Database Queries that Explain their Work

Citation for published version:

Digital Object Identifier (DOI):
10.1145/2643135.2643143

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
PPDP '14 Proceedings of the 16th International Symposium on Principles and Practice of Declarative Programming

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Database Queries that Explain their Work

James Cheney
University of Edinburgh
jcheney@inf.ed.ac.uk

Amal Ahmed
Northeastern University
amal@ccs.neu.edu

Umut A. Acar
Carnegie Mellon University &
INRIA-Rocquencourt
umut@cs.cmu.edu

Abstract
Provenance for database queries or scientific workflows is often motivated as providing explanation, increasing understanding of the underlying data sources and processes used to compute the query, and reproducibility, the capability to recompute the results on different inputs, possibly specialized to a part of the output. Many provenance systems claim to provide such capabilities; however, most lack formal definitions or guarantees of these properties, while others provide formal guarantees only for relatively limited classes of changes. Building on recent work on provenance traces and slicing for functional programming languages, we introduce a detailed tracing model of provenance for multiset-valued Nested Relational Calculus, define trace slicing algorithms that extract substraces needed to explain or recompute specific parts of the output, and define query slicing and differencing techniques that support explanation. We state and prove correctness properties for these techniques and present a proof-of-concept implementation in Haskell.

Keywords provenance, database queries, slicing

1. Introduction
Over the past decade, the use of complex computer systems in science has increased dramatically: databases, scientific workflow systems, clusters, and cloud computing based on frameworks such as MapReduce [16] or PigLatin [26] are now routinely used for scientific data analysis. With this shift to computational science based on (often) unreliable components and noisy data comes decreased transparency, and an increased need to understand the results of complex computations by auditing the underlying processes.

This need has motivated work on provenance in databases, scientific workflow systems, and many other settings [8, 25]. There is now a great deal of research on extending such systems with rich provenance-tracking features. Generally, these systems aim to provide high-level explanations intended to aid the user in understanding how a computation was performed, by recording and presenting additional “trace” information.

Over time, two distinct approaches to provenance have emerged: (1) the use of annotations propagated through database queries to illustrate where-provenance linking results to source data [6], lineage or why-provenance linking result records to sets of witnessing input records [13], or how-provenance describing how results were produced via algebraic expressions [28], and (2) the use of graphical provenance traces to illustrate how workflow computations construct final results from inputs and configuration parameters [4, 21, 55]. However, to date few systems formally specify the semantics of provenance or give formal guarantees characterizing how provenance “explains” results.

For example, scientists often conduct parameter sweeps to search for interesting results. The provenance trace of such a computation may be large and difficult to navigate. Since the most promising results have been identified, a scientist may want to extract just that information that is needed to explain the result, without showing all of the intermediate search steps or uninteresting results. Conversely, if the results are counterintuitive, the scientist may want to identify the underlying data that contributed to the anomalous result. Missier et al. [24] introduced the idea of a “golden trail”, or a subset of the provenance trace that explains, or allows reproduction of, a high-value part of the output. They proposed techniques for extracting “golden trails” using recursive Datalog queries over provenance graphs; however, they did not propose definitions of correctness or reproducibility.

It is a natural question to ask how we know when a proposed solution, such as Missier et al.’s “golden trail” queries, correctly explains or can be used to correctly reproduce the behavior of the original computation. It seems to have been taken for granted that simple graph traversals suffice to at least overapproximate the desired subset of the graph. As far as we know, it is still an open question how to define and prove such correctness properties for most provenance techniques. In fact, these properties might be defined and formalized in a number of ways, reflecting different modeling choices or requirements. In any case, in the absence of clear statements and proofs of correctness, claims that different forms of provenance “explain” or allow “reproducibility” are difficult to evaluate objectively.

The main contribution of this paper is to formalize and prove the correctness of an approach to fine-grained provenance for database queries. We build on our approach developed in prior work, which we briefly recapitulate. Our approach is based on analogies between the goals of provenance tracking for databases and workflows, and those of classical techniques for program comprehension and analysis, particularly program slicing [31] and information flow [28]. Both program slicing and information flow rely critically on notions of dependence, such as the familiar control-flow and data-flow dependences in programming languages.

We previously introduced a provenance model for NRC (including difference and aggregation operations) called dependency provenance [12], and showed how it can be used to compute data slices, that is, subsets of the input to the query that include all of the information relevant to a selected part of the output. Some other forms of provenance for database query languages, such as how-provenance [20], satisfy similar formal guarantees that can be used to predict how the output would change under certain classes of input changes, specifically those expressible by semiring homomorphisms. For example, Amsterdamer et al.’s system [3] is based on the semiring provenance model, so the effects of deletions on parts of the output can be predicted by inspecting their provenance, but other kinds of changes are not supported.

More recently, we proposed an approach to provenance called self-explaining computation [11] and explored it in the context of a general-purpose functional programming language [1, 23]. In this approach, detailed execution traces are used as a form of
provenance. Traces explain results in the sense that they can be
replayed to recompute the results, and they can be sliced to obtain
smaller traces that provide more concise explanations of parts of
the output. Trace slicing also produces a slice of the input showing
what was needed by the trace to compute the output. Moreover,
other forms of provenance can be extracted from traces (or slices),
and we also showed that traces can be used to compute program
slices efficiently through lazy evaluation. Finally, we showed how
traces support differential slicing techniques that can highlight the
differences between program runs in order to explain and precisely
localize bugs in the program or errors in the input data.

Our long-term vision is to develop self-explaining computation
techniques covering all components used in day-to-day scientific
practice. Databases are probably the single most important such
component. Since our previous work already applies to a general-
purpose programming language, one way to proceed would be to
simply implement an interpreter for NRC in this language, and in-
herit the slicing behavior from that. However, without some further
inlining or optimization, this naive strategy would yield traces that
record both the behavior of the NRC query and its interpreter, along
with internal data structures and representation choices whose de-
tails are (intuitively) irrelevant to understanding the high-level be-
behavior of the query.

1.1 Technical overview

In this paper, we develop a tracing semantics and trace slicing tech-
niques tailored to NRC (over a multiset semantics). This seman-
tics evaluates a query \( Q \) over an input database (i.e. environment \( \gamma \)
mapping relation names to table values), yielding the usual result
value \( v \) as well as a trace \( T \). Traces are typically large and difficult
to decipher, so we consider a scenario where a user has run \( Q \), in-
pected the results \( v \), and requests an explanation for a part of the
result, such as a field value of a single record. As in our previous
work for functional programs, we use partial values with “holes” \( \square \)
to describe parts of the output that are to be explained. For exam-
ple, if the result of a program is just a pair \( (1, 2) \) then the pattern
(1, \( \square \)) can be used to request an explanation for just the first com-
ponent. Given a partial value \( p \) matching the output, our approach
computes a “slice” consisting of a partial trace and a partial input
environment, where components not necessary for recomputing the
explained output part \( p \) have been deleted.

The main technical contribution of this paper over our previous work\([1, 2]\) is its treatment of tracing and slicing for collections. There
are two underlying technical challenges; we illustrate both (and our solutions) via a simple example query \( Q(R) = \sigma_{A < B}(R) \cup \rho_{A \rightarrow B, B \rightarrow A} (\sigma_{A > B}(R)) \) over a table \( R \) with attributes \( A, B \). Here, \( \sigma_\phi \) is relational selection of all tuples satisfying a predicate \( \phi \) and \( \rho_{A \rightarrow B, B \rightarrow A} \) is renaming. Thus, \( Q \) simply swaps the fields of records where \( A \geq B \), and leaves other records alone.

The first challenge is how to address elements of multisets reliably across different executions and support propagation of
addresses in the output backwards towards the input. Our solution
is to use a mildly enriched semantics in which multiset elements
carry explicit labels; that is, we view multisets of elements from \( X \)
as functions \( I \rightarrow X \) from some index set to \( X \). For example, if \( R \)
was labeled as follows and we use this enriched semantics to evaluate
the above query \( Q \) on \( R \), we get a result:

\[
R = \begin{array}{ccc}
1 & 2 & 3 \\
1 & 2 & 3 \\
r_1 & r_2 & r_3
\end{array}
\]

\[
Q(R) = \begin{array}{ccc}
1 & 2 & 3 \\
1 & 2 & 3 \\
r_1 & r_2 & r_3
\end{array}
\]

where in each case the \( id \) column contains a distinct index \( r_i \). In
\( Q(R) \), the first ‘1’ or ‘2’ in each index indicates whether the row
was generated by the left or right subexpression in the union (‘\( \cup \)’).

In general, we use sequences of natural numbers \( [i_1, \ldots, i_n] \in \mathbb{N}^n \)
as indices, and we maintain a stronger invariant: the set of indexes
used in a multiset must form a prefix code. We define a semantics
for NRC expressions over such collections that is fully determin-
istic and does not resort to generation of fresh intermediate labels;
in particular, the union operation adjusts the labels to maintain dis-
tinctness.

The second technical challenge involves extending patterns for
partial collections. In our previous work, any subexpression of a
value can be replaced by a hole. This works well in a conven-
tional functional language, where typical values (such as lists and
trees) are essentially initial algebras built up by structural induction.
However, when we consider unordered collections such as bags,
our previous approach becomes awkward.

For example, if we want to use a pattern to focus on only the
\( B \) field of the second record in query result \( Q(R) \), we can only
do this by deleting the other record values, and the smallest such
pattern is \( \{1, r_1\}, \{2, r_2\}, \{A, \emptyset\}, B:3, C:3, \} \). This is
tolerable if there are only a few elements, but if there are hundreds
or millions of elements and we are only interested in one, this is
a significant overhead. Therefore, we introduce enriched patterns
that allow us to replace entire subsets with holes, for example,
\( p' = \{2, r_2\} : (B:3, \emptyset) \cup \emptyset \). Enriched patterns are not just a
convenience; we show experimentally that they allow traces and
slices to be smaller (and computed faster) by an order of magnitude
or more.

1.2 Outline

The rest of this paper is structured as follows. Section 2 reviews
the (multiset-valued) Nested Relational Calculus and presents our trac-
ing semantics and deterministic labeling scheme. Section 3 presents
trace slicing, including a simple form of patterns. Section 4 shows
how to enrich our pattern language to allow for partial record and
partial set patterns, which considerably increase the expressiveness
of the pattern language, leading to smaller slices. Section 5 presents
the query slicing algorithm and shows how to compute differential
slices. Section 6 presents additional examples and discussion. Sec-
ction 7 presents our implementation demonstrating the benefits of
 laziness and enriched patterns for trace slicing. Section 8 discusses
related future work and Section 9 concludes.

Due to space limitations, and in order to make room for exam-

ple and high-level discussion, some (mostly routine) formal details
and proofs are relegated to the appendix.

2. Traced Evaluation for NRC

The nested relational calculus \([3]\) is a simply-typed core language
with collection types that can express queries on nested data similar
to those of SQL on flat relations, but has simpler syntax and cleaner
semantics. In this section, we show how to extend the ideas and
machinery developed in our previous work on traces and slicing for
functional languages \([2]\) to NRC. Developing formal foundations
for tracking provenance in the presence of unordered collections
presents a number of challenges not encountered in the functional
programming setting, as we will explain.

2.1 Syntax and Dynamic Semantics

Figure 1 presents the abstract syntax of NRC expressions, values,
and traces. The expression \( 0 \) denotes the empty collection, \( \{e\} \) con-
structs a singleton collection, and \( e_1 \cup e_2 \) takes the (multiset)
union of two collections. The operation \( \sum e \) computes the sum of a
collection of integers, while the predicate \( \emptyset e \) tests whether the
collection denoted by \( e \) is empty. Additional aggregation operations
such as count, maximum and average can easily be accommodated.
Finally, the comprehension operation \( \{x \mid e \} \) iterates over
the collection obtained by evaluating $e$, evaluating $e'(x)$ with $x$ bound to each element of the collection in turn, and returning a collection containing the union of all of the results. We sometimes consider pairs $(e_1, e_2)$, a special case of records $(\#1: e_1, \#2: e_2)$ using two designated field names $\#1$ and $\#2$. Many trace forms are similar to those for expressions; only the labels are shown.

Labels are sequences $\ell = [i_1, \ldots, i_n] \in \mathbb{N}^n$, possibly empty. The empty sequence is written $\epsilon$, and labels can be concatenated $\ell \cdot \ell'$; concatenation is associative. Record field names are written $A, B, A_1, A_2, \ldots$.

Values in NRC include constants $c$, which we assume include at least boolean and integers. Record field names are essentially partial functions from field names to values, written $(A_1 : v_1, \ldots, A_n : v_n)$. Collection values are essentially partial, finite-domain functions from labels to values, which we write $\{\ell_1, v_1, \ldots, \ell_n, v_n\}$. Since they denote functions, collections and records are identified up to reordering of their elements, and their field names or labels are always distinct. We write $\ell \cdot v$ for the operation that prepends $\ell$ to each of the labels in a set $v$, that is, $\ell \cdot \{\ell_1, v_1, \ldots, \ell_n, v_n\} = \{\ell \cdot \ell_1, v_1, \ldots, \ell \cdot \ell_n, v_n\}$.

