Optimizing Database-Backed Applications with Query Synthesis

Alvin Cheung Armando Solar-Lezama Samuel Madden *

MIT CSAIL {akcheung, asolar, madden}@csail.mit.edu

Abstract

Object-relational mapping libraries are a popular way for applications to interact with databases because they provide transparent access to the database using the same language as the application. Unfortunately, using such frameworks often leads to poor performance, as modularity concerns encourage developers to implement relational operations in application code. Such application code does not take advantage of the optimized relational implementations that database systems provide, such as efficient implementations of joins or push down of selection predicates.

In this paper we present QBS, a system that automatically transforms fragments of application logic into SQL queries. QBS differs from traditional compiler optimizations as it relies on synthesis technology to generate invariants and postconditions for a code fragment. The postconditions and invariants are expressed using a new theory of ordered relations that allows us to reason precisely about both the contents and order of the records produced complex code fragments that compute joins and aggregates. The theory is close in expressiveness to SQL, so the synthesized postconditions can be readily translated to SQL queries. Using 75 code fragments automatically extracted from over 120k lines of open-source code written using the Java Hibernate ORM, we demonstrate that our approach can convert a variety of imperative constructs into relational specifications and significantly improve application performance asymptotically by orders of magnitude.

Categories and Subject Descriptors. D.3.2 [Programming Languages]: Processors—Compilers; I.2.2 [Artificial Intelligence]: Automatic Programming—Program Synthesis

Keywords. program optimization; program synthesis; performance

1. Introduction

In this paper, we develop QBS (Query By Synthesis), a new code analysis algorithm designed to make database-backed applications more efficient. Specifically, QBS identifies places where application logic can be pushed into the SQL queries issued by the application, and automatically transforms the code to do this. Moving application code into the database reduces the amount of data sent from the database to the application, and it also allows the database query optimizer to choose more efficient implementations of some operations—for instance, using indices to evaluate predicates or selecting efficient join algorithms.

One specific target of QBS is programs that interact with the database through object-relational mapping layers (ORMs) such as Hibernate for Java. Our optimizations are particularly important for such programs because ORM layers often lead programmers to write code that iterates over collections of database records, performing operations like filters and joins that could be better done inside of the database. Such ORM layers are becoming increasingly popular; for example, as of March, 2013, on the job board dice.com 15% of the 17,000 Java developer jobs are for programmers with Hibernate experience.

We are not the first researchers to address this problem; Wiedermann et al. [37][38] identified this as the query extraction problem. However, our work is able analyze a significantly larger class of source programs and generate a more expressive set of SQL queries than this prior work. Specifically, to the best of our knowledge, our work is the first that is able to identify joins and aggregates in general purpose application logic and convert them to SQL queries. Our analysis ensures that the generated queries are precise in that both the contents and the order of records in the generated queries are the same as those produced by the original code.

At a more foundational level, our paper is the first to demonstrate the use of constraint-based synthesis technology to attack a challenging compiler optimization problem. Our approach builds on the observation by Lu et al. [29] that if we can express the postcondition for an imperative code block in relational algebra, then we can translate that code block into SQL. Our approach uses constraint-based synthesis to automatically derive loop invariants and postconditions, and then uses an SMT solver to check the resulting verification conditions. In order to make synthesis and verification tractable, we define a new theory of ordered relations (TOR) that is close in expressiveness to SQL, while being expressive enough to concisely describe the loop invariants necessary to verify the codes of interest. The postconditions expressed in TOR can be readily translated to SQL, allowing them to be optimized by the database query planner and leading in some cases to orders of magnitude performance improvements.

In summary, this paper makes the following contributions:

1. We demonstrate a new approach to compiler optimization based on constraint-based synthesis of loop invariants and apply it to the problem of transforming low-level loop nests into high-level SQL queries.
2. We define a theory of ordered relations that allows us to concisely represent loop invariants and postconditions for code fragments that implement SQL queries, and to efficiently translate those postconditions into SQL.
3. We define a program analysis algorithm that identifies candidate code blocks that can potentially be transformed by QBS.
4. We demonstrate our full implementation of QBS and the candidate identification analysis for Java programs by automatically identifying and transforming 75 code fragments in two large open source projects. These transformations result in order-of-magnitude performance improvements. Although those projects are not the first to address the use of constraint-based synthesis technology to attack a challenging compiler optimization problem, our approach is the first to demonstrate the feasibility of this approach in practice.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

PLDI’13, June 16–19, 2013, Seattle, WA, USA.
Copyright © 2013 ACM 978-1-4503-2014-6/13/06…$15.00
This section gives an overview of our compilation infrastructure

2. Overview

2.1 QBS Architecture

We now discuss the architecture of QBS and describe the steps in inferring SQL queries from imperative code. The architecture of QBS is shown in Fig. 5.

Identify code fragments to transform. Given a web application written in Java, QBS first finds the persistent data methods in the application, which are those that fetch persistent data via ORM li-
brary calls. It also locates all entry points to the application such as servlet handlers. From each persistent data method that is reachable from the entry points, the system inlines a neighborhood of calls, i.e. a few of the parent methods that called the persistent data method and a few of the methods called by them. If there is ambiguity as to the target of a call, all potential targets are considered up to a budget. A series of analyses is then performed on each inlined method body to identify a continuous code fragment that can be potentially transformed to SQL; ruling out, for example, code fragments with side effects. For each candidate code fragment, our system automatically detects the program variable that will contain the results from the inferred query (in the case of the running example it is \texttt{listUsers}) — we refer to this as the “result variable.” At the end of the process, each code fragment is converted to our kernel language as discussed.

**Compute verification conditions.** As the next step, the system computes the verification conditions of the code fragment expressed in the kernel language. The verification conditions are written using the predicate language derived from the theory of ordered relations to be discussed in Sec. 3. The procedure used to compute verification conditions is a fairly standard one \cite{12, 16}; the only twist is that the verification condition must be computed in terms of an unknown postcondition and loop invariants. The process of computing verification conditions is discussed in more detail in Sec. 4.1.

**Synthesize loop invariants and postconditions.** The definitions of the postcondition and invariants need to be filled in and validated before translation can proceed. QBS does this using a synthesis-based approach that is similar to \cite{11}, where a synthesizer is used to come up with a postcondition and invariants that satisfy the computed verification conditions. The synthesizer uses a symbolic representation of the space of candidate postconditions and invariants and efficiently identifies candidates within the space that are correct according to a bounded verification procedure. It then uses a theorem prover \cite{Z3} specifically to check if those candidates can be proven correct. The space of candidate invariants and postconditions is described by a template generated automatically by the compiler. To prevent the synthesizer from generating trivial postconditions (such as True), the template limits the synthesizer to only generate postconditions that can be translated to SQL as defined by our theory of ordered relations, such as that shown at the top of Fig. 4.

