Context Reasoning for Role-Based Models

Stephan Böhme

Summary

Nowadays, we are literally everywhere surrounded by software systems. Current developments indicate a continuing growth in the future. Not only the amount of systems increases, but also the requirements and expectations users impose on current software steadily rise. Modern software systems should cope with very complex scenarios. This includes the ability of context-awareness and self-adaptability. For example, a robot in a smart factory should recognize when a human co-worker approaches and switch to a different, human-friendly working mode accordingly. Similarly, software in autonomous cars or in the area of smart homes needs to adapt to various situations of which some are not even stated explicitly. Furthermore, software must be easily maintainable and, when necessary, changes on the system should be realised without much down time which, for example, in a smart factory is very costly.

In order to achieve all these goals, the concept of *roles* is very promising. First introduced by Bachman [BD77], roles appeared over the last decades in several fields of computer science. Most prominent is the *role-based access control* [FKC03; AF11; SCF+96], albeit it is only a special application for roles with a narrow scope. Roles are also introduced, for example, in data modelling [Hal06], conceptual modelling [Ste00; Gui05; Ste07] and programming languages [BBT06; Her07; BGE07].

The relational or context-dependent properties and behaviour of objects are transferred into the roles that an object plays in a certain context. This paradigm also supports Dijkstra's separation of concerns [Dij82] which simplifies development and maintenance of such systems. Due to the use of roles, *role-based systems* can model application domains cleaner and more structured, since ontologically different entities are modelled by different concepts.

Let us consider, for example, the concepts of Person and Customer. With an object-oriented approach of inheritance as a specialization relation, we could model Customer as a subclass of Person, as not every person is a customer. On the other hand, if we restrict our domain to a business context and add the concept of a Company, the inheritance relation would flip and we also have Company as subclass of Customer. This conflict can be resolved by recognising Person and Company as context-independent basic concepts, so-called *natural types* and Customer as a role a person or company can play in a business context. Here, it also becomes apparent that the concept of a *context* is closely related to a role.

While role-based modelling provides the means to handle and model complex and context-dependent domains in a well-structured and modular way, the process can still be tedious,

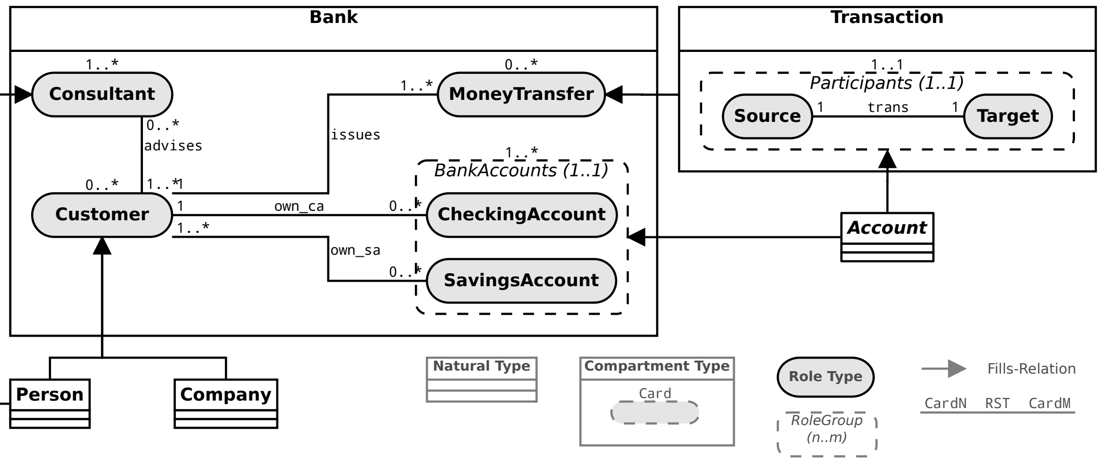

Figure 1: A bank example in CROM graphical notation

hard and error-prone. Due to the sophisticated semantics of roles, contexts and many different kinds of constraints, unintended implications or even inconsistencies can easily be hidden within such a model. Since it is nearly impossible to uncover all inferences, it becomes imperative for domain analysts to reason on role-based models to find such implicit knowledge. Here, a formally defined role modelling language and a feasible logical formalism are required.

In this thesis we focus on the *Compartment Role Object Model (CROM)* [KBG+15] to model dynamic, context-dependent domains. It introduces so-called *compartment types* to represent objectified contexts. These contain a set of *role types*, i.e. the roles that can be played in that context, a *fills*-relation that constrains which natural types are allowed to play certain role types, and a set of *relationship types*, i.e. a set of binary relations. Due to brevity we omit here the precise definitions of CROM and rather explain its expressiveness with the help of an example. Figure 1 shows a small banking example. In the context of a Bank there are the natural types Person and Company which can "play" the role of a Customer while only Persons can be Consultants. Additionally Accounts can be either CheckingAccounts or SavingsAccounts which in return can be owned by a customer. Furthermore, an Account can be either the Source or the Target in the context of a Transaction. Then, this transaction can be a MoneyTransfer that is issued by a Customer in the context of a Bank. This illustrates that compartments can again play roles within other compartments. At last, further constraints can be imposed on the model. These include, among others, *occurrence constraints* which restrict the number of roles played within a compartment, i.e. a Bank has at least one Consultant, and *cardinality constraints* which restrict the cardinalities of relationship types, i.e. a CheckingsAccount is owned by exactly one Customer.

