A. Formica

SATISFIABILITY OF OBJECT-ORIENTED DATABASE CONSTRAINTS WITH SET AND BAG ATTRIBUTES

R. 549  Maggio 2001

Anna Formica  –  Istituto di Analisi dei Sistemi ed Informatica "Antonio Ruberti" del CNR, Viale Manzoni 30 - 00185 Roma, Italy. Email : anna.formica@iasi.cnr.it


ISSN: 1128–3378
Abstract

The definition of methodologies for checking database constraint satisfiability, i.e., the absence of contradictions independently of any database state, is a fundamental and critical problem that has been marginally addressed in the literature. In this paper, a sound and complete algorithm is proposed for checking the satisfiability of a specific class of database integrity constraints in a simplified Object-Oriented model. Such a class includes cardinality constraints, set and bag attributes, and explicit integrity constraints involving comparison operators. The algorithm, conceived to support database schema design, allows the designer to distinguish among five different kinds of contradictions, each identified by an ad-hoc procedure.

Keywords: Object-Oriented databases, types, constraint satisfiability, typed properties, set attributes, bag attributes, cardinality constraints.
1. INTRODUCTION

With the advent of data models more expressive than the relational one, the existence of facilities to handle semantic integrity constraints is an essential premise to manage semantically rich data. In particular, the definition of methodologies for checking database constraint satisfiability, i.e., the absence of contradictions independently of any database state [20], becomes a fundamental problem, and the need for automatic tools supporting schema design becomes mandatory. This paper focuses on the satisfiability of a specific class of integrity constraints in a simplified Object-Oriented database (OODB) [2] model. Even if we concentrate on the static component of the Object-Oriented model, neglecting the behavioural part, the verification of the satisfiability of integrity constraints is a difficult activity that has been marginally addressed in the literature [24]. In particular, the class of integrity constraints addressed in this paper includes cardinality constraints, and explicit integrity constraints involving comparison operators, referred to as $\theta$-constraints. Particular emphasis is given to the presence of set and bag attributes, i.e., multivalued attributes that allow an object to be associated with a set or a bag of values, respectively. In the data model, recursive properties are also allowed and, furthermore, attributes can be typed with enumerated sets of values and intervals (value_set types). In this work, we will see how the coexistence of set attributes, bag attributes, value_set types, cardinality constraints, and $\theta$-constraints impacts on schema satisfiability. The need for bags has been recognized not only in the database area, such as, for instance, in [21] (since they allow aggregate functions to be expressed in a natural way), but also in different fields, such as, for instance, in the Object-Oriented Analysis & Design area, where the Object Constraint Language (OCL) has been proposed as a standard for constraint specification [28].

The data model adopted in this paper is $TQL^\ast$, a fragment of the language $TQL^{++}$ [19], [26] for conceptual modeling of OODB applications. The contribution of this work consists in the definition of a sound and complete algorithm that allows the satisfiability of $TQL^\ast$ schemas to be checked in polynomial time. The algorithm also allows the designer to distinguish among five different kinds of contradictions, each identified by an ad-hoc procedure. Furthermore, one more contribution of this paper concerns the definition of the formal semantics of bag attributes according to Description Logics [10].

The paper is organized as follows. In Section 2, the data model is formally introduced, and the formal semantics of the $TQL^\ast$ specification language is presented. In Section 3, five procedures are defined on which the satisfiability algorithm mentioned above is based. Successively, the algorithm is introduced, followed by the related soundness and completeness proof. In Section 4, the conclusion and future work are briefly discussed. Below the related work is given.

1.1. Related work

Implication constraints and referential constraints are commonly used to specify semantic integrity constraints in database and knowledge base systems. The former generalize functional dependencies, whereas the latter are inclusion dependencies. Since the implication problem for functional and inclusion dependencies is, in general, undecidable [12], in the literature the analysis focused on the identification of specific classes of integrity constraints that allow the implication problem to be decidable. For instance, in [29] the problem of reasoning with implication constraints and acyclic referential constraints has been addressed. In particular, the decidability of the IRC (Implication and Referential Constraints) refuting problem has been
proved, and a novel characterization for it has been given. In [16], a decidable, sound, and complete method for checking finite satisfiability of a restricted form of cyclic referential constraints for Object-Oriented databases has been proposed. In [24], the satisfiability problem has been investigated in the context of the Entity Relationship model, for a specific class of integrity constraints, namely the cardinality ratio constraints, used to express functional and numerical dependencies. In [9], a technique has been presented for checking the satisfiability of class definitions in an extended Object-Oriented data model, where it is possible to specify ISA relationships, disjointness constraints, inverse attributes (properties), and cardinality constraints. In [4], the satisfiability of Object-Oriented database schemas enriched with integrity constraints has been addressed. In particular, two alternative formalisms have been presented: one including path relations (that are more general than $\theta$-constraints), but disallowing recursive schemas, the other one with the capability of expressing recursive schemas, but disallowing path relations. The implication problem has been investigated in the context of semistructured data and XML, for instance, in [8] and [15]. In [8], path constraints have been investigated, that are a generalization of the explicit integrity constraints addressed in this paper. In particular, the implication and finite implication problems for path constraints have been analyzed in the context of two Object-Oriented models, namely $\mathcal{M}^+$, essentially containing record types and set types, and $\mathcal{M}$, a restriction of the former that does not allow sets. Both problems are decidable in $\mathcal{M}$, whereas are undecidable in $\mathcal{M}^+$. In [15], the implication problem has been addressed for two subclasses of functional and inclusion dependencies, keys and foreign keys respectively, extensively analyzed in relational databases. In particular, in the mentioned paper, four classes of constraints including keys and foreign keys for XML have been studied, and the implication problem for each of them has been analyzed. However, it is important to notice that the assumptions made in that paper for XML data model are quite different from those generally addressed in the Object-Oriented database setting (e.g., at an extensional level, finite trees vs cyclic graphs).