We observe that it is not necessary to determine the strongest (in terms of logical implication) invariants or postconditions: we are only interested in finding postconditions that allow us transform the input code fragment into SQL. In the case of the running example, we are only interested in finding a postcondition of the form \texttt{listUsers} = \texttt{query}, where \texttt{query} is an expression translatable to SQL. Similarly, we only need to discover loop invariants that are strong enough to prove the postcondition of interest. From the example shown in Fig. 4 our system infers the postcondition shown at the top of Fig. 5 where \( \pi, \sigma, \text{ and } \preceq \) are ordered versions of relational projection, selection, and join, respectively to be defined in Sec. 3. The process of automatic template generation from the input code fragment and synthesis of the postcondition from the template are discussed in Sec. 4.

Unfortunately, determining loop invariants is undecidable for arbitrary programs \cite{6}, so there will be programs for which the necessary invariants fall outside the space defined by the templates. However, our system is significantly more expressive than the state of the art as demonstrated by our experiments in Sec. 7.

**Convert to SQL.** After the theorem prover verifies that the computed invariants and postcondition are correct, the input code fragment is translated to SQL, as shown in the bottom of Fig. 3. The predicate language defines syntax-driven rules to translate any expressions in the language into valid SQL. The details of validation are discussed in Sec. 5 while the rules for SQL conversion are introduced in Sec. 3.2. The converted SQL queries are patched back into the original code fragments and compiled as Java code.

### 3. Theory of Finite Ordered Relations

QBS uses a theory of finite ordered relations to describe postconditions and invariants. The theory is defined to satisfy four main requirements: precision, expressiveness, conciseness and ease of translation to SQL. For precision, we want to be able to reason about both the contents and order of records retrieved from the database. This is important because in the presence of joins, the order of the result list will not be arbitrary even when the original list was arbitrary, and we do not know what assumptions the rest of the program makes on the order of records. The theory must also be expressive enough not just to express queries but also to express invariants, which must often refer to partially constructed lists. For instance, the loop invariants for the sample code fragment in Fig. 4 must express the fact that \texttt{listUsers} is computed from the first i and \( j \) records of \texttt{users} and \texttt{roles} respectively. Conciseness, e.g. the number of relational operators involved, is important because the complexity of synthesis grows with the size of the synthesized expressions, so if we can express invariants succinctly, we will be able to synthesize them more efficiently. Finally, the inferred postconditions must be translatable to standard SQL.

There are many ways to model relational operations (see Sec. 8), but we are not aware of any that fulfills all of the criteria above. For example, relational algebra is not expressive enough to describe sufficiently precise loop invariants. Defined in terms of sets, relational algebra cannot naturally express concepts such as “the first \( i \) elements of the list.” First order logic (FOL), on the other hand, is very expressive, but it would be hard to translate arbitrary FOL expressions into SQL.

#### 3.1 Basics

Our theory of finite ordered relations is essentially relational algebra defined in terms of lists instead of sets. The theory operates on three types of values: scalars, records, and ordered relations of finite length. Records are collections of named fields, and an ordered relation is a finite list of records. Each record in the relation is labeled with an integer index that can be used to fetch the record. Figure 6 presents the abstract syntax of the theory and shows how to combine operators to form expressions.

| \( c \in \text{constant} \) | \( e \in \text{expression} \) |
| \( := \) | \( ::= \) |
| True | \([ \) | program var \( \mid \{ f_1 = e_1 \} \mid e_1 \) op \( e_2 \) \( \neg e \) |
| Query (...) | size \( e \) | get \( e \) \( \top \) \( e \) |
| \( \pi \top_{f_1,...,f_n} e \) | \( \sigma \phi \) \( e \) | \( \omega \forall \phi \) \( e \), \( e_2 \) |
| sum \( e \) | max \( e \) | min \( e \) |
| append \( e \), \( e \) | sort \( f_{i_1,...,i_n} \) \( e \) | unique \( e \) |

**Figure 6:** Abstract syntax for the predicate language based on the theory of ordered relations.
Figure 7: Some of the axioms that define the theory of ordered relations, Appendix C contains the full list of axioms.

Figure 8: Syntactic rules to convert translatable expressions to SQL.

Theorem 1 (Completeness of Translation Rules). All expressions in the predicate grammar in Fig. 5 except for those that contain append or unique, can be converted into translatable expressions.

The theorem is proved by defining a function Trans that maps any expression to a translatable expression and showing that the mapping is semantics preserving. Definition of Trans is shown in Appendix B. Semantic equivalence between the original and the translatable expression is proved using the expression equivalences listed in Thm. 2. Using those equivalences, for example, we can show that for $s \in \text{sortedExp}$ and $b \in \text{baseExp}$:

\[
\text{Trans}(\sigma_{\varphi}(s)) = \text{Trans}(\sigma_{\varphi}(\pi_i(s, \sigma_{\varphi}(b)))) [\text{sortedExp def.}]
\]

Thus the semantics of the original TOR expression is preserved.

Translatable expressions to SQL. Following the syntax-directed rules in Fig. 6 any translatable expression can be converted into an equivalent SQL expression. Most rules in Fig. 6 are direct translations from the operators in the theory into their SQL equivalents.

One important aspect of the translation is the way that ordering of records is preserved. Ordering is problematic because although the operators in the theory define the order of the output in terms of the order of their inputs, SQL queries are not guaranteed to preserve the order of records from nested sub-queries; e.g., the ordering imposed by an ORDER BY clause in a nested query is not guaranteed to be respected by an outer query that does not impose any ordering on the records.

To solve this problem, the translation rules introduce a function Order—defined in Fig. 7—which scans a translatable expression $t$ and returns a list of fields that are used to order the subexpressions.
Append and Unique. The append operation is not included in translatable expressions because there is no simple means to combine two relations in SQL that preserves the ordering of records in the resulting relation. We can still translate unique, however, using the SELECT DISTINCT construct at the outermost level, as Fig. 8 shows. Using unique in nested expressions, however, can change the semantics of the results in ways that are difficult to reason about (e.g., unique(top(_r)) is not equivalent to top(_r(unique(_r))). Thus, the only expressions with unique that we translate to SQL are those that use it at the outermost level. In our experiments, we found that omitting those two operators did not significantly limit the expressiveness of the theory.

With the theory in mind, we now turn to the process of computing verification conditions of the input code fragments.

4. Synthesis of Invariants and Postconditions

Given an input code fragment in the kernel language, the next step in QBs is to come up with an expression for the result variable of the form resultVar = e, where e is a translatable expression as defined in Sec. 3.2.4

4.1 Computing Verification Conditions

In order to infer the postcondition, we compute verification conditions for the input code fragment using standard techniques from axiomatic semantics [19]. As in traditional Hoare style verification, computing the verification condition of the while statements involves a loop invariant. Unlike traditional computation of verification conditions, however, both the postcondition and the loop invariants are unknown when the conditions are generated. This does not pose problems for QBs as we simply treat invariants (and the postcondition) as unknown predicates over the program variables that are currently in scope when the loop is entered.

