\mathcal{O}$ an ontology and let $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$. Concept C is **implicitly definable** from Σ under $\mathcal{O}$, if for every two models $\mathcal{I}$ and $\mathcal{J}$ of $\mathcal{O}$ satisfying $\mathcal{D}^{\mathcal{I}} = \mathcal{D}^{\mathcal{J}}$, for all $A \in \Sigma \cap N_c$, $A^{\mathcal{I}} = A^{\mathcal{J}}$ and for all $r \in \Sigma \cap N_r$, $r^{\mathcal{I}} = r^{\mathcal{J}}$, then it holds that $C^{\mathcal{I}} = C^{\mathcal{J}}$.

There is a well-known characterization of implicit definability (see *e.g.* [HM02]). Let us introduce some notation. For every concept symbol $A \in \mathsf{Sig}(C, \mathcal{O}) \setminus \Sigma$ and role symbol $r \in \mathsf{Sig}(C, \mathcal{O}) \setminus \Sigma$ introduce a new concept symbol A' and role symbol r', respectively, which are not in $\mathsf{Sig}(C, \mathcal{O})$. Let $\tilde{C}$ be the concept obtained by replacing each occurrence of $A \notin \Sigma$ and $r \notin \Sigma$ in C by A' and r', respectively. Similarly so for $\tilde{\mathcal{O}}$.

Lemma 5.8. *Let C be an $\mathcal{L}$-concept, let $\mathcal{O}$ be an ontology, and let $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$. Then C is implicitly definable from Σ under $\mathcal{O}$ if and only if $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \equiv \tilde{C}$.*

Example 5.9 ([tCFS13])**.** Recall Example 5.2. The concept name Mother is implicitly definable from $\Sigma = \{\mathsf{hasChild}, \mathsf{Woman}\}$. To see this let $\mathcal{I}$ and $\mathcal{J}$ be two models of $\mathcal{O}$ that agree on the interpretation of hasChild and Woman. We have to show that $\mathsf{Mother}^{\mathcal{I}} = \mathsf{Mother}^{\mathcal{J}}$. Let $d \in \mathsf{Mother}^{\mathcal{I}}$ be an element in the $\mathcal{I}$ interpretation of Mother. By semantic reasoning in model $\mathcal{I}$ we have $d \in \mathsf{Woman}^{\mathcal{I}}$ and $d \in (\exists \mathsf{hasChild}.\top)^{\mathcal{I}}$. Since $\mathcal{I}$ and $\mathcal{J}$ agree on these we have $d \in \mathsf{Woman}^{\mathcal{J}}$ and $d \in (\exists \mathsf{hasChild}.\top)^{\mathcal{J}}$. Now by using semantic reasoning in $\mathcal{J}$ we may infer $d \in \mathsf{Mother}^{\mathcal{J}}$ as desired. So $\mathsf{Mother}^{\mathcal{I}} \subseteq \mathsf{Mother}^{\mathcal{J}}$. The other inclusion is symmetric.

Definition 5.10 (Explicit definition)**.** Let C be a concept, let $\mathcal{O}$ be an ontology and let $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$. Concept C is **explicitly definable** from Σ under $\mathcal{O}$ if there is some concept D such that $\mathcal{O} \models C \equiv D$ and $\mathsf{Sig}(D) \subseteq \Sigma$.

Example 5.11 ([tCFS13])**.** Recall Example 5.2 again. In Example 5.9 we have seen that Mother is implicitly definable. The proof that we used actually already shows that Mother has an explicit definition, namely by the $\mathcal{ALC}$-concept Woman $\sqcap$ $\exists$hasChild.$\top$.

Proposition 5.12. *Let C be a concept, let $\mathcal{O}$ be an ontology, and let $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$. If C is explicitly definable from Σ under $\mathcal{O}$, then C is implicitly definable from Σ under $\mathcal{O}$.*

Exercise 5.13. Provide a proof of Proposition 5.12. This is a good exercise to get acquainted with the definitions of implicit and explicit definitions. One proof method is known as Padoa's method.

The converse of Proposition 5.12 is not always true. When it is true, we say that the logic has the Beth definability property.