With respect to all the aforementioned papers, this work addresses the satisfiability of a specific class of Object-Oriented integrity constraints, including recursive types, bags, sets, cardinality constraints, and a restricted form of path constraints. Due to the different data model assumptions or modeling constructs addressed, none of the above mentioned papers contains the class of constraints investigated in this work.

It is worth recalling that, in the context of deductive databases, constraint satisfiability checking has been widely investigated by relying on theorem prover techniques. For instance in [7] a schema is a set of First Order Logic formulas, and schema satisfiability checking is performed by using the theorem prover Satchmo, successively refined in Sic [6]. However, in general, checking the satisfiability of schemas containing set attributes and cardinality constraints is one of the 75 problems that have been recognized difficult to be processed by theorem provers (but suitable to test their efficiency) [27].

Furthermore, in [5] and [13], path equation constraints on complex objects have been addressed, that can be compared with the equality constraints defined in this paper. In particular, such constraints have been analyzed in combination with functional dependencies, without addressing the satisfiability of constraints involving sets, bags, cardinality constraints and comparison operators.

Finally, regarding the bag constructor, in the literature we find some results concerning, for instance, the extension of the usual set operations to bags (see for instance [1]), algebraic query optimizations for data models supporting bags (as for instance [14]), or the expressive power of algebras for manipulating bags (see for instance [22]). However, again, these proposals do not
address constraint satisfiability checking in the presence of set and bag attributes.

2. FORMAL BASIS

The data model on which this work is based is $TQL^*$, that is a derivation of the language $TQL^{++}$ [19], [26] aimed at modeling the structural aspects and the integrity constraints of an OODB application. $TQL^*$ is a language compliant with ODMG [11], a standard for OODBs that is gaining a wide consensus within the database community.

2.1. $TQL^*$ Syntax

In $TQL^*$, a schema is a set of types. A type contains the description of the structure of the objects that will populate the related class (i.e., the set of all the type instances), together with the integrity constraints that these objects have to satisfy. The formal syntax of $TQL^*$ is presented in Definition 2.1: non-terminal symbols are enclosed between angular parenthesis, terminal symbols are in bold, whereas the remainder symbols represent user-defined strings (the underscore character stands for iteration).

**Definition 2.1.** [Syntax of $TQL^*$]

\[
\text{\langle type \rangle ::= t \text{_term} \preceq \langle tuple \rangle} \\
\text{\langle tuple \rangle ::= [(\text{tp}_1), \ldots, (\text{tp}_m)]} \\
\text{\langle tp \rangle ::= p \text{_term} : \{(\text{a}_\text{type})\}_{m,M}} \\
\text{\langle body \rangle ::= \langle \text{a}_\text{type} \rangle} \\
\text{\langle \text{a}_\text{type} \rangle ::= \text{integer} | \text{real} | \text{boolean} | \text{string} | \text{value_set}} \\
\text{\langle c\text{_expr} \rangle ::= \text{label} : \text{this}.(\text{path})\{(\theta)\}C} \\
\text{\langle \text{path} \rangle ::= \text{p\_term}_1 \ldots \text{p\_term}_h \preceq \text{p\_term}_1 \ldots \text{p\_term}_{h-1} \ldots \text{p\_term}_h} \\
\text{\langle \theta \rangle ::= \leq | < | > | \geq | = | \neq}
\]

**Example 2.1.** The following types form a schema:

- $\text{person} \preceq [\text{name} : \text{string}, \text{age} : \text{integer}]$
- $\text{ic}_1 : \text{this} \text{.age} \leq 150$
- $\text{student} \preceq [\text{teacher} : \{\text{person}\}+,\text{friend} : \{\text{student}\},\text{exam\_mark}^* : \{\text{integer}\}_{0,40},\text{topic} : \{\text{comp\_sc, engin, math}\}]$
- $\text{ic}_2 : \text{this} \text{.exam\_mark}^* \geq 18$

A type has a label ($t\text{_term}$) and a tuple, that is a set of typed properties ($tp$). A property is identified by a label ($p\text{_term}$), and can be typed by using: (i) atomic types ($a\text{_type}$), e.g., integer or string (for instance, in the example, $\text{person.age}$) or value_set types, that are specified between ordinary parenthesis by the interval extremes, or by enumeration, as for instance $\text{student.topic}$; (ii) $t\text{_terms}$ (as, in the example, $\text{student.teacher}$), establishing an explicit link (or association) between two types. In a tuple, multiple occurrences of the same property label are not allowed.
Properties may be either attributes or relationships, according to ODMG. The former are typed according to the case (i) above, while the latter according to the case (ii). Relationships can form cycles, hence resulting in recursive types (for instance, in the example, student is a self recursive type). Properties are multivalued, that is, it is possible to specify that an object, instance of a type, can take more than one value in correspondence to a given property. Multivalued properties are specified by using curly braces (see, for instance, friend in the type student). In particular, multivalued relationships are set relationships, i.e., an object can be associated with a set of objects, whereas multivalued attributes may be set or bag attributes, i.e., it is possible to associate an object with a set or a bag of values, respectively. Notationally, bag attributes differ from set attributes since they are followed by the superscript symbol *. For instance, in the Example 2.1, exam mark* is a bag attribute, whereas friend is a set relationship, both of the student type.