As an example, Fig. 11 shows the verification conditions that are generated for the running example. In this case, the verification conditions are split into two parts, with invariants defined for both loops.

The first two assertions describe the behavior of the outer loop on line 5 with the first one asserting that the outer loop invariant must be true on entry of the loop (after applying the rule for the assignments prior to loop entry), and the second one asserting that the postcondition for the loop is true when the loop terminates. The third assertion asserts that the inner loop invariant is true when it is first entered, given that the outer loop condition and loop invariant are in t. The list is then used to imposing an ordering on the outer SQL query with an ORDER BY clause. One detail of the algorithm not shown in the figure is that some projections in the inner queries need to be modified so they do not eliminate fields that will be needed by the outer ORDER BY clause, and that we assume Query(….) is ordered by the order in which the records are stored in the database (unless the query expression already includes an ORDER BY clause).

Figure 9: Definition of Order

4.4 Creating Templates for Postconditions

The mechanism used to generate possible expressions for the result variable is similar to that for invariants, but we have stronger
Figure 10: Space of possible invariants for the outer loop of the running example.

restrictions, since we know the postcondition must be of the form
resultVar = e in order to be translatable to SQL.

For the running example, QBS considers the following possible set of postconditions:

\[
\text{listUsers} = \begin{cases}
\text{users} | \sigma_2(\text{users}) | \top_2(\text{users}) | \\
\sigma_1(\top_2(\text{users}), \top_2(\text{roles})) | \\
\sigma_1(\top_2(\text{users}), \sigma_2(\top_2(\text{roles})))) | \\
[\text{other relational expressions that return an ordered list}]
\end{cases}
\]

\[
\mathbf{i} \text{ op} \left\{ \begin{array}{c}
\text{size(\text{users})} | \text{size(\text{roles})} | \text{size(\text{listUsers})} | \\
\sum(\pi_1(\text{users}) | \sum(\pi_1(\text{roles}) | \max(\pi_1(\text{users}) | \\
[\text{other relational expressions that return a scalar value}]
\end{array} \right\} \land \text{listUsers} = \begin{cases}
\text{listUsers} | \sigma_2(\text{users}) | \\
\pi_1(\top_2(\text{users}), \top_2(\text{roles})) | \\
\pi_1(\top_2(\text{users}), \sigma_2(\top_2(\text{roles})))) | \\
[\text{other relational expressions that return an ordered list}]
\end{cases}
\]

4.5 Optimizations

The basic algorithm presented above for generating invariant and postcondition templates is sufficient but not efficient for synthesis. In this section we describe two optimizations that improve the synthesis efficiency.

Incremental solving. As an optimization, the generation of templates for invariants and postconditions is done in an iterative manner: QBS initially scans the input code fragment for specific patterns and creates simple templates using the production rules from the predicate grammar, such as considering expressions with only one relational operator, and functions that contains one boolean clause. If the synthesizer is able to generate a candidate that can be used to prove the validity of the verification conditions, then our job is done. Otherwise, the system repeats the template generation process, but increases the complexity of the template that is generated by considering expressions consisting of more relational operators, and more complicated boolean functions. Our evaluation using real-world examples shows that most code examples require only a few (≤ 3) iterations before finding a candidate solution. Additionally, the incremental solving process can be run in parallel.

Breaking symmetries. Symmetries have been shown to be one of sources of inefficiency in constraint solvers [11,34]. Unfortunately, the template generation algorithm presented above can generate highly symmetrical expressions. For instance, it can generate the following potential candidates for the postcondition:

\[
\sigma_{\varphi_1}(\sigma_{\varphi_2}(\text{users})) \\
\sigma_{\varphi_2}(\sigma_{\varphi_1}(\text{users}))
\]

Notice that the two expressions are semantically equivalent to the expression \(\sigma_{\varphi_1 \land \varphi_2}(\text{users})\). These are the kind of symmetries that are known to affect solution time dramatically. The template generation algorithm leverages known algebraic relationships between expressions to reduce the search space of possible expressions. For example, our algebraic relationships tell us that it is unnecessary to consider expressions with nested \(\sigma\) like the ones above. Also, when generating templates for postconditions, we only need to consider translatable expressions as defined in Sec. 3.2 as potential candidates. Our experiments have shown that applying these symmetric breaking optimizations can reduce the amount of solving time by half.

Even with these optimizations, the spaces of invariants considered are still astronomically large; on the order of \(2^{100}\) possible combinations of invariants and postconditions for some programs. Thanks to these optimizations, however, the spaces can be searched very efficiently by the constraint based synthesis procedure.

4.5 Optimizations

The basic algorithm presented above for generating invariant and postcondition templates is sufficient but not efficient for synthesis. In this section we describe two optimizations that improve the synthesis efficiency.

Incremental solving. As an optimization, the generation of templates for invariants and postconditions is done in an iterative manner: QBS initially scans the input code fragment for specific patterns and creates simple templates using the production rules from the predicate grammar, such as considering expressions with only one relational operator, and functions that contains one boolean clause. If the synthesizer is able to generate a candidate that can be used to prove the validity of the verification conditions, then our job is done. Otherwise, the system repeats the template generation process, but increases the complexity of the template that is generated by considering expressions consisting of more relational operators, and more complicated boolean functions. Our evaluation using real-world examples shows that most code examples require only a few (≤ 3) iterations before finding a candidate solution. Additionally, the incremental solving process can be run in parallel.

Breaking symmetries. Symmetries have been shown to be one of sources of inefficiency in constraint solvers [11,34]. Unfortunately, the template generation algorithm presented above can generate highly symmetrical expressions. For instance, it can generate the following potential candidates for the postcondition:

\[
\sigma_{\varphi_1}(\sigma_{\varphi_2}(\text{users})) \\
\sigma_{\varphi_2}(\sigma_{\varphi_1}(\text{users}))
\]

Notice that the two expressions are semantically equivalent to the expression \(\sigma_{\varphi_1 \land \varphi_2}(\text{users})\). These are the kind of symmetries that are known to affect solution time dramatically. The template generation algorithm leverages known algebraic relationships between expressions to reduce the search space of possible expressions. For example, our algebraic relationships tell us that it is unnecessary to consider expressions with nested \(\sigma\) like the ones above. Also, when generating templates for postconditions, we only need to consider translatable expressions as defined in Sec. 3.2 as potential candidates. Our experiments have shown that applying these symmetric breaking optimizations can reduce the amount of solving time by half.

Even with these optimizations, the spaces of invariants considered are still astronomically large; on the order of \(2^{100}\) possible combinations of invariants and postconditions for some programs. Thanks to these optimizations, however, the spaces can be searched very efficiently by the constraint based synthesis procedure.