Operations $f ::= + | - | \star | / | = | < | \leq | \cdots$

Expressions $e ::= c | f(e_1, \ldots, e_n) | \text{let } e = x \text{ in } e' | (A_1 : e_1, \ldots, A_n : e_n) | e.A | \text{if } (e, e', e'') | \emptyset | \{e\} | e_1 \cup e_2 | \bigcup (e' \mid x \in e)$

Labels $\ell ::= \ell' \cdot e | \emptyset$

Values $v ::= c | (A_1 : v_1, \ldots, A_n : v_n) | \emptyset | \{\ell_1, v_1, \ldots, \ell_n, v_n\}$

Environments $\gamma ::= \{x \mapsto v_1, \ldots, x_n \mapsto v_n\}$

Traces $T ::= \cdots | \text{if } (T, e', e'') \text{ or } T_2 | \text{if } (T', e', e'') \text{ or } T_2 | \{e\} \mid \bigcup (e' \mid x \in e) \mid \emptyset$

Trace Sets $\Theta ::= \{\ell_1, T_1, \ldots, T_n\}$

Types $\tau ::= \text{int} | \text{bool} | (A_1 : \tau_1, \ldots, A_n : \tau_n) | \{\tau\}$

Type Contexts $\Gamma ::= \{x_1 : \tau_1, \ldots, x_n : \tau_n\}$

Figure 1. NRC expressions, values, traces, and types.

Other operations on labels and labeled collections will be introduced in due course.

The labels on the elements of a collection provide us with a persistent address for a particular element of the collection. This capability is essential when asking and answering provenance queries about parts of the source or output data, and when tracking fine-grained dependencies.

Both expressions and traces are subject to a type system. NRC types include collection types $\{\tau\}$ which are often taken to be sets, bags (multisets), or lists, though in this paper, we consider multiset collections only. However, types do not play a significant role in this paper so the typing rules are omitted. For expressions, the typing judgment $\Gamma \vdash e : \tau$ is standard and the typing rules for trace well-formedness $\Gamma \vdash T : \tau$ are presented in Appendix A.

Traced evaluation. NRC traces include a trace form corresponding to each of the expressions described above. The structure of the traces is best understood by inspecting the typing rules (Figure 1) and the traced evaluation rules (Figure 2), which define a judgment $\gamma, e \Downarrow v, T$ indicating that evaluating an expression $e$ in environment $\gamma$ yields a value $v$ and a trace $T$. We assume an environment $\Sigma$ associating constants and function symbols with their types, and write $f \Downarrow v$ for the semantic operations corresponding to $f$, or $+$ for the semantical operations corresponding to $+$ and so on. In most cases, the trace form is similar to the expression form; for example the trace of a constant or variable is a constant and so on. The traced evaluation rules for conditionals illustrate that traces is a trace of the conditional test, the trace of a primitive operation $f(e_1, \ldots, e_n)$ is a primitive operation trace $f(T_1, \ldots, T_n)$ applied to the traces $T_i$ of the arguments $e_i$, the trace of a record expression is a trace record constructor $(A_1 : T_1, \ldots, A_n : T_n)$, and the trace of a field projection $e.A$ is a trace $T.A$. Also, the trace of a let-binding is a let-binding trace $let \ x = T_1 \ in \ T_2$, where $x$ is bound in $T_2$. In these cases, the traces mimic the expression structure.

The traced evaluation rules for conditionals illustrate that traces differ from expressions in recording control flow decisions. The trace of a conditional is a conditional trace $\text{if } (T, e_1, e_2) \Downarrow T'$ where $T$ is the trace of the conditional test, $b$ is the Boolean value of the test $e_1$, and $T'$ is the trace of the taken branch. The expressions $e_1$ and $e_2$ are not strictly necessary but retained to preserve structural similarity to the original expression.

The trace of $\emptyset$ is a constant trace $\emptyset$. To evaluate a singleton-collection constructor $\{e\}$, we evaluate $e$ to obtain a value $v$ and return the singleton $\{e.v\}$ with empty label $c$. We return the sin-
There exists code that when no element of disjoint prefix code. Similarly, we say that a trace is prefix-labeled if every such that for every \( y \) and \( y' \) with \( y 
less 
less y' \), \( \Theta \) evaluate \( e' \) repeatedly with \( x \) bound to each element \( v_i \) of the collection \( v \) to get resulting values \( v'_i \) and corresponding traces \( T' \). We return a new collection \( v' = \{ \ell_1 \cdot v'_1, \ldots, \ell_n \cdot v'_n \} \); similarly we return a labeled set of traces \( \Theta = \{ \{ \ell_1, T_1 \}, \ldots, \ell_n, T_n \} \). (Analogously to values, trace sets are essentially finite partial functions from labels to traces). For each of these collections, we prepend the appropriate label \( \ell_i \) of the corresponding input element.

A technical point of note is that the resulting trace \( T_1 \) may contain free occurrences of \( x \). As in our trace semantics for functional programs, these variables serve as markers in \( T_1 \) that will be critical for the trace replay semantics. The comprehension trace records, using the notation \( \bigcup \{ e' \mid x \in e \} \supset \{ \ell_1, T_1, \ldots, \ell_n, T_n \} \), that the trace \( T \) was used to compute a multiset \( v \) and \( x \) was bound to each element \( \ell_i, v_i \) in \( v \) in turn, with trace \( T_1 \) showing how the corresponding subset of the result was computed. The comprehension trace also records the expression \( e' \) and bound variable \( x \), which are again not strictly necessary but preserve the structural similarity to the original expression.

At this point it is useful to provide some informal motivation for the labeling semantics, compared for example to other semantics that use annotations or labels as a form of provenance. We do not view the labels themselves as provenance; instead, they provide a useful infrastructure for traces, which do capture a form of provenance. Moreover, by calculating the label of each part of an intermediate or final result deterministically (given the labels on the input), we provide a way to reliably refer to parts of the output, which otherwise may be unaddressable in a multiset-valued semantics. This is essential for supporting compositional slicing for operations such as let-binding or comprehension, where the output of one subexpression becomes a part of the input for another.

A central point of our semantics is that evaluation preserves the property that labels uniquely identify the elements of each multiset. This naturally assumes that the labels on the input collections are distinct. In fact, a stronger property is required: evaluation preserves the property that sets labels form a prefix code. In the following, we write \( x \leq y \) to indicate that sequence \( x \) is a prefix of sequence \( y \).

**Definition 2.1.** A prefix code over \( \Sigma \) is a set of sequences \( L \subseteq \Sigma^* \) such that for every \( x, y \in L \), if \( x \leq y \) then \( x = y \). A sub-prefix code of a prefix code \( L \) is a prefix code \( L' \) such that for all \( x \in L \) there exists \( y \in L' \) such that \( y \leq x \). We write \( L' \leq L \) to indicate that \( L' \) is a sub-prefix code of \( L \). We say that \( L \) and \( L' \) are prefix-disjoint when no element of \( L \) is a prefix of an element of \( L' \) and vice versa.

Let \( v \) be a collection \( v = \{ \ell_1, v_1, \ldots, \ell_n, v_n \} \). We define the domain of \( v \) to be \( \text{dom}(v) = \{ \ell_1, \ldots, \ell_n \} \). We say that a value or value environment is prefix-labeled if for every collection \( v \) occurring in it, the labels \( \ell_i, v_i \) are distinct and \( \text{dom}(v) \) is a prefix code. Similarly, we say that a trace is prefix-labeled if every labeled trace set \( \Theta = \{ \ell_1, T_1, \ldots, \ell_n, T_n \} \) is prefix-labeled.

**Theorem 2.2.** If \( \gamma \) is prefix-labeled and \( \gamma, e \nless \nless v, T \) then \( v \) and \( T \) are both prefix-labeled. Moreover, if \( \gamma \) and \( v \) are prefix-labeled and \( \gamma, x \in v, e \nless v', \Theta \) then \( v' \) and \( \Theta \) are prefix-labeled, and in addition \( \text{dom}(\Theta) = \text{dom}(v) \leq \text{dom}(v') \).

**Proof.** By induction on derivations. The key cases are those for union, which is straightforward, and for comprehensions. For the latter case we need the second part, to show that whenever \( \gamma \) and \( v \) are prefix-labeled, if \( \gamma, x \in v, e \nless v', \Theta \) then \( v' \) and \( \Theta \) are prefix-labeled, and in addition \( \text{dom}(\Theta) = \text{dom}(v) \) and \( \text{dom}(v) \) is a sub-prefix code of \( \text{dom}(v') \).

The prefix code property is needed later in the slicing algorithms, when we will need it to match elements of collections produced by comprehensions with corresponding elements of the trace set \( \Theta \). From now on, we assume that all values, environments, and traces are prefix-labeled, so any labeled set is assumed to have the prefix code property.

We will use the following query as a running example,

\[
Q = \bigcup \{ \text{if}(x.B = 3, \{ \{A.x.A, B; x.C \}, \}) | \ x \in R \}
\]

This is a simple selection query; it identifies records in \( R \) that have \( B \)-value of 3, and returns record \( \{A.x.A, B; x.C \} \) containing \( x \)'s \( A \) value and its \( C \) value renamed to \( B \). The result of \( Q \) on the input \( R \) in the introduction is \( Q(R) = \{ \{r_2\}.\{A; 2, B; 8\}, \{r_3\}.\{A; 4, B; 9\} \} \). In particular, the query has two subexpressions, \( r_1 \) and \( r_2 \), that are both prefix-disjoint.
where _ indicates omitted (easily inferable) subexpressions.

**Replay** We introduce a judgment \( \gamma, T \vdash \nu \) for replaying a trace on a (possibly different) environment \( \gamma \). The rules for replaying NRC traces are presented in Figure 3. Many of the rules are straightforward or analogous to the corresponding evaluation rules. Here we only discuss the replay rules for conditional and comprehension traces.

For the conditional rules, the basic idea is as follows. If replaying the trace \( T \) of the test yields the same boolean value \( b \) as recorded in the trace, we replay the trace of the taken branch. If the test yields a different value, then replay fails.

To replay a comprehension trace \( \bigcup \{ [e \mid x \in T] \} \vdash \Theta \), rule RCOMP first replays trace \( T \) to update the set of elements \( v \) over which we will iterate. We define a separate judgment \( \gamma, x \in v, \Theta \vdash \nu, v' \) to iterate over set \( v \) and replay traces on the corresponding elements. For elements \( \ell_i \in \text{dom}(\Theta) \), we replay the corresponding trace \( \Theta(\ell_i) \). Replay fails if \( v \) contains any labels not present in \( \Theta \).

Replaying a trace can fail if either the branch taken in a conditional test differs from that recorded in the trace, or the intermediate set obtained from rerunning a comprehension trace includes values whose labels are not present in the trace. This means, in particular, that changes to the input can be replayed if they only change base values or delete set elements, but changes leading to additions of new labels to sets involved in comprehensions typically cannot be replayed.

Returning to the running example, suppose we change field \( B \) of row \( r_1 \) of \( R \) from 2 to 5. This change has no effect on the control flow choice taken in \( Q \), and replaying the trace \( T \) succeeds. Likewise, changing the \( A \) or \( C \) field of any column of \( R \) has no effect, since these values do not affect the control flow choices in \( T \). However, changing the \( B \) field of a row to 3 (or changing it from 3 to something else) means that replay will fail.

### 2.2 Key properties

Before moving on to consider trace slicing, we identify some properties that formalize the intuition that traces are consistent with and faithfully record execution.

**Proposition 2.3 (Determinacy).** If \( \gamma, e \Downarrow \nu, T \) and \( \gamma, e \Downarrow \nu', T' \) then \( \nu = \nu' \) and \( T = T' \). If \( \gamma, T \vdash \nu \) and \( \gamma', T \vdash \nu' \) then \( \nu = \nu' \).

When the trace is irrelevant, we write \( \gamma, e \Downarrow \nu \) to indicate that \( \gamma, e \Downarrow \nu, T \) for some \( T \).

**Traced evaluation is type-safe and produces well-typed traces, and trace replay is also type-safe.**

**Theorem 2.4.** If \( \gamma : \Gamma \vdash e : \tau \) and \( \gamma, e \Downarrow \nu, T \) then \( \nu : \tau \) and \( \Gamma \vdash T : \tau \). If \( \gamma : \Gamma \vdash T : \tau \) and \( \gamma, T \vdash \nu \) then \( \nu : \tau \).

Traces can be represented using pointers to share common subexpressions; using this DAG representation, traces can be stored in space polynomial in the input. (This sharing happens automatically in our implementation in Haskell.)

**Proposition 2.5.** For a fixed \( e \), if \( \gamma, e \Downarrow \nu, T \) then the sizes of \( \nu \) and of the DAG representation of \( T \) are at most polynomial in \(|\gamma|\).

**Proof.** Most cases are straightforward. The only non-trivial case is for comprehensions, where we need a stronger induction hypothesis: if \( \gamma, x \in v, e \Downarrow^* v', \Theta \) then the sizes of \( v' \) and of the DAG representation of \( \Theta \) are at most polynomial in \(|\gamma|\).

Furthermore, traced evaluation produces a trace that replays to the same value as the original expression run on the original environment. We call this property **consistency**.

**Proposition 2.6 (Consistency).** If \( \gamma, e \Downarrow \nu, T \) then \( \gamma, T \vdash \nu \).

Finally, trace replay is faithful to ordinary evaluation in the following sense: if \( T \) is generated by running \( e \) in \( \gamma \) and we successfully replay \( T \) on \( \gamma' \) then we obtain the same value (and same trace) as if we had run \( e \) from scratch in \( \gamma' \), and vice versa.

**Proposition 2.7 (Fidelity).** If \( \gamma, e \Downarrow \nu, T \), then for any \( \gamma', \nu' \) we have \( \gamma', e \Downarrow \nu', T' \) if and only if \( \gamma', T \vdash \nu' \).