As already mentioned, a property can be typed by using enumeration or an interval specification (in the case of ordered domains). In both these cases, the values that the objects can take are only the ones specified in the enumerated set or belonging to the interval, respectively.

In TQL*, it is possible to express constraints on the minimum and maximum cardinality of the sets or bags of objects associated through multivalued properties. In the case of minimum cardinality equal to 0, the property is also referred to as a null property. In the previous example, exam mark* is a null property, and a student instance may have from 0 to 40 values (possibly with duplicates) associated with it, through this attribute. In TQL*, the absence of curly braces is a short form to denote singlevalued properties (as, for instance, person.name), curly braces that are not followed by cardinality constraints stand for any cardinality (as, for instance, student.friend), whereas curly braces followed by the + symbol stand for minimum cardinality 1 (as, for instance, student.teacher).

TQL* explicit integrity constraints are \( \theta \)-constraints \( (c_{expr}) \), where \( \theta \) stands for a comparison operator, such as \( "=" \), \( "\geq" \), \( "\gt" \). A \( \theta \)-constraint has label identifying the constraint, a left hand side specified by the keyword this followed by a path, and a right hand side represented by a constant, say \( C \), that can be an integer, a real, a string, or a boolean constant. The keyword this refers to a single object of the class of the type the integrity constraint is associated with. A path is a sequence of \( p\text{-terms} \), expressed according to the dot-notation formalism, that allows navigation through types. In a path, the same property label may occur more than once. \( \theta \)-constraints are specified in the schema, being an integral part of types. For example, in the Example 2.1, the explicit integrity constraint \( ic_{2} \) states that the examination marks of a student must be all greater than 18.

In order to present the notion of a schema, the \( T \) function is introduced below. Such a function is defined on a \( t\text{-term} \) followed by a path, and returns the type of the first property of the path (as defined in the tuple associated with the \( t\text{-term} \)), followed by the remainder sequence of properties of that path.

**Definition 2.2. [The \( T \) function]** Given a schema \( \Sigma \), the \( T \) function is defined on a \( t\text{-term} \), say \( \tau \), followed by a sequence of \( n \ (\geq 1) \) \( p\text{-terms} \) of \( \Sigma \), as follows:

- \( T(\tau.p_{1}, \ldots.p_{n}) = \sigma.p_{2}. \ldots.p_{n} \)
  if \( \tau = [\ldots.p_{1} : \{\sigma\}_{m,M}, \ldots] \)

- \( T(\tau.p_{1}, \ldots.p_{n}) \) is undefined otherwise.

For \( h = 1 \ldots n \), \( T^{h} \) is the composition of \( T \) \( h \) times, i.e.:

\[ T^{h}(\tau.p_{1}, \ldots.p_{n}) = \]
\[ T(\ldots(T(\tau.p_1 \ldots p_n))\ldots) \]

and \( T^0(\tau.p_1 \ldots p_n) = \tau.p_1 \ldots p_n \) (the identity function).

For instance, in Example 2.1:

\[ T(\text{student.friend.exam.mark}^*) = \text{student.exam.mark}^* \]

and:

\[ T^2(\text{student.friend.exam.mark}^*) = \text{integer} \]

whereas:

\[ T(\text{student.child}) \]

is undefined.

**Definition 2.3. [Non-null integrity constraint]** Consider a type \( \tau \) and an integrity constraint:

\[ \text{ic: this.p}_1 \ldots p_n \theta C \]

associated with \( \tau \). Then \( \text{ic} \) is non-null if each \( p_i, i = 1 \ldots n \), is not a null property, i.e., the minimum cardinality associated with the \( p_i \) property in the traversed type is strictly greater than zero.

The formal definition of a \( TQL^* \) schema follows.

**Definition 2.4. [TQL* schema]** A finite set of types is a \( TQL^* \) schema (schema, for short) if:

- every type and integrity constraint label is uniquely defined (i.e., the same label is not associated with more than one definition);
- there are no dangling type labels (i.e., every \( t \)-term declared in the schema is defined);
- for each type \( \tau \) and each associated integrity constraint, say \( \text{ic: this.p}_1 \ldots p_n \theta C \), \( T^h(\tau.p_1 \ldots p_n) \) are defined, for \( h = 1 \ldots n \).

The first two requirements, in the above definition, are obvious: to prevent ambiguity, types and integrity constraints must have unique definitions, and every type label appearing in the schema must be defined. The last point requires that, for each integrity constraint, paths must be defined according to the tuples defined in the schema (i.e., each property of a path must be present in the tuple of the “traversed” type).

Notice that in a schema, besides the above requirements, the integrity constraints are supposed to be correctly typed, e.g., in Example 2.1, the integrity constraint:

\[ \text{ic2: this.friend} > 27 \]

associated with \( \text{student} \) would be rejected at a pre-processing stage, by using a type-checker. Therefore, we suppose that, for each \( \theta \)-constraint, the constant \( C \) is compatible with the type associated with the last property of the path, in the related type definition. Notice that in this paper inheritance hierarchies (extensively investigated by the author, for instance, in [3], [17], [18]) are not addressed.

**2.2. Semantics of \( TQL^* \)**

The formal semantics of a \( TQL^* \) schema is given according to the formal semantics of Description Logics, as defined in [10]. In particular, in this paper the notion of interpretation has been extended in order to deal with bag attributes.
Given a TQL* schema $\Sigma$, let $S$ be the set of $t$-terms, atomic types, and value set types of $\Sigma$ (that correspond to the atomic concepts in [10]). Furthermore, let $P$ and $P^*$ be a partition of the set of properties, say $Q$, of $\Sigma$, i.e., $P \cap P^* = \emptyset$ and $P \cup P^* = Q$. In particular, $P$ contains all the set properties ($p$-terms) of $\Sigma$ (corresponding to the atomic roles in [10]), whereas $P^*$ contains all the bag attributes ($p$-terms*) of $\Sigma$.

