Controlled Query Evaluation over Ontologies through Policies with Numerical Restrictions

Gianluca Cima
CNRS & University of Bordeaux
0000-0003-1783-5605

Domenico Lembo
Sapienza University of Rome
0000-0002-0628-242X

Lorenzo Marconi
Sapienza University of Rome
0000-0001-9633-8476

Riccardo Rosati
Sapienza University of Rome
0000-0002-7697-4958

Domenico Fabio Savo
University of Bergamo
0000-0002-8391-8049

Daniele Sinibaldi
Sapienza University of Rome
daniele.sinibaldi@hotmail.it

***Abstract*—We study Controlled Query Evaluation (CQE), a declarative approach to privacy-preserving query answering. In particular, we focus on the application of CQE to ontologies and analyze the possibility of using role cardinality restrictions in the formulas expressing a data protection policy. We start from an existing framework for CQE over *DL-Lite* ontologies, and extend the policy language of the existing framework defining a class of formulas (called *numerical restriction axioms*) with role number restrictions. We show that the computational properties of the existing framework are not affected by the extension of the policy language. In particular, conjunctive query answering over *DL-Lite*$_{horn}^{\mathcal{H}}$ ontologies under the CQE semantics (IGA) is still FO-rewritable and is in AC^0 with respect to data complexity.**

***Index Terms*—Description Logics, Information Disclosure, Numerical Restrictions, First-Order Rewritability**

I. Introduction

Controlled Query Evaluation (CQE) is an approach to privacy-preserving query answering that recently has gained attention in the context of ontologies and Description Logics (DLs) [1]–[4]. In this framework, a data protection policy is specified over an ontology in terms of logical statements declaring confidential information that must not be revealed to the users. Of course, the ontology may violate the data protection policy. However, the enforcement of the policy can be done in a virtual way, without modifying the ontology, but changing the query answering mechanism, which filters the answers provided to the users based on the policy.

Almost all the studies [3]–[6] conducted so far consider a framework for CQE in which the policy is constituted by a set of formulas, and each of such formulas is the negation of a conjunctive query (without inequality/comparison predicates). More precisely, a data protection policy is formalized through a set of sentences of the form $q \rightarrow \bot$, where q is a Boolean conjunctive query over the concepts and roles of the ontology.

Although expressive, such a policy language does not seem always sufficient to fully formalize data protection policies in real-world domains. In particular, one of the most important missing aspects is the possibility of expressing role/property number (a.k.a. cardinality) restrictions in data protection formulas. This seems a pivotal aspect towards the practical usage of the CQE approach as shown in the following example.

Example 1: During the initial phase of the Covid-19 vaccination campaign, the minors who have been given both doses of the vaccine are only those with specific diseases. This sensitive information can be kept secret by the following DL concept inclusion axiom (where vaccinatedWith is the role representing that an individual has been vaccinated with a specific vaccine lot):

$$\mathsf{minor} \sqcap (\geq 2\ \mathsf{vaccinatedWith}) \sqsubseteq \bot$$

corresponding to the following negation of a conjunctive query with inequality atoms:

$$\exists p, l_1, l_2.\quad \mathsf{minor}(p) \wedge \mathsf{vaccinatedWith}(p, l_1) \wedge \mathsf{vaccinatedWith}(p, l_2) \wedge l_1 \neq l_2 \rightarrow \bot$$

In this paper, we try to fill this gap. Specifically, we start from the framework for CQE over *DL-Lite* ontologies studied in [5], and extend the policy language of such a framework, defining a class of formulas called *numerical restrictions*, which allow for the presence of (unqualified) role number restrictions. Furthermore, we consider here the *DL-Lite*$_{horn}^{\mathcal{H}}$ ontology language, which is more expressive than *DL-Lite*$_{\mathcal{R}}$ studied in [5]. We show that the computational properties of the framework presented in [5] are not affected by the extension of the policy and the ontology language. In particular, conjunctive query answering under the so-called IGA semantics for CQE is still first-order (FO) rewritable and thus is in AC^0 with respect to data complexity.