Definition 5.14 (Beth definability)**.** Description logic $\mathcal{L}$ has the **Beth definability property** if for all $\mathcal{L}$-concepts C, all $\mathcal{L}$-ontologies $\mathcal{O}$ and all signatures $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$, if C is implicitly definable from Σ under $\mathcal{O}$, then C is explicitly definable from Σ under $\mathcal{O}$.

Theorem 5.15. *Concept Craig interpolation implies Beth definability.*

Proof. Assume that C is implicitly definable from $\Sigma \subseteq \mathsf{Sig}(C, \mathcal{O})$ under ontology $\mathcal{O}$. By Lemma 5.8 we obtain $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \equiv \tilde{C}$. Now by concept Craig interpolation, there is an interpolant D for $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \equiv \tilde{C}$. Especially, $\mathsf{Sig}(D) \subseteq \mathsf{Sig}(\mathcal{O}, C) \cap \mathsf{Sig}(\tilde{\mathcal{O}}, \tilde{C}) = \Sigma$. Moreover, $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \sqsubseteq D$ and $\mathcal{O} \cup \tilde{\mathcal{O}} \models D \sqsubseteq \tilde{C}$ which together with implies $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \equiv \tilde{C}$ implies $\mathcal{O} \cup \tilde{\mathcal{O}} \models C \equiv D$. Since $C \equiv D$ does not contain fresh symbols used in $\tilde{\mathcal{O}}$ we have $\mathcal{O} \models C \equiv D$. So D is an explicit definition from Σ under $\mathcal{O}$. $\square$

We have the following result as an immediate corollary from Theorem 5.6.

Theorem 5.16. *Logic $\mathcal{ALC}$ has the Beth definability property.*

An example of the use of Beth definability in description logic is in **ontology engineering**, which is concerned with the design of ontologies. For example, Beth definability is used to extract an equivalent so-called acyclic ontology from a general ontology. An acyclic ontology consists only of inclusions $C \sqsubseteq D$ without going into a dependency cycle $C_1 \sqsubseteq C_2, C_2 \sqsubseteq C_3, \ldots, C_{n-1} \sqsubseteq C_n$, where concept C_1 occurs in concept C_n. This extraction is helpful, because acyclic ontologies are in general easier to reason with than cyclic ones.

Now we turn to the second application of Craig interpolation: **separation**. In classical logic there is an easy equivalent way to express Craig interpolation in terms of separation.

Definition 5.17. Let L be a logic. We say that L has the **separation property** if whenever $\vdash_{\mathsf{L}} \varphi \wedge \psi \to \bot$ there is a formula χ such that

1. $\mathsf{Voc}(\chi) \subseteq \mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi)$, and
2. $\vdash_{\mathsf{L}} \varphi \to \chi$ and $\vdash_{\mathsf{L}} \chi \wedge \psi \to \bot$.

Formula χ is called a **separator** for φ and ψ.

Exercise 5.18. Suppose we work in CPC. Show that formula χ is a separator for φ and ψ iff χ is a Craig interpolant for $\varphi \to \neg\psi$

One might draw the following picture on the left describing Craig interpolation in a model. Note that this picture is not taking into account the variable condition as Figure 3.1 represents. Separation is the dual notion as pictured on the right.

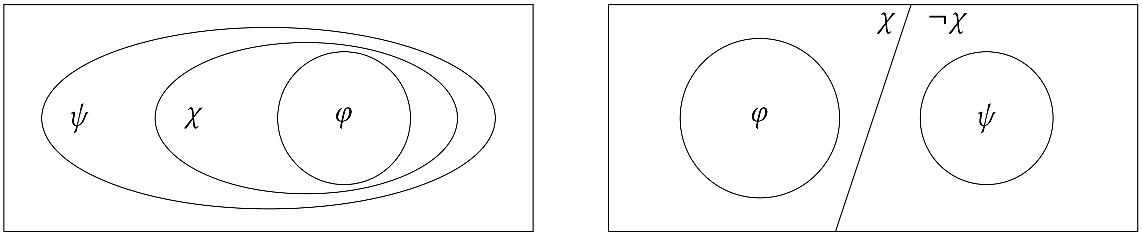


Figure 5.1: The set with φ means the set of elements in the model satisfying φ, etc. We assume $\mathsf{Voc}(\chi) \subseteq \mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi)$. Left: χ is a Craig interpolant of φ and ψ. Right: χ is separator of φ and ψ.