Observe that consistency is a special case of fidelity (with \( \gamma' = \gamma, \nu' = \nu \)). Moreover, the “if” direction of fidelity holds even though replay can fail, because we require that \( \gamma', e \Downarrow \nu', T \) holds for the *same* trace \( T \). If \( \gamma', e \Downarrow \nu', T' \) is derivable but only for a different trace \( T' \), then replay fails.

### 3. Trace Slicing

The goal of the trace slicing algorithm we consider is to remove information from a trace and input that is not needed to recompute a part of the output. To accommodate these requirements, we introduce traces and values with holes and more generally, we consider **patterns** that represent relations on values capturing possible changes. In this section, we limit attention to pairs, and consider slicing for a class of **simple** patterns. We consider records and more expressive **enriched** patterns in the next section.

We extend traces with holes \( \square \)

\[
T ::= \cdots \square \cdots
\]

and define a subtrace relation \( \sqsubseteq \) that is essentially a syntactic precongregation on traces and trace sets such that \( \square \sqsubseteq T \) holds and \( T \sqsubseteq T' \) implies \( T \sqsubseteq T' \).

The syntax of **simple patterns** \( p \), **set patterns** \( \text{sp} \), and **pattern environments** \( \rho \) is:

\[
\begin{align*}
p & ::= \square \mid \diamond \mid e \mid \{p_1, p_2\} \mid \text{sp} \\
\text{sp} & ::= \emptyset \mid \{\ell_1, p_1, \ldots, \ell_n, p_n\} \\
\rho & ::= \{x_1 \mapsto p_1, \ldots, x_n \mapsto p_n\}
\end{align*}
\]

Essentially, a pattern is a value with holes in some positions. The meaning of each pattern is defined through a relation \( \equiv_p \) that says when two values are equivalent with respect to a pattern. This relation is defined in Figure 5. A hole \( \square \) indicates that the part of the value is unimportant, that is, for slicing purposes we don’t care about that part of the result. Its associated relation \( \equiv\circ \) relates any two values. An **identity pattern** \( \diamond \) is similar to a hole: it says that the value is important but its exact value is not specified, and its associated relation \( \equiv\circ \) is the identity relation on values. Complete set patterns \( \{\ell_1, p_1, \ldots, \ell_n, p_n\} \) specify the labels and patterns for all of the elements of a set; that is, such a pattern relates only sets that have exactly the labeled elements specified and whose corresponding values match according to the corresponding patterns.

We define the union of two set patterns as \( \{\ell, p\} \cup \{\ell', p'\} = \{\ell, p\} \cup \{\ell', p'\} \) provided their domains \( \ell_i \) and \( \ell'_j \) are prefix-disjoint. We define a (partial) least upper bound operation on patterns \( p \sqcup p' \) such that for any \( v, v' \) we have \( v \equiv_{p \sqcup p'} v' \) if and only if \( v \equiv_p v' \) and \( v \equiv_{p'} v' \). The full definition is shown in Figure 5.

We define the partial ordering \( p \sqsubseteq p' \) as \( p \sqsubseteq p' = p' \). We say that a value \( v \) **matches** pattern \( p \) if \( p \sqsubseteq v \). Observe that this implies \( v \equiv_{p} v \). We extend the **union** and **intersection** operations to pattern environments \( \rho \) pointwise, that is, \( (\rho \sqcup \rho')(x) = \rho(x) \sqcup \rho'(x) \).

We define several additional operations on patterns that are needed for the slicing algorithm. Consider the following singleton
\[ \Box \cup p = p \quad \Diamond \cup p = p \quad C \cup c = c \]
\[ \{p_1, p_2\} \cup \{p'_1, p'_2\} = \{p_1 \cup p'_1, p_2 \cup p'_2\} \]
where:
\[ \Diamond \left[ \overline{\Box} \right] = \overline{\Diamond} \left[ \overline{\Box} \right] = \Diamond \]
\[ \{p_1, p_2\} \left[ \overline{\Box} \right] = \{p_1 \left[ \overline{\Box} \right], p_2 \left[ \overline{\Box} \right] \} \]
\[ \{p_1, p_2\} \left[ \overline{\Box} \right] = \{p_1 \left[ \overline{\Box} \right], p_2 \left[ \overline{\Box} \right] \} \]

Figure 4. Least upper bound for simple patterns

\[ v \equiv_p v' \]
\[ \llbracket \Box \rrbracket = \overline{\ell} \quad \llbracket \overline{\Box} \rrbracket = \overline{\ell} \quad C \equiv_c C \]
\[ \llbracket \ell. v \rrbracket = \llbracket \ell'. v' \rrbracket \]
\[ \llbracket v_1 \rrbracket = p_1 \quad \llbracket v_1 \rrbracket = p_2 \quad \llbracket v_1 \rrbracket = p_2 \quad \llbracket v_1 \rrbracket = p_2 \]
\[ \{\ell_1, v_1, \ldots, \ell_n, v_n\} \llbracket \{\ell_1, v_1, \ldots, v_n\} \]
\[ \gamma \equiv_p \gamma' \iff \forall x \in \text{dom}(\rho). \gamma(x) \equiv_{\rho(x)} \gamma'(x) \]

Figure 5. Simple pattern equivalence.

\[ v \equiv_{\rho} v' \]
\[ v \equiv_{\Box} v' \quad v \equiv_{\overline{\Box}} v' \quad C \equiv_c C \quad v_1 \equiv_{p_1} v_1' \quad v_1 \equiv_{p_2} v_2' \]
\[ \llbracket \ell. v \rrbracket = \llbracket \ell'. v' \rrbracket \]
\[ \llbracket v_1 \rrbracket = p_1 \quad \llbracket v_1 \rrbracket = p_2 \quad \llbracket v_1 \rrbracket = p_2 \quad \llbracket v_1 \rrbracket = p_2 \]

These operations are only used for the above cases; they have no effect on constant or pair patterns. For sets, \( p[\ell] \) extracts the subset of \( p \) whose labels start with \( \ell \), truncating the initial prefix \( \ell \), while if \( p \equiv \Box \) or \( \Box \) then again \( p[\ell] \) returns the same kind of hole. Moreover, \( \text{dom}(p[\ell]) \) is a prefix code if \( \text{dom}(p) \) is.

Suppose \( L \) is a prefix code. We define restriction of a set pattern \( p \) to \( L \) as follows:
\[ \llbracket \ell. p \rrbracket = \{ \ell'. v \in p : \ell \in L \} \quad \llbracket \Box. l \rrbracket = \Box \quad \llbracket L \rrbracket = \Box \]

It is easy to see that \( \text{dom}(p[\ell] \subseteq \text{dom}(p) \) so \( \text{dom}(p)[\ell] \) is also a prefix code if \( \text{dom}(p) \) is, so this operation is well-defined on collections.

**Lemma 3.1.** If \( sp \) is prefix-labeled and \( L \) is a prefix code then \( \llbracket p \rrbracket \) and \( \llbracket sp \rrbracket \) are prefix-labeled.

**Backward Slicing** The rules for backward slicing are given in Figure 6. The judgment \( p, T \searrow p, T' \) slices trace \( T \) with respect to a pattern \( p \) to yield the slice \( T' \) and sliced input environment \( p \). The sliced input environment records what parts of the input are needed to produce \( p \); this is needed for slicing operations such as let-binding or comprehensions. The main new ideas are in the rules for collection operations, particularly comprehensions. The slicing rules \( S\text{CONST}, S\text{PRIM}, S\text{VAR}, S\text{LET}, S\text{PAIR}, S\text{PROJ}, \) and \( S\text{IP} \) follow essentially the same idea as in our previous work [1][25]. We focus discussion on the new cases, but we review the key ideas for these operations here in order to make the presentation self-contained.

The rules for collections use labels and set pattern operations to effectively undo the evaluation of the set pattern. The rule \( S\text{EMPTY} \) is essentially the same as the constant rule. The rule \( S\text{SNG} \) uses the singleton extraction operation \( p.e \) to obtain a pattern describing the single element of a singleton set value matching \( p \). The rule \( S\text{UNION} \) uses the two projections \( p[1] \) and \( p[2] \) to obtain the patterns describing the subsets obtained from the first and second substructures in the union pattern, respectively.

The rule \( S\text{COMP} \) uses a similar idea to let-binding. We slice the trace set \( \Theta \) using an auxiliary judgment \( p, x, \Theta \searrow p, \Theta, p_0 \) obtaining a sliced input environment, sliced trace set \( \Theta, p_0 \), and pattern \( p_0 \) describing the set of values to which \( x \) was bound. We then use \( p_0 \) to slice backwards through the subtrace \( T \) that constructed the set. The auxiliary slicing judgment for trace sets has three rules: a trivial rule \( S\text{EMP} \) when the set is empty, rule \( S\text{SSG} \) that uses label projection \( p[\ell] \) to handle a singleton trace set, and a rule \( S\text{UNION} \) handling larger trace sets by decomposing them into subsets. This is essentially a structural recursion over the trace set, and is deterministic even though the rules can be used to decompose the trace sets in many different ways, because \( \searrow \) is associative. Rule \( S\text{UNION} \) also requires that we restrict the set pattern to match the domains of the corresponding trace patterns.

The slicing rules \( S\text{SUM} \) and \( S\text{EMP} \) follow the same idea as for primitive operations at base type: we require that the whole set value be preserved exactly. As discussed by Perera et al. [27] with primitive operations, this is a potential source of overapproximation, since (for example) for an emptiness test, all we really need is to preserve the number of elements in the set, not their values. The last rule shows how to slice pair patterns when the pattern is \( \Box \); we slice both of the subtraces by \( \Box \) and combine the results.

It is straightforward to show that the slicing algorithm is well-defined for consistent traces. That is, if \( \gamma, T \searrow v \) and \( p \subseteq v \) then there exists \( \rho, S \) such that \( p, T \searrow \rho, S \) holds, where \( \rho \subseteq \gamma \) and \( S \subseteq T \). We defer the correctness theorem for slicing using simple patterns to the end of the next section, since it is a special case of correctness for slicing using enriched patterns.

Continuing our running example, consider the pattern \( p = \{ \ell_2, \ell_4, A : \emptyset, B : S, r_3, \emptyset \} \). The slice of \( T \) with respect to this pattern is of the form:
\[ T' = \bigcup \{ \ell. x \in R \} \]
\[ r_1, \emptyset \] \[ r_2, \Theta \]
\[ r_3, \emptyset \]
and the slice of \( R \) is \( R' = \{ r_1, \emptyset, r_2, \Theta, A : \emptyset, B : 3, C : 8, r_3, \emptyset \} \).

This is awkward, as we already can observe in our running example above: to obtain a slice describing how one record was computed, we need to use a set pattern that lists all of the indexes in the output. Moreover, the slice with respect to such a pattern may also include labeled subtraces explaining why the other elements exist in the output (and no others). This information seems intuitively irrelevant to the value at \( \ell_1 \), and can be a major overhead if the collection is large. We also have considered only binary pairs; it would be more convenient to support record patterns directly.

**4. Enriched Patterns**

So far we have considered only complete set patterns of the form \( \{ \ell_1, p_1, \ldots, \ell_n, p_n \} \). These patterns relate pairs of values that have exactly \( n \) elements labeled \( \ell_1, \ldots, \ell_n \), each of which matches \( p_1, \ldots, p_n \) respectively.

This is awkward, as we already can observe in our running example above: to obtain a slice describing how one record was computed, we need to use a set pattern that lists all of the indexes in the output. Moreover, the slice with respect to such a pattern may also include labeled subtraces explaining why the other elements exist in the output (and no others). This information seems intuitively irrelevant to the value at \( \ell_1 \), and can be a major overhead if the collection is large. We also have considered only binary pairs; it would be more convenient to support record patterns directly.
In this section we sketch how to enrich the language of patterns to allow for partial set and partial record patterns, as follows:

\[
p ::= \Box | \lozenge | c | s | p \lor p
\]

\[
sp ::= () | (A_i : p_i) | (A_i : p_i) \lor (A_i : p_i) \lor \Box
\]

\[
rp ::= () | (\Box : p_1) | (\Box : p_1) \lor (\Box : p_1)
\]

Record patterns are of the form \((A_i : p_i)\), listing the fields and the patterns they must match, possibly followed by \(\Box\) or \(\lor\), which the remainder of the record must match. The pattern \((\Box : p_1) \lor \Box\) stands for a set with labeled elements matching patterns \(p_1\) and \(p_1\) plus any additional elements whose values we don’t care about. For example, we can use the pattern \(\{\ell_1 : p_1\} \lor \Box\) to express interest in why element \(\ell_1\) matches \(p_1\), when we don’t care about the rest of the set. The second partial pattern, \((\Box : p_1) \lor \Box\), has similar behavior, but it says that the rest of the set being considered must be equal. For example, \(\{\ell, \Box\} \lor \Box\) says that the two sets are equal except possibly at label \(\ell\). This pattern is needed mainly in order to ensure that we can define a least upper bound on enriched patterns, since we cannot express \(\{\ell_1 : p_1, \ldots, \ell_n : p_n\} \lor \Box\) unless we know all of the labels are equal.

We define \(\text{dom}(\{\ell_i : p_i\} \lor \Box) = \text{dom}(\{\ell_i : p_i\} \lor \Box) = \{\ell_1, \ldots, \ell_n\}\). Disjoint union of enriched patterns \(sp \lor sp'\) is defined only if the domains are prefix-disjoint, so that the labels of the result still form a prefix code; this definition is in Figure 7.