The rest of the paper is organized as follows. After some preliminaries in Section II, we introduce the CQE framework and the new policy language in Section III, and show the computational properties of the new CQE framewok for the *DL-Lite*$_{horn}^{\mathcal{H}}$ case in Section IV. Section V concludes the paper.

II. Preliminaries

Description Logics (DLs) are fragments of FO logic using only unary and binary predicates, called concepts and roles, respectively. We assume to have the pairwise disjoint countably infinite sets $\Sigma_C, \Sigma_R, \Sigma_I$ and $\Sigma_{\mathcal{V}}$ for *atomic concepts*, *atomic roles*, *constants* (a.k.a. individuals), and *variables*, respectively. A DL ontology $\mathcal{O}$ is a set $\mathcal{T} \cup \mathcal{A}$, where $\mathcal{T}$ is the TBox

and $\mathcal{A}$ is the ABox, specifying intensional and extensional knowledge, respectively. The set of atomic concepts and roles occurring in $\mathcal{O}$ is the *signature* of $\mathcal{O}$. The semantics of $\mathcal{O}$ is given in terms of FO models over the signature of $\mathcal{O}$, in the standard way. In particular, we consider only models satisfying the *unique name assumption (UNA)*. An ontology $\mathcal{O} = \mathcal{T} \cup \mathcal{A}$ *entails* an FO sentence ϕ specified over the signature of $\mathcal{O}$, denoted $\mathcal{O} \models \phi$, if ϕ is implied by every model of $\mathcal{O}$. We say that an ontology is *consistent* if it has at least one model, *inconsistent* otherwise. Also, we say that an ABox $\mathcal{A}$ is *consistent with* (resp. *inconsistent with*) a TBox $\mathcal{T}$, if $\mathcal{T} \cup \mathcal{A}$ is consistent (resp. inconsistent). Given a TBox $\mathcal{T}$, we denote by $\mathsf{cl}_{\mathcal{T}}(\cdot)$ the function that, for an ABox $\mathcal{A}$ consistent with $\mathcal{T}$, returns the deductive closure of $\mathcal{A}$ w.r.t. $\mathcal{T}$, i.e., the set of ground atoms γ such that $\mathcal{T} \cup \mathcal{A} \models \gamma$.

As usual in DLs, complex concept and role expressions are defined starting from atomic concepts and roles by applying suitable constructs. In this paper, we are interested in TBoxes expressed in *DL-Lite*$^{\mathcal{H}}_{horn}$ [7] (a.k.a. *DL-Lite*$_{R,\sqcap}$ [8]), a member of the extended *DL-Lite* family. The language for *DL-Lite*$^{\mathcal{H}}_{horn}$ concepts and roles is defined as follows:

$$R ::= P \mid P^- \qquad\qquad B ::= A \mid \exists R \mid \bot$$

where $A \in \Sigma_C$, $P \in \Sigma_R$, B and R are *basic concept* and *basic role*, respectively, P^- denotes the inverse of the atomic role P, $\exists R$ denotes the unqualified existential restriction over the basic role R, i.e., the set of individuals occurring as first argument of R, and $\bot$ denotes the empty concept.

A TBox $\mathcal{T}$ in *DL-Lite*$^{\mathcal{H}}_{horn}$ is a finite set of *concept inclusion assertions* of the form $B_1 \sqcap \ldots \sqcap B_n \sqsubseteq B$ and *role inclusion assertions* of the form $R_1 \sqsubseteq R_2$. Moreover, an ABox $\mathcal{A}$ is simply a finite set of ground atoms. In the following, given a TBox $\mathcal{T}$, an ABox $\mathcal{A}$ for $\mathcal{T}$ has the same signature as $\mathcal{T}$.