However, reasoning directly on CROM models is not recommended as no elaborate reasoning algorithms exist and due to the lack of tool support. Therefore, we translate CROMs into a feasible logical formalism which allows for efficient reasoning.

As logical formalism we start with Description Logics (DLs) [BCM+07]. DLs are a well-known formalism for knowledge representation. They possess formal semantics and allow to define a variety of reasoning problems. The basic building blocks in description logics are so-called *concept names* and *role names*. Concept names denote sets of domain elements. For example, the concept names Person or Bank denote the sets of all persons or banks in a domain. Relational structures are represented by so-called DL *role names*, which are essentially binary relations on the domain. The term "role" originates from the early knowledge representation system KL-ONE [WS92] and has only little in common with roles of role-based systems except that it reflects the relational property of a role. A person which is related to a bank via a DL role customer could be seen as someone playing the role of a customer in the context of a bank. Besides that, DL roles are merely binary relations. With the help of *concept* and *role constructors*, complex concepts and roles can be defined. Which constructors are allowed depends on the specific DL. Complex concepts can be used as descriptions and to classify domain elements, e.g. the complex concept

$$\mathsf{NFL\_Player} \sqcap \mathsf{Healthy} \sqcap \exists.\mathsf{wins}(\mathsf{NFL\_Game}) \tag{1}$$

describes the set of all healthy NFL players who win NFL games.

With the help of concepts, we can express our knowledge about a domain through *DL axioms*. General knowledge is phrased via *general concept inclusions (GCIs)*, which state that one concept is a sub-concept of another. For example the GCI

$$\mathsf{NFL\_Player} \sqcap \mathsf{Healthy} \sqcap \exists.\mathsf{wins}(\mathsf{NFL\_Game}) \sqsubseteq \mathsf{Happy\_NFL\_Player} \tag{2}$$

states that a healthy NFL player who wins NFL games is a happy NFL player. Conversely, it does not say anything on whether every happy NFL player is healthy or wins games. Facts about a domain can be expressed via *concept* and *role assertions*. To express facts, we also introduce *individual names* which denote single domain elements. As an example consider the following axioms:

$$(\mathsf{NFL\_Player} \sqcap \mathsf{Healthy})(\mathit{AaronRodgers}) \tag{3}$$

$$\mathsf{NFL\_Game}(\mathit{SuperBowlXLV}), \tag{4}$$

$$\mathsf{wins}(\mathit{AaronRodgers}, \mathit{SuperBowlXLV}) \tag{5}$$

The first two concept assertions (3) and (4) state that Aaron Rodgers is a healthy NFL player and that Super Bowl XLV is an NFL game, while (5) expresses that he won Super Bowl XLV. So he is also a happy NFL player, even if not stated explicitly. A *DL knowledge base* is a set of such axioms.

The semantics of DLs are defined in a model-theoretic way and capture exactly the above mentioned intentions. An interpretation $\mathcal{I}$ consists of a domain and an interpretation function $\cdot^{\mathcal{I}}$ which maps concept, role and individual names, respectively, to subsets, binary relations and elements of the domain. From there, it is exactly defined how complex concepts must be interpreted. For example, $(A \sqcap B)^{\mathcal{I}}$ is the intersection of $A^{\mathcal{I}}$ and $B^{\mathcal{I}}$. The concept name NFL_Player itself has no meaning and an interpretation must make sure that $\mathsf{NFL\_Player}^{\mathcal{I}}$ actually is the set of all NFL players.

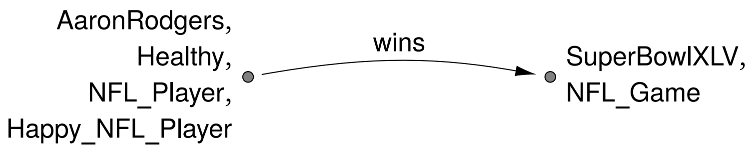

Figure 2: Interpretation that models axioms (2) to (6).

Now, the most interesting reasoning problems are the *consistency problem* and the *entailment problem*. A knowledge base is consistent if there exists some interpretation that *models* the knowledge base, i.e. an interpretation that fulfils all the axioms. An axiom is *entailed* by a knowledge base if every model of the knowledge base also models that axiom. For example, the following axiom is entailed by (2) to (5):

$$\mathsf{Happy\_NFL\_Player}(\mathit{AaronRodgers}). \tag{6}$$

Figure 2 depicts an interpretation which is a model of axioms (2) to (6).

However, classical DLs lack expressive power to formalise that some individuals satisfy certain concepts and relate to other individuals depending on a *specific context* which is needed to reason on role-based systems.

To overcome that deficiency in expressiveness of classical DLs, often two-dimensional DLs are employed [KG10; KG11b; KG11a; KG16]. This approach uses one DL $\mathcal{L}_\mathsf{M}$ as the *meta logic* to represent the contexts and their relationships to each other, and combines it with the *object logic* $\mathcal{L}_\mathsf{O}$ that captures the relational structure within each context. Moreover, while some pieces of information depend on the context, e.g. the roles played by an object within a compartment, other pieces of information are shared throughout all contexts, e.g. the name or the age of a person typically stays the same independent of the actual context. Expressing this context-independent information requires that some concepts and roles are designated to be *rigid*, i.e. they are required to be interpreted the same in all contexts. Unfortunately, if rigid roles are admitted, reasoning in the above mentioned two-dimensional DLs of context turns out to be undecidable; see [KG10].