We now extend the definitions of \(\lor / \lor\) and \(\lor\) to account for extended patterns. We extend the \(\lor / \lor\) substitution operation as follows:

\[
\begin{align*}
(A_i : p_i) \lor / \lor & = (A_i : p_i) \lor / \lor \\
(A_i : p_i) \lor / \lor & = (A_i : p_i) \lor / \lor \\
((\ell_i : p_i) \lor \Box) \lor / \lor & = (\ell_i : p_i) \lor / \lor \\
((\ell_i : p_i) \lor \Box) \lor / \lor & = (\ell_i : p_i) \lor / \lor \\
((\ell_i : p_i) \lor \Box) \lor / \lor & = (\ell_i : p_i) \lor / \lor \\
((\ell_i : p_i) \lor \Box) \lor / \lor & = (\ell_i : p_i) \lor / \lor
\end{align*}
\]

We handle the additional case of the \(\lor\) operation in Figure 8 and extend the \(~_p\) relation as shown in Figure 9. Note that taking the least upper bound of a partial pattern with a complete pattern yields a complete pattern, while taking the least upper bound of partial patterns involving \(\Box\) again relies on the \(\lor / \lor\) substitution operation.

\[
\begin{align*}
\Diamond, T_1 \downarrow p_1, S_1 & \quad \cdots \quad \Diamond, T_n \downarrow p_n, S_n & \text{Sprim} & \quad p, x \downarrow [x \mapsto p], x \\
\Diamond(p(T_1), \ldots, T_n) \downarrow p_1 \lor \cdots \lor p_n, f(S_1, \ldots, S_n) & \text{Slet} & \quad p, \ell \in \#1 \lor p, \ell. \#1 & \text{Sproc1}
\end{align*}
\]

\[
\begin{align*}
\Diamond(p(T_\#1), T_\#1) \downarrow p, T & \text{Sprim} & \quad p, x \downarrow [x \mapsto p], x \\
\Diamond(p, T_\#1) \downarrow p, T & \text{Slet} & \quad p, \ell \in \#1 \lor p, \ell. \#1 & \text{Sproc1}
\end{align*}
\]
Lemma 4.1

Let $\Theta, T$ be enriched patterns. Suppose $\Theta \cup \{A_p: \square\}$ in the case for a field projection trace. The added rules $\text{SHOLE}^*$ and $\text{SDIAMOND}^*$ handle the possibility that a partial pattern reduces to $\square$ or $\square$ through projection; we did not need to handle this case earlier because a simple set pattern is either a hole (which could be handled by the rule $\square$, $T \cup \{A_p: \square\}$ or a complete set pattern showing all of the labels of the result.

Both simple and extended patterns satisfy a number of lemmas that are required to prove the correctness of trace slicing.

Lemma 4.1 (Properties of union and restriction).

Figure 8. Least upper bound for enriched patterns (excluding some symmetric cases).

Figure 9. Enriched pattern equivalence.

Figure 10. Backward trace slicing over enriched patterns.

1. If $p_1 \subseteq v_1$ and $p_2 \subseteq v_2$ and $v_1 \cup p_1 \cup p_2 \subseteq v_2 \cup v_1$ then $v_1 \cup p_1 \cup p_2 = v_1 \cup v_2$ provided all of these disjoint unions are defined.

2. If $p \subseteq \{v_1 \cup p_1 \cup p_2 \subseteq v_1 \cup v_2 \}$ and $L_1 \leq \text{dom}(v_1)$ and $L_2 \leq \text{dom}(v_2)$ then $p_{|L_1} \subseteq v_1$ and $p_{|L_2} \subseteq v_2$.

Lemma 4.2 (Projection and $\subseteq$).

1. If $p \subseteq \{v.e\}$ then $p.e \subseteq v$.

2. If $p \subseteq \{v_1 \cup v_2 \}$ then $p[1] \subseteq v_1$ and $p[2] \subseteq v_2$.

3. If $p \subseteq \{v \}$ then $p[\ell \cdot v \subseteq v]$.

4. If $p \subseteq \{v_1 \}$ then $p.A_{v_1}$.

Lemma 4.3 (Projection and $\sim_p$).

1. If $p \subseteq \{v.e\}$ and $v \sim_p v'$ then $v.e \sim_p \{v'.e\}$.

2. If $p \subseteq \{v_1 \cup v_2 \}$ and $v_1 \sim_p \{v_1\} v'_1$ and $v_2 \sim_p \{v_2\} v'_2$ then $1 \cdot v_1 \cup 2 \cdot v_2 \sim_p 1 \cdot v_1 \cup v'_2 \sim_p v_2 \cdot v'$.

3. If $p \subseteq \{v \cdot v \}$ and $v \sim_p v'$ then $v \cdot v \sim_p \{v'.e\}$.

4. If $p \subseteq \{v_1 \}$ and $v_1 \sim_p \{v_1 \}$, then $v_1 \sim_p \{v_1 \}$.

Proofs are collected in Appendix B.

We now state the key correctness property for slicing. Intuitively, it says that if we slice $T$ with respect to output pattern $p$, obtaining a slice $\rho$ and $S$, then $\rho$ will be reproduced on recomputation under any change to the input and trace that is consistent with the slice — formally, that means that the changed trace $T'$ must match the sliced trace $S$, and the changed input $\gamma'$ must match $\gamma$ modulo $\rho$.

Theorem 4.4 (Correctness of Slicing).

1. Suppose $\gamma, T \gamma \cup \{v.e\}$ and $p \subseteq \{v \}$ and $T \gamma \cup \{v \} p, S$. Then for all $\gamma' \sim_p \gamma$ and $T' \gamma' \cup \{v \} p, S$.

2. Suppose $\gamma, x \in v_0, \Theta \gamma \cup \{v \}$ and $p \subseteq \{v \}$ and $p, x, \Theta_0 \gamma$ and $\Theta_0, \Theta_0 \gamma$ where $\Theta_0 \subseteq \Theta$. Then for all $\gamma' \sim_p \gamma$ and $v_0 \sim_p v_{v_0}$ and $\Theta' \gamma' \cup \{v \} p, S$ such that $\gamma', x \in v_0, \Theta' \gamma' \cup \{v \} p, S$.

Returning to our running example, we can use the enriched pattern $p' = \{v_{r_1}, v_{B:3}: \square\}$ in $\square$ to indicate interest in the $B$ field of $r_2$, without naming the other fields of the row or the other row indexes. Slicing with respect to this pattern yields the following slice:

$$T'' = \bigcup \{x: x \in R \} \cup \{x, B:3 = 3, x.a = \text{true}(x)\}$$

and the slice of $R$ is $R'' = \{v_{r_1}: (B:3, C:8, \square)\}$. This indicates that (as before) the values of $r_1$ and $r_3$ and of the $A$ field of $r_2$
are irrelevant to \( r_2 \) in the result; unlike \( T' \), however, we can also potentially replay if \( r_1 \) and \( r_3 \) have been deleted from \( R \). Likewise, we can replay if the \( A \) field has been removed from a record, or if some other field such as \( D \) is added. This illustrates that enriched patterns allow for smaller slices than simple patterns, with greater flexibility concerning possible updates to the input.

A natural question is whether slicing computes the (or a) smallest possible answer. Because our definition of correct slices is based on recomputation, minimal slices are not computable, by a straightforward reduction from the undecidability of minimizing dependency provenance \([1, 12]\).

5. Query and Differential Slicing

We now adapt slicing techniques to provide explanations in terms of query expressions, and show how to use differences between slices to provide precise explanations for parts of the output.

5.1 Query slicing

Our previous work \([27]\) gave an algorithm for extracting a program slice from a trace. We now adapt this idea to queries. A trace slice shows the parts of the trace that need to be replayed in order to compute the desired part of the output; similarly, a query slice shows the part of the query expression that is needed in order to ensure that the desired part of the output is recomputed. As with traces, we allow holes \( \Box \) in programs to allow deleting subexpressions, and define \( \Box \) as a syntactic precongruence such that \( \Box \subseteq e \). We also define a least upper bound operation \( e \sqcup e' \) on partial query expressions in the obvious way, so that \( \Box \sqcup e = e \).

We define a judgment \( p, T \Downarrow \rho, e \) that traverses \( T \) and "unevaluates" \( p \), yielding a partial input environment \( \rho \) and partial program \( e \). The rules are illustrated in Figure 11. Many of the rules are similar to those for trace slicing; the main differences arise in the cases for conditionals and comprehensions, where we collapse the sliced expressions back into expressions, possibly inserting holes or merging sliced expressions obtained by running the same code in different ways (as in a comprehension that contains a conditional).

Again, it is straightforward to show that if \( \gamma, e \not\Downarrow v, T \) and \( p \not\Downarrow \rho \) then there exist \( \rho, e' \) such that \( p, T \Downarrow \rho, e' \), where \( \rho \supseteq \gamma \) and \( e' \equiv e \). The essential correctness property for query slices is similar to that for trace slices: again, we require that rerunning any sufficiently similar query on a sufficiently similar input produces a result that matches \( p \). The proof of this result is in Appendix D.

**Theorem 5.1** (Correctness of Query Slicing).

1. Suppose \( \gamma, T \not\Downarrow v \) and \( p \not\Downarrow v \) and \( p, T \Downarrow \rho, e, e' \). Then for all \( \gamma' \equiv \rho, \gamma \) and \( e' \equiv e \) such that \( \gamma', \gamma' \Downarrow v' \) we have \( v' \Downarrow e, e' \).

2. Suppose \( \gamma, x \in v_0, \Theta \not\Downarrow v \) and \( p, \Theta \Downarrow \rho, \rho_0, p_0 \).

Then for all \( \gamma' \equiv \rho, \gamma \) and \( e' \equiv e \) such that \( \gamma', \gamma' \Downarrow v' \) we have \( v' \Downarrow e, e' \).

Combining with the consistency property (Proposition 2.4), we have:

**Corollary 5.2.** Suppose \( \gamma, e \Downarrow v \), \( T \not\Downarrow v \) and \( \rho, e, e' \). Then for all \( \gamma' \equiv \rho, \gamma \) and \( e' \equiv e \) such that \( \gamma', \gamma' \Downarrow v' \), we have \( v' \Downarrow e, e' \).

Continuing our running example, the query slice for the pattern \( p' \) considered above is

\[
Q' = \{ \{ t(x, B = 3, \{ (A: \Box, B:B), C \}), \{ \} \} \mid x \in R \}
\]

since only the computation of the \( A \) field in the output is irrelevant to \( p' \).

5.2 Differential slicing

We consider a pattern difference to be a pair of patterns \( (p, p') \) where \( p \not\subseteq p' \). Intuitively, a pattern difference selects the part of a value present in the outer component \( p' \) and not in the inner component \( p \). For example, the pattern difference \((\{B: \Box, \}, \{B: 8; \Box\})\) selects the value \( 8 \) located in the \( B \) component of a record. We can also write this difference as \( \langle B, 8; \Box \rangle \), using \( \Box \) to highlight the boundary between the inner and outer pattern. Trace and query pattern differences are defined analogously.

![Figure 11. Unevaluation (selected rules).](image-url)
It is straightforward to show by induction that slicing is monotonic in both arguments:

**Lemma 5.3 (Monotonicity).** If \( p \subseteq p' \) and \( T \subseteq T' \) and \( p', T' \setminus T \subseteq p, S \) then there exist \( p, S \) such that \( p \setminus T \subseteq p, S \) and \( p \subseteq p' \) and \( S \subseteq S' \). In addition, \( p, S \subsetneq p, S \).

This implies that given a pattern difference and a trace, we can compute a trace difference using the following rule:

\[
(p_{2}, T \setminus p_{2}, S_{2}) \setminus (p_{1}, T \setminus p_{1}, S_{1}) = (p_{2}, T \setminus p_{2}, S_{2})
\]

It follows from monotonicity that \( p_{1} \subseteq p_{2} \) and \( S_{1} \subseteq S_{2} \), thus, pattern differences yield trace differences. Furthermore, the second part of monotonicity implies that we can compute the smaller slice \( S_{1} \) from the larger slice \( S_{2} \), rather than re-traverse \( T \). It is also possible to define a simultaneous differential slicing judgment, as an optimization to ensure we only traverse the trace once.

Query slicing is also monotone, so differential query slices can be obtained in exactly the same way. Revisiting our running example one last time, consider the differential pattern \([r_2], B \underline{\{ x \}} \) \( \cup \) \( \Box \). The differential query slice for the pattern \( p' \) considered above is

\[
Q'' = \bigcup \{ \text{false} \} \cup \{ (A, \Box, B, \underline{\{ x \}}) \}, \{ \} \} | x \in R \}
\]

6. Examples and Discussion

In this section we present some more complex examples to illustrate key points.

**Renaming** Recall the swapping query from the introduction, written in NRC as

\[
Q_1 = \bigcup \{ \{ \text{false} \} \cup \{ (A, \Box, B, \underline{\{ x \}}) \}, \{ \} \} \}
\]

This query illustrates a key difference between our approach and the how-provenance model of Green et al. [20]. As discussed in [13], renaming operations are ignored by how-provenance, so the how-provenance annotations of the results of \( Q_1 \) are the same as for a query that simply returns \( R \). In other words, the choice to swap the fields when \( A > B \) is not reflected in the how-provenance, which shows that it is impossible to extract where-provenance (or traces) from how-provenance. Extracting where-provenance from traces appears straightforward, extending our previous work [1].