An interpretation $I^* = (\Delta^{\sigma^*}, \mathcal{I})$ over $\Sigma$ consists of a non-empty finite set $\Delta^{\sigma^*}$, that is the domain of $I^*$, and a function $\mathcal{I}$, that is the interpretation function of $I^*$, that maps:

- every type $\tau \in S$ to an element $(\tau)^{\mathcal{I}^*}$ of the powerset $\mathcal{P}(\sigma^*)$ (i.e., $(\tau)^{\mathcal{I}^*}$ is the set of instances of $\tau$);
- every $p$-term $\in P$ to an element $(p$-term$)^{\mathcal{I}^*}$ of the powerset $\mathcal{P}(\Delta^{\sigma^*} \times \Delta^{\sigma^*})$;
- every $p$-term* $\in P^*$ to an element ($p$-term$^*$) of the powerset $\mathcal{P}(\Delta^{\sigma^*} \times \Delta^{\sigma^*})$.

Then, a type:

$$\tau \subseteq \text{tuple, c_expr}_1, ..., c_expr_n$$

is an inclusion assertion as defined in [10] (i.e., it specifies only necessary conditions for an object to be an instance of the type $\tau$), for which the interpretation function is defined as follows ($\#S$ denotes the cardinality of the set $S$):

1. $(\text{tuple, c_expr}_1, ..., c_expr_n)^{\mathcal{I}^*} = (\text{tuple})^{\mathcal{I}^*} \cap (\cap_i (c_expr_i)^{\mathcal{I}^*})$

2. $(\text{tuple})^{\mathcal{I}^*} = \bigcap_j ([p_j; \{\text{type}_j\}_{m_j,M_j}])^{\mathcal{I}^*}$
   where $p_j$ can be either a set or a bag property, and $\text{type}_j$ an atomic type or a $t$-term according to the syntax;

3. $([p; \{\text{type}\}_{m,M}])^{\mathcal{I}^*} = \{ x \in \Delta^{\sigma^*} | m \leq \# \{ y : (x,y) \in (p)^{\mathcal{I}^*}, \ y \in (\text{type})^{\mathcal{I}^*} \} \leq M \}$
   where $p$ and $\text{type}$ are defined similarly to $p_j$ and $\text{type}_j$ above, respectively;

4. $(c_expr)^{\mathcal{I}^*} =$
   - $(\text{label: this.path } \theta C)^{\mathcal{I}^*} = (\text{label: this.p}_1\text{.p}_2\ldots\text{.p}_h \theta C)^{\mathcal{I}^*} =$
     $\{ x \in \Delta^{\sigma^*} | \forall y_1, ..., y_h : (x,y_1) \in (p_1)^{\mathcal{I}^*},$ $ (y_1,y_2) \in (p_2)^{\mathcal{I}^*} \ldots$ $ (y_{h-1},y_h) \in (p_h)^{\mathcal{I}^*} \Rightarrow y_h \theta C \}$
   where $p_i, i = 1 \ldots h-1$, are set properties, $p_h$ can be either a set or a bag attribute, and $\theta$ is one of the comparison operators $\geq, >, =, \neq$, etc..

A model of $\Sigma$ is an interpretation $I^* = (\Delta^{\sigma^*}, \mathcal{I})$ that satisfies all the inclusion assertions in $\Sigma$, i.e.:

- $(\tau)^{\mathcal{I}^*} \subseteq (\text{tuple, c_expr}_1, ..., c_expr_n)^{\mathcal{I}^*}$.

A type $\tau \in S$ is satisfiable in the schema $\Sigma$ if the schema admits a model for which $(\tau)^{\mathcal{I}^*} \neq \emptyset$.

\[1\]Therefore set attributes and bag attributes having the same name, as for instance phone and phone*, will be considered different properties.
Finally, the schema $\Sigma$ is *satisfiable* if it admits a model for which each type is satisfiable in $\Sigma$.

**Example 2.2.** Consider the following schema:

university $\leq$ [name : string, 
teacher : {graduate}+], 
ic : this.teacher.exam_mark $\geq$ 27
graduate $\leq$ [name : string, 
exam_mark : $\{(18..30)\}_{10,40}$, 
topic : string]

In this schema, exam_mark is a set attribute. In particular, for a graduate at least 10 examination marks are required and, in the case of graduates that are teachers of a university, they must be greater than 27, according to the explicit integrity constraint ic (but not exceeding 30, as specified by the value_set type of exam_mark). Since exam_mark is a set attribute, it is not possible to instantiate any graduate object that is a teacher of a university, since it is not possible to define any set of cardinality at least 10 with a set of 4 elements. Therefore this schema is unsatisfiable. Notice that the graduate type is satisfiable since the cardinality of the value_set type is compliant with the minimum cardinality required. Of course, if the set attribute exam_mark is replaced with the bag attribute exam_mark*, the schema becomes satisfiable.

In the rest of the paper, an algorithm for checking the satisfiability of a $TQL^*$ schema is introduced.