We propose and investigate a family of two-dimensional context DLs $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ that meets the above requirements, but is a restricted form of the ones defined in [KG10] in the sense that we limit the interaction of $\mathcal{L}_\mathsf{M}$ and $\mathcal{L}_\mathsf{O}$. More precisely, in our family of context DLs the meta logic can refer to the internal structure of each context, but not vice versa. That means that information is viewed in a top-down manner, i.e. information of different contexts is strictly capsuled and can only be accessed from the meta level. Hence, we cannot express, for instance, that everybody who is employed by a company has a certain property in the context of private life. We show that reasoning in $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ stays decidable with such a restriction, even in the presence of rigid roles. In some sense this restriction is similar to what is done in [BGL08; BGL12; Lip14] to obtain a decidable temporalised DL with rigid roles.

The syntax and semantics of the object logic $\mathcal{L}_\mathsf{O}$ are defined in the standard way. See the upper part of Table 1 for the case where $\mathcal{L}_\mathsf{O}$ is $\mathcal{SHOIQ}$. The syntax of the meta logic $\mathcal{L}_\mathsf{M}$ is enriched by the additional concept constructor of *referring concepts* which considers object

Table 1: Syntax and Semantics of $\mathcal{SHOIQ}[\![\mathcal{SHOIQ}]\!]$

	syntax	semantics	
inverse object role	R^-	$\{(e,d) \in \Delta \times \Delta \mid (d,e) \in R^{\mathcal{I}_c}\}$	
object negation	$\neg C$	$\Delta \setminus C^{\mathcal{I}_c}$	
object conjunction	$C \sqcap D$	$C^{\mathcal{I}_c} \cap D^{\mathcal{I}_c}$	
object existential restriction	$\exists R.C$	$\{d \in \Delta \mid \text{there is some } e \in C^{\mathcal{I}_c} \text{ with } (d,e) \in R^{\mathcal{I}_c}\}$	
object nominal	$\{a\}$	$\{a^{\mathcal{I}_c}\}$	
object at-most restriction	$\leqslant_n S.C$	$\{d \in \Delta \mid \sharp\{e \in C^{\mathcal{I}_c} \mid (d,e) \in S^{\mathcal{I}_c}\} \leq n\}$	
object general concept inclusion	$C \sqsubseteq D$	$C^{\mathcal{I}_c} \subseteq D^{\mathcal{I}_c}$	
object concept assertion	$C(a)$	$a^{\mathcal{I}_c} \in C^{\mathcal{I}_c}$	α
object role assertion	$R(a,b)$	$(a^{\mathcal{I}_c}, b^{\mathcal{I}_c}) \in R^{\mathcal{I}_c}$	
object role inclusion	$R \sqsubseteq S$	$R^{\mathcal{I}_c} \subseteq S^{\mathcal{I}_c}$	$\mathcal{R}_\mathsf{O}$
object transitivity axiom	$\mathsf{Trans}(R)$	$R^{\mathcal{I}_c}$ is transitive.	
inverse meta role	P^-	$\{(e,d) \in \mathbb{C} \times \mathbb{C} \mid (d,e) \in P^{\mathcal{J}}\}$	
meta negation	$\neg E$	$\mathbb{C} \setminus E^{\mathcal{J}}$	
meta conjunction	$E \sqcap F$	$E^{\mathcal{J}} \cap F^{\mathcal{J}}$	
meta existential restriction	$\exists P.E$	$\{d \in \mathbb{C} \mid \text{there is some } e \in E^{\mathcal{J}} \text{ with } (d,e) \in P^{\mathcal{J}}\}$	
meta nominal	$\{u\}$	$\{u^{\mathcal{J}}\}$	
meta at-most restriction	$\leqslant_n Q.E$	$\{d \in \mathbb{C} \mid \sharp\{e \in E^{\mathcal{J}} \mid (d,e) \in Q^{\mathcal{J}}\} \leq n\}$	
referring concept	$[\![\alpha]\!]$	$\{d \in \mathbb{C} \mid \mathcal{I}_d \models \alpha\}$	
meta general concept inclusion	$E \sqsubseteq F$	$E^{\mathcal{J}} \subseteq F^{\mathcal{J}}$	
meta concept assertion	$E(u)$	$u^{\mathcal{J}} \in E^{\mathcal{J}}$	$\mathcal{B}$
meta role assertion	$T(u,v)$	$(u^{\mathcal{J}}, v^{\mathcal{J}}) \in T^{\mathcal{J}}$	
meta role inclusion	$R \sqsubseteq S$	$R^{\mathcal{I}_c} \subseteq S^{\mathcal{I}_c}$	$\mathcal{R}_\mathsf{M}$
meta transitivity axiom	$\mathsf{Trans}(R)$	$R^{\mathcal{I}_c}$ is transitive.	