As for query answering, we focus on conjunctive queries (CQs). For the sake of presentation, we limit our technical treatment to Boolean CQs only, but our results can be extended to non-Boolean CQs in the standard way. A *Boolean CQ (BCQ)* q is an FO sentence of the form $\exists \vec{x}.\phi(\vec{x})$, where $\vec{x}$ are variables in $\Sigma_{\mathcal{V}}$, and $\phi(\vec{x})$ is a finite, non-empty conjunction of atoms of the form $\alpha(\vec{t})$, where $\alpha \in \Sigma_C \cup \Sigma_R$, and $\vec{t}$ is a tuple of terms, i.e., each component of $\vec{t}$ is either a constant in Σ_I or a variable in $\vec{x}$.

Our complexity results are for data complexity, i.e., are w.r.t. the size of the ABox only.

III. Framework

We now extend the CQE framework studied in [5]. We first recall that the policy considered in [5] accounts only for *denials*, i.e., axioms of the form $\forall \vec{x}.\phi(\vec{x}) \rightarrow \bot$, such that $\exists \vec{x}.\phi(\vec{x})$ is a BCQ. We enrich this policy language with (a particular form of) numerical restrictions axioms [7]. More formally, here *numerical restrictions* are axioms of the form:

$$A_1 \sqcap \cdots \sqcap A_k \sqcap (\geq n_1 R_1) \sqcap \cdots \sqcap (\geq n_h R_h) \sqsubseteq \bot \qquad (1)$$

where $k \geq 0$, $h \geq 0$, $k+h \geq 1$, each A_i is an atomic concept, and each $(\geq n_i R_i)$ denotes a *number restriction*, where R_i is basic role and n_i is a positive integer. We recall that each $(\geq n_i R_i)$ in (1) corresponds to the FO sentence

$$\exists x, y_1, \ldots, y_{n_i}.R_i(x, y_1) \wedge \ldots \wedge R_i(x, y_{n_i}) \wedge ineq(y_1, \ldots, y_{n_i}),$$

where either $R_i(x, y_j) = P_i(x, y_j)$ if $R_i = P_i$ or $R_i(x, y_j) = P_i(y_j, x)$ if $R_i = P^-$, for $1 \leq j \leq n_i$, and $ineq(y_1, \ldots, y_{n_i})$ is the conjunction of all inequalities $y_\ell \neq y_j$ such that $\ell, j \in \{1, \ldots, n_i\}$ and $\ell \neq j$. In more intuitive terms, $(\geq n_i R_i)$ denotes the set of objects that participate at least n_i times in the role R_i. Observe that $(\geq 1R)$ is equivalent to $\exists R$.

A policy $\mathcal{P}$ over a TBox $\mathcal{T}$ is a finite set of denials and numerical restrictions (i.e., axioms of the form of (1)), both specified over the signature of $\mathcal{T}$. An $\mathcal{L}$ *CQE specification* $\mathcal{E}$ is a pair $\langle \mathcal{T}, \mathcal{P} \rangle$, where $\mathcal{T}$ is a TBox expressed in the DL $\mathcal{L}$ and $\mathcal{P}$ is a policy over $\mathcal{T}$ such that $\mathcal{T} \cup \mathcal{P}$ is consistent. An ABox $\mathcal{A}$ for $\mathcal{E}$ is an ABox for $\mathcal{T}$ such that $\mathcal{T} \cup \mathcal{A}$ is consistent.

A GA (Ground Atom) *censor* [5], [6] for an $\mathcal{L}$ CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ is a function $\mathsf{cens}(\cdot)$ that, given an ABox $\mathcal{A}$ for $\mathcal{E}$, returns a set $\mathsf{cens}(\mathcal{A}) \subseteq \mathsf{cl}_{\mathcal{T}}(\mathcal{A})$ such that $\mathcal{T} \cup \mathcal{P} \cup \mathsf{cens}(\mathcal{A})$ is consistent.

A GA censor $\mathsf{cens}(\cdot)$ for $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ is said to be *optimal* if there is no other GA censor $\mathsf{cens}'(\cdot)$ for $\mathcal{E}$ such that (*i*) $\mathsf{cens}(\mathcal{A}) \subseteq \mathsf{cens}'(\mathcal{A})$ for each ABox $\mathcal{A}$ for $\mathcal{E}$; and (*ii*) $\mathsf{cens}(\mathcal{A}) \subset \mathsf{cens}'(\mathcal{A})$ for an ABox $\mathcal{A}$ for $\mathcal{E}$. We denote by $\mathsf{OptCens}_{\mathcal{E}}$ the set of all optimal GA censors for $\mathcal{E}$.