In description logic separation is used in the context of **concept learning** and **data separation**. The idea is to define/learn new concepts in an ontology $\mathcal{O}$ by analysing a database $\mathcal{B}$ which is defined on top of the ontology containing information about individuals $a, b, \ldots$.

Example 5.19. In the lecture I provided an informal example of an ontology $\mathcal{O}$ with information about birds and separating data individuals a's of concepts Parrot and Cockatoo from data individuals b's of concepts Kiwi and Pinguin. The separator is the concept Flies. It separates data in the following sense: $\mathcal{O}, \mathcal{B} \models \mathsf{Flies}(a)$ for every a such that $\mathcal{O}, \mathcal{B} \models \mathsf{Parrot}(a) \sqcup \mathsf{Cockatoo}(a)$ and $\mathcal{O}, \mathcal{B} \models \neg\mathsf{Flies}(b)$ for every b such that $\mathcal{O}, \mathcal{B} \models \mathsf{Kiwi}(b) \sqcup \mathsf{Pinguin}(b)$.

There are techniques in description logic using Craig interpolation to *learn* concept by *positive data examples* (in the above example the a's) and *negative data examples* (in the example the b's). We will not formalize the full idea and we will not go further into the connection between this type of separation (*aka* separating data examples) and Craig interpolation. For a nice formal explanation see page 9 of [AJM+23].

5.3 Uniform interpolation

Uniform interpolation in knowledge representation is also known as *knowledge forgetting*. It uses the uniform version of ontology Craig interpolation defined in Definition 5.5.

Definition 5.20. Let $\mathcal{O}$ be an ontology and $\Sigma \subseteq N_c \cup N_r$ a signature. A **uniform (post)-interpolant** of $\mathcal{O}$ *wrt* Σ is an ontology $\mathcal{O}'$ such that the following hold:
- $\mathsf{Sig}(\mathcal{O}') \subseteq \Sigma$
- for all $C \sqsubseteq D$ with $\mathsf{Sig}(C \sqsubseteq D) \cap \mathsf{Sig}(O) \subseteq \Sigma$, then

$$\text{if } \mathcal{O} \models C \sqsubseteq D, \text{ then } \mathcal{O} \models \mathcal{O}' \text{ and } \mathcal{O}' \models C \sqsubseteq D.$$

Description logic $\mathcal{L}$ has the **uniform interpolation property** if uniform (post)-interpolants exist for every ontology $\mathcal{O}$ *wrt* every signature Σ.

Knowledge forgetting is the term used in knowledge representation for this type of uniform interpolation. Knowledge forgetting plays a big role in ontology engineering. It is used in for example the following situations (see *e.g.* [KS13; EK19]):

- Re-sizing ontologies to a smaller ontology in a specified signature Σ. This can be represented by uniform interpolant $\mathcal{O}'$ *wrt* Σ. In other words, ontology $\mathcal{O}'$ summarizes what $\mathcal{O}$ says about Σ.
- Hiding sensitive data by forgetting about symbols not in Σ. This is useful when different users of a knowledge base have different accessibility rights based on security reasons.

Uniform interpolation is a very strong property and not many description logics have it.

Theorem 5.21. *Logic $\mathcal{ALC}$ does not have the uniform interpolation property.*

Remark 5.22. In Remark 5.1 we have seen that $\mathcal{ALC}$ is a notational variant of multi-modal logic K. We have seen in Theorem 4.24 that modal logic K has uniform interpolation and the same holds for multi-modal logic K. This means that $\mathcal{ALC}$ also has uniform interpolation. However, this does not contradict Theorem 5.21! The observation is that the former applies to the uniform version of concept Craig interpolation interpolating implications $C \sqsubseteq D$. Whereas Definition 5.20 provides a *global* definition of uniform interpolation interpolating the entailment relation $\models$. This explains the difference in results.

Similarly to the lack of Craig interpolation, one can obtain results for logics that lack uniform interpolation.