axioms that would occur in a TBox or ABox, i.e. GCIs, concept and role assertions, as meta concepts (lower part of Table 1). An $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$-*Boolean knowledge base (BKB)* consists of a Boolean combination $\mathcal{B}$ of meta TBox and ABox axioms, a set $\mathcal{R}_\mathsf{O}$ of object role axioms and a set $\mathcal{R}_\mathsf{M}$ of meta role axioms. The semantics of $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ are defined by *nested interpretations*. A nested interpretation $\mathcal{J} = (\mathbb{C}, \cdot^{\mathcal{J}}, \Delta^{\mathcal{J}}, (\cdot^{\mathcal{I}_c})_{c \in \mathbb{C}})$ consists of a set $\mathbb{C}$ of *contexts* (or possible worlds), an interpretation function $\cdot^{\mathcal{J}}$ for the meta dimension, an object domain $\Delta^{\mathcal{J}}$ and a set of interpretation functions $(\cdot^{\mathcal{I}_c})_{c \in \mathbb{C}}$ for the object dimension. The interpretation functions and the entailment relation $\models$ are defined in the standard way and they are extended to complex concepts as shown in the right column of Table 1. An $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$-BKB is called *consistent* if there exists a nested interpretation $\mathcal{J}$ such that $\mathcal{J}$ models $\mathcal{B}$, $\mathcal{R}_\mathsf{M}$ and $\mathcal{R}_\mathsf{O}$. The *consistency problem* in $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ is the problem of deciding whether a given $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$-BKB is consistent.

To provide a better intuition on how our formalism works, we examine the following example. Consider the following axioms:

$$\top \sqsubseteq [\![\exists \mathsf{worksFor}.\{\mathit{Siemens}\} \sqsubseteq \exists \mathsf{hasAccessRights}.\{\mathit{Siemens}\}]\!] \tag{7}$$

$$\mathsf{Work} \sqsubseteq [\![\mathsf{worksFor}(\mathit{Bob}, \mathit{Siemens})]\!] \tag{8}$$

$$[\![(\exists \mathsf{worksFor}.\top)(\mathit{Bob})]\!] \sqsubseteq \exists \mathsf{related}.(\mathsf{Private} \sqcap [\![\mathsf{HasMoney}(\mathit{Bob})]\!]) \tag{9}$$

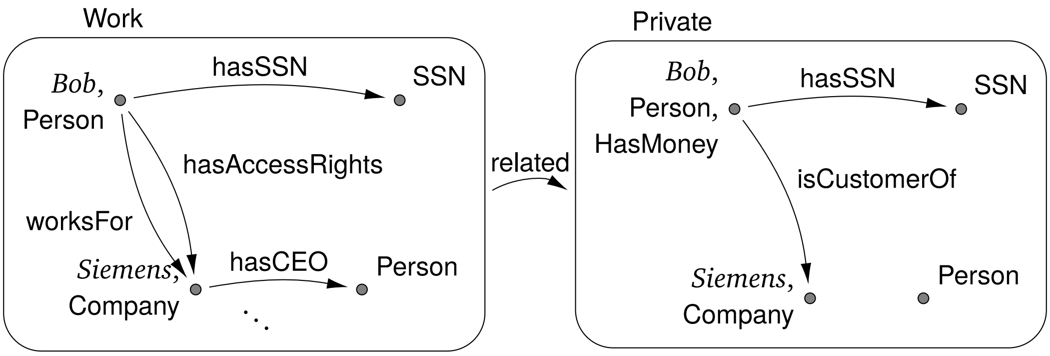

Figure 3: Nested interpretation that models of Axioms (7)– (13)

$$\top \sqsubseteq [\![\exists \mathsf{isCustomerOf}.\top \sqsubseteq \mathsf{HasMoney}]\!] \tag{10}$$

$$\mathsf{Private} \sqsubseteq [\![\mathsf{isCustomerOf}(\mathit{Bob}, \mathit{Siemens})]\!] \tag{11}$$

$$\mathsf{Private} \sqcap \mathsf{Work} \sqsubseteq \bot \tag{12}$$

$$\neg\mathsf{Work} \sqsubseteq [\![\exists \mathsf{worksFor}.\top \sqsubseteq \bot]\!] \tag{13}$$

The first axiom states that in all contexts somebody who works for Siemens also has access rights to certain data. The second axiom states that Bob is an employee of Siemens in any work context. Furthermore, Axioms (9) and (10) say intuitively that if Bob has a job, he will earn money, which he can spend as a customer. Axiom (11) formalises that Bob is a customer of Siemens in any private context. Moreover, Axiom (12) ensures that the private contexts are disjoint from the work contexts. Finally, Axiom (13) states that the worksFor relation only exists in work contexts. Figure 3 depicts a model of Axioms (7) – (13).

As a basis for any further application of a newly defined logical framework a thorough analysis of the computational complexities is necessary. We focus in this thesis on the complexity of the consistency problem in $\mathcal{L}_{\mathsf{M}}[\![\mathcal{L}_{\mathsf{O}}]\!]$. The results are shown in Table 2 In this summary we only want to sketch the ideas how to obtain the upper bounds, since the main lemma is reused for the implementation of the reasoner later.

We proceed similar to what was done for $\mathcal{ALC}$-LTL in [BGL08; BGL12] and reduce the consistency problem to two separate decision problems. For the first decision problem, we consider the so-called *outer abstraction*, which is the $\mathcal{L}_{\mathsf{M}}$ knowledge base obtained by replacing each referring m-concept of the form $[\![\alpha]\!]$ by a fresh concept name such that there is a 1–1 relationship between them.