This example also illustrates how traces and slices can be used for partial recomputation. The slice for output pattern \([\{ r_1, r_2 \}, (B:2)] \cup \Box \) \( \cup \Box \), for example, will show that this record was produced because the \( A \) component of \((A:1, B:2, C:7)\) at index \( [r_1] \) in the input was less than or equal to the \( B \) component. Thus, we can replay after any change that preserves this ordering information.

**Union** Consider query

\[
Q_2 = \bigcup \{ \{ (B:x.B) \} \} \cup R \}
\]

that projects the \( B \) fields of elements of \( R \) and adds another copy of \((B:3)\) to the result. This yields

\[
Q_2(R) = \{ \{ 1, r_1, (B:2) \}, \{ 1, r_2, (B:3) \}, \{ 1, r_3, (B:3) \}, \{ 2, (B:3) \}\}
\]

This illustrates that the indexes may not all have the same length, but still form a prefix code. If we slice with respect to \([\{ 1, r_2, (B:3) \}] \cup \Box \) then the query slice is:

\[
Q_2' = \bigcup \{ \{ (B:x.B) \} \} \cup \Box
\]

and \( R' = \{ \{ r_2, (B:3) \} \cup \Box \) whereas if we slice with respect to \([\{ 2, (B:3) \}] \cup \Box \) then the query slice is \( Q_2'' = \Box \cup \{ (B:3) \} \) and \( R'' = \Box \), indicating that this part of the result has no dependence on the input.

A related point: one may wonder whether it makes sense to select a particular copy of \((B:3)\) in the output, since in a conventional multiset, multiple copies of the same value are indistinguishable. We believe it is important to be able to distinguish different copies of a value, which may have different explanations. Treating \( n \) copies of a value as a single value with multiplicity \( n \) would obscure this distinction and force us to compute the slices of all of the copies even if only a single explanation is required. This is why we have chosen to work with indexed sets, rather than pure multisets.

**Joins** So far all examples have involved a single table \( R \). Consider a simple join query

\[
Q_3 = \{ (A:x.A, B:y.C) | x \in R, y \in S, x.B = y.B \}
\]

and consider the following table \( S \), and the result \( Q_3(R, S) \).

\[
S = \begin{bmatrix}
| s_1 | & 2 & 4 \\
| s_2 | & 3 & 4 \\
| s_3 | & 4 & 5 \\
\end{bmatrix}
\]

\[
Q_3(R, S) = \begin{bmatrix}
| r_1, s_1 | & 1 & 4 \\
| r_2, s_2 | & 2 & 4 \\
| r_3, s_3 | & 4 & 5 \\
\end{bmatrix}
\]

The full trace of this query execution is as follows:

\[
T_3 = \bigcup \{ \{ x \in R \} \cup \{ \{ s_1, s_2, s_3 \} \}, \{ \{ r_1, r_2, r_3 \} \} \}
\]

which yields trace slice

\[
T_3' = \bigcup \{ \{ x \in R \} \cup \{ \{ s_1, s_2, s_3 \} \}, \{ \{ r_1, r_2, r_3 \} \} \}
\]

and input slice \( S' = \{ \{ s_1, s_2, s_3 \} \} \) \( \cup \Box \) and \( S'' = \{ \{ s_1, s_2, s_3 \} \} \) \( \cup \Box \) and \( S''' = \{ \{ s_1, s_2, s_3 \} \} \) \( \cup \Box \).

**Workflows** NRC expressions can be used to represent workflows, if primitive operations are added representing the workflow steps [22]. To illustrate query slicing and differential slicing for a workflow-style query, consider the following more complex query:

\[
Q_4 = \{ f(x, y) | x \in T, y \in T, z \in U, p(x, y), q(x, y, z) \}
\]

where \( f \) computes some function of \( x \) and \( y \) and \( p \) and \( q \) are selection criteria. Here, we assume \( T \) and \( U \) are collections of data files and \( f, p, q \) are additional primitive operations on them. This query exercises most of the distinctive features of our approach; we can of course translate it to the NRC core calculus used in the rest of the paper. If \( \text{dom}(T) = \{ t_1, \ldots, t_{10} \} \) and \( \text{dom}(U) = \{ u_1, \ldots, u_{10} \} \) then we might obtain result \([\{ t_3, t_4, u_5, v_1, t_6, t_8, u_{10}, v_2 \}] \cup \Box \).

If we focus on the value \( v_1 \) using the pattern \([\{ t_3, t_4, u_5, v_1 \}] \cup \Box \) then the program slice we obtain is \( Q_4 \) itself, while the data slice might be \( T' = \{ t_4, t_3, \} \cup \Box \) whereas \( U' = \{ u_5 \} \cup \Box \), indicating that if the values at \( t_3, t_4, u_5 \) are held fixed then the end result will still be \( v_1 \). The trace slice is similar, and shows that \( v_1 \) was computed by applying \( f \) with \( x \) bound to the value at \( t_3 \) in \( T \), \( y \) bound to \( t_4 \), and \( z \) bound to \( u_5 \), and that \( p(x, y) \) and \( q(x, y, z) \) succeeded for these values.

If we consider a differential slice using pattern difference \([\{ t_3, t_4, u_5, v_1 \}] \cup \Box \) then we obtain the following program difference:

\[
Q_4' = \bigcup \{ f(x, y) | x \in T, y \in T, z \in U, p(x, y), q(x, y, z) \}
\]
This shows that most of the query is needed to ensure that the result at $[t_3, t_4, u_5]$ is produced, but the subterm $f(x, y)$ is only needed to compute the value $v_1$. This can be viewed as a query-based explanation for this part of the result.

7. Implementation

To validate our design and experiment with larger examples, we extended our Haskell implementation of Slicer with the traces and slicing techniques presented in this paper. We call the resulting system NRCSlicer; it supports a free combination of NRC and general-purpose functional programming features. NRCSlicer interprets expressions in-memory without optimization. As reported previously for Slicer, we have experimented with several alternative tracing and slicing strategies, which use Haskell’s lazy evaluation strategy in different ways. The alternatives we consider here are:

- **eager**: the trace is fully computed during evaluation.
- **lazy**: the value is computed eagerly, but the trace is computed lazily using Haskell’s default lazy evaluation strategy.

To evaluate the effectiveness of enriched patterns, we measured the time needed for the eager and lazy techniques to trace and slice the workflow example $Q_1$ in the previous section. We considered a instantiation of the workflow where the data values are simply integers and with input tables $T, U = \{1, \ldots, 50\}$, and defined the operations $f(x, y) = x * y$, $p(x, y)$ as $x < y$, and $q(x, y, z)$ as $x^2 + y^2 = z^2$. This is not a realistic workflow, and we expect that the time to evaluate the basic operations of a realistic workflow following this pattern would be much larger. However, the overheads of tracing and slicing do not depend on the execution time of primitive operations, so we can still draw some conclusions from this simplistic example.

The comprehension iterates over $50^3 = 125,000$ triples, producing 20 results. We considered simple and enriched patterns selecting a single element of the result. We measured evaluation time, and the overhead of tracing, trace slicing, and query slicing. The experiments were conducted on a MacBook Pro with 2GB RAM and a 2.8GHz Intel Core Duo, using GHC version 7.4.

<table>
<thead>
<tr>
<th></th>
<th>eval</th>
<th>trace</th>
<th>slice</th>
<th>qslice</th>
</tr>
</thead>
<tbody>
<tr>
<td>eager-simple</td>
<td>0.5</td>
<td>1.5</td>
<td>2.5</td>
<td>1.6</td>
</tr>
<tr>
<td>eager-enriched</td>
<td>0.5</td>
<td>1.5</td>
<td>&lt;0.1</td>
<td>&lt;0.1</td>
</tr>
<tr>
<td>lazy-simple</td>
<td>0.5</td>
<td>0.7</td>
<td>1.3</td>
<td>1.7</td>
</tr>
<tr>
<td>lazy-enriched</td>
<td>0.5</td>
<td>0.7</td>
<td>&lt;0.1</td>
<td>&lt;0.1</td>
</tr>
</tbody>
</table>

The times are in seconds. The “eval” column shows the time needed to compute the result without tracing. The “trace”, “slice”, and “qslice” columns show the added time needed to trace and compute slices. The full traces in each of these runs have over 2.1 million nodes; the simple pattern slices are almost as large, while the enriched pattern slices are only 95 nodes. For this example, slicing is over an order of magnitude faster using enriched patterns. The lazy tracing approach required less total time both for tracing and slicing (particularly for simple patterns). Thus, Haskell’s built-in lazy evaluation strategy offers advantages by avoiding explicitly constructing the full trace in memory when it is not needed; however, there is still room for improvement. Again, however, for an actual workflow involving images or large data files, the evaluation time would be much larger, dwarfing the time for tracing or slicing.

Our implementation is a proof-of-concept that evaluates queries in-memory via interpretation, rather than compilation; further work would be needed to adapt our approach to support fine-grained provenance for conventional database systems. Nevertheless, our experimental results do suggest that the lazy tracing strategy and use of enriched patterns can effectively decrease the overhead of tracing, making it feasible for in-memory execution of workflows represented in NRC.

8. Related and future work

Program slicing has been studied extensively [7,8,30,31], as has the use of execution traces, for example in dynamic slicing. Our work contrasts with much of this work in that we regard the trace and underlying data as being of interest, not just the program. Some of our previous work [12] identified analogies between program slicing and provenance, but to our knowledge, there is no other prior work on slicing in databases.

Lineage and why-provenance were motivated semantically in terms of identifying witnesses, or parts of the input needed to ensure that a given part of the output is produced by a query. Early work on lineage in relational algebra [15] associates each output record with a witness. Buneman et al. studied a more general notion called why-provenance that maps an output part to a collection of witnesses [8]. This idea was generalized further to the how-provenance or semiring model [18,20], based on using algebraic expressions as annotations; this approach has been extended to handle some forms of negation and aggregation [5]. Semiring homomorphisms commute with query evaluation; thus, homomorphic changes to the input can be performed directly on the output without re-running the query. However, this approach only applies to changes describable as semiring homomorphisms, such as deletion.

Where-provenance was also introduced by Buneman et al. [8]. Although the idea of tracking where input data was copied from is natural, it is nontrivial to characterize semantically, because where-provenance does not always respect semantic equivalence. In later work, Buneman et al. [6] studied where-provenance for the pure NRC and characterized its expressiveness for queries and updates. It would be interesting to see whether their notion of expressive completeness for where-provenance could be extended to richer provenance models, such as traces, possibly leading to an implementation strategy via translation to plain NRC.

Provenance has been studied extensively for scientific workflow systems [2,12], but there has been little formal work on the semantics of workflow provenance. The closest work to ours is that of Hidders et al. [21], who model workflows by extending the NRC with nondeterministic, external function calls. They sketch an operational semantics that records runs that contain essentially all of the information in a derivation tree, represented as a set of triples. They also suggest ways of extracting subruns from runs, but their treatment is partial and lacks strong formal guarantees analogous to our results.

There have been some attempts to reconcile the database and workflow views of provenance; Hidders et al. [21] argued for the use of Nested Relational Calculus (NRC) as a unifying formalism for both workflow and database operations, and subsequently Kwasiukowska and Van den Bussche [22] showed how to map this model to the Open Provenance Model. Acar et al. [23] later formalized a graph model of provenance for NRC. The most advanced work in this direction appears to be that of Amstelamer et al. [2], who combined workflow and database styles of provenance in the context of the PigLatin system (a MapReduce variant based on nested relational queries). Lipstick allows analyzing the impact of restricted hypothetical changes (such as deletion) on parts of the output, but to our knowledge no previous work provides a formal guarantee about the impact of changes other than deletion.

In our previous work [12], we introduced dependency provenance, which conservatively over-approximates the changes that can take place in the output if the input is changed. We developed definitions and techniques for dependency provenance in full NRC including nonmonotone operations (empty, sum) and princi-
tive functions. Dependency provenance cannot predict exactly how the output will be affected by a general modification to the source, but it can guarantee that some parts of the output will not change if certain parts of the input are fixed. Our notion of equivalence modulo a pattern is a generalization of the equal-except-at relation used in that work. Motivated by dependency provenance, an earlier technical report [10] presented a model of traced evaluation for NRC and proved elementary properties such as fidelity. However, it did not investigate slicing techniques, and used nondeterministic label generation instead of our deterministic scheme; our deterministic approach greatly simplifies several aspects of the system, particularly for slicing.

There are several intriguing directions for future work, including developing more efficient techniques for traced evaluation and slicing that build upon existing database query optimization capabilities. It appears possible to translate multiset queries so as to make the labels explicit, since a fixed given query increases the impact of changes in hypothetical scenarios similar to the original foundations of self-explaining computation for database queries, particularly for slicing.

9. Conclusion

The importance of provenance for transparency and reproducibility is widely recognized, yet there has been little explicit discussion of correctness properties formalizing intuitions about how provenance is to provide reproducibility. In self-explaining computation, traces are considered to be explanations of a computation in the sense that the trace can be used to recompute (parts of) the output under hypothetical changes to the input. This paper develops the foundations of self-explaining computation for database queries, by defining a tracing semantics for NRC, proposing a formal definition of correctness for tracing (fidelity) and slicing, and defining a correct (though potentially overapproximate) algorithm for trace slicing. Trace slicing can be used to obtain smaller “golden trail” traces that explain only a part of the input or output, and explore the impact of changes in hypothetical scenarios similar to the original run. At a technical level, the main contributions are the careful use of prefix codes to label multiset elements, and the development of enriched patterns that allow more precise slices. Our design is validated by a proof-of-concept implementation that shows that laziness and enriched patterns can significantly improve performance for small (in-memory) examples.