5. Formal Validation and Source Transformation

After the synthesizer comes up with candidate invariants and postconditions, they need to be validated using a theorem prover, since the synthesizer used in our prototype is only able to perform bounded reasoning as discussed earlier. We have implemented the theory of ordered relations in the Z3 [3] prover for this purpose. Since the theory of lists is not decidable as it uses universal quantifiers, the theory of ordered relations is not decidable as well. However, for practical purposes we have not found that to be limiting in our experiments. In fact, given the appropriate invariants and postconditions, the prover is able to validate them within seconds by making use of the axioms that are provided.

If the prover can establish the validity of the invariants and postcondition candidates, the postcondition is then converted into SQL according to the rules discussed in Sec. 3.2. For instance, for the running example our algorithm found the invariants and postcondition as shown in Fig. 12 and the input code is transformed into the results in Fig. 4.

If the prover is unable to establish validity of the candidates (detected via a timeout), we ask the synthesizer to generate other candidate invariants and postconditions after increasing the space of possible solutions as described in Sec. 4.5. One reason that the prover may not be able to establish validity is because the maximum size of the relations set for the synthesizer was not large enough. For instance, if the code returns the first 100 elements from the relation but the synthesizer only considers relations up to size 10, then it will incorrectly generate candidates that claim that the code was performing a full selection of the entire relation. In such cases our algorithm will repeat the synthesis process after increasing the maximum relation size.

5.1 Incorporating inferred queries into original code

After verifying the transformation, the inferred queries are merged back into the code fragment. Before replacing the original fragment, we run a def-use analysis (which uses the points-to information to be described in Sec. 3.2) starting at the beginning of the code fragment until the end of the inlined method body. This is to ensure that none of the variables that are defined in the code fragment to be replaced is used in the rest of the inlined method after replacement.

6. Preprocessing of Input Programs

In order to handle real-world Java programs, QBS performs a number of initial passes to identify the code fragments to be transformed to kernel language representation before query inference. The code

Figure 12: Inferred expressions for the running example.

<table>
<thead>
<tr>
<th>Type</th>
<th>Expression inferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>outer loop invariant</td>
<td>(i \leq \text{size(\text{users})} \land \text{listUsers} = \pi_1(\top_2(\text{users}), \text{roles})) )</td>
</tr>
<tr>
<td>inner loop invariant</td>
<td>(i &lt; \text{size(\text{users})} \land j \leq \text{size(\text{roles})} \land \text{listUsers} = \text{append}(\text{listUsers}, \text{listUsers} = \pi_1(\top_2(\text{users}), \text{roles}) \land \pi_1(\top_2(\text{users}), \text{roles}))), \pi_1(\top_2(\text{users}), \text{roles}))) )</td>
</tr>
<tr>
<td>postcondition</td>
<td>(\text{listUsers} = \pi_1(\top_2(\text{users}, \text{roles})) )</td>
</tr>
</tbody>
</table>

where \(\varphi(\epsilon_{\text{users}}, \epsilon_{\text{roles}}) := \epsilon_{\text{users}, \text{role} \leq d = \epsilon_{\text{roles}, \text{role} \leq d}, \epsilon \) contains all the fields from the \text{User} class
identification process makes use of several standard analysis techniques, and in this section we describe them in detail.

6.1 Generating initial code fragments
As discussed in Sec. 2, code identification first involves locating application entry point methods and data persistent methods. From each data persistent method, our system currently inlines a neighborhood of 5 callers and callees. We only inline callees that are defined in the application, and provide models for native Java API calls. For callers we only inline those that can be potentially invoked from an entry point method. The inlined method bodies are passed to the next step of the process. Inlining improves the precision of the points-to information for our analysis. While there are other algorithms that can be used to obtain such information \[36, 40\], we chose inlining for ease of implementation and is sufficient in processing the code fragments used in the experiments.

6.2 Identifying code fragments for query inference
Given a candidate inlined method for query inference, we would like to identify the code fragment to transform to our kernel language representation. While we can simply use the entire body of the inlined method for this purpose, we would like to limit the amount of code to be analyzed, since including code that does not manipulate persistent data will increase the difficulty in synthesizing invariants and postconditions with no actual benefit. We accomplish this goal using a series of analyses. First, we run a flow-sensitive pointer analysis \[27\] on the body of the inlined method. The results of this analysis is a set of points-to graphs that map each reference variable to one or more abstract memory locations at each program point. Using the points-to information, we perform two further analyses on the inlined method.

Location tainting. We run a dataflow analysis that conservatively marks values that are derived from persistent data retrieved via ORM library calls. This analysis is similar to taint analysis \[33\], and the obtained information allows the system to remove regions of code that do not manipulate persistent data and thus can be ignored for our purpose. For instance, all reference variables and list contents in Fig. 1 will be tainted as they are derived from persistent data.

Value escapement. After that, we perform another dataflow analysis to check if any abstract memory locations are reachable from references that are outside of the inlined method body. This analysis is needed because if an abstract memory location is accessible from the external environment (e.g., via a global variable) after program point \( p \), then converting \( m \) might break the semantics of the original code, as there can be external references to \( m \) that rely on the contents of \( m \) before the conversion. This analysis is similar to classical escape analysis \[36\]. Specifically, we define an abstract memory location \( m \) as having escaped at program point \( p \) if any of the following is true:

- It is returned from the entry point method.
- It is returned from the entry point method.
- It is assigned to a global variable that persists after the entry point method returns (in the web application context, these can be variables that maintain session state, for instance).
- It is assigned to a Runnable object, meaning that it can be accessed by other threads.
- It is passed as a parameter into the entry point method.
- It can be transitively reached from an escaped location.

With that in mind, we define the beginning of the code fragment to pass to the \( QBS \) algorithm as the program point \( p \) in the inlined method where tainted data is first retrieved from the database, and the end as the program point \( p' \) where tainted data first escapes, where \( p' \) appears after \( p \) in terms of control flow. For instance, in

<table>
<thead>
<tr>
<th>App</th>
<th># persistent data code fragments</th>
<th>translated</th>
<th>rejected</th>
<th>failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wilos</td>
<td>33</td>
<td>21</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>itracker</td>
<td>16</td>
<td>12</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>49</td>
<td>33</td>
<td>9</td>
<td>7</td>
</tr>
</tbody>
</table>

Figure 13: Real-world code fragments experiment

6.3 Compilation to kernel language
Each code fragment that is identified by the previous analysis is compiled to our kernel language. Since the kernel language is based on value semantics and does not model heap updates for lists, during the compilation process we translate list references to the abstract memory locations that they point to, using the results from earlier analysis. In general, there are cases where the preprocessing step fails to identify a code fragment from an inlined method (e.g., persistent data values escape to multiple result variables under different branches, code involves operations not supported by the kernel language, etc.), and our system will simply skip such cases. However, the number of such cases is relatively small as our experiments show.