This outer abstraction does not only need to be consistent, it must be consistent in the sense that only certain sets of object axioms hold in each context. This additional request is defined by the *outer consistency w.r.t $\mathcal{X}$*. Furthermore, the second decision problem that we use for deciding consistency is needed to make sure that such a set of abstracted concept names is admissible in the following sense.

Definition 1 (Admissibility). *Let $\mathcal{X} = \{X_1, \ldots, X_k\} \subseteq \mathcal{P}(\mathsf{ran}(\mathsf{b}))$. We call $\mathcal{X}$* admissible *if there exist* O*-interpretations $\mathcal{I}_1 = (\Delta, \cdot^{\mathcal{I}_1}), \ldots, \mathcal{I}_k = (\Delta, \cdot^{\mathcal{I}_k})$ such that*

Table 2: The complexity results for the consistency problem in $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$

Setting	$\mathcal{L}_\mathsf{M}$ \ $\mathcal{L}_\mathsf{O}$	$\mathcal{EL}$	$\mathcal{ALC}$	$\mathcal{SHOQ}$	$\mathcal{SHOIQ}$
Setting (i)	$\mathcal{EL}$	constant	ExpTime-complete	ExpTime-complete	NExpTime-complete
	$\mathcal{ALC}$	ExpTime-complete	ExpTime-complete	ExpTime-complete	NExpTime-complete
	$\mathcal{SHOQ}$	ExpTime-complete	ExpTime-complete	ExpTime-complete	NExpTime-complete
	$\mathcal{SHOIQ}$	NExpTime-complete	NExpTime-complete	NExpTime-complete	NExpTime-complete
Setting (ii)	$\mathcal{EL}$	constant	NExpTime-complete	NExpTime-complete	NExpTime-hard and in N2ExpTime
	$\mathcal{ALC}$	NExpTime-complete	NExpTime-complete	NExpTime-complete	NExpTime-hard and in N2ExpTime
	$\mathcal{SHOQ}$	NExpTime-complete	NExpTime-complete	NExpTime-complete	NExpTime-hard and in N2ExpTime
	$\mathcal{SHOIQ}$	NExpTime-complete	NExpTime-complete	NExpTime-complete	NExpTime-hard and in N2ExpTime
Setting (iii)	$\mathcal{EL}$	constant	2ExpTime-complete	2ExpTime-complete	2ExpTime-hard and in N2ExpTime
	$\mathcal{ALC}$	NExpTime-complete	2ExpTime-complete	2ExpTime-complete	2ExpTime-hard and in N2ExpTime
	$\mathcal{SHOQ}$	NExpTime-complete	2ExpTime-complete	2ExpTime-complete	2ExpTime-hard and in N2ExpTime
	$\mathcal{SHOIQ}$	NExpTime-complete	2ExpTime-complete	2ExpTime-complete	2ExpTime-hard and in N2ExpTime

Settings: (i) No rigid names are allowed. (ii) Only rigid concepts are allowed. (iii) Rigid roles are allowed.

- *$x^{\mathcal{I}_i} = x^{\mathcal{I}_j}$ for all $x \in \mathsf{O_I} \cup \mathsf{O_{Crig}} \cup \mathsf{O_{Rrig}}$ and all $i, j \in \{1, \ldots, k\}$, and*
- *every $\mathcal{I}_i$, $1 \leq i \leq k$, is a model of the $\mathcal{L}_\mathsf{O}$-BKB $\mathfrak{B}_{X_i} = (\mathcal{B}_{X_i}, \mathcal{R}_\mathsf{O})$ over O where*

$$\mathcal{B}_{X_i} := \bigwedge_{\mathsf{b}([\![\alpha]\!]) \in X_i} \alpha \wedge \bigwedge_{\mathsf{b}([\![\alpha]\!]) \in \mathsf{ran}(\mathsf{b}) \setminus X_i} \neg\alpha.$$

$\diamondsuit$

Now, the main lemma in this section states that the consistency problem in $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ can be reduced into two separate decision problems.

Lemma 2. *The $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$-BKB $\mathcal{B}$ is consistent iff there is a set $\mathcal{X} \subseteq \mathcal{P}(\mathsf{ran}(\mathsf{b}))$ such that*

1. *$\mathcal{X}$ is admissible, and*
2. *the outer abstraction of $\mathcal{B}$ is outer consistent w.r.t. $\mathcal{X}$.*

Based on this lemma, we can distinguish the three settings whether rigid concepts or rigid roles are admitted in the BKB. Depending on these settings and on which DL is used as object or meta logic, several complexity results were obtained and are summarized in Table 2.

Besides the capability of context description logics to formalise role-based models, it is rather hard for domain analysts—who in general are not experts in DLs—to grasp the precise semantics of the ontology, and to define the contextualised ontology in a way that all entities and constraints appearing in the role-based model are mapped correctly. Therefore, it would be ideal to have an algorithm that translates role-based models into context DL knowledge bases. In this thesis, we present exactly such a mapping.

We already decided for CROM as a modelling language due to its formal semantics. This is important since otherwise we cannot ensure that the intended meaning of every model is correctly translated into the ontology.

There is also some freedom on how to express roles and role-playing in an ontology. While it is important to consider the ontological nature of roles such as identity or rigidity, we also have to consider practical reasons. Whether some constraints of a role-based model can be expressed in an ontology highly depends on how roles and other predicates are translated.