In the near term, we plan to combine our work on self-explaining functional programs and database queries (this paper) to obtain slicing and provenance models for programming languages with query primitives, such as F# or Links. Ultimately, our aim is to extend self-explaining computation to programs that combine several execution models, including workflows, databases, conventional programming languages, Web interaction, or cloud computing.

Acknowledgments

We are grateful to Peter Buneman, Jan Van den Bussche, and Roly Perera for comments on this work and to the anonymous reviewers for detailed suggestions. Effort sponsored by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant number FA8655-13-1-3006. The U.S. Government and University of Edinburgh are authorized to reproduce and distribute reprints for their purposes notwithstanding any copyright notation thereon. Cheney is supported by a Royal So-


A. Auxiliary definitions

Figure 12 summarizes the typing rules for traces. Figure 13 defines the subtrace relation.

B. Proofs of pattern properties

We prove the required properties for enriched patterns. The corresponding properties for the sublanguage of simple patterns follow immediately since simple patterns are closed under the relevant operations.

Lemma B.1. If \( p, p' \subseteq v \) then \( p \sqcup p' \) exists and is the least upper bound of \( p \) and \( p' \).

Proof. If both \( p \) and \( p' \) match some pattern \( q \), then it is straightforward to show by induction on \( q \) that \( p \sqcup p' \) is defined and \( p \sqcup p' \subseteq q \). Specifically, if \( p \) or \( p' \) is \( \Box \) or \( \Diamond \) then we are done; if \( p \) and \( p' \) are both constants then we are done; otherwise, in each case, the toplevel structure of \( p \) and \( p' \) must match \( q \), so that we can apply one of the rules for \( \sqcup \) on smaller terms that match part of \( q \). When \( q = v \), the desired result follows. The second part (that \( \sqcup \) is a least upper bound) also follows directly since clearly, \( p, p' \subseteq p \sqcup p' \) and if \( p, p' \subseteq q \) then a similar argument shows that \( p \sqcup p' \subseteq q \).

Lemma B.2. For any \( v', p, v \approx_{p[\Box/\Diamond]} v' \) holds if and only if \( v \approx_p v' \) holds and \( v = v' \).

Proof. Straightforward induction on the derivation of \( v \approx_{p[\Box/\Diamond]} v' \).

Lemma B.3. For any \( v', v, p, p' \), we have \( v \approx_{p[p',p']} v' \) if and only if \( v \approx_{p'} v' \) and \( v \approx_{p'} v' \). Moreover, if \( p \subseteq p' \) if and only if for all \( v, v' \), we have \( v \approx_{p'} v' \) implies \( v \approx_{p'} v' \).

Proof. For the first part, we proceed by induction on the total size of \( p, p' \). The cases where one of \( p, p' \) is \( \Box \) or \( \Diamond \) are straightforward; for \( \Diamond \) we also need Lemma B.3. The cases involving constants, pairs, or complete set and record patterns are also straightforward.

There are several similar cases involving partial set or record patterns. We illustrate two representative cases:

1. If \( p = \{ e_i, \ell_i \} \) and \( p' = \{ e_i', \ell_i' \} \), then \( p \sqcup p' = \{ e_i \sqcup e_i', \ell_i \sqcup \ell_i' \} \). First, suppose \( v \approx_{p[p',p']} v' \). This means \( v = \{ e_{i_1}, \ell_{i_1} w_{i_1} \} \) and \( v' = \{ e_{i_2}, \ell_{i_2} w_{i_2} \} \), where \( v_i \approx_{p[p',p']} v'_i \) and \( w_i \approx_{q_i} w'_i \). Therefore, by induction, \( v_i \approx_{p_i} v'_i \) and \( v_i \approx_{p_i} v'_i \), so we can conclude that \( \{ e_{i_1}, \ell_{i_1} w_{i_1} \} \approx_{p_1} \{ e_{i_1}, \ell_{i_1} w_{i_1} \} \) and \( \{ e_{i_2}, \ell_{i_2} w_{i_2} \} \approx_{p_2} \{ e_{i_2}, \ell_{i_2} w_{i_2} \} \), as required.

Figure 13. Subtrace relation.
Conversely, if we assume $v \sim_p v'$ and $v \sim_{p'} v''$, then we must have $v = \big{(} \ell_i, v_i, \ell_i', u_i' \big{)}$ and $v' = \big{(} \ell_i', v_i', \ell_i'' u_i'' \big{)}$, where $v_i \sim_{p_i} v_i'$ and $v_{i'} \sim_{p_{i'}} u_i'$. Thus, by induction we have $v_i \sim_{p_{i|\ell_i'}} v_{i'}$ and $u_{i'} \sim_{q_{i'}} u_{i''}$, so we can conclude $\big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \sim_{p_{i|\ell_i'}} \big{(} \ell_i', v_{i'}, \ell_i'' u_{i'}' \big{)}$.

2. If $p = \big{(} \ell_i, v_i, q_i \big{)} \cup \emptyset$ and $p' = \big{(} \ell_i', v_i', q_i \big{)} \cup \emptyset$ then $p \cup p' = \big{(} \ell_i, v_i, \ell_i', v_i', q_i \big{)} \cup \emptyset$. First, suppose $v \sim_{p_{i|\ell_i'}} v'$. This means $v = \big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \cup w_0$ and $v' = \big{(} \ell_i', v_i', \ell_i'', u_i'' \big{)} \cup w_0$, where $v_i \sim_{p_{i|\ell_i'}} v_{i'}$ and $w_0 \sim_{q_i} w_0$, so we can conclude that $\big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \cup w_0 \sim_{p_{i|\ell_i'}} \big{(} \ell_i', v_{i'}, \ell_i'', u_{i''} \big{)} \cup w_0$ and $\big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \cup w_0 \sim_{p_{i|\ell_i'}} \big{(} \ell_i', v_{i'}, \ell_i'', u_{i''} \big{)} \cup w_0$, as required.

Conversely, if we assume $v \sim_{p_{i|\ell_i'}} v'$ and $v \sim_{p_{i|\ell_i''}} v''$, then we must have $v = \big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \cup w_0$ and $v' = \big{(} \ell_i, v_i', \ell_i'', u_i'' \big{)} \cup w_0$, where $v_{i'} \sim_{p_{i'}} v_{i'}$ and $w_0 \sim_{q_i} w_0$ and $v_{i''} \sim_{p_{i''}} v_{i''}$, so we can conclude that $\big{(} \ell_i, v_i, \ell_i', u_i' \big{)} \cup w_0 \sim_{p_{i|\ell_i'}} \big{(} \ell_i', v_{i'}, \ell_i'', u_{i''} \big{)} \cup w_0$, as required.

The second part follows immediately from the definition of $p \subseteq p'$ as $p \cup p' = p'$.

Lemma B.4 (Properties of union and restriction).

1. If $p_1 \subseteq v_1$ and $p_2 \subseteq v_2$ and $v_1 \sim_{p_1} v_1'$ and $v_2 \sim_{p_2} v_2'$ then $v_1 \cup v_2 \sim_{p_1 \cup p_2} v_1' \cup v_2'$, provided all of these disjoint unions are defined.

2. If $p \subseteq v_1 \cup v_2$ and $L_1 \leq \text{dom}(v_i)$ and $L_2 \leq \text{dom}(v_i)$ and $L_1, L_2$ are prefix-disjoint, then $p|_{L_1} \subseteq v_1$ and $p|_{L_2} \subseteq v_2$.

Proof. For part 1, assume $p_1 \subseteq v_1, p_2 \subseteq v_2, v_1 \sim_{p_1} v_1', v_2 \sim_{p_2} v_2'$, and assume that the domains of $p_1$ and $p_2, v_1$ and $v_2$, and $v_1'$ and $v_2'$ are prefix-disjoint respectively, so that the unions exist. There are several cases. If $p_1$ or $p_2$ is $\emptyset$ then the conclusion is immediate. If both are $\emptyset$ then $v_1 = v_1'$ and $v_2 = v_2'$, so $v_1 \cup v_2 = v_1' \cup v_2'$.

Most of the remaining cases are straightforward; we illustrate with the case $p_1 = \big{(} \ell_i, p_i \big{)} \cup \emptyset$ and $p_2 = \big{(} \ell_i, q_i \big{)} \cup \emptyset$. In this case, we have $v_1 = \big{(} \ell_i, v_i \big{)} \cup 0$ and $v_2 = \big{(} \ell_i, v_i \big{)} \cup 0$.

and we also know that $v_i \sim_{p_i} v_i'$ and $v_i' \sim_{q_i} v_i''$ for each $i$.

For part 2, assume $p \subseteq v_1 \cup v_2$ and $L_i \leq \text{dom}(v_i)$ for $i \in \{1, 2\}$. We proceed by case analysis on $p$. The cases for $\emptyset$ and $\emptyset$ are immediate since $\emptyset \subseteq \emptyset$. If $p = \big{(} \ell_i, p_i \big{)}$ is a complete set pattern, then $p|_{L_1}$ selects just those elements of $\ell_i$ that have a prefix in $L_1$, and since every element of $v_i$ has its label’s prefix in $L_i$, we must have that $v_1 = \big{(} \ell_i, v_i \big{)}$ for each $i$ and $p|_{L_1} = \big{(} \ell_i, p_i \big{)}$, which is what we need to show. The cases for $p = \big{(} \ell_i, p_i \big{)} \cup \emptyset$ and $p = \big{(} \ell_i, p_i \big{)} \cup \emptyset$ are similar. A symmetric argument suffices to show $p|_{L_2} \subseteq v_2$.

Lemma B.5 (Projection and $\emptyset$).

1. If $p \subseteq \{ \epsilon \cdot v \}$ then $p \cdot \epsilon \subseteq v$.

2. If $p \subseteq \{ 1 \cdot v, 2 \cdot v \}$ then $p[1] \subseteq v_1$ and $p[2] \subseteq v_2$.

3. If $p \subseteq \ell \cdot v$ then $p[\ell] \subseteq v$.

4. If $p \subseteq \langle A_i \cdot v \rangle$ then $p \subseteq v_i$.

Proof. For part (1), suppose $p \subseteq \{ \epsilon \cdot v \}$. We proceed by case analysis on $p$. The cases for $\emptyset$ and $\emptyset$ are trivial. If $p = \{ \epsilon \cdot p \}$ then $\epsilon \cdot p = \emptyset$ so the conclusion follows. The cases for $p = \{ \epsilon \cdot p \} \cup \emptyset$ or $p = \{ \epsilon \cdot p' \} \cup \emptyset$ are similar.

For part (2), suppose $p \subseteq 1 \cdot v_i \cup 2 \cdot v_i'$. Suppose $v_1 = \big{(} \ell_i, v_i \big{)}$ and $v_2 = \big{(} \ell_i', v_i' \big{)}$. If $p$ is a complete set pattern, then it must be of the form $\{ 1 \cdot \ell_i, 2 \cdot \ell_i', q_i \}$, where $p_i \subseteq v_i$ and $q_i \subseteq v_i'$. The desired conclusion follows since $p[1] = \big{(} \ell_i, p_i \big{)}$, and a symmetric argument shows that $p[2] \subseteq v_2$.

For part (3), suppose $p \subseteq \ell \cdot v$. The proof is analogous to the previous case.

For part (4), suppose $p \subseteq \langle A_i \cdot v_i \rangle$. If $p = \emptyset$ or $\emptyset$, the result is immediate; otherwise, $p$ is a record pattern. If it is a total record pattern $(A_i : p_i)$ then clearly $p.A_i = p_i \subseteq v_i$. Otherwise, it is a partial pattern, in which case either $p.A_i$ is a pattern $p_i$ mentioned in $p$, in which case we are done, or $p.A_i = \emptyset$ or $p.A_i = \emptyset$, and the conclusion follows immediately.

Lemma B.6 (Projection and $\subseteq$).

1. If $p \subseteq \{ \epsilon \cdot v \}$ and $v \supseteq p \cdot \epsilon \cdot v'$ then $\{ \epsilon \cdot v \} \subseteq p \cdot \{ \epsilon \cdot v' \}$.

2. If $p \subseteq 1 \cdot v_i \cup 2 \cdot v_i$ and $v_i \supseteq p[1] v_i$ and $v_i \supseteq p[2] v_i'$ then $1 \cdot v_i \cup 2 \cdot v_i \supseteq 1 \cdot v_i' \cup 2 \cdot v_i'$.

3. If $p \subseteq \ell \cdot v$ and $v \supseteq p[\ell] v'$ then $\ell \cdot v \supseteq p \cdot \ell \cdot v'$.

4. If $p \subseteq \langle A_i : v_i \rangle$ and $v_i \supseteq p.A_i v_i' \ldots v_n \supseteq p.A_n v_n' \ldots$ then $\langle A_i : v_i \rangle \supseteq \langle A_i : v_i' \rangle$.
Proof. For part (1), suppose \( p \subseteq \{ \varepsilon, v \} \) and \( v \approx_{p, \epsilon} v' \). If \( p = \emptyset \) or \( \diamond \) then the result is immediate (this is the case for all three parts of the lemma). If \( p = \{ \varepsilon_p' \}, p = \{ \varepsilon_p' \} \cup \emptyset \), or \( p = \{ \varepsilon_p' \} \cup \diamond \) then \( p, \epsilon = p' \) so \( v \approx_{p'} v' \). We can conclude \( \{ \varepsilon, v \} \approx_{p'} \{ \varepsilon, v' \} \).