Example 2: Consider the CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$, where $\mathcal{P}$ contains the numerical restriction of Example 1, and $\mathcal{T} = \{\mathsf{minor} \sqsubseteq \mathsf{person}, \exists \mathsf{vaccinatedWith}^- \sqsubseteq \mathsf{vaccineLot}\}$, i.e., $\mathcal{T}$ says that minors are persons, and that an individual can be vaccinated only with vaccine lots. The function cens below is an optimal GA censor for $\mathcal{E}$:

> cens: given an ABox $\mathcal{A}$, $\mathsf{cens}(\mathcal{A})$ returns the set of ground atoms obtained by removing $\mathsf{minor}(o)$ from $\mathsf{cl}_{\mathcal{T}}(\mathcal{A})$, for each individual o such that, for some individuals $l1$ and $l2$, both $\mathsf{vaccinatedWith}(o, l1)$ and $\mathsf{vaccinatedWith}(o, l2)$ are in $\mathcal{A}$.

In the following, we focus on the IGA censor proposed in [5], [6], which is a particularly well-behaved type of GA censor allowing to soundly approximate the skeptical reasoning over all optimal GA censors. Notice that, by definition, the IGA censor is unique.

Definition 1: The *IGA censor* $\mathsf{cens}_{IGA}(\cdot)$ for a CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ is the function such that $\mathsf{cens}_{IGA}(\mathcal{A}) = \bigcap_{\mathsf{cens}(\cdot) \in \mathsf{OptCens}_{\mathcal{E}}} \mathsf{cens}(\mathcal{A})$, for each ABox $\mathcal{A}$ for $\mathcal{E}$.

Example 3: Consider the CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ of Example 2, and the following ABox for $\mathcal{E}$:

$\mathcal{A} = \{\ \mathsf{minor}(sam), \mathsf{vaccinatedWith}(sam, l21),$
$\mathsf{vaccinatedWith}(sam, l85), \mathsf{minor}(tom),$
$\mathsf{vaccinatedWith}(tom, l44)\}.$

We have that:

$\mathsf{cens}_{IGA}(\mathcal{A}) = \{\ \mathsf{person}(sam), \mathsf{person}(tom), \mathsf{minor}(tom),$
$\mathsf{vaccinatedWith}(tom, l44), \mathsf{vaccineLot}(l21),$
$\mathsf{vaccineLot}(l85), \mathsf{vaccineLot}(l44)\}.$

We conclude this section by defining the decision problem we are interested in, and which we study in the context of *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specifications in the next section.

Definition 2: Let $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ be an $\mathcal{L}$ CQE specifications, $\mathcal{A}$ be an ABox for $\mathcal{E}$, and q be a BCQ. *IGA-Cens-Ent*$(\mathcal{T}, \mathcal{P}, \mathcal{A}, q)$ is the problem of deciding whether $\mathcal{T} \cup \mathsf{cens}_{IGA}(\mathcal{A}) \models q$.

IV. Complexity results

In this section we study the data complexity of *IGA-Cens-Ent* for CQE specifications whose TBox is specified in *DL-Lite*$^{\mathcal{H}}_{horn}$. We first notice that simply combining a TBox in this language with a policy containing numerical restrictions leads to deal with ontologies where standard BCQ entailment (i.e., not under censors) does not enjoy the nice computational property of the logics of the *DL-Lite* family, i.e., this problem is not in AC^0 in data complexity [7], [8]. To regain membership in AC^0, *DL-Lite* dialects allowing for both role inclusions and number restrictions impose a syntactic condition that limits the interaction between these two constructs. To this aim, we here cast in our framework condition (A$_3$) adopted in [7]. Namely, we say that a set $\mathcal{S}$ of *DL-Lite*$^{\mathcal{H}}_{horn}$ TBox assertions, denials, and numerical restrictions is *safe* if for every number restriction $(\geq n_i R_i)$, with $n_i \geq 2$, occurring in an axiom of the form (1) in $\mathcal{S}$ we have that both R_i and R_i^- do not occur in the right-hand side of role inclusion assertions in $\mathcal{S}$. Then, we say that a *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ is *safe* if $\mathcal{T} \cup \mathcal{P}$ is safe.

