Fiat: Deductive Synthesis of Abstract Data Types in a Proof Assistant

Benjamin Delaware  Clément Pit-Claudel  Jason Gross  Adam Chlipala

MIT CSAIL

(bendy, cpitcla, jgross, adambc)@csail.mit.edu

Abstract

We present Fiat, a library for the Coq proof assistant supporting refinement of declarative specifications into efficient functional programs with a high degree of automation. Each refinement process leaves a proof trail, checkable by the normal Coq kernel, justifying its soundness. We focus on the synthesis of abstract data types that package methods with private data. We demonstrate the utility of our framework by applying it to the synthesis of query structures—abstract data types with SQL-like query and insert operations. Fiat includes a library for writing specifications of query structures in SQL-inspired notation, expressing operations over relations (tables) in terms of mathematical sets. This library includes a suite of tactics for automating the refinement of specifications into efficient, correctness-preserving OCaml code. Using these tactics, a programmer can generate such an implementation completely automatically by only specifying the equivalent of SQL indexes, data structures capturing useful views of the abstract data. Throughout we speculate on the new programming modularity possibilities enabled by an automated refinement system with proved-correct rules.

“Every block of stone has a statue inside it and it is the task of the sculptor to discover it.”

— Michelangelo

1. Introduction

Deductive synthesis allows users to derive correct-by-construction programs interactively via stepwise refinement of specifications. The programmer starts with a very underconstrained nondeterministic program, which may be nonobvious how to execute efficiently. Step by step, the developer applies refinement rules, which replace program subterms with others that are “at least as deterministic,” introducing no new behaviors beyond those of the terms they replace. Eventually, the program has been refined to a completely deterministic form, ideally employing efficient data structures and algorithms. At its core, deductive synthesis decomposes a program into a high-level specification of its functionality and a sequence of semantics-preserving optimizations that produces an efficient, executable implementation. So long as the library of primitive refinement steps is sound, developers using this approach can modify the optimizations to suit their performance requirements, remaining confident that the implementation produced meets the original specification.

This paper introduces an approach for the deductive synthesis of abstract data types (ADTs) combining computational refinement [7] and abstraction relations [9, 10]. An important novelty of our approach is that all refinement derivations are carried out inside the Coq proof assistant, thereby achieving a previously unmatched degree of confidence in the correctness of the resulting implementations. Derivations in our prototype system Fiat are optimization scripts that transform programs in correctness-preserving ways, possibly resolving nondeterminism. These optimization scripts yield machine-checkable refinement theorems certifying the correctness of the resulting implementations.

Systems like Specware [20] and its predecessors [2, 16] at the Kestrel Institute have enabled interactive synthesis by refinement since the 1970s. Only recently has Specware supported any kind of mechanized proof about refinement correctness, by instrumenting refinement primitives to generate Isabelle/HOL proof scripts, although each of these generators expands Specware’s trusted code base. Specware also follows a very manual model of choosing refinement steps, which is understandable given the challenging problems it has been used to tackle, in domains like artificial intelligence and programming-language runtime systems.

With Fiat, we instead focus (for now, at least) on more modest programming tasks, like those faced by mainstream Web application developers interacting with persistent data stores. The ultimate goal of Fiat is to enable refinement derivations using the sort of push-button automation found in traditional SQL query planners, while adding a high level of assurance about their correctness by carrying them out inside of Coq with full proofs. At the same time, the framework allows seamless integration with manual derivations where they are called for, without weakening the formal guarantee that a derived implementation meets its specification.

By combining the core of Fiat with domain-specific libraries, programmers can write derivations with a high degree of automation. These libraries combine domain-specific refinement theorems and automation tactics to build what amount to first-class, semantics-preserving compilers. Our main case study to date involves a library for synthesizing ADTs with SQL-like operations, operating in the style of query planners from the database community. We start with declarative queries over relational tables, transforming them into efficient, correctness-preserving OCaml code. This library implements “domain compilers” at varying levels of automation; users can do completely automated planning for a common class of queries, and with more work they can apply some of our more advanced strategies for choosing data structures or algorithms.

Figure 1 shows an example Fiat derivation for a simple data structure representing a book store. We consider this example in
AbsR abs
|
←
Any sequence accepted by Coq is guaranteed to preserve correctness, which knows how to use indexes to implement queries efficiently.

we have defined. Finally, we begin an
we want computed than how to compute it. These expressions
The programmer is free to chain sequences of library invocations
and more manual steps, as needed to meet his performance target.
Most of the work is done by a "domain compiler" called
considering this idea more carefully, we can spot opportunities
for these domain-specific libraries to provide automation that goes
beyond the programmer’s usual relationship with her compilers.
Compilers generally do not play too well with each other, and any
optimization not built into a compiler goes unapplied in the final
code. By relying on Fiat’s core as a common foundation, users
can freely compose the automation tactics provided by domain-
specific libraries. Furthermore, this foundation enables programmers
to take an existing domain-specific library and safely extend it with
novel optimizations, without affecting the soundness of any program
optimized with the extended library.

Figure 1. Specification for a bookstore ADT

Definition BookstoreSpec := QueryADTRep BookstoreSchema {
  const Init (ₚ : unit) : rep := empty,
  update AddBook (book: Book) : bool :=
    Insert book into Books,
  update PlaceOrder (order: Order) : bool :=
    Insert order into Orders,
  query GetTitles (author: string) : list string :=
    For (b in Books)
    Where (author = b!Author)
    Returns b!Title,
  query NumOrders (author: string) : nat :=
    Count (For (o in Orders) (b in Books)
    Where (author = b!Author)
    Returns (b!Title),
}

Definition BookStorage : IndexFor Book.
mkIndex [ BookSchema/Author; BookSchema/ISBN ].
Defined.