For part (2), suppose \( p \subseteq \{ 1 \cdot v_1 \otimes 2 \cdot v_2 \) and \( v_1 \approx_{p_1} v_1' \) and \( v_2 \approx_{p_2} v_2' \). As usual, the cases \( p = \emptyset \) and \( p = \diamond \) are trivial. Suppose \( v_1 = (t_1, v''_1) \) and \( v_2 = (t_2, v''_2) \). If \( p \) is a complete set pattern it must be of the form \((T, t_1, p_1), 2(T', t_1, p_1)\), and \( v_1 \approx_{(\bar{v}_1, p_1)} v_1' \) and \( v_2 \approx_{(\bar{v}_2, p_1)} v_2' \).

It is straightforward to show that \( 1 \cdot v_1 \approx_{\{ \bar{v}_1, \bar{v}_2 \}} 1 \cdot v_1' \) and \( 2 \cdot v_2 \approx_{\{ \bar{v}_2, \bar{v}_2 \}} 2 \cdot v_2' \), so by previous results we have \( 1 \cdot v_1 \otimes 2 \cdot v_2 \approx_{p} 1 \cdot v_1' \otimes 2 \cdot v_2' \).

The cases for partial patterns follow the same reasoning, making use of the fact that projection preserves the partial pattern.

For part (3), suppose \( p \subseteq \{ \varepsilon, v \} \). The argument is similar to the previous case.

For part (4) suppose \( p \subseteq \{ A_i : v_i \} \) and \( v_i \approx_{p, A_i} v_i' \) for each \( i \). If \( p = \emptyset \), \( \diamond \), or a complete record pattern then the conclusion is immediate. Otherwise, if \( p = (B_i : q_i) \cup \emptyset \), the conclusion is immediate since each component of the records \( \{ A_i : v_i \} \) and \( \{ A_i : v_i' \} \) either match the appropriate \( q_i \) or need not match because of the hole. Finally, if \( p = (B_i : q_i) \cup \diamond \), the conclusion follows since each pair of corresponding components of the records \( \{ A_i : v_i \} \) and \( \{ A_i : v_i' \} \) either match the appropriate \( q_i \) or are equal because \( p.A_i = \diamond \) if \( A_i \) is not among the \( B_j \).

\[ \square \]

C. Proof of correctness of trace slicing

Lemma C.1. If \( \gamma, x \in v_1, \Theta \cap^* v_2 \) and \( v_1' \subseteq v_1 \) then there exists \( v_2' \subseteq v_2 \) such that \( \gamma, x \in v_1' \cap^* v_2' \).

Proof. The proof is straightforward by induction on derivations. The cases for \( v_1 = \emptyset \) and \( v_1 = \{ \varepsilon, x \} \) are immediate; if \( v_1 = w_1 \cup w_2 \) then we proceed by induction on the subsets \( w_1' = w_1 \cap v_1 \) and \( w_2' = w_2 \cap v_1 \).

We prove correctness of the full trace slicing algorithm, with enriched patterns, since the correctness for simple patterns follows as a special case.

Theorem C.2 (Correctness of Slicing).

1. Suppose \( \gamma, T \cap^* v \) and \( p \subseteq v \) and \( p, T \smallsetminus \rho, S \). Then for all \( \gamma' \approx_{p, v} \gamma \) and \( T' \subseteq S \) such that \( \gamma', T' \cap^* v' \) we have \( v' \approx_{p, v} v \).

2. Suppose \( \gamma, x \in v_0, \Theta \cap^* v \) and \( p \subseteq v \) and \( p, x, \Theta_0 \cap^* \rho, \Theta_0, p_0, \) where \( \Theta_0 \subseteq \Theta \). Then for all \( \gamma' \approx_{p, v} \gamma \) and \( v_0 \approx_{p_0, v_0} v_0 \) and \( \Theta' \subseteq \Theta_0 \) such that \( \gamma', x \in v_0, \Theta' \cap^* v' \) we have \( v' \approx_{p, v} v \).

Proof. For part (1), the proof is by induction on the structure of slicing derivations, using inversion to extract information from other derivations. The cases for variables, constants, primitive operations, and let-binding are exactly as in previous work [1]. The cases for conditionals are similar to the those for variant types and case constructs in previous work.

We show the cases for records and set operations, which are new to this paper (records are handled similarly to pairs in our previous work, so the cases for pairs are omitted).

- Field projection. If the last step in the slicing derivation is \( \langle A_i : p ; \emptyset \rangle, T \smallsetminus \rho, p, S \) then the evaluation derivation must be of the form \( \gamma, T \cap A_i \cap v_1 \\Rightarrow \langle A_1 : v_1, \ldots, A_n : v_n \rangle \) let \( \gamma' \approx_{p, v} \gamma \) and \( T' \subseteq S.A_i \) be given, where \( \gamma', T' \cap v' \). Then \( T' \) must have the form \( T'' : A_i \) for some \( T'' \subseteq S \) so the replay derivation is of the form \( \gamma', T'' \cap A_i \cap v_1' \) let \( \gamma' \approx_{p, v} \gamma \) and \( v_0 \approx_{p_0, v_0} v_0 \) and \( \Theta' \subseteq \Theta_0 \) such that \( \gamma', x \in v_0, \Theta' \cap^* v' \) we have \( v' \approx_{p, v} v \).

The induction hypothesis applies since it is easy to show that \( \langle A_i : p ; \emptyset \rangle \not\subseteq \langle A_1 : v_1, \ldots, A_n : v_n \rangle \). Therefore \( \langle A_1 : v_1', \ldots, A_n : v_n' \rangle \approx_{\langle A_i : p, p_0 \rangle} \langle A_1 : v_1, \ldots, A_n : v_n \rangle \).

- Record. If the last step in the slicing derivation is \( p, A_1, T_1 \smallsetminus \rho_1, S_1 \) then the evaluation derivation must be of the form \( \gamma, T \cap v_1 \) let \( \gamma' \approx_{p, v} \gamma \) and \( T' \subseteq S.A_i \) be given, where \( \gamma', T' \cap v' \). Then \( T' \) must have the form \( \langle A_1 : T_1, \ldots, A_n : T_n \rangle \) let \( \gamma, \langle A_1 : T_1, \ldots, A_n : T_n \rangle \cap A_i \cap \langle A_1 : v_1, \ldots, A_n : v_n \rangle \) then the evaluation derivation must be of the form \( \gamma, T \cap v_1' \) let \( \gamma' \approx_{p_1, v} \gamma \) and \( T'' \subseteq S.A_i \) be given, where \( \gamma', T'' \cap v'' \). Then \( T'' \) must have the form \( \langle A_1 : T_1, \ldots, A_n : T_n \rangle \) let \( \gamma, \langle A_1 : T_1, \ldots, A_n : T_n \rangle \cap \langle A_1 : v_1', \ldots, A_n : v_n' \rangle \)
By Lemma 3.3, we know $p.A_i \subseteq v_i$ for each $i$, and $\gamma' \simeq_{p_i} \gamma$ for each $i$, so by induction $v_i' \simeq_{p_i} A_i v_i$ for each $i$. Using Lemma 4.6, we can conclude that $\langle A_1; v_1', \ldots, A_n; v_n' \rangle \simeq_{p} \langle A_1; v_1, \ldots, A_n; v_n \rangle$.

- Empty set. This case is trivial, similar to the usual case for constants.
- Singleton. This case follows immediately from the relevant properties of $p.e$, using similar reasoning to the record projection case.
- Union. If the last step in the slicing derivation is
  \[
  \frac{p[1], T_1 \rhd \rho_1, S_1 \quad p[2], T_2 \rhd \rho_2, S_2}{p, T_1 \cup T_2 \rhd \rho_1 \cup \rho_2, S_1 \cup S_2}
  \]
  then the evaluation derivation must be of the form
  \[
  \gamma, T_1 \rhd v_1 \quad \gamma, T_2 \rhd v_2
  \]
  Let $\gamma' \simeq_{p_1 \cup p_2} \gamma$ and $T' \supseteq T_1 \cup T_2$ be given, where $\gamma', T' \rhd v'$. Then $T'$ must have the form $T'_1 \cup T'_2$ where $T'_i \supseteq S_i$ so the replay derivation is of the form
  \[
  \gamma', T'_1 \rhd v'_1 \quad \gamma', T'_2 \rhd v'_2
  \]
  By Lemma 3.5, we know $p[1] \subseteq v_1$ and $p[2] \subseteq v_2$, and $\gamma' \simeq_{p_1} \gamma$, so by induction we have $v'_1 \simeq_{p[1]} v_1$ and $v'_2 \simeq_{p[2]} v_2$, and therefore by Lemma 4.6, we can conclude $1 \cdot v'_1 \cup 2 \cdot v'_2 \simeq_{p} 1 \cdot v_1 \cup 2 \cdot v_2$.

- Sum and emptiness. In both cases, since the slice ensures that the whole argument to the sum or emptiness test is preserved, the argument is straightforward. For example, for emptiness suppose the derivation is of the form:
  \[
  \boxed{}, T \rhd \rho, S \quad \boxed{}, \emptyset \subseteq \rho, \emptyset
  \]
  then there are two cases. If replay derivation is of the form
  \[
  \gamma, T \rhd \emptyset
  \]
  Suppose $\gamma' \simeq_{\rho} \gamma$ and $T' \supseteq \emptyset$ with $\gamma', T' \rhd v'$. Then $T'$ is of the form empty $T''$ with $T'' \supseteq S$, so the replay derivation must be of the form:
  \[
  \gamma', T'' \rhd v''
  \]
  By induction, $v'' \simeq_{\emptyset} \emptyset$, which implies $v'' = \emptyset$ so $v' = \text{true} \simeq_{\rho} \text{true}$ (since $p \subseteq \text{true}$). The cases where the argument to empty $T$ evaluates to a nonempty set, and for sum $T$, are similar.

- Comprehension. If the derivation is of the form
  \[
  \frac{p, x, \Theta \rhd x \ast \rho' \ast \Theta, p_0, T \rhd \rho, S}{p, \bigcup \{x \mid x \in T \} \triangleright \Theta \rhd \rho \cup \rho', \bigcup \{x \mid x \in S \} \triangleright \Theta_0}
  \]
  then the replay derivation must be of the form
  \[
  \gamma, T \rhd v_0 \quad \gamma, x \in v_0 \Theta \rhd x \ast v
  \]
  Suppose $\gamma' \simeq_{\rho \cup \rho'} \gamma$ and $T' \supseteq \bigcup \{x \mid x \in S \} \triangleright \Theta_0$ with $\gamma', T' \rhd v'$. Then $T'$ must be of the form $\bigcup \{x \mid x \in T'' \} \triangleright \Theta'$ for some $T'' \supseteq S$ and $\Theta' \supseteq \Theta_0$ so the replay derivation must be of the form
  \[
  \gamma', T'' \rhd v'_0 \quad \gamma', x \in v'_0 \Theta' \rhd x \ast v'
  \]
  Since $p_0 \subseteq v_0$ and $\gamma' \simeq_{\rho'} \gamma$ and $\gamma' \simeq_{\rho'} \gamma$ we have $v'_0 \simeq_{p_0} v_0$ by induction. Thus, by the second induction hypothesis, since $p \subseteq v$ and $\gamma' \simeq_{\rho'} \gamma$ and $v'_0 \simeq_{p_0} v_0$ we have $v' \simeq_{\rho} v$.

For part (2), the proof is again by induction on the structure of derivations.

- If the slicing derivation is of the form
  \[
  \emptyset, x, \emptyset \rhd \emptyset
  \]
  then the conclusion is immediate, since rerunning an empty trace set always yields the empty set.
- If the slicing derivation is of the form
  \[
  \boxed{}, x, \emptyset \rhd \emptyset
  \]
  then the conclusion is immediate as before, since rerunning an empty trace set always yields the empty set.
• If the slicing derivation is of the form

\[ \square, x, \Theta \not\vdash w, p, \square \]

then the conclusion is immediate, since any two values match according to \( \square \).

• If the slicing derivation is of the form

\[
p[l], T \setminus \gamma \vdash p[x \mapsto p_0], S
\]

\[
p, x, \{\ell.T\} \setminus \rho, \{\ell.S\}, \{\ell.p_0\}
\]

then observe that \( \Theta \supseteq \{\ell.T\} \) by assumption, so \( \Theta(\ell) = T \). So, the replay derivation must have the form

\[
\ell \in \text{dom}(\Theta) \quad \gamma[x \mapsto v_0], T \supseteq v
\]

\[
\gamma, x \in \{\ell.v_0\}, \Theta \not\supseteq \ell \cdot v
\]

Now suppose that \( \gamma' \equiv \gamma \) and \( v_0' \equiv (\ell.p_0) \) \{\ell.v_0\} and \( \Theta' \supseteq \{\ell.S\} \) are given where \( \gamma', x \in v_0', \Theta' \not\supseteq v' \). It follows that \( v_0' = \{\ell.v_0''\} \) and \( v_0'' \equiv v_0 \), so \( \gamma'[x \mapsto v_0'] \equiv \gamma[x \mapsto v_0] \). Moreover, by inversion the derivation must have the form:

\[
\ell \in \text{dom}(\Theta') \quad \gamma'[x \mapsto v_0'], \Theta'(\ell) \not\supseteq v'
\]

\[
\gamma', x \in \{\ell.v_0''\}, \Theta' \not\supseteq \ell \cdot v'
\]

Since by Lemma B.5 \( p[\ell] \subseteq v \) and \( \Theta'(\ell) \supseteq S \) (which holds because \( \Theta' \supseteq \{\ell.S\} \)), we have by induction that \( v' \equiv p[\ell], v \), and using Lemma B.6 we can conclude that \( \ell \cdot v' \equiv \ell \cdot v \) as desired.