### 3. SCHEMA SATISFIABILITY CHECKING

In this section the notion of a range of an integrity constraint is first introduced. Successively, five procedures are presented, on which the algorithm for checking the satisfiability of a $TQL^*$ schema is based. Regarding the notation, in the following, given a schema $\Sigma$ and a t-term $\tau$ of $\Sigma$, $I(\tau)$ indicates the set of $\theta$-constraints associated with the type $\tau$ in $\Sigma$. Furthermore, in the absence of specific assumptions, given any ic: this.p_1...p_n $C$, the attribute $p_n$ can be either a set or a bag attribute.

**Definition 3.1.** [The range $R$] Given a schema $\Sigma$, consider a t-term $\tau$ of $\Sigma$ such that $I(\tau)$ $\neq \emptyset$, and suppose that ic $\in I(\tau)$ where:
ic : this.path $\theta$ $C$

Then, the range of the integrity constraint ic, indicated as $R(ic)$, is defined as follows:

- if $C$ is an integer or a real constant, $R(ic)$ is a set of integers or reals respectively, defined by the intervals:
  \[ R(ic) = (-\infty, C) \] if $\theta$ is "$<";
  \[ R(ic) = (-\infty, C] \] if $\theta$ is "$\leq";
  \[ R(ic) = [C, C] \] if $\theta$ is "$=";
  ... (and so on in all the other cases)

  where square brackets and ordinary parenthesis denote closed and open intervals, respectively;

- if $C$ is a string or a boolean constant, there are two possible cases. If $\theta$ is "$=" $R(ic)$ is the singleton formed by the $C$ constant; otherwise, if $\theta$ is "$\neq$", $R(ic)$ is the complement of $C$
Procedure \textit{IntraTuple}(\tau): boolean

\textbf{input:} \tau \preceq [q_1 : \{\delta_1\}_{r_1}, R_1, \ldots, q_n : \{\delta_n\}_{r_n}, R_n];
\textbf{output:} true or false.

\textit{IntraTuple}(\tau) := true;
if for some set attribute \(q_j\) of \(\tau\), \(1 \leq j \leq n\),
\(\delta_j\) is \textit{value_set}_j, and \(\#\{\textit{value_set}_j\} < r_j\),
then \textit{IntraTuple}(\tau) := false.

Figure 1: The \textit{IntraTuple} procedure

in the set of all possible strings, or the singleton formed by the opposite boolean constant, respectively.

In Figure 6, the algorithm for schema satisfiability checking is presented. It is organized according to five procedures. The first one, called \textit{IntraTuple}, is shown in Figure 1 and concerns the compatibility between the cardinality of the \textit{value_set} type and the minimum of the associated cardinality constraints, in the case of set attributes. Given a \textit{t-term} \(\tau\), this procedure returns a boolean value, corresponding to the absence of \textit{IntraTuple} cardinality contradictions. For instance, in the following type:

\begin{verbatim}
graduate \preceq [name : string,
exem\_mark : \{(18..30)\}_{20,40}, topic : string]
\end{verbatim}

the set attribute \textit{exem\_mark} generates an \textit{IntraTuple} cardinality contradiction since it is not possible to define any set of cardinality (at least) 20 with a set of 13 elements.

Once the absence of \textit{IntraTuple} cardinality contradictions has been checked, the rationale on which the algorithm is based is the following. For each integrity constraint of the schema, the range is progressively refined by the \textit{IntraType}, \textit{InterType}, and \textit{ValueSet} procedures, each devoted to check the absence of specific kinds of contradictions. Finally, if the resulting range is non-empty, the \textit{CardCheck} procedure allows the designer to check if there are further incompatibilities due to the cardinality constraints. Such procedures are illustrated below, and an example for each kind of detected contradictions is shown.

The \textit{IntraType} procedure concerns the presence of contradicting integrity constraints within the same type. It takes a type and one integrity constraint as input, and returns the range of the integrity constraint, possibly refined. For instance, consider the types:

\begin{verbatim}
university \preceq [name : string,
teacher : \{graduate\}+],
\quad ic_1 : this.teacher.exam\_mark^* \geq 27,
\quad ic_2 : this.teacher.exam\_mark^* \leq 25
graduate \preceq [name : string,
exem\_mark^* : \{integer\}+, topic : string]
\end{verbatim}

Procedure \textbf{IntraType}($\tau, ic_i$): \textit{V}
\begin{itemize}
  \item \text{input}: $\tau$, $ic_i \in I(\tau)$, $ic_i$: this.$p_1$. ... $p_n \theta_i C_i$;
  \item \text{output}: an interval $V$.
\end{itemize}

$V := R(ic_i)$

for each non-null $ic_j \in I(\tau)$ s.t.:

$ic_j$: this.$p_1$. ... $p_n \theta_j C_j$

$V := V \cap R(ic_j)$. \\

\textbf{Figure 2}: The \textit{IntraType} procedure

(recall that the + symbol stands for minimum cardinality 1). In this case, the range of the constraint $ic_1$ (and similarly of $ic_2$) is refined with the empty set, since the ranges of $ic_1$ and $ic_2$ are disjoint. This is an example of an \textit{IntraType contradiction} detected by the procedure shown in Figure 2.

The \textit{InterType} procedure shown in Figure 3, as well as the other three remaining procedures, takes as input a type $\tau$, an integrity constraint $ic_i$ associated with $\tau$, and an interval, standing for the refined range of the constraint $ic_i$, at that stage. In this procedure such a range is further refined taking into account the other integrity constraints associated with the traversed types of the schema.

For instance, the following types:

\begin{verbatim}
university $\preceq$ [name : string,
   teacher : {graduate}+],
   ic1 : this.teacher.exam_mark* $\geq$ 27
graduate $\preceq$ [name : string,
   exam_mark* : {integer}+,topic : string],
   ic2 : this.exam_mark* $\leq$ 25
\end{verbatim}

contain an \textit{InterType contradiction} in correspondence to the integrity constraint $ic_1$, since the attribute \text{iexam mark}\* requires values greater than 27, within the type \textit{university}, and values lesser than 25 within the type \textit{graduate}.