In the following, we show that BCQ entailment under IGA censors for safe *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specifications is in AC^0 in data complexity. We achieve this result by showing that the above problem is *FO rewritable*, i.e., for every safe *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specification $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ and every BCQ q, one can effectively compute an FO query q_r, such that for every ABox $\mathcal{A}$ for $\mathcal{E}$, *IGA-Cens-Ent*$(\mathcal{T}, \mathcal{P}, \mathcal{A}, q)$ is true iff $\mathcal{A} \models q_r$. We call q_r the *IGA-perfect reformulation* of q with respect to $\mathcal{E}$.

To obtain the above result, we look for a correspondence between *IGA-Cens-Ent* and the analogous entailment problem in consistent query answering (CQA) over ontologies [9], a connection that we have already investigated in [4], [5]. In particular, for the less expressive CQE framework of [5], we have shown that BCQ entailment under IGA censors can be reduced to BCQ entailment in CQA under the so-called IAR semantics. This is an interesting result since the latter problem is FO rewritable. Here, we adopt the same approach, but considering more expressive ontology and policy languages.

We proceed as follows: (i) we first recall the IAR semantics in CQA; (ii) we show that, when the TBox is a safe set of *DL-Lite*$^{\mathcal{H}}_{horn}$ assertions, denials, and numerical restrictions, BCQ entailment under IAR semantics is FO rewritable (notice that this is a novel result that is valuable per se in the context of CQA); (iii) we finally extend the above rewritability result to *IGA-Cens-Ent* in our framework.

Let us start with the IAR-semantics. Formally, given an ontology $\mathcal{O} = \mathcal{T} \cup \mathcal{A}$, an ABox repair (*A*-repair) of $\mathcal{O}$ is an inclusion-maximal subset $\mathcal{A}_r$ of $\mathcal{A}$ such that the ontology $\mathcal{T} \cup \mathcal{A}_r$ is consistent. Then, the *IAR*-repair of $\mathcal{O}$ is defined as the intersection of all A-repairs of $\mathcal{O}$. Let q be a BCQ, *IAR-Ent*$(\mathcal{T}, \mathcal{A}, q)$ is the problem of verifying whether $\mathcal{T} \cup \mathcal{A}_{iar} \models q$, where $\mathcal{A}_{iar}$ is the *IAR*-repair of $\mathcal{O}$. FO rewritability of BCQ entailment under the IAR-semantics for a DL $\mathcal{L}$ is defined as usual: we say that the above problem is FO rewritable if for every TBox in $\mathcal{L}$ and every BCQ q, one can effectively compute a first-order query q_r, such that for every ABox $\mathcal{A}$, *IAR-Ent*$(\mathcal{T}, \mathcal{A}, q)$ is true if and only if $\mathcal{A} \models q_r$. We call q_r the *IAR-perfect reformulation* of q with respect to $\mathcal{T}$.

We now deal with point (ii) above. To this aim, we need a preliminary definition.

Definition 3: Given an ontology $\mathcal{O} = \mathcal{T} \cup \mathcal{A}$, a *Minimal Inconsistent Set* in $\mathcal{O}$ is a set *MIS* $\subseteq \mathcal{A}$, such that (a) *MIS* is inconsistent with $\mathcal{T}$; (b) *MIS* is minimal, i.e., *MIS* $\setminus \{\alpha\}$ is consistent with $\mathcal{T}$, for every $\alpha \in$ *MIS*.