Exemplarily, we illustrate how the fills-relation is encoded into the ontology. The fills-relation specifies which natural or compartment types are allowed to play which role types. Hence, elements that play a certain role type can only be naturals or o-compartments of types which fill that role type:

$$\top \sqsubseteq \bigsqcap_{RT \in \mathsf{N}_{\mathsf{RT}}} \left[\!\!\left[\exists \mathsf{plays}.RT \sqsubseteq \left(\bigsqcup\nolimits_{(T,RT) \in \mathsf{fills}} T \right) \right]\!\!\right]. \tag{14}$$

For the above introduced banking example the following axiom is generated:

$$\begin{aligned} \top \sqsubseteq & [\![\exists \mathsf{plays}.\mathsf{Consultant} \sqsubseteq (\mathsf{Person})]\!] \sqcap [\![\exists \mathsf{plays}.\mathsf{Customer} \sqsubseteq (\mathsf{Person} \sqcup \mathsf{Company})]\!] \\ & \sqcap [\![\exists \mathsf{plays}.\mathsf{SavingsAccount} \sqsubseteq \mathsf{Account}]\!] \sqcap \ldots . \end{aligned} \tag{15}$$

We proved the semantical correctness of our translation from role-based models into an $\mathcal{L}_{\mathsf{M}}[\![\mathcal{L}_{\mathsf{O}}]\!]$ ontology, but for practical application there must exist some implementation of the mapping. We based our implementation on the reference implementation for CROM, which in turn can be used by FRaMED, a graphical editor allowing the specification of role-based models. In the end, our implemented mapping produces an ontology which is specially formatted in the Web Ontology Language (OWL). This leads to the last open part in the overall workflow.

A contextualised DL capable of formalising role-based models and an automated mapping from role-based models into an ontology still helps only little in practice, if there is no DL reasoner available which can process such ontologies. Usually DL reasoners use OWL as language for the input ontology. But OWL in general does not have the syntactical means to express contextualised DL axioms. However, OWL enables us to annotate axioms which we use to encode $\mathcal{L}_{\mathsf{M}}[\![\mathcal{L}_{\mathsf{O}}]\!]$-axioms.

Although the reasoning tasks in DLs have a high complexity, DLs have been successfully introduced as a formalism for knowledge representation. One reason for the success of DLs is the availability of highly optimised reasoners which makes drawing logical inferences feasible. A black-box approach for deciding consistency of an $\mathcal{L}_{\mathsf{M}}[\![\mathcal{L}_{\mathsf{O}}]\!]$-ontology could benefit from these optimised reasoners. In order to reuse an existing reasoner, we convert the consistency problem in ConDL to classical reasoning tasks. As shown above the consistency problem can be reduced into two separate decision problems; firstly reasoning on the meta level, and secondly checking whether the object level is consistent in each context. For several reasons we base our implementation on the hypertableau reasoner HermiT [MSH09; GHM+14]. A model construction-based reasoner is necessary since we need information about the appearing o-axioms when reasoning on the meta level. Besides that HermiT is implemented in Java and

Algorithm 1: Algorithm for checking consistency with hypertableau

Input : $\mathcal{SHOIQ}[\![\mathcal{SHOIQ}]\!]$-ontology $\mathcal{O}$
Output : true if $\mathcal{O}$ is consistent, false otherwise
Preprocessing (results in $(\mathcal{C},\mathcal{A})$):
1. Elimination of transitivity axioms, normalisation, clausification
2. Repletion of DL-clauses

Let (T,λ) be any derivation for $(\mathcal{C},\mathcal{A})$.
$\mathfrak{A} := \{\mathcal{A}' \mid$ there exists a leaf node in (T,λ) that is labelled with $\mathcal{A}'\}$
for $\mathcal{A}' \in \mathfrak{A}$ **do**
    if $\mathcal{A}'$ *is clash-free* **then**
        if $\mathcal{O}$ *contains rigid names* **then**
            if $\mathcal{K}_{\mathsf{rig}} := (\mathcal{O}_{\mathcal{A}'}, \mathcal{R}_{\mathsf{O}}{}'''')$ *is consistent* **then**
                return true
        else
            Let $\{c_1,\ldots,c_k\}$ be the individuals occurring in $\mathcal{A}'$
            if $\mathcal{K}_i := (\mathcal{O}_{c_i}, \mathcal{R}_{\mathsf{O}})$ *is consistent for all* $1 \le i \le k$ **then**
                return true

return *false*

according to the ORE Report [PMG+15] the most perfomant, model-based reasoner in the discipline *OWL DL Consistency*.

For brevity, we omit the details of the hypertableau algorithm here. The sound, complete and terminating algorithm that we construct on the basis of hypertableau is shown in Algorithm 1. Here, $\mathcal{C}$ is the set of DL clauses, $\mathcal{A}$ the ABox obtained in the clausification of $\mathcal{O}$ and $\mathcal{K}_i$ is the object ontology for the world c_i which collects all o-axioms in $\mathcal{A}'$ that are asserted to hold in $c_i$and all other o-axioms as negated axioms. $\mathcal{K}_{\mathsf{rig}}$ is defined analogously to $\mathcal{K}_i$, but using the renaming technique as single ontology for all worlds.