The \textit{ValueSet} procedure, shown in Figure 4, regards the check between the range of the integrity constraint, as refined at that stage, and the \textit{value_set} type (if there are any) associated with the last property of the path, in the related type. Notice that the \textit{IntraType}, \textit{InterType}, and \textit{ValueSet} contradictions are independent of the presence of bag or set attributes. For instance, in the following schema:

\begin{verbatim}
university $\preceq$ [name : string,
   teacher : {graduate}+],
   ic : this.teacher.exam_mark* $\geq$ 27
graduate $\preceq$ [name : string,
   exam_mark* : {(18..26)}+,topic : string]
\end{verbatim}

\begin{verbatim}
university $\preceq$ [name : string,
   teacher : {graduate}+],
   ic1 : this.teacher.exa
Procedure **InterType**($\tau, ic_i, V$): $W$

**input**: $\tau$, $ic_i \in I(\tau)$, $ic_i$: $this.p_1 ... .p_n \theta_i C_i$, an interval $V$;

**output**: an interval $W$.

$W := V$;

for each non-null $ic_j$, $\sigma$, and $k$,

$1 \leq k \leq n - 1$, s.t.:

$ic_j$: $this.p_{k+1} ... .p_n \theta_j C_j$, $ic_j \in I(\sigma)$,

and $T^k(\tau.p_1 ... .p_n) = \sigma.p_{k+1} ... .p_n$,

$W := W \cap R(ic_j)$.

---

Figure 3: The **InterType** procedure

Procedure **ValueSet**($\tau, ic_i, W$): $U$

**input**: $\tau$, $ic_i \in I(\tau)$, $ic_i$: $this.p_1 ... .p_n \theta_i C_i$, an interval $W$;

**output**: an interval $U$.

$U := W$;

if $T^{n-1}(\tau.p_1 ... .p_n) = \delta.p_n$,

and $\delta \preceq [... , p_n : \{value_set.p_n\}_m,M,...]$,

then $U := U \cap \{value_set.p_n\}$.

---

Figure 4: The **ValueSet** procedure

we have a **ValueSet contradiction** since a university must have teachers of type graduate, with examination marks greater than 27 (according to the explicit integrity constraint), but lesser than 26 (as required for graduate).

Finally the last procedure, namely **CardCheck**, is shown in Figure 5 and concerns the verification about the compatibility between the cardinality of the range of the input integrity constraint, and the minimum cardinality constraint associated with the last property of the path, in the case it is a set attribute. This procedure returns a boolean value corresponding to the absence of an **InterType cardinality contradiction**. This is the case of the Example 2.2.

Regarding the complexity of the algorithm, consider a schema with $n$ types, each having at most $m$ properties and $r$ integrity constraints. Furthermore, suppose that for each integrity constraint the length (number of property occurrences) of the path is at most $s$. Then the satisfiability algorithm of Figure 6 has complexity $O(n(m + r^2s^2))$, taking into account that the cost for the comparison between paths is linear in the length of the paths.
Procedure **CardCheck**($\tau, ic_i, U$): boolean

**input:** $\tau$, $ic_i \in I(\tau)$, $ic_i$: this.$p_1 \ldots p_n \theta_i C_i$, an interval $U$;

**output:** true or false.

$CardCheck(\tau, ic_i, U) := true$

if $T^{n-1}(.p_1 \ldots .p_n) = \delta.p_n$,

$\delta \preceq [..., p_n : \{value\_set_{p_n}\}_{m,M}, ...]$,

$p_n$ is a set attribute, and $\#U < m$

then $CardCheck(\tau, ic_i, U) := false$.

---

**Figure 5:** The **CardCheck** procedure

---

Algorithm **Sat($\Sigma$)**: boolean

**input:** a schema $\Sigma$;

**output:** true or false.

$Sat(\Sigma) := false$;

if for some $\tau \in \Sigma$, $IntraTuple(\tau) = false$, then

print **‘IntraTuple cardinality contradiction’**,

exit;

else

for all $\tau \in \Sigma$

for all non-null $ic_i \in I(\tau)$

$IntraType(\tau, ic_i) = V$

if $V = \emptyset$, then print

**‘IntraType contradiction’**, exit;

$InterType(\tau, ic_i, V) = W$,

if $W = \emptyset$, then print

**‘InterType contradiction’**, exit;

$ValueSet(\tau, ic_i, W) = U$,

if $U = \emptyset$, then print

**‘ValueSet contradiction’**, exit;

if $CardCheck(\tau, ic_i, U) = false$, then print **‘InterType cardinality contradiction’**, exit;

$Sat(\Sigma) := true$, and print **‘$\Sigma$ is satisfiable’**.

---

**Figure 6:** The **Sat** algorithm for schema satisfiability checking
3.1. Soundness and completeness of the algorithm

In this section, the satisfiable TQL* schemas are characterized, that is, the soundness and the completeness of the algorithm shown in Figure 6 are given.

**Theorem 3.1. [Characterization of satisfiable schemas]** A TQL* schema $\Sigma$ is satisfiable if and only if $\text{Sat}(\Sigma) = \text{true}$.