Theorem 5.23. *In $\mathcal{ALC}$, given ontology $\mathcal{O}$ and signature Σ, it is decidable whether there is a uniform interpolant $\mathcal{O}'$ of $\mathcal{O}$ wrt Σ. This existence problem is 2ExpTime-complete for $\mathcal{ALC}$.*

Chapter 6

Interpolation and proof complexity

6.1 Introduction to proof complexity

Proof complexity aims to understand how difficult it is to prove a formula. It studies the *size* of proofs in different proof systems. In this course we have seen the sequent calculus, but there are many other proof systems such as resolution proofs, natural deduction proofs, or algebraic proof systems like cutting planes. Questions addressed in proof complexity are for example: Given a theorem how big is the shortest proof for it in terms of the size of the theorem? Which proof systems allow for short proofs?

Proof complexity got a boost by the work of [CR79]. They provide a general notation of a proof system. We will see the conjecture that for every proof system of CPC there are always theorems that are hard to prove! Here we discuss the main results. These notes are mainly based on a course in Proof Complexity in the Proof Society School in Utrecht 2022 by Raheleh Jalali. The slides can be found on her personal webpage https://sites.google.com/view/rahelehjalali/talks.

We assume some familiarity of complexity theory, such as the complexity classes P (the collection of decision problems that can be solved by a deterministic Turing machine in polynomial time), NP (the collection of decision problems that can be solved by a non-deterministic Turing machine in polynomial time), and coNP (the class of problems of which their complement is in NP). A famous complexity problem is the P vs coNP problem.

Definition 6.1. A **propositional proof system** is is a polynomial time computable function on finite strings $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ such that $\varphi \in \mathrm{CPC}$ iff $\varphi = Rng(f)$. We call any $w \in \{0,1\}^*$ with $f(w) = \varphi$ an f**-proof** of φ.

This is a very general definition of a proof system. Using *encodings* of formulas and proofs into finite strings, one can see that many proof systems can be seen as a propositional proof system.

Example 6.2. The sequent calculus G3pc is a propositional proof system in the following way:

$$f(w) = \begin{cases} \text{end-sequent in } w & \text{if } w \text{ is a valid sequent proof in G3pc} \\ p \vee \neg p & \text{otherwise} \end{cases}$$

Since G3pc is sound and complete with CPC we have that $\varphi \in \text{CPC}$ iff $\varphi \in Rng(f)$.

Definition 6.3. Propositional proof system f is **polynomially bounded** if for some polynomial $q(n)$, every tautology $\varphi \in \text{CPC}$ has an f-proof of size smaller than $q(|\varphi|)$

We present an important result in proof complexity.

Theorem 6.4 ([CR79]). *There exists a polynomial bounded proof system (for* CPC*) if and only if* NP = coNP.

Proof. From left to right, suppose there exists a polynomial bounded proof system for CPC. This means that the problem to check whether φ is a tautology (*aka* in CPC) is in NP: the NP algorithm guesses a proof for φ and checks this using the polynomial bounded proof system. It is well-known that SAT, the set of satisfiable formulas, is NP-complete, so CPC as a set of tautologies is coNP-complete. Now from this and CPC ∈ NP it follows that coNP ⊆ NP. And so NP ⊆ coNP and therefore NP = coNP.

Now we prove from right to left. Suppose NP = coNP. Then there is a nondeterministic polynomial time Turing machine M that accepts exactly the formulas $\varphi \in \text{CPC}$. Now we treat computations as proofs and define propositional proof system f:

$$f(w) = \begin{cases} \varphi & \text{if } w \text{ is an accepting computation of } M \text{ on } \varphi \\ p \vee \neg p & \text{otherwise.} \end{cases}$$

f is polynomially bounded, because M runs in polynomial time. □

Theorem 6.4 is very important. It is conjectured that NP ≠ coNP, because otherwise P = NP! Therefore we have the following conjecture.

Conjecture 6.5. There is no polynomially bounded proof system for CPC. And therefore all proof systems for CPC have theorems that do not have a short proof, *i.e.* all proof systems contain *hard* theorems.

Showing that a proof system contains hard theorems is done by establishing so-called **lower bounds** for proof systems. Lower bounds indicate the minimal size of proofs for certain formulas. If this lower bound is hard, then the proof system is not polynomially bounded.

6.2 Feasible interpolation

Feasible interpolation is a technique to provide lower bounds for several proof systems. Before we turn to feasible interpolation, we first introduce results on the complexity of interpolants.