7. Experiments
In this section we report our experimental results. The goal of the experiments is twofold: first, to quantify the ability of our algorithm to convert Java code into real-world applications and measure the performance of the converted code fragments, and second to explore the limitations of the current implementation.

We have implemented a prototype of \( QBS \). The source code analysis and computation of verification conditions are implemented using the Polyglot compiler framework \[25\]. We use Sketch as the synthesizer for invariants and postconditions, and Z3 for validating the invariants and postconditions.

7.1 Real-World Evaluation
In the first set of experiments, we evaluated \( QBS \) using real-world examples from two large-scale open-source applications, Wilos and itracker, written in Java. Wilos (rev. 1196) \[2\] is a project management application with 62k LOC, and itracker (ver. 3.0.1) \[1\] is a software issue management system with 61k LOC. Both applications have multiple contributors with different coding styles, and use the Hibernate ORM library for data persistence operations. We passed in the entire source code of these applications to \( QBS \) to identify code fragments. The preprocessor initially found 120 unique code fragments that invoke ORM operations. Of those, it failed to convert 21 of them into the kernel language representation, as they use data structures that are not supported by our prototype (such as Java arrays), or access persistent objects that can escape from multiple control flow points and hence cannot be converted.

Meanwhile, upon manual inspection, we found that those 120 code fragments correspond to 49 distinct code fragments inlined in different contexts. For instance, if A and C both call method B, our system automatically inlines B into the bodies of A and C, and those become two different code fragments. But if all persistent data manipulation happens in B, then we only count one of the two as part of the 49 distinct code fragments. \( QBS \) successfully translated 33 out of the 49 distinct code fragments (and those 33 distinct code fragments correspond to 75 original code fragments).

The results are summarized in Fig. 13 and the details can be found in Appendix A.

This experiment shows that \( QBS \) can infer relational specifications from a large fraction of candidate fragments and convert them...
into SQL equivalents. For the candidate fragments that are reported as translatable by QBS, our prototype was able to synthesize post-conditions and invariants, and also validate them using the prover. Furthermore, the maximum time that QBS takes to process any one code fragment is under 5 minutes (with an average of 2.1 minutes). In the following, we broadly describe the common types of relational operations that our QBS prototype inferred from the fragments, along with some limitations of the current implementation.

**Projections and Selections.** A number of identified fragments perform relational projections and selections in imperative code. Typical projections include selecting specific fields from the list of records that are fetched from the database, and selections include filtering a subset of objects using field values from each object (e.g., user ID equals to some numerical constant), and a few use criteria that involve program variables that are passed into the method.

One special case is worth mentioning. In some cases only a single field is projected out and loaded into a set data structure, such as a set of integer values. One way to translate such cases is to generate SQL that fetches the field from all the records (including duplicates) into a list, and eliminate the duplicates and return the set to the user code. Our prototype, however, improves upon that scheme by detecting the type of the result variable and inferring a postcondition involving the unique operator, which is then translated to a SELECT DISTINCT query that avoids fetching duplicate records from the database.

**Joins.** Another set of code fragments involve join operations. We summarize the join operations in the application code into two categories. The first involves obtaining two lists of objects from two base queries and looping through each pair of objects in a nested for or while loop. The pairs are filtered and (typically) one of the objects from each pair is retained. The running example in Fig. [1] represents such a case. For these cases, QBS translates the code fragment into a relational join of the two base queries with the appropriate join predicate, projection list, and sort operations that preserve the ordering of records in the results.

Another type of join also involves obtaining two lists of objects from two base queries. Instead of a nested loop join, however, the code iterates through each object e from the first list, and searches if e (or one of its fields) is contained in the second. If true, then e (or some of its fields) is appended to the resulting list. For these cases QBS converts the search operation into a contains expression in the predicate language, after which the expression is translated into a correlated subquery in the form of

\[ SELECT * FROM r1, r2 WHERE r1.\text{ID} = r2.\text{ID} \]

QBS handles both join idioms mentioned above. However, the loop invariants and postconditions involved in such cases tend to be more complex as compared to selections and projections, as illustrated by the running example in Fig. [2]. Thus, they require more iterations of synthesis and formal validation before finding a valid solution, with up to 5 minutes in the longest case. Here, the majority of the time is spent in synthesis and bounded verification. We are not aware of any prior techniques that can be used to infer join queries from imperative code, and we believe that more optimizations can be devised to speed up the synthesis process for such cases.

**Aggregations.** Aggregations are used in fragments in a number of ways. The most straightforward ones are those that return the length of the list that is returned from an ORM query, which are translated into COUNT queries. More sophisticated uses of aggregates include iterating through all records in a list to find the max or min values, or searching if a record exists in a list. Aggregates such as maximum and minimum are interesting as they introduce loop-carried dependencies [S], where the running value of the aggregate is updated conditionally based on the value of the current record as compared to previous ones. By using the top operator from the theory of ordered relations, QBS is able to generate a loop invariant of the form \( v = \text{agg}(	ext{top}(r)) \) and then translate the postcondition into the appropriate SQL query.

As a special case, a number of fragments check for the existence of a particular record in a relation by iterating over all records and setting a result boolean variable to be true if it exists. In such cases, the generated invariants are similar to other aggregate invariants, and our prototype translates such code fragments into

\[ SELECT \text{COUNT}(*) > 0 \text{ FROM ... WHERE e, where e is the expression to check for existence in the relation. We rely on the database query optimizer to further rewrite this query into the more efficient form using EXISTS.}\]

**Limitations.** We have verified that in all cases where the generated template is expressive enough for the invariants and postconditions, our prototype does indeed find the solution within a preset timeout of 10 minutes. However, there are a few examples from the two applications where our prototype either rejects the input code fragment or fails to find an equivalent SQL expression from the kernel language representation. Fragments are rejected because they involve relational update operations that are not handled by TOR. Another set of fragments include advanced use of types, such as storing polymorphic records in the database, and performing different operations based on the type of records retrieved. Incorporating type information in the theory of ordered relations is an interesting area for future work. There are also a few that QBS fails to translate into SQL, even though we believe that there is an equivalent SQL query without updates. For instance, some fragments involve sorting the input list by Collections.sort, followed by retrieving the last record from the sorted list, which is equivalent to max or min depending on the sort order. Including extra axioms in the theory would allow us to reason about such cases.

7.2 Performance Comparisons

Next, we quantify the amount of performance improvement as a result of query inference. To do so, we took a few representative code fragments for selection, joins, and aggregation, and populated databases with different number of persistent objects. We then compared the performance between the original code and our transformed versions of the code with queries inferred by QBS. Since Hibernate can either retrieve all nested references from the database (eager) when an object is fetched, or only retrieve the top level references (lazy), we measured the execution times for both modes (the original application is configured to use the lazy retrieval mode). The results shown in Fig. [14] compare the time taken to completely load the webpages containing the queries between the original and the QBS inferred versions of the code.