**Proof.**

$\Rightarrow$ By contradiction. Suppose that $\text{Sat}(\Sigma) = \text{false}$. Then, in $\Sigma$ there exists at least one type $\tau$, such that one of the following conditions holds:

- $\text{IntraTuple}(\tau) = \text{false}$. Therefore, there exists at least one set attribute $p$ of $\tau$, $\tau \preceq [..., p : \{\text{value}_p\}, r, ...]$, such that $\#\{\text{value}_p\} < r$: contradiction;

- there exists at least one non-null $ic_i \in I(\tau)$ s.t.:
  - $\text{IntraType}(\tau, ic_i) = V = \emptyset$. Therefore, there exists at least one non-null $ic_j \in I(\tau)$ such that the refined range of $ic_j$ is empty: contradiction;
  - $\text{InterType}(\tau, ic_i, V) = W \neq \emptyset$ and $\text{InterType}(\tau, ic_i, V) = W = \emptyset$. Therefore, there exists at least one non-null $ic_j$, one type $\sigma$, $ic_j \in I(\sigma)$, and an integer $1 \leq k \leq n - 1$, such that the refined range of $ic_j$ is empty: contradiction;
  - $\text{InterType}(\tau, ic_i, V) = W \neq \emptyset$ and $\text{ValueSet}(\tau, ic_i, W) = U = \emptyset$. Therefore, the intersection between the refined range of $ic_i$ and the value_set type of the last property of the path of $ic_i$ is empty: contradiction;
  - $\text{ValueSet}(\tau, ic_i, W) = U \neq \emptyset$ and $\text{CardCheck}(\tau, ic_i, U) = \text{false}$. Therefore, the last property of the path of $ic_i$ is a set attribute whose associated minimum cardinality constraint, in the traversed type, is strictly greater than the cardinality of the refined range of $ic_i$: contradiction.

$\Leftarrow$ By construction. Let $S$ be the set of type labels ($t$_terms), atomic types ($a$_types), and value_set types of $\Sigma$. For each $t$_term $\tau \in S$, construct a labeled directed graph $G_\tau = (N_\tau,A_\tau)$ as follows. Let $x_0^\tau \in N_\tau$ be one node of the graph $G_\tau$, that is referred to as the representative element of $\tau$ instances. Furthermore:

- **tuple drawing**: for each set or bag property $p$ defining the tuple of $\tau$, where:
  $\tau \preceq [..., p : \{\eta\}, r, ...]$
  let $x_i^\tau \in N_\tau$, $i = 1...r$, be $r$ nodes of $G_\tau$, and $(x_0^\tau, x_i^\tau)_p \in A_\tau$, $i = 1...r$, be $r$ directed arcs of $G_\tau$, labeled with the property $p$, taking into account that different properties of $\tau$ require the introduction of disjoint sets of nodes. Therefore, if the type $\tau$ has $u$ properties, each associated with minimum cardinality $r_i$, $i = 1...u$, the number of nodes introduced so far is $1 + r_1 + r_2 + ... + r_u$.

- **path drawing**: for each non-null integrity constraint $ic \in I(\tau)$:
  $ic : \text{this}.p_1.p_2 ... .p_n \not\in C$
  where:
  $T(\tau.p_1.p_2 ... .p_n) = \eta.p_1...p_n$ and
  $\eta \preceq [..., p : \{\eta\}, s_1, s_1, ...]$}
  $T^2(\tau.p_1.p_2 ... .p_n) = \eta_1.p_2...p_n$ and
Suppose the graph $G_\tau = (N_\tau, A_\tau)$ has been constructed for any $t$-term $\tau \in S$. Then, for each $G_\tau$, consider all the paths starting from the representative element of $\tau$ instances $x_0^\tau$, i.e., each defined as:

$$\{\langle x_0^\tau, w_1^\delta, \ldots, w_k^\delta, \ldots, w_v^\delta \rangle_{v_1}, \langle w_1^\delta_1, w_2^\delta, \ldots, w_l^\delta_{l-1}, w_l^\delta \rangle_{v_1}\}$$

where, for $k = 1, \ldots, \delta_k \in S$ and $v_k$ are properties of $\Sigma$. Then, for each node $w_k^\delta$, $k = 1, \ldots, l$, where $\delta_k$ is a $t$-term (that can also coincide with $\tau$):

- **path sharing**: consider the graph $G_{\delta_k}$ and all the sets of paths starting from the representative element of $\delta_k$ instances, say $y_0^\delta$, labeled with the same sequences of properties, that is, suppose that $q = q_1, q_2, \ldots, q_m$ is one of these sequences, consider the set:

$$P_q = \{\ldots, \{\langle y_0^\delta, z_1^\eta, \ldots, z_1^\eta_q, \ldots, z_1^\eta \rangle_{q_{k+1}}, \ldots, \rangle_{q_m}\}, \ldots\}$$

and let $s_q$ be the cardinality of the set $P_q$. If there exists in $G_\tau$ a path starting from the node $w_k^\delta$, labeled with the sequence of properties $q_1, \ldots q_h$, $1 \leq h \leq m$, assume that $v_{k+1} = q_1$, $\ldots$, $v_{k+h} = q_h$, where $k + h < l$. Then, connect the graphs $G_\tau$ and $G_{\delta_k}$ by adding $s_q$ arcs labeled with $q_{k+1}$, in such a way that the paths of $G_{\delta_k}$ labeled with the sequences $q_{k+2}, \ldots, q_m$ can be shared also by $G_\tau$. That is, from the node $x_0^\tau$ of $G_\tau$ the paths:

$$\{\langle u_0^\delta, w_1^\delta_1, \ldots, w_k^\delta_{k-1}, w_k^\delta \rangle_{v_k}, \langle w_k^\delta_{k+1} \rangle_{v_{k+1} = q_1}, \ldots, \langle w_{k+h-1}^\delta \rangle_{v_{k+h} = q_1}, \ldots, \langle w_{k+b-1}^\delta \rangle_{v_{k+b-1} = q_1}, \ldots, \langle z_{m-1}^\eta \rangle_{q_{m-1}}, \langle z_m^\eta \rangle_{q_m}\}$$

are defined, where $\langle w_{k+b-1}^\delta, z_{m}^\eta\rangle_{q_{m-1}}$ are $s_q$ newly defined arcs. Otherwise, in the case the node $w_k^\delta$ of $G_\tau$ has no outgoing arcs labeled with $q_1$, then $h = 0$, that is, the previous paths are replaced with the following:

$$\{\langle u_0^\delta, w_1^\delta_1, \ldots, w_k^\delta_{k-1}, w_k^\delta \rangle_{v_k}, \langle w_k^\delta, z_{1}^\eta \rangle_{q_1}, \ldots, \langle z_{m-1}^\eta \rangle_{q_{m-1}}, \langle z_m^\eta \rangle_{q_m}\}$$

where $\langle w_k^\delta, z_{1}^\eta \rangle_{q_1}$ are $s_q$ newly defined arcs.

Once the above steps have been performed for any $t$-term $\tau \in S$, let $G_\Sigma = (N_\Sigma, A_\Sigma)$ be the resulting (possibly non-connected) graph, and consider an interpretation $I^* = (\Delta^*, I^*)$ over $\Sigma$.
greater than 10.

for any \( \tau \in S \):
\[
(\tau)^{\Delta} = \{ y^k \in N_\Sigma \mid k \geq 0 \}
\]
and for any property \( p \) of the types of \( \Sigma \):
\[
(p)^{\Delta} = \{ (x^k_1, y^k_0) \mid (x^k_2, y^k_0)p \in A_\Sigma, \tau, \eta \in S, k, h \geq 0 \}
\]

From the hypothesis of the theorem, i.e., \( Sat(\Sigma) = true \), it is possible to instantiate all the variables, say \( y^gamma_j \), \( gamma \in S, j \geq 0 \), labeling the nodes of the graph \( G_\Sigma \) in such a way that \( y^gamma_j \) is an instance the type \( gamma \), i.e., the interpretation \( I^* = (\Delta^{\Sigma}, I^*) \) over \( \Sigma \) is also a model\(^3\) of \( \Sigma \).

4. CONCLUSION AND FUTURE WORK

In this paper a sound and complete algorithm for checking the satisfiability of a specific class of OODB integrity constraints has been proposed. The schema is specified by using TQL\(^*\), a fragment of the language TQL\(^++\) for conceptual modeling of OODB applications. As a future work, there are no obstacles in extending this result to more expressive OODB schemas including, for instance, inverse attributes, keys, inheritance, and explicit integrity constraints comparing paths. In particular, the satisfiability of TQL\(^*\) schemas enriched with integrity constraints comparing paths is an interesting topic to investigate, however requiring a deeper understanding of the underlying theory. For instance, the methodology defined in [16], mentioned in the Related Work, has been conceived as an ad-hoc methodology to deal with integrity constraints comparing paths that is not suited to deal also with the integrity constraints defined in this paper.

References


\(^4\)For instance, consider the types:

\[\begin{align*}
\text{person} & \leq \text{child} \{ \text{person} \}_{2,10}, \text{age} : \text{integer}, \\
\text{ic}_1 & : \text{this.child.age} < 10, \\
\text{course} & \leq \text{taken.by} \{ \text{person} \}_{1,30}, \\
\text{ic}_2 & : \text{this.taken.by.age} > 10
\end{align*}\]

the resulting model is defined by mapping types and properties of the schema as follows:

\[
\begin{align*}
(\text{person})^{I^*} & = \{ x^0_{\text{person}}, x^1_{\text{person}}, x^2_{\text{person}}, w^1_{\text{person}} \}, \\
(\text{course})^{I^*} & = \{ w^1_{\text{course}} \}, \\
(\text{child})^{I^*} & = \{ (x^0_{\text{person}}, x^1_{\text{person}}), (x^0_{\text{person}}, x^2_{\text{person}}), \\
& (x^1_{\text{person}}, x^0_{\text{person}}), (x^2_{\text{person}}, x^1_{\text{person}}), \\
& (w^0_{\text{person}}, x^0_{\text{person}}), (w^0_{\text{person}}, x^1_{\text{person}}), \\
& (w^1_{\text{person}}, x^0_{\text{person}}), (w^1_{\text{person}}, x^1_{\text{person}}) \}, \\
(\text{age})^{I^*} & = \{ (x^0_{\text{person}}, x^2_{\text{integer}}), (x^1_{\text{person}}, x^1_{\text{integer}}), \\
& (x^2_{\text{person}}, x^1_{\text{integer}}), (w^1_{\text{person}}, y^1_{\text{integer}}) \}, \\
(\text{taken.by})^{I^*} & = \{ (w^1_{\text{course}}, w^1_{\text{person}}) \},
\end{align*}
\]

where the instances \( x^0_{\text{person}}, x^1_{\text{person}}, \) and \( w^1_{\text{person}} \) share the objects associated with \( x^0_{\text{person}} \) (the representative element of \( \text{person} \) instances) as regards the property \( \text{child} \). Whereas, since the attribute \( \text{age} \) is constrained by \( \text{ic}_1 \) and \( \text{ic}_2 \), the further instances \( z^1_{\text{integer}} \) and \( y^1_{\text{integer}} \) have been introduced, the former lesser than 10, the latter greater than 10.