Definition 6.6. We define the **DAG-size** $|\varphi|$ of a propositional formula φ as the number of its *subformulas*. This corresponds to the representation of a formula as a *directed acyclic graphs* (DAG). Formulas represented as a DAG are also known as *circuits*.
The **formula-size** $s(\varphi)$ of a propositional formula φ is the number of symbols it consists of.

The DAG-size of φ cannot be bigger than the formula-size of φ.

Looking at Craig interpolation, one can look at the complexity of interpolants in terms of the size of the *formula* $\varphi \to \psi$. The following result I found on the ESSLLI 2024 slides of the course 'A Modern Introduction to Craig Interpolation' by Balder ten Cate and Frank Wolter.

Theorem 6.7. *If there is a superpolynomial gap between DAG-size and formula-size, then in the worst case,* CPC *does not have Craig interpolants whose formula-size is polynomial in the formula-size of the input implication.*

The following result is important for proof complexity. The class P/poly is defined as the class of decision problems that can be solved by a polynomial time Turing machine with advice strings of length polynomial in the input size.

Theorem 6.8 ([Mun82])**.** *In* CPC*, if for every provable implication $\varphi \to \psi$ there exist Craig interpolants whose DAG-size are polynomial in the DAG-size of $\varphi \to \psi$, then* $\mathrm{NP} \cap \mathrm{coNP} \subseteq \mathrm{P/poly}$*.*

Conjecture 6.9. Since it is conjectured that it is very unlikely that $\mathrm{NP} \cap \mathrm{coNP} \subseteq \mathrm{P/poly}$, it is believed that CPC has implications for which there are no small DAG-size Craig interpolants with respect to the input implication.

The complexity of Craig interpolants are measured in terms of the size of the *formula* $\varphi \to \psi$. However, one can also evaluate the complexity of the interpolants in terms of the size of the *proof* of implication $\varphi \to \psi$ as the input. This is done in feasible interpolation.

Definition 6.10. A propositional proof system f has the **feasible interpolation property**, if there is an algorithm that reads an f-proof π of $\varphi \to \psi$ and computes a Craig interpolant of $\varphi \to \psi$ presented as a DAG in polynomial time.

Examples of proof systems that admit feasible interpolation are resolution and the sequent calculus.

Theorem 6.11. *Sequent calculus* G3pc *has the feasible interpolation property.*

Proof. This follows essentially from a complexity analysis of Maehara's method from Section 3.12. Indeed, Maehara's method applied to a proof with k inferences produces a formula with at most k subformulas. So the DAG-representation of the interpolant is at most of DAG-size k, hence polynomial in the size of the proof. □

The following theorem relates feasible interpolation of a proof system to the existence of theorems that are hard to prove in that proof system. The link is based on the assumption that NP ∩ coNP $\not\subseteq$ P/poly. This is considered to be a mild assumption.

Theorem 6.12. *Let P be a propositional proof system with feasible interpolation. If* NP ∩ coNP $\not\subseteq$ P/poly, *then P is not polynomially bounded.*

Proof idea. Given NP ∩ coNP $\not\subseteq$ P/poly, we can apply Theorem 6.8 to find a sequence $\{\varphi_n \to \psi_n\}_{n=0}^{\infty}$ of tautologies such that these might grow only polynomially in the size of n, but the DAG-size of their smallest interpolants θ_n for these implications grow superpolynomial in n. Now given that the proof system has feasible interpolation, it must be the case that the shortest proofs for $\{\varphi_n \to \psi_n\}_{n=0}^{\infty}$ (on which we can compute the interpolants) must grow superpolynomially. This means that P is not polynomially bounded. □

Theorem 6.11 and Theorem 6.12 imply the following.

Corollary 6.13. *If* NP ∩ coNP $\not\subseteq$ P/poly, *then sequent calculus* G3pc *is not polynomially bounded. That is, there are formulas that do not have a short proof in* G3pc.

It is possible to obtain a stronger results using what is known as *monotone feasible interpolation*. We will not go into much detail here, but the idea is that it allows to mimic the proof of Theorem 6.12 for several proof systems, but where we do not rely on the assumption NP ∩ coNP $\not\subseteq$ P/poly. It turns out that the following two ingredients of the proof can be shown for several proof systems:

- Find a sequence $\{\varphi_n \to \psi_n\}_{n=0}^{\infty}$ of tautologies that only grow polynomial in n, but such that the *monotone* interpolants θ_n for these implications grow in superpolynomial DAG-size in n.
- Show that your proof systems has the *monotone* feasible interpolation property.