From the definition of IAR-repair it immediately follows that the *IAR*-repair of $\mathcal{O}$ can be obtained by removing from $\mathcal{A}$ all the ground atoms participating in at least a minimal inconsistent set in $\mathcal{O}$.

We now prove an important property that is needed to show the first-order rewritability of IAR-entailment.

Lemma 1: Let $\mathcal{T}$ be a TBox constituted by a safe set of *DL-Lite*$^{\mathcal{H}}_{horn}$ assertions, denials, and numerical restrictions. For every ABox $\mathcal{A}$ for $\mathcal{T}$, the maximal size of a minimal inconsistent set of $\mathcal{T} \cup \mathcal{A}$ is independent of the size of $\mathcal{A}$.

Proof. [sketch] Let N and M be the number of atomic concepts and atomic roles in $\mathcal{T}$, respectively, let $\hat{k}$ the maximal size of a denial in $\mathcal{T}$, i.e., the maximal number of atoms in the CQ in the left-hand side of a denial, and let $\hat{h}$ be the maximal h in axioms of the form (1) in $\mathcal{T}$. It can be shown that the maximal size of a non-redundant denial[1] that can be inferred by $\mathcal{T}$ is $\hat{k}(N+2M)$ (since every atom can be at most rewritten into a conjunction of atoms corresponding to all basic concepts constructible on the signature of $\mathcal{T}$). Then, the maximal size of a minimal inconsistent set in $\mathcal{T} \cup \mathcal{A}$ violating a denial is $\hat{k}(N+2M)$, which is independent from the size of the ABox.

As for numerical restrictions, the maximal size of a non-redundant numerical restriction that can be inferred by $\mathcal{T}$ is $N+2M+\hat{h}$. Indeed, one such axiom ρ can conjoin at most N atomic concepts, M number restriction of the form $(\geq 1P)$, and M number restriction of the form $(\geq 1P^-)$, where P is an atomic role. It remains to prove that ρ cannot conjoin more than $\hat{h}$ number restrictions of the form $(\geq n_i R_i)$, with $n_i \geq 2$, but this follows easily from the safeness condition imposed on the TBox. Let now $\hat{n}$ be the maximal integer occurring in an axiom of the form (1). The maximal size of a minimal inconsistent set in $\mathcal{T} \cup \mathcal{A}$ violating a numerical restriction is bounded by $N + 2M + \hat{h}\hat{n}$. Indeed, to violate one such axiom $\hat{\rho}$ of maximal size, we need at most N ABox assertions to match the at most N atomic concepts occurring in $\hat{\rho}$, at most $2M$ ABox assertions to match the at most $2M$ number restrictions of the form $(\geq 1R)$ occurring in $\hat{\rho}$, and at most $\hat{n}$ ABox assertions to match each number restriction of the form $(\geq gR)$, with $g \leq \hat{n}$, occurring in $\hat{\rho}$ (which contains

[1] A non-redundant formula ρ is such that there is no other formula ρ' derived by $\mathcal{T}$ such that $\rho' \models \rho$.

$\hat{h}$ such restrictions). Again, $N + 2M + \hat{h}$ is independent from the size of the ABox. ∎

The next theorem concludes point (ii) of our investigation.

Theorem 1: BCQ entailment under the IAR-semantics for safe sets of *DL-Lite*$^{\mathcal{H}}_{horn}$ assertions, denials, and numerical restrictions is FO rewritable, and thus in AC^0 in data complexity.

Proof. [Sketch] To prove the thesis we can adapt the algorithm for BCQ entailment in *DL-Lite*$_{A,id,den}$ under the IAR-semantics, which has been shown to be first-order rewritable in [9]. Indeed, by Lemma 1 we have that the maximal size of a minimal inconsistent set in our setting is independent on the size of the ABox, which is a crucial property holding for *DL-Lite*$_{A,id,den}$ ontologies and exploited in [9]. We recall that the algorithm IAR-Rewriting given in [9] makes use of the procedures MinUnsatQuery and PerfectRef. The former computes a first-order query whose evaluation over the ABox identifies all minimal inconsistent sets of an ontology, whereas the latter is used to initially rewrite the input BCQ according to the positive inclusions in the TBox. To devise our query rewriting algorithm it is sufficient to extend the procedure MinUnsatQuery to manage the presence of numerical restrictions in the TBox. Furthermore, we need to adopt the version of PerfectRef proposed in [8] to deal with conjunctions of concepts in the left-hand side of positive inclusions. ∎

We now turn our attention to *IGA-Cens-Ent*. The following key result can be proved analogously to [5, Theorem 6].