• Suppose the slicing derivation is of the form:

\[
p[\text{dom}(\Theta_1), x, \Theta_1 \not\vdash \gamma, p_1, \Theta_1, \{\ell.p_1\}, p_1]
\]

\[
p[\text{dom}(\Theta_2), x, \Theta_2 \not\vdash \gamma, p_2, \Theta_2, \{\ell.p_2\}, p_2]
\]

and suppose that \( \gamma, x \equiv v_0, \Theta \not\supseteq \gamma' \) where \( \Theta \equiv \Theta_1 \cup \Theta_2 \). Suppose that \( \gamma' \equiv \gamma_1 \cup \gamma_2 \) \{\ell.p_1 \cup p_2\} \{\ell.v_0\} \) and \( \Theta' \equiv \Theta_1' \cup \Theta_2' \) are given, where \( \gamma', x \equiv v_0', \Theta' \not\supseteq \gamma' \). We need to show that \( v' \equiv \gamma' \).

Since \( v_0' \equiv (\ell.p_1 \cup p_2) \), it is straightforward to show that there must exist \( v_1, v_2, v_1', v_2' \) such that \( v_1 \equiv v_2 \equiv v_0', v_1' \equiv v_2' \equiv v_0, v_1 \equiv p_1 \), \( v_1 \) and \( v_2 ' \equiv p_2 \). Furthermore, by Lemma C.1 we know that \( \gamma, x \equiv v_1, \Theta \not\supseteq \gamma', x \equiv v_1', \Theta' \not\supseteq \gamma', x \equiv v_2, \Theta' \not\supseteq \gamma', x \equiv v_2' \) for some \( w_1, w_2, w_1', w_2' \).

Therefore, we can conclude that:

\[
\gamma, x \equiv v_1, \Theta \not\supseteq \gamma, x \equiv v_2, \Theta \not\supseteq \gamma'
\]

\[
\gamma', x \equiv v_1', \Theta' \not\supseteq \gamma', x \equiv v_2', \Theta' \not\supseteq \gamma'
\]

Furthemore, since \( v_1 \equiv v_0 \), by determinacy we know that \( w_1 \equiv w_2 \equiv v \) and similarly \( w_1' \equiv w_2 \equiv v' \) by induction since \( p_1 \equiv v_1 \) and \( \Theta_1 \equiv \Theta_1 \). Hence, we know that \( w_1' \equiv p[\text{dom}(\Theta_1)] \) \( w_1 ' \equiv p[\text{dom}(\Theta_1)] \) \( w_1 \equiv w_2 = v \).

To conclude, since \( p \equiv p[\text{dom}(\Theta_1)] \equiv w \) and \( \text{dom}(\Theta_1) \leq w_1 \) and \( \text{dom}(\Theta_2) \leq w_2 \), it follows that \( p = p[\text{dom}(\Theta_1)] \equiv p[\text{dom}(\Theta_2)] \), so we can conclude \( w_1 \equiv w_2 \equiv p[\text{dom}(\Theta_1)] \equiv w_1' \equiv w_2 ' \) as desired.

This exhausts all cases and completes the proof.

\( \square \)

**D. Proof of correctness of query slicing**

Lemma D.1. If \( \gamma, x \equiv v_1, e \not\vdash v_2 \) and \( v_1' \not\subseteq v_1 \) then there exists \( v_1'' \not\subseteq v_2 \) such that \( \gamma, x \equiv v_1', e \not\vdash v_2 ' \).

*Proof.* The proof is straightforward by induction on derivations. The cases for \( v_1 = \emptyset \) and \( v_1 = \{\ell.v\} \) are immediate; if \( v_1 = v_2 \) then we proceed by induction using the subsets \( v_1' = v_1 \cap v_1 ' \) and \( w_1 = w_1 ' = v_1 \cap v_1 ' \).

We prove Theorem 5.1 by strengthening the induction hypothesis as follows:

**Theorem D.2** (Correctness of Query Slicing).

1. Suppose \( \gamma, T \not\supseteq v \) and \( p \subseteq v \) and \( T \not\supseteq \rho, e \). Then for all \( \gamma' \equiv \gamma \) and \( e' \equiv e \) such that \( \gamma', e' \not\vdash v' \) we have \( v' \equiv p, v \).

2. Suppose \( \gamma, x \equiv v_1, \Theta \not\supseteq v \) and \( v_1 \equiv v \) and \( p, \Theta_0 \not\supseteq \rho, e_0, p_0 \), where \( \Theta_0 \equiv \Theta_1 \). Then for all \( \gamma' \equiv \gamma \) and \( v_0' \equiv p_0 \) \( v_0 \) and \( e_0 \equiv e_0 \) such that \( \gamma', x \equiv v_0, e_0 \not\vdash v' \) we have \( v' \equiv p, v \).

*Proof.* The proof is by induction on the structure of query slicing derivations. Many of the cases are essentially the same as for trace slicing. The cases for conditionals are straightforward, since in either case the sliced trace and environment retain enough information to force the same branch to be taken on recompuation. We show the details of the cases involving conditionals and comprehensions.

For part (1), we consider a conditional and comprehension rule:

- If the slicing derivation is of the form:

\[
p[\ell], T \not\supseteq p_1, e_1 \quad \text{true, } T \not\supseteq \rho, e'
\]

\[
p_1, \text{if}(T, e_1, e_2) \not\supseteq \text{true, } T \not\supseteq p_1 \cup \rho, \text{if}(e, e_1, \emptyset)
\]

18
then the replay derivation must be of the form:
\[
\begin{array}{c}
\gamma, T \land \text{true} \\
\gamma, \text{if}(T, e_1, e_2) \lor \text{true} \\
T \land v_1
\end{array}
\]

Suppose \(\gamma' \approx_{\rho \cup \ell} \gamma\) and \(e'' \sqsubseteq \text{if}(e', e'_1, e'_2)\) are given where \(\gamma', e' \Downarrow v'.\) Then \(e'' = \text{if}(e'_0, e'_1, e'_2)\), where \(e'_0 \sqsubseteq e'\) and \(e'_i \sqsubseteq e'_i\), so there are two cases for the evaluation derivation. If it has the form
\[
\gamma', e'_0 \Downarrow \text{false} \\
\gamma', e'_2 \Downarrow v'_2 \\
\gamma', \text{if}(e'_0, e'_1, e'_2) \Downarrow v'_2
\]
then since \(\gamma' \approx_{\rho} \gamma\) and \(\gamma' \approx_{\rho_1} \gamma\), by induction we would have that \(\text{false} \approx_{\text{true}} \text{true}\), which is absurd. So this case cannot arise.

Otherwise, the derivation must have the form:
\[
\gamma', e'_0 \Downarrow \text{true} \\
\gamma', e'_1 \Downarrow v'_1 \\
\gamma', \text{if}(e'_0, e'_1, e'_2) \Downarrow v'_1
\]

Since \(\gamma' \approx_{\rho} \gamma\) and \(\gamma' \approx_{\rho_1} \gamma\), by induction we have that \(v'_1 \approx_{\rho_1} v_1\) as desired.

- Comprehension. If the derivation is of the form
\[
p, x. \Theta \ldots p, e_1, p_0 \Gamma \quad p_0, T \approx_{\rho, e_0} \Gamma
\]
then the replay derivation must be of the form
\[
\begin{array}{c}
\gamma, T \land v_0 \\
\gamma, \bigcup \{e \mid x \in T \} \lor \Theta \land v
\end{array}
\]

Suppose \(\gamma' \approx_{\rho \cup \ell} \gamma\) and \(e'' \sqsubseteq \bigcup \{e'_1 \mid x \in e'_0\}\) with \(\gamma', e'' \Downarrow v'.\) Then \(e''\) must be of the form \(\bigcup \{e''_1 \mid x \in e'_0\}\) for some \(e''_1 \sqsubseteq e'_1\) and \(e''_0 \sqsubseteq e'_0\), so the evaluation derivation must be of the form
\[
\gamma', e''_0 \Downarrow v'_0 \\
\gamma', x \in v_0, e''_1 \Downarrow v'
\]

Since \(p_0 \sqsubseteq v_0\) and \(\gamma' \approx_{\rho} \gamma\) and \(\gamma' \approx_{\rho_1} \gamma\) we have \(v'_0 \approx_{p_0} v_0\) by induction. Thus, by the second induction hypothesis, since \(p \sqsubseteq v\) and \(\gamma' \approx_{\rho} \gamma\) and \(v'_0 \approx_{p_0} v_0\) we have \(v \approx_{p'} v'.\)

For part (2), we consider the singleton and union rules:

- If the slicing derivation is of the form
\[
p[\ell], T \approx_{\rho} p[x \mapsto p_0], e' \\
\begin{array}{c}
p, x. \ell, T \approx_{\rho, e'} \ell, p_0 \Gamma
\end{array}
\]
then recall that by assumption, \(\Theta(\ell) \supseteq \{\ell, T\}\), so \(\Theta(\ell) = T\), so the replay derivation must have the form
\[
\begin{array}{c}
\ell \in \text{dom}(\Theta) \\
\gamma[x \mapsto v_0], T \land v
\end{array}
\]

Now suppose that \(\gamma' \approx_{\rho} \gamma\) and \(v'_0 \approx_{(p_0)} \{\ell, v_0\}\) and \(e'' \sqsubseteq e'\) are given where \(\gamma', x \in v_0, e'' \Downarrow v'.\) It follows that \(v'_0 = \{\ell, v''_0\}\) and \(v'_0 \approx_{p_0} v_0\), so \(\gamma'[x \mapsto v'_0] \approx_{p[x \mapsto p_0]} \gamma[x \mapsto v_0]\). Moreover, by inversion the derivation must have the form:
\[
\gamma'[x \mapsto v'_0], e'' \Downarrow v' \\
\gamma', x \in v_0, e'' \Downarrow v', \ell \not\vdash v'
\]

Since by Lemma [B.3] \(p[\ell] \sqsubseteq v\) we have by induction that \(v' \approx_{p}[\ell] v\), and using Lemma [B.6] we can conclude that \(\ell \cdot v' \approx_{\rho} \ell \cdot v\), as desired.

- Suppose the slicing derivation is of the form:
\[
p[\text{dom}(\Theta_1)], x. \Theta_1 \ldots p_1, e'_1, p_1 \Gamma \\
\begin{array}{c}
p, x. \Theta_1 \lor \Theta_2, p_2, e_2, p_2 \Gamma
\end{array}
\]
and suppose that \(\gamma, x \in v_0, \Theta \land v\) where \(\Theta \supseteq \Theta_1 \lor \Theta_2\). Suppose that \(\gamma' \approx_{p_1 \lor p_2} \gamma\) and \(v_0 \approx_{p_1 \lor p_2} v_0\) and \(e_0 \sqsubseteq e_0\) are given, where \(\gamma', x \in v_0, e_0 \Downarrow v'.\) We need to show that \(v \approx_{p_0} v\).

Since \(v'_0 \approx_{p_1 \lor p_2} v_0\), it is straightforward to show that there must exist \(v_1, v_2, v'_1, v'_2\) such that \(v_1 \uplus v_2 = v_0, v'_1 \uplus v'_2 = v'_0, v_1 \approx_{p_1} v_1\) and \(v'_2 \approx_{p_2} v_2\). Furthermore, by Lemmas [C.1] and [C.2] we know that \(\gamma, x \in v_1, \Theta \land v_1\) and \(\gamma', x \in v'_1, e_0 \Downarrow v'_1\) for some \(v_1, w_1, w'_1, w'_2\). Therefore, we can conclude that:
\[
\begin{array}{c}
\gamma, x \in v_1, \Theta \land w_1 \\
\gamma, x \in v_2, \Theta \land w_2 \\
\gamma', x \in v'_1, e_0 \Downarrow w'_1 \\
\gamma', x \in v'_2, e_0 \Downarrow w'_2
\end{array}
\]
Furthermore, since \(v_1 \uplus w_1 = v_0\), by determinacy we know that \(w_1 \uplus w_2 = v\) and similarly \(w'_1 \uplus w'_2 = v'.\) By induction since \(p_1 \sqsubseteq v_1\) and \(\Theta_1 \subseteq \Theta\), we know that \(w'_1 \approx_{\text{dom}(\Theta_1)} w_1\), so we know that
\[
v' = w'_1 \uplus w'_2 \approx_{\text{dom}(\Theta_1)} w_1 \uplus w_2 = v.
\]
To conclude, since $p \sqsubseteq w_1 \sqcup w_2$ and $\text{dom}(\Theta_1) \leq w_1$ and $\text{dom}(\Theta_2) \leq w_2$, it follows that $p = p|_{\text{dom}(\Theta_1)} \sqcup p|_{\text{dom}(\Theta_2)}$, so we can conclude $w_1 \sqcup w_2 \preceq_p w'_1 \sqcup w'_2$ as desired.

This exhausts all cases and completes the proof.