**Selection Code Fragment.** Fig. [14a] and Fig. [14b] show the results from running a code fragment that includes persistent data manipulations from fragment #40 in Appendix [A]. The fragment returns the list of unfinished projects. Fig. [14a] shows the results where 10% of the projects stored are unfinished, and Fig. [14b] shows the results with 50% unfinished projects. While the original version performs the selection in Java by first retrieving all projects from the database, QBS inferred a selection query in this case. As expected, the query inferred by QBS outperforms the original fragments in all cases as it only needs to retrieve a portion (specifically 10 and 50%) of all persistent objects.

**Join Code Fragment.** Fig. [14c] shows the results from a code fragment with contents from fragment #46 in Appendix [A] (which is the same as the example from Fig. [1]). The fragment returns the projection of User objects after a join of Roles and Users in the
Our second synthetic test case joins two lists, Sort-Merge Joins, accordingly, similar to the join code fragments mentioned above. Recognize this process as a join operation and convert the fragment whose keys are the values of the $r$ where we first iterate through records in $r$ to join with, using the $a$ field as the lookup key. QBS currently models hashtables using lists, and with that our prototype is able recognize this process as a join operation and convert the fragment accordingly, similar to the join code fragments mentioned above.

Sort-Merge Joins. Our second synthetic test case joins two lists by first sorting $r$ and $s$ on fields $a$ and $b$ respectively, and then iterating through both lists simultaneously. We advance the scan of $r$ as long as the current record from $r$ is less than (in terms of fields $a$ and $b$) the current record from $s$, and similarly advance the scan of $s$ as long as the current $s$ record is less than the current $r$ record. Records that represent the join results are created when the current record from $r$ equals to that from $s$ on the respective fields. Unfortunately, our current prototype fails to translate the code fragment into SQL, as the invariants for the loop cannot be expressed using the current the predicate language, since that involves expressing the relationship between the current record from $r$ and $s$ with all the records that have been previously processed.

Iterating Over Sorted Relations. We next tested our prototype with two usages of sorted lists. We created a relation with one unsigned integer field $id$ as primary key, and sorted the list using the sort method from Java. We subsequently scanned through the sorted list as follows:

```java
List records = Query("SELECT id FROM t + ORDER BY id LIMIT 10");
List results = new ArrayList();
Collections.sort(records); // sort by id
for (int i = 0; i < 10; ++i)
{ results.add(records.get(i)); }
```

Our prototype correctly processes this code fragment by translating it into `SELECT id FROM t ORDER BY id LIMIT 10`. However, if the loop is instead written as follows:

```java
List records = Query("SELECT id FROM t + ORDER BY id LIMIT 10");
List results = new ArrayList();
Collections.sort(records); // sort by id
int i = 0;
while (records.get(i).id < 10)
{ results.add(records.get(i)); ++i; }
```

The two loops are equivalent since the $id$ field is a primary key of the relation, and thus there can at most be 10 records retrieved. However, our prototype is not able to reason about the second code fragment, as that requires an understanding of the schema of the relation, and that iterating over $id$ in this case is equivalent to iterating over $i$ in the first code fragment. Both of which require additional axioms to be added to the theory before such cases can be converted.

### 8. Related Work

Inferring relational specifications from imperative code was studied in [37][38]. The idea is to compute the set of data access paths that the imperative code traverses using abstract interpretation, and replace the imperative code with SQL queries. The analysis is applicable to recursive function calls, but does not handle code with loop-carried dependencies, or those with join or aggregation. It is unclear how modeling relational operations as access paths can be extended to handle such cases. Our implementation is able to infer both join and aggregation from imperative code. We currently do
not handle recursive function calls, although we have not encountered such uses in the applications used in our experiments.

Modeling relational operations. Our ability to infer relational specifications from imperative code relies on using the TOR to connect the imperative and relational worlds. There are many prior works in modeling relational operations, for instance using bags [7], sets [22], and nested relational calculus [39]. There are also theoretical models that extend standard relational algebra with order, such as 3-valued logic. In particular, the ORM libraries provide ordered data structures and imperative implementations of join proves to be common at least in the benchmarks we studied.

Finding invariants to validate transformations. Our verification-based approach to finding a translatable postcondition is similar to earlier work [20, 21], although they acknowledge that finding invariants is difficult. Similar work has been done for general-purpose language compilers [33]. Scanning the source code to generate the synthesis template is inspired by the PINS algorithm [32], although QBS does not need user intervention. There has been earlier work on automatically inferring loop invariants, such as using predicate refinement [14] or dynamic detection [13, 18].

Constraint-based synthesis. Constraint-based program synthesis has been an active topic of research in recent years. For instance, there has been work on using synthesis to discover invariants [31]. Our work differs from previous approaches in that we only need to find invariants and postconditions that are strong enough to validate the transformations and our predicate language greatly reduces the space of invariants to those needed for common relational operations. Synthesis has also been applied in other domains, such as generating data structures [29], processor instructions [15], and learning queries from examples [8].

Integrated query languages. Integrating application and database query languages into has been an active research area, with projects such as LINQ [23], Kleisli [39], Links [19], JReq [20], the functional language proposed in [9], Ferry [12], and DBPL [22]. These solutions embed database queries in imperative programs without ORM libraries. Unfortunately, many of them do not support all relational operations, and the syntax of such languages resemble SQL, thus developers still need to learn new programming paradigms and rewrite existing applications.

Improving performance of database programs by code transformation. There is also work in improving application performance by transforming loops to allow query batching [24], and pushing computations into the database [7]. Our work is orthogonal to this line of research. After converting portions of the source code into SQL queries, such code transformation can be applied to gain additional performance improvement.

9. Conclusions
In this paper, we presented QBS, a system for inferring relational specifications from imperative code that retrieves data using ORM libraries. Our system automatically infers loop invariants and postconditions associated with the source program, and converts the validated postcondition into SQL queries. Our approach is both sound and precise in preserving the ordering of records. We developed a theory of ordered relations that allows efficient encoding of relational operations into a predicate language, and we demonstrated the applicability using a set of real-world code examples.

References
### A. Persistent Data Code Fragment Details

In this section we describe the code fragments from real-world examples that are used in our experiments. The table below shows the details of the 49 distinct code fragments as mentioned in Sec. 7.1. The times reported correspond to the time required to synthesize the invariants and postconditions. The time taken for the other initial analysis and SQL translation steps are negligible.