Theorem 2: Let $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ be a safe *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specification, $\mathcal{A}$ be an ABox for $\mathcal{E}$, and q be a BCQ. *IGA-Cens-Ent*$(\mathcal{T}, \mathcal{P}, \mathcal{A}, q)$ is true iff *IAR-Ent*$(\mathcal{T} \cup \mathcal{P}, \mathsf{cl}_{\mathcal{T}}(\mathcal{A}), q)$ is true.

According to the above result, to solve *IGA-Cens-Ent* we first have to compute $\mathsf{cl}_{\mathcal{T}}(\mathcal{A})$ and then we can resort to a query rewriting technique to solve *IAR-Ent*. We can in fact avoid the computation of $\mathsf{cl}_{\mathcal{T}}(\mathcal{A})$ with an additional rewriting step. To this aim, we define below the function atomRewr, which extends to *DL-Lite*$^{\mathcal{H}}_{horn}$ the analogous function given in [5]. More precisely, given a *DL-Lite*$^{\mathcal{H}}_{horn}$ TBox and a BCQ q, $\mathsf{atomRewr}(q, \mathcal{T})$ substitutes each atom α of q with the formula $\phi(\alpha)$ defined as follows:

$$\phi(A(t)) \quad = \quad \bigvee_{\mathcal{T} \models \sqcap_{k=1}^{n} B_k \sqsubseteq A} \psi(t);$$

$$\phi(P(t_1, t_2)) \quad = \quad \bigvee_{\mathcal{T} \models S \sqsubseteq P} S(t_1, t_2) \quad \vee \quad \bigvee_{\mathcal{T} \models S^- \sqsubseteq P} S(t_2, t_1)$$

where A is an atomic concept, each B_k is a basic concept, P and S are atomic roles, t, t_1, t_2 are terms, i.e., each of them is either a variable or a constant, $\psi(t) = \bigwedge_{k=1}^{n} \lambda_k(t)$ and for $1 \leq k \leq n$, $\lambda_k(t)$ can assume one of the following forms:

- $\lambda_k(t) = A'(t)$, if $B_k = A'$ with A' an atomic concept,
- $\lambda_k(t) = \exists x.P'(t, x)$, if $B_k = \exists P'$ with P' an atomic role,
- $\lambda_k(t) = \exists x.P'(x, t)$, if $B_k = \exists P'^{-}$ with P' an atomic role.

It is easy to see that $\mathsf{atomRewr}(q, \mathcal{T})$ returns an FO query. The following lemma, whose proof can be immediately obtained from the definitions of $\mathsf{cl}_{\mathcal{T}}(\cdot)$ and $\mathsf{atomRewr}(\cdot, \cdot)$, states the property we are looking for.

Lemma 2: Let $\mathcal{T}$ be a *DL-Lite*$^{\mathcal{H}}_{horn}$ TBox, $\mathcal{A}$ be an ABox, and q be an FO sentence. Then $\mathsf{cl}_{\mathcal{T}}(\mathcal{A}) \models q$ iff $\mathcal{A} \models \mathsf{atomRewr}(q, \mathcal{T})$.

We are now able to establish FO rewritability of *IGA-Cens-Ent* in our setting.

Lemma 3: Let $\mathcal{E} = \langle \mathcal{T}, \mathcal{P} \rangle$ be a *DL-Lite*$^{\mathcal{H}}_{horn}$ safe CQE specification, q be a BCQ, and q_r be an FO sentence that is the IAR-perfect reformulation of q w.r.t. $\mathcal{T} \cup \mathcal{P}$. Then, the FO sentence $\mathsf{atomRewr}(q_r, \mathcal{T})$ is the IGA-perfect reformulation of q w.r.t. $\mathcal{E}$.