Theorem 6.14. *Sequent calculus* G3pc *is not polynomially bounded.*

Here we only showed a glance of the use of feasible interpolation in proof complexity. There are many more results, see [Kra19].

Bibliography

[ABM01] Carlos Areces, Patrick Blackburn, and Maarten Marx. "Hybrid logics: characterization, interpolation and complexity". In: *Journal of Symbolic Logic* 66.3 (2001), pp. 977–1010. DOI: 10.2307/2695090 (cit. on p. 35).

[AJ18a] Amirhossein Akbar Tabatabai and Raheleh Jalali. *Universal proof theory: Semi-analytic rules and Craig interpolation.* 2018. arXiv: 1808.06256 [cs.LO] (cit. on pp. 1–2, 20).

[AJ18b] Amirhossein Akbar Tabatabai and Raheleh Jalali. *Universal proof theory: Semi-analytic rules and uniform interpolation.* 2018. arXiv: 1808.06258 [cs.LO] (cit. on p. 2).

[AJM+23] Alessandro Artale, Jean Christoph Jung, Andrea Mazzullo, Ana Ozaki, and Frank Wolter. "Living without Beth and Craig: Definitions and Interpolants in Description and Modal Logics with Nominals and Role Inclusions". In: *ACM Trans. Comput. Logic* 24.4 (Oct. 2023). ISSN: 1529-3785. DOI: 10.1145/3597301. URL: https://doi.org/10.1145/3597301 (cit. on pp. 1–2, 36, 38).

[Avr96] Arnon Avron. "The Method of Hypersequents in the Proof Theory of Propositional Non-Classical Logics". In: *Logic: from Foundations to Applications: European Logic Colloquium.* Ed. by Wilfrid Hodges, Martin Hyland, Charles Steinhorn, and John Truss. Clarendon Press, 1996, pp. 1–32. URL: https://dl.acm.org/doi/10.5555/246814.246817 (cit. on p. 9).

[Bet53] E. W. Beth. "On Padoa's Method in the Theory of Definition". In: *Indagationes Mathematicae (Proceedings)* 56 (1953), pp. 330–339. DOI: 10.1016/S1385-7258(53)50042-3 (cit. on pp. 1, 36).

[BHLS17] Franz Baader, Ian Horrocks, Carsten Lutz, and Uli Sattler. *An Introduction to Description Logic.* Cambridge University Press, 2017 (cit. on pp. 2, 33).

[Bíl06] M. Bílková. "Interpolation in Modal Logics". PhD thesis. UK Praha, 2006 (cit. on pp. 2, 29).

[BRV01] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2001. DOI: 10.1017/CBO9781107050884 (cit. on pp. 3, 5).

[CM21] A.E. Chang and J. Mostafa. "The use of SNOMED CT, 2013-2020: a literature review". In: *Journal of the American Medical Informatics Association* 28.9 (2021), pp. 2017–2026 (cit. on p. 33).

[CR79] Stephen A. Cook and Robert A. Reckhow. "The relative efficiency of propositional proof systems". In: *Journal of Symbolic Logic* 44.1 (1979), pp. 36–50. DOI: 10.2307/2273702 (cit. on pp. 40–41).

[Cra57] W. Craig. "Review: Paul Lorenzen, Einführung in die Operative Logik und Mathematik". In: *Bulletin of the American Mathematical Society* 63.5 (1957), pp. 316–320. DOI: 10.1090/S0002-9904-1957-10127-X (cit. on p. 1).

[CZ97] Alexander V. Chagrov and Michael Zakharyaschev. *Modal Logic*. Vol. 35. Oxford logic guides. Oxford University Press, 1997. ISBN: 978-0-19-853779-3 (cit. on p. 12).

[DM00] Francesco M. Donini and Fabio Massacci. "EXPtime tableaux for ALC". In: *Artificial Intelligence* 124.1 (2000), pp. 87–138. ISSN: 0004-3702. DOI: https://doi.org/10.1016/S0004-3702(00)00070-9. URL: https://www.sciencedirect.com/science/article/pii/S0004370200000709 (cit. on p. 35).