#### wilos code fragments

<table>
<thead>
<tr>
<th>#</th>
<th>Java Class Name</th>
<th>Line</th>
<th>Operation</th>
<th>Status</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ActivityService</td>
<td>401</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>AffectedListDao</td>
<td>13</td>
<td>B</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>19</td>
<td>ConcreteActivityDao</td>
<td>139</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>ConcreteActivityService</td>
<td>133</td>
<td>D</td>
<td>✓</td>
<td>310</td>
</tr>
<tr>
<td>22</td>
<td>ConcreteRoleJoinService</td>
<td>181</td>
<td>F</td>
<td>✓</td>
<td>284</td>
</tr>
<tr>
<td>23</td>
<td>ConcreteRoleJoinService</td>
<td>55</td>
<td>G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>ConcreteRoleJoinService</td>
<td>236</td>
<td>F</td>
<td>✓</td>
<td>284</td>
</tr>
<tr>
<td>26</td>
<td>GuidanceService</td>
<td>140</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>GuidanceService</td>
<td>154</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>IterationService</td>
<td>103</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>LoginService</td>
<td>103</td>
<td>H</td>
<td>✓</td>
<td>125</td>
</tr>
<tr>
<td>30</td>
<td>LoginService</td>
<td>83</td>
<td>H</td>
<td>✓</td>
<td>164</td>
</tr>
<tr>
<td>31</td>
<td>ParticipantBean</td>
<td>1079</td>
<td>B</td>
<td>✓</td>
<td>31</td>
</tr>
<tr>
<td>32</td>
<td>ParticipantBean</td>
<td>681</td>
<td>H</td>
<td>✓</td>
<td>121</td>
</tr>
<tr>
<td>33</td>
<td>ParticipantService</td>
<td>146</td>
<td>E</td>
<td>✓</td>
<td>281</td>
</tr>
<tr>
<td>34</td>
<td>ParticipantService</td>
<td>119</td>
<td>E</td>
<td>✓</td>
<td>301</td>
</tr>
<tr>
<td>35</td>
<td>ParticipantService</td>
<td>266</td>
<td>F</td>
<td></td>
<td>260</td>
</tr>
<tr>
<td>36</td>
<td>PhaseService</td>
<td>98</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>ProcessBean</td>
<td>248</td>
<td>H</td>
<td></td>
<td>82</td>
</tr>
<tr>
<td>38</td>
<td>ProcessManagerBean</td>
<td>243</td>
<td>B</td>
<td>✓</td>
<td>50</td>
</tr>
<tr>
<td>39</td>
<td>ProjectService</td>
<td>266</td>
<td>K</td>
<td></td>
<td>39</td>
</tr>
<tr>
<td>40</td>
<td>ProjectService</td>
<td>297</td>
<td>A</td>
<td>✓</td>
<td>19</td>
</tr>
<tr>
<td>41</td>
<td>ProjectService</td>
<td>338</td>
<td>G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>ProjectService</td>
<td>394</td>
<td>A</td>
<td>✓</td>
<td>21</td>
</tr>
<tr>
<td>43</td>
<td>ProjectService</td>
<td>410</td>
<td>A</td>
<td>✓</td>
<td>39</td>
</tr>
<tr>
<td>44</td>
<td>ProjectService</td>
<td>248</td>
<td>H</td>
<td></td>
<td>150</td>
</tr>
<tr>
<td>45</td>
<td>RoleDao</td>
<td>15</td>
<td>I</td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>46</td>
<td>RoleService</td>
<td>15</td>
<td>E</td>
<td></td>
<td>150</td>
</tr>
<tr>
<td>47</td>
<td>WilosUserBean</td>
<td>717</td>
<td>B</td>
<td>✓</td>
<td>23</td>
</tr>
<tr>
<td>48</td>
<td>WorkProductsExpTableBean</td>
<td>990</td>
<td>B</td>
<td>✓</td>
<td>52</td>
</tr>
<tr>
<td>49</td>
<td>WorkProductsExpTableBean</td>
<td>974</td>
<td>J</td>
<td>✓</td>
<td>50</td>
</tr>
</tbody>
</table>

**itracker code fragments**

<table>
<thead>
<tr>
<th>#</th>
<th>Java Class Name</th>
<th>Line</th>
<th>Operation</th>
<th>Status</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EditProjectFormActionImpl</td>
<td>219</td>
<td>F</td>
<td></td>
<td>289</td>
</tr>
<tr>
<td>2</td>
<td>IssueServiceImpl</td>
<td>1437</td>
<td>D</td>
<td>✓</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>IssueServiceImpl</td>
<td>1456</td>
<td>L</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IssueServiceImpl</td>
<td>1567</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IssueServiceImpl</td>
<td>1583</td>
<td>M</td>
<td>✓</td>
<td>130</td>
</tr>
<tr>
<td>6</td>
<td>IssueServiceImpl</td>
<td>1592</td>
<td>M</td>
<td>✓</td>
<td>133</td>
</tr>
<tr>
<td>7</td>
<td>IssueServiceImpl</td>
<td>1601</td>
<td>M</td>
<td>✓</td>
<td>128</td>
</tr>
<tr>
<td>8</td>
<td>IssueServiceImpl</td>
<td>1422</td>
<td>D</td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>9</td>
<td>ListProjectsAction</td>
<td>77</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>MoveIssueFormAction</td>
<td>144</td>
<td>K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>NotificationServiceImpl</td>
<td>568</td>
<td>O</td>
<td>✓</td>
<td>57</td>
</tr>
<tr>
<td>12</td>
<td>NotificationServiceImpl</td>
<td>848</td>
<td>A</td>
<td>✓</td>
<td>132</td>
</tr>
<tr>
<td>13</td>
<td>NotificationServiceImpl</td>
<td>941</td>
<td>H</td>
<td>✓</td>
<td>160</td>
</tr>
<tr>
<td>14</td>
<td>NotificationServiceImpl</td>
<td>244</td>
<td>O</td>
<td>✓</td>
<td>72</td>
</tr>
<tr>
<td>15</td>
<td>UserServiceImpl</td>
<td>155</td>
<td>M</td>
<td>✓</td>
<td>146</td>
</tr>
<tr>
<td>16</td>
<td>UserServiceImpl</td>
<td>412</td>
<td>A</td>
<td>✓</td>
<td>142</td>
</tr>
</tbody>
</table>

where:

- **A**: selection of records
- **B**: return literal based on result size
- **C**: retrieve the max / min record by first sorting and then returning the last element
- **D**: projection / selection of records and return results as a set
- **E**: nested-loop join followed by projection
- **F**: join using contains
- **G**: type-based record selection
- **H**: check for record existence in list
- **I**: record selection and only return the one of the records if multiple ones fulfill the selection criteria
- **J**: record selection followed by count
- **K**: sort records using a custom comparator
- **L**: projection of records and return results as an array
- **M**: return result set size
- **N**: record selection and in-place removal of records
- **O**: retrieve the max / min record

✓ indicates those that are translated by QBS
* indicates those that QBS failed to find invariants for.
† indicates those that are rejected by QBS due to TOR / pre-processing limitations.

### B. TOR Expression Equivalences and Definition of Trans

Before defining Trans, we first list the set of TOR expression equivalences that are used in the definition.