Proof. [sketch] From the definition of IAR-perfect reformulation, we have that, for every ABox $\mathcal{A}$ for $\mathcal{T}$, *IAR-Ent*$(\mathcal{T} \cup \mathcal{P}, \mathsf{cl}_{\mathcal{T}}(\mathcal{A}), q)$ is true iff $\mathsf{cl}_{\mathcal{T}}(\mathcal{A}) \models q_r$. By Lemma 2, $\mathsf{cl}_{\mathcal{T}}(\mathcal{A}) \models q_r$ iff $\mathcal{A} \models \mathsf{atomRewr}(r_r, \mathcal{T})$. By Theorem 2, we then have that *IAR-Ent*$(\mathcal{T} \cup \mathcal{P}, \mathsf{cl}_{\mathcal{T}}(\mathcal{A}), q)$ iff *IGA-Cens-Ent*$(\mathcal{T}, \mathcal{P}, \mathsf{cl}_{\mathcal{T}}(\mathcal{A}), q)$. ∎

Below we exhibit the main result of this section, which is a consequence of Theorem 1 and Lemma 3.

Theorem 3: BCQ entailment under IGA censors for safe *DL-Lite*$^{\mathcal{H}}_{horn}$ CQE specifications is FO rewritable, and thus in AC^0 in data complexity.

V. Conclusions

In this paper we focused on policy axioms containing unqualified number restrictions of the form $(\geq nR)$. The next step is to consider their qualified version, i.e., restrictions of the kind $(\geq nR.C)$. Of course, number restrictions of the form $(\leq nR)$ or $(\leq nR.C)$ are also of interest. This latter extension requires some major development, since standard inference with this kind of atoms in policy axioms would infer positive knowledge when coupled with the TBox, which is something that is not considered in the current version of our framework. We finally remark that we are currently working to implement our approach, extending the development presented in [6].

References

[1] P. A. Bonatti and L. Sauro, "A confidentiality model for ontologies," in *Proc. of ISWC*, ser. LNCS, vol. 8218, 2013, pp. 17–32.

[2] B. Cuenca Grau, E. Kharlamov, E. V. Kostylev, and D. Zheleznyakov, "Controlled query evaluation over OWL 2 RL ontologies," in *Proc. of ISWC*, ser. LNCS, vol. 8218, 2013, pp. 49–65.

[3] ——, "Controlled query evaluation for datalog and OWL 2 profile ontologies," in *Proc. of IJCAI*, 2015, pp. 2883–2889.

[4] D. Lembo, R. Rosati, and D. F. Savo, "Revisiting controlled query evaluation in description logics," in *Proc. of IJCAI*, 2019, pp. 1786–1792.

[5] G. Cima, D. Lembo, R. Rosati, and D. F. Savo, "Controlled query evaluation in description logics through instance indistinguishability," in *Proc. of IJCAI*, 2020, pp. 1791–1797.

[6] G. Cima, D. Lembo, L. Marconi, R. Rosati, and D. F. Savo, "Controlled query evaluation in Ontology-Based Data Access," in *Proc. of ISWC*, ser. LNCS, vol. 12506, 2020, pp. 128–146.

[7] A. Artale, D. Calvanese, R. Kontchakov, and M. Zakharyaschev, "The *DL-Lite* family and relations," *JAIR*, vol. 36, pp. 1–69, 2009.

[8] D. Calvanese, G. De Giacomo, D. Lembo, M. Lenzerini, and R. Rosati, "Data complexity of query answering in description logics," *AIJ*, vol. 195, pp. 335–360, 2013.

[9] D. Lembo, M. Lenzerini, R. Rosati, M. Ruzzi, and D. F. Savo, "Inconsistency-tolerant query answering in ontology-based data access," *J. of Web Semantics*, vol. 33, pp. 3–29, 2015.