The second step of the preprocessing, i.e. the *repletion*, is necessary to ensure completeness of Algorithm 1. The hypertableau algorithm avoids the unnecessary non-determinism which is usually introduced by the GCI-rule in tableau algorithms [MSH09]. But this optimisation disguises some implicit contradictions in the DL clauses. Consider $\mathcal{C}_{\mathsf{ex}} = \{[\![\neg A(a)]\!](x) \to C(x), \top \to C(x) \vee [\![A \sqsubseteq \bot]\!](x)\}$ and $\mathcal{A}_{\mathsf{ex}} = \{\neg C(s)\}$. Here, only $[\![A \sqsubseteq \bot]\!](s)$ would be derived and the ontology seems to be consistent. Let $\mathcal{J}$ be a model, then we have $s \in (\neg C)^{\mathcal{J}}$, $s \in [\![A \sqsubseteq \bot]\!]^{\mathcal{J}}$ and $s \notin [\![\neg A(a)]\!]^{\mathcal{J}}$ which, by the semantics of ConDL, implies $s \in [\![A(a)]\!]^{\mathcal{J}}$. This contradicts $[\![A \sqsubseteq \bot]\!](s)$ and $(\mathcal{C}_{\mathsf{ex}}, \mathcal{A}_{\mathsf{ex}})$ is indeed inconsistent. To make these implicitly negated o-axioms visible, we introduce the repletion of $\mathcal{C}$.

Definition 3 (Repletion of DL-Clauses). *Let $\mathcal{C}$ be a set of DL-clauses. The* repletion *of $\mathcal{C}$ is obtained from $\mathcal{C}$ by adding the DL-clause $\top \to [\![\alpha]\!](x) \vee [\![\neg\alpha]\!](x)$ for each o-axiom $[\![\alpha]\!]$ occurring in $\mathcal{C}$.* ◊

A drawback of the repletion is the high amount of non-determinism it introduces, but it is only necessary if o-axioms occur in the antecedent of a DL-clause and only if compartments play roles, such o-axioms are introduced in the antecedent. Therefore, only then the repletion is necessary when reasoning on CROMs. Arguably, when constraints are omitted, CROM can be mapped to a less expressive ConDL, which further reduces the reasoning time.

To conclude, in this thesis we introduced the new contextualised description logic $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ and conducted a thorough analysis of the computational complexity of the consistency problem. We then utilised $\mathcal{L}_\mathsf{M}[\![\mathcal{L}_\mathsf{O}]\!]$ in order to transform role-based models into contextualised ontologies. With the help of this transformation and the implementation of the first reasoner capable of processing such ontologies we are able to reason on role-based models. This overall workflow is available to the modelling expert (and fellow RoSI students) due to its integration into the CROM reference implementation and its graphical editor FRaMED.

References

[AF11] Vijay Alturi and David F. Ferraiolo: 'Role-Based Access Control'. In *Encyclopedia of Cryptography and Security, 2nd Ed.* Edited by Henk C. A. van Tilborg and Sushil Jajodia. Springer-Verlag, 2011, pages 1053–1055 (cited on page 1).

[BCM+07] Franz Baader, Diego Calvanese, Deborah L. McGuinness, Daniele Nardi, and Peter F. Patel-Schneider, editors: *The Description Logic Handbook: Theory, Implementation, and Applications*. 2nd edition. Cambridge University Press, 2007 (cited on page 2).

[BGL08] Franz Baader, Silvio Ghilardi, and Carsten Lutz: 'LTL Over Description Logic Axioms'. In *Proc. of the 11th Int. Conf. on Principles of Knowledge Representation and Reasoning (KR 2008)*, Sydney, Australia. Edited by Gerhard Brewka and Jérôme Lang. AAAI Press, Sept. 2008, pages 684–694 (cited on pages 4, 6, 10).

[BGL12] Franz Baader, Silvio Ghilardi, and Carsten Lutz: 'LTL Over Description Logic Axioms'. In *ACM Transactions on Computational Logic* **13**(3): 2012. This is an extended version of [BGL08] (cited on pages 4, 6).

[BD77] Charles W. Bachman and Manilal Daya: 'The Role Concept in Data Models'. In *Proc. of the 3rd Int. Conf. on Very Large Data Bases (VLDB 1977)*, Tokyo, Japan. IEEE Computer Society, Oct. 1977, pages 464–476 (cited on page 1).

[BBT06] Matteo Baldoni, Guido Boella, and Leendert W. N. van der Torre: 'powerJava: Ontologically Founded Roles in Object Oriented Programming Languages'. In *Proc. of the 21st Annual ACM Symposium on Applied Computing (SAC 2006)*, Dijon, France. Edited by Hisham Haddad. ACM, Apr. 2006, pages 1414–1418 (cited on page 1).

[BGE07] Stephanie Balzer, Thomas R. Gross, and Patrick Eugster: 'A Relational Model of Object Collaborations and Its Use in Reasoning About Relationships'. In *Proc. of the 21st European Conf. on Object-Oriented Programming (ECOOP 2007)*, Berlin, Germany. Edited by Erik Ernst. Volume 4609. Lecture Notes in Computer Science. Springer-Verlag, July 2007, pages 323–346 (cited on page 1).

[Dij82] Edsger W. Dijkstra: 'On the role of scientific thought'. In *Selected Writings on Computing: A Personal Perspective*. Springer-Verlag, 1982, pages 60–66 (cited on page 1).

[FKC03] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli: *Role-based Access Control*. Artech House, 2003 (cited on page 1).