[DŠ17] C. Dessimoz and N. Škunca, eds. *The Gene Ontology Handbook*. Methods in Molecular Biology. Humana New York, 2017. DOI: 10.1007/978-1-4939-3743-1 (cit. on p. 33).

[EK19] T. Eiter and G. Kern-Isberner. "A Brief Survey on Forgetting from a Knowledge Representation and Reasoning Perspective". In: *Künstliche Intelligenz* 33 (2019), pp. 9–33 (cit. on pp. 1–2, 39).

[Gie22] Iris van der Giessen. "Uniform Interpolation and Admissible Rules. Proof-theoretic investigations into (intuitionistic) modal logics". PhD thesis. Utrecht University, 2022. URL: https://dspace.library.uu.nl/bitstream/handle/1874/423244/proefschrift%20-%206343c2623d6ab.pdf (cit. on p. 6).

[GM05] D. M. Gabbay and Larisa L. Maksimova. *Interpolation and Definability: Modal and Intuitionistic Logics*. English. New York: Oxford University Press, 2005. DOI: 10.1093/acprof:oso/9780198511748.001.0001 (cit. on p. 2).

[GSS08] D. M. Gabbay, R. A. Schmidt, and A Szalas. *Second-Order Quantifier Elimination: Foundations, Computational Aspects and Applications*. English. Vol. 12. Studies in Logic. United Kingdom: College Publications, 2008. ISBN: 978-1-904987-56-7 (cit. on p. 1).

[GZ02] Silvio Ghilardi and Marek Zawadowski. *Sheaves, Games, and Model Completions. A Categorical Approach to Nonclassical Propositional Logics.* Vol. 14. Trends in Logic Series. Kluwer, Jan. 2002. DOI: 10.1007/978-94-015-9936-8 (cit. on p. 27).

[HJ24] Stefan Hetzl and Raheleh Jalali. "On the Completeness of Interpolation Algorithms". In: *Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science.* LICS '24. Tallinn, Estonia: Association for Computing Machinery, 2024. ISBN: 9798400706608. DOI: 10.1145/3661814.3662112. URL: https://doi.org/10.1145/3661814.3662112 (cit. on p. 15).

[HM02] E. Hoogland and M. Marx. "Interpolation and Definability in Guarded Fragments". In: *Studia Logica* 70.3 (2002), pp. 373–409. DOI: 10.1023/A:1015154431342 (cit. on p. 36).

[Iem19] Rosalie Iemhoff. "Uniform interpolation and the existence of sequent calculi". In: *Annals of Pure and Applied Logic* 170.11 (2019), p. 102711. ISSN: 0168-0072. DOI: 10.1016/j.apal.2019.05.008. URL: https://www.sciencedirect.com/science/article/pii/S0168007219300624 (cit. on pp. 1–2).

[KL18] Roman Kuznets and Björn Lellmann. "Interpolation for Intermediate Logics via Hyper- and Linear Nested Sequents". In: *Advances in Modal Logic, AiML 2018.* Ed. by Guram Bezhanishvili, Giovanna D'Agostino, George Metcalfe, and Thomas Studer. Vol. 12. College Publications, 2018, pp. 473–492 (cit. on p. 22).

[KLWW09] Boris Konev, Carsten Lutz, Dirk Walther, and Frank Wolter. "Formal Properties of Modularisation". In: *Modular Ontologies: Concepts, Theories and Techniques for Knowledge Modularization.* Ed. by Heiner Stuckenschmidt, Christine Parent, and Stefano Spaccapietra. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 25–66. ISBN: 978-3-642-01907-4. DOI: 10.1007/978-3-642-01907-43. URL: https://doi.org/10.1007/978-3-642-01907-43 (cit. on p. 35).

[Kra19] Jan Krajíček. *Proof Complexity.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019 (cit. on pp. 1–2, 43).

[KS13] P. Koopmann and R. A. Schmidt. "Uniform interpolation of $\mathcal{ALC}$-ontologies using fixpoints". In: *The International Symposium on Frontiers of Combining Systems, FroCos 2013.* 2013, pp. 87–102 (cit. on p. 39).