**Theorem 2 (Operator Equivalence).** The following equivalences hold, both in terms of the contents of the relations and also the ordering of the records in the relations:

- $\pi_{\sigma}(r) = \pi_{\sigma}(r')$
- $\pi_{\sigma}(\sigma_{\varphi}(r)) = \sigma_{\varphi'}(r)$, where $\varphi' = \varphi \land \varphi$
- $\pi_{\ell}(\pi_{\ell}(r)) = \pi_{\ell'}(r)$, where $\ell'$ is the concatenation of all the fields in $\ell_1$ and $\ell_2$.
- $\operatorname{top}_{\sigma}(\pi_{\ell}(r)) = \pi_{\ell}(\operatorname{top}_{\sigma}(r))$
- $\operatorname{top}_{\sigma}(\operatorname{top}_{\sigma}(r)) = \operatorname{top}_{\sigma}(r)$
- $\sigma_{\varphi}(r, r_2) = \sigma_{\varphi'}(r)$, i.e., joins can be converted into cross products with selections with proper renaming of fields.

Except for the equivalences involving sort, the other ones can be proven easily from the axiomatic definitions.
B.1 Definition of Trans

Let $s = \pi_{e_1}(\text{sort}_{e_2}(\sigma_{e_2}(b)))$. Trans is defined on expressions whose sub-expressions (if any) are in translatable form, so we have to consider cases where the sub-expressions are either $s$ or $\text{top}_e(s)$. Each case is defined below.

$$\text{Query}(...)$$

Trans($\text{Query}(...)\)) = \pi_1(\text{sort}_1(\sigma_{\text{true}}(\text{Query}(...))))$

where $\ell$ projects all the fields from the input relation.

$$\pi_\ell(t)$$

$\text{Trans}(\pi_\ell(s)) = \pi_\ell(\text{sort}_{\ell}(\sigma_{\ell}(b)))$

$\text{Trans}(\pi_\ell(\text{sort}_e(s))) = \text{sort}_e(\pi_\ell(\text{sort}_{\ell}(\sigma_{\ell}(b))))$

where $\ell'$ is the composition of $\ell_\alpha$ and $\ell_\beta$.

$$\sigma_{\varphi_1}$$

$\text{Trans}(\sigma_{\varphi_1}(s)) = \pi_\ell(\text{sort}_{\ell}(\sigma_{\varphi_1}(b)))$

$\text{Trans}(\sigma_{\varphi_1}(\text{sort}_e(s))) = \text{sort}_e(\pi_\ell(\text{sort}_{\ell}(\sigma_{\varphi_1}(b))))$

$\text{Trans}(\sigma_{\varphi_1}(\text{sort}_e(s))) = \text{sort}_e(\pi_\ell(\text{sort}_{\ell}(\sigma_{\varphi_1}(b))))$

where $\varphi' = \varphi_{\varphi_1} \land \varphi_{\varphi_2} \land \varphi_{\varphi_3}$ with field names properly renamed, $\ell'$ is $\ell_{\alpha}$ and $\ell_{\beta}$ is $\ell_{\alpha}$. $\ell_{\alpha}$ is the minimum value of $e_1$ and $e_2$.

$\text{top}_e(t)$

$\text{Trans}(\text{top}_e(s)) = \text{top}_e(s)$

$\text{Trans}(\text{top}_e((\text{sort}_e(s)))) = \text{top}_e(s)$

where $e'$ is the minimum value of $e_1$ and $e_2$.

$\text{agg}(t)$

$\text{Trans}(\text{agg}(s)) = \pi_\ell(\text{sort}_1(\sigma_{\text{true}}(\text{agg}(s))))$

$\text{Trans}(\text{agg}(\text{sort}_e(s))) = \pi_\ell(\text{sort}_1(\sigma_{\text{true}}(\text{agg}(s))))$

where $\ell$ contains all the fields from $s$.

$\text{sort}_{e_2}(t)$

$\text{Trans}(\text{sort}_{e_2}(s)) = \pi_\ell(\text{sort}_{\ell}(\sigma_{e_2}(b)))$

$\text{Trans}(\text{sort}_{e_2}(\text{sort}_e(s))) = \text{sort}_e(\pi_\ell(\text{sort}_{\ell}(\sigma_{e_2}(b))))$

where $\ell_{\alpha}$ is $\text{cat}(\ell_{\alpha}, \ell_{\beta})$.

C. TOR Axioms

Below is a listing of all the axioms currently defined in the theory of ordered relations (TOR). $\text{cat}(\ell_1, \ell_2)$ concatenates the contents of lists $\ell_1$ and $\ell_2$. 

$$r = []$$

(size

$$\text{size}(r) = 0$$

$$\text{size}(r) = 1 + \text{size}(t)$$

$$i = 0$$

$$\text{get}(r) = h$$

$$i > 0$$

$$\text{get}(r) = \text{get}_{i-1}(t)$$

$$r = []$$

$$\text{append}(r, t) = [t]$$

$$\text{append}(r, t') = h: \text{append}(t, t')$$

$$r = []$$

$$\text{top}_i(i) = []$$

$$i > 0$$

$$\text{top}_i(i) = []$$

$$\text{top}_i(i) = h: \text{top}_{i-1}(t)$$

$$r = []$$

$$\text{join}(\varnothing)$$

$$r_1 = []$$

$$r_2 = []$$

$$\text{top}(r) = []$$

$$\text{top}(r) = \{f_i \in \ell : h.f_i = e_i\}$$

$$\text{projection}(\pi)$$

$$r = []$$

$$\text{proj}(r) = \{f_i : h.f_i = e_i\}$$

$$\text{selection}(\sigma)$$

$$r = []$$

$$\sigma_{\varphi}(r) = []$$

$$\sigma_{\varphi}(r) = h : \sigma_{\varphi}(t)$$

$$\sigma_{\varphi}(r) = \sigma_{\varphi}(t)$$

$$\text{sum}(r) = 0$$

$$\text{sum}(r) = h + \text{sum}(t)$$

$$r = []$$

$$\text{max}(r) = -\infty$$

$$\text{max}(r) = h$$

$$\text{max}(r) = \text{max}(t)$$

$$r = []$$

$$h > \text{max}(t)$$

$$h = \text{max}(t)$$

$$\text{min}(r) = \infty$$

$$\text{min}(r) = h$$

$$\text{min}(r) = \text{min}(t)$$

$$r = []$$

$$h < \text{min}(t)$$

$$h = \text{min}(t)$$

$$r = []$$

$$h \geq \text{min}(t)$$

$$h = \text{min}(t)$$

$$\text{contains}(e, r) = \text{False}$$

$$e = h$$

$$r = h : t$$

$$e \neq h$$

$$r = h : t$$

$$\text{contains}(e, r) = \text{True}$$

$$\text{contains}(e, r) = \text{contains}(e, t)$$