[GHM+14] Birte Glimm, Ian Horrocks, Boris Motik, Giorgos Stoilos, and Zhe Wang: 'HermiT: An OWL 2 Reasoner'. In *Journal of Automated Reasoning* **53**(3): 2014, pages 245–269 (cited on page 8).

[Gui05] Giancarlo Guizzardi: 'Ontological Foundations for Structural Conceptual Models'. PhD thesis. Enschede, Netherlands: University of Twente, 2005 (cited on page 1).

[Hal06] Terry A. Halpin: 'Object-role modeling (ORM/NIAM)'. In *Handbook on Architectures of Information Systems*. Edited by Peter Bernus, Kai Mertins, and Günter Schmidt. 2nd edition. Springer-Verlag, 2006. Chapter 4, pages 81–103 (cited on page 1).

[Her07] Stephan Herrmann: 'A Precise Model for Contextual Roles: The Programming Language ObjectTeams/Java'. In *Applied Ontology* **2**(2): 2007, pages 181–207 (cited on page 1).

[KG10] Szymon Klarman and Víctor Gutiérrez-Basulto: '$\mathcal{ALC}_{\mathcal{ALC}}$: A Context Description Logic'. In *Proceedings of the 12th European Conference on Logics in Artificial Intelligence (JELIA 2010)*. Edited by Tomi Janhunen and Ilkka Niemelä. Volume 6341. Lecture Notes in Computer Science. Springer, 2010, pages 208–220 (cited on page 4).

[KG11a] Szymon Klarman and Víctor Gutiérrez-Basulto: 'Two-Dimensional Description Logics for Context-Based Semantic Interoperability'. In *Proc. of the 25th AAAI Conf. on Artificial Intelligence (AAAI 2011)*, San Francisco, CA, USA. Edited by Wolfram Burgard and Dan Roth. AAAI Press, Aug. 2011 (cited on page 4).

[KG11b] Szymon Klarman and Víctor Gutiérrez-Basulto: 'Two-Dimensional Description Logics of Context'. In *Proceedings of the 24th International Workshop on Description Logics (DL 2011)*. Edited by Riccardo Rosati, Sebastian Rudolph, and Michael Zakharyaschev. Volume 745. CEUR-WS.org, 2011 (cited on page 4).

[KG16] Szymon Klarman and Víctor Gutiérrez-Basulto: 'Description logics of context'. In *Journal of Logic and Computation* **26**(3): 2016, pages 817–854 (cited on page 4).

[KBG+15] Thomas Kühn, Stephan Böhme, Sebastian Götz, and Uwe Aßmann: 'A combined formal model for relational context-dependent roles'. In *Proc. of the 8th ACM SIGPLAN Int. Conf. on Software Language Engineering (SLE 2015)*, Pittsburgh, PA, USA. Edited by Richard F. Paige, Davide Di Ruscio, and Markus Völter. ACM, Oct. 2015, pages 113–124 (cited on page 2).

[KLG+14] Thomas Kühn, Max Leuthäuser, Sebastian Götz, Christoph Seidl, and Uwe Aßmann: 'A Metamodel Family for Role-Based Modeling and Programming Languages'. In *Proc. of the 7th Int. Conf. on Software Language Engineering (SLE 2014)*, Västerås, Sweden. Edited by Benoît Combemale, David J. Pearce, Olivier Barais, and Jurgen J. Vinju. Volume 8706. Lecture Notes in Computer Science. Springer-Verlag, Sept. 2014, pages 141–160.

[Lip14] Marcel Lippmann: 'Temporalised Description Logics for Monitoring Partially Observable Events'. PhD thesis. Dresden, Germany: TU Dresden, 2014 (cited on page 4).

[MSH09] Boris Motik, Rob Shearer, and Ian Horrocks: 'Hypertableau Reasoning for Description Logics'. In *Journal of Artificial Intelligence Research* **36**: 2009, pages 165–228 (cited on pages 8, 9).

[PMG+15] Bijan Parsia, Nicolas Matentzoglu, Rafael S. Gonçalves, Birte Glimm, and Andreas Steigmiller: 'The OWL Reasoner Evaluation (ORE) 2015 Competition Report'. In *Proc. of the 11th Int. Workshop on Scalable Semantic Web Knowledge Base Systems (SSWS 2015) co-located with 14th Int. Semantic Web Conference (ISWC 2015)*, Bethlehem, PA, USA. Edited by Thorsten Liebig and Achille Fokoue. Volume 1457. CEUR Workshop Proceedings. `CEUR-WS.org`, Oct. 2015, pages 2–15 (cited on page 9).

[SCF+96] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman: 'Role-Based Access Control Models'. In *IEEE Computer* **29**(2): Feb. 1996, pages 38–47 (cited on page 1).

[Ste00] Friedrich Steimann: 'On the representation of roles in object-oriented and conceptual modelling'. In *Data & Knowledge Engineering* **35**(1): Oct. 2000, pages 83–106 (cited on page 1).

[Ste07] Friedrich Steimann: 'The Role Data Model Revisited'. In *Applied Ontology* **2**(2): 2007, pages 89–103 (cited on page 1).

[WS92] William A. Woods and James G. Schmolze: 'The KL-ONE Family'. In *Computers & Mathematics with Applications* **23**(2-5): 1992, pages 133–177 (cited on page 3).