[Kuz16] Roman Kuznets. "Craig Interpolation via Hypersequents". In: *Concepts of Proof in Mathematics, Philosophy, and Computer Science.* Ed. by Dieter Probst and Peter Schuster. Berlin, Boston: De Gruyter, 2016, pp. 193–214. ISBN: 9781501502620. DOI: doi:10.1515/9781501502620-012. URL: https://doi.org/10.1515/9781501502620-012 (cit. on p. 22).

[Mae61] S. Maehara. "On the Interpolation Theorem of Craig'". In: *Sugaku* 12 (1961). (Japanese), pp. 235–237 (cit. on p. 2).

[Mak77] L. L. Maksimova. "Craig's theorem in superintuitionistic logics and amalgamable varieties of pseudo-boolean algebras". In: *Algebra i Logika* 16.6 (1977). (Russian). English translation (1977). *Algebra and Logic*, 16:427–455. DOI: 10.1007/BF01670006, pp. 643–681 (cit. on p. 12).

[Mak79] L. L. Maksimova. "Interpolation theorems in modal logic and amalgamable varieties of topoboolean algebras". In: *Algebra i Logika* 18.5 (1979). (Russian), pp. 556–586 (cit. on p. 12).

[McM03] K. L. McMillan. "Interpolation and SAT-based model checking". In: *CAV 2023*. Springer, 2003, pp. 1–13 (cit. on p. 1).

[Min68] G. E. Mints. "Some calculi of modal logic". In: *Logical and logical-mathematical calculus. Part I.* Vol. 98. Trudy Matematicheskogo Instituta Steklov. (Russian). English translation (1968): *Proceedings of the Steklov Institute of Mathematics*, 98:97–124. AMS, 1968, pp. 88–111 (cit. on p. 9).

[Mun82] Daniele Mundici. "Complexity of Craig's Interpolation". In: *Fundamenta Informaticae* 5.3-4 (1982), pp. 261–278. DOI: 10.3233/FI-1982-53-403. eprint: https://doi.org/10.3233/FI-1982-53-403. URL: https://doi.org/10.3233/FI-1982-53-403 (cit. on p. 42).

[NvPR01] Sara Negri, Jan von Plato, and Aarne Ranta. *Structural Proof Theory.* Cambridge University Press, 2001. DOI: 10.1017/CBO9780511527340 (cit. on p. 6).

[Ono98] Hiroakira Ono. "Proof-theoretic methods in nonclassical logic–an introduction". In: *Theories of types and proofs* 2 (1998), pp. 207–254 (cit. on p. 2).

[Pit92] Andrew M. Pitts. "On an interpretation of second order quantification in first order intuitionistic propositional logic". In: *The Journal of Symbolic Logic* 57.1 (1992), pp. 33–52. DOI: 10.2307/2275175 (cit. on pp. 2, 29).

[Pot83] Garrel Pottinger. "Uniform, cut-free formulations of T, $S4$, and $S5$". In: *The Journal of Symbolic Logic* 48.3 (Sept. 1983). (Abstract), p. 900. DOI: 10.2307/2273495 (cit. on p. 9).

[Rob56] A. Robinson. "A result on consistency and its application to the theory of definition". In: *Indagationes Mathematicae (Proceedings)* 59 (1956), pp. 47–58 (cit. on p. 1).

[Sau24] Alexis Saurin. *Interpolation as Cut-Introduction.* draft. 2024 (cit. on p. 17).

[Tak87] G. Takeuti. *Proof Theory*. Vol. 81. Studies in logic and the Foundations of Mathematics. North-Holland, 1987. ISBN: 9780444879431 (cit. on p. 2).

[tCFS13] B. ten Cate, E. Franconi, and I. Seylan. "Beth Definability in Expressive Description Logics". In: *Journal of Artificial Intelligence Research* 48 (2013), pp. 347–414. DOI: 10.1613/jair.4057 (cit. on pp. 34, 36–37).

[TS00] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory.* Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2000. ISBN: 9780521779111 (cit. on p. 6).

[TvD88] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics, Vol 1.* Vol. 121. ISSN. Elsevier, 1988. ISBN: 9780080570884 (cit. on p. 3).

[vBen08] Johan van Benthem. "The many faces of interpolation". In: *Synthese* 164.3 (July 2008), pp. 451–460. ISSN: 1573-0964. DOI: 10.1007/s11229-008-9351-5. URL: http://dx.doi.org/10.1007/s11229-008-9351-5 (cit. on p. 1).