Definition OrderStorage : IndexFor Order.
mkIndex [ OrderSchema/ISBN ].
Defined.

Definition Bookstore_AbsR abs
(conc : BookStorage × OrderStorage) :=
  abs!Books ≃ bnumerate (fst conc) ∧ abs!Orders ≃ bnumerate (snd conc).

Definition Bookstore : Sharpened BookstoreSpec.
plan Bookstore_AbsR.
finish sharpening.
Defined.

Figure 2. Computation combinators

Consider the following (particularly permissive) specification of
an insert function for a cache represented as a list of key-value pairs:

ret a ≡ \{ a \} \{ a | P \ a \} ≡ \{ a | P \ a \}

\[ x \leftarrow c_
\]

This specification only requires that insert does not inject extraneous
values into the list. When a key is not included in the original cache,
the specification imposes no ordering on the result and somewhat
counterintuitively does not require that the result include the new
key-value pair. Such underspecification is not a bug. It allows for a
wide range of caching behaviors: existing keys can be replaced or
retained when they are reinserted, new keys can be inserted in an
order that facilitates lookup, and old values can be dropped from the
cache to maintain a constant memory footprint.

Each of these choices represents a more refined version of insert,
with refinement defined by the superset relation \( \sqsubseteq \) between the set
of implementations of insert and that of each choice. Refinement
forms a partial order on computations. Intuitively, a computation
\( c' \) is a refinement of a computation \( c \) if \( c' \) only "computes" to
values that \( c \) can "compute" to. Figure 3 shows a subset of the

2. Refinement

The foundation of deductive synthesis in Fiat is refinement: a user
starts out with a high-level specification that can be implemented
in any number of different ways and iteratively refines the possible
implementations until producing an executable (and hopefully
efficient) implementation.

Specifications in Fiat are represented as computations, or sets
of values satisfying some defining property. Figure 2 lists the three
combinators Fiat uses to define these sets: ret builds a singleton set,
set comprehension \( \{ \cdot \mid \cdot \} \) "picks" an arbitrary element satisfying
a characteristic property, and the “\( \leftarrow \)" combinator, "\( \cdot \leftarrow \cdot \)",
combines two computations. Throughout the text we will use the
notation \( c \sim v \equiv v \in c \) to emphasize that computations denote
sets of "computed" values.

\[ \text{ret } a \equiv \{ a \} \] \[ \{ a | P \ a \} \equiv \{ a | P \ a \} \] \[ x \leftarrow c_i; c_0(x) \equiv \{ b \mid \exists a \in c_a. b \in c_b(a) \} \]

Figure 3. Computation combinators

Consider the following (particularly permissive) specification of
an insert function for a cache represented as a list of key-value pairs:

\[ \text{insert } k v l \equiv \{ l' \mid l' \subseteq \{ (k, v) \} \} \cup l \]

This specification only requires that insert does not inject extraneous
elements in the list. When a key is not included in the original cache,
the specification imposes no ordering on the result and somewhat
counterintuitively does not require that the result include the new
key-value pair. Such underspecification is not a bug. It allows for a
wide range of caching behaviors: existing keys can be replaced or
retained when they are reinserted, new keys can be inserted in an
order that facilitates lookup, and old values can be dropped from the
cache to maintain a constant memory footprint.

Each of these choices represents a more refined version of insert,
with refinement defined by the superset relation \( \sqsubseteq \) between the set
of implementations of insert and that of each choice. Refinement
forms a partial order on computations. Intuitively, a computation
\( c' \) is a refinement of a computation \( c \) if \( c' \) only "computes" to
values that \( c \) can "compute" to. Figure 3 shows a subset of the
space of computations that we can explore through sequences of refinements from the initial definition of insert. The second column shows a number of refinements of the initial specification, each of which admits a smaller set of implementations. The computation in the second row of this column, for example, only permits implementations that ignore the insertion of duplicate keys.

The third column shows a sequence of refinements progressing towards such an implementation. The first entry further requires implementations to add new keys to the cache. The next computation is an equivalent but more operational version that decomposes the pick into

\[ b \leftarrow \{ b \mid \text{if } b \text{ then } k \not\in l \text{ else } k \in l \}; \]

\[ \text{if } b \text{ then } \text{ret } [(k, v)] \cup l \text{ else } \{l' \mid l' \subseteq l\} \]

where \( b \) is bound to the negation of a nondeterministic membership check for key \( k \) in list \( l \). \( b \) is passed to a computation that adds the key-value pair to the list if \( k \) is not already used and nondeterministically shrinks \( l \) otherwise. The third entry moves closer to an implementation by implementing the membership check using a notKey function and the pick in the else case with ret \( l \). A few basic properties of our computation combinators justify implementing each of these subterms of the bind. Refinement may be pushed down through "bind" in two different ways:

\[ c_\alpha \supseteq c_\alpha' \quad \Rightarrow \quad (x \leftarrow c_\alpha; c_\alpha(x)) \supseteq (x \leftarrow c_\alpha'; c_\alpha'(x)) \]

\[ (\forall x, c_\alpha(x)) \supseteq (\forall x, c_\alpha'(x)) \quad \Rightarrow \quad (x \leftarrow c_\alpha; c_\alpha(x)) \supseteq (x \leftarrow c_\alpha'; c_\alpha'(x)) \]

The usual monad laws \cite{21} hold for computations under set equality =.

\[ (x \leftarrow \text{ret } a; c(x)) = c(a) \]
\[ (x \leftarrow c; \text{ret } x) = c \]
\[ (y \leftarrow (x \leftarrow c_\alpha; c_\alpha(x)); c_\alpha(y)) = x \leftarrow c_\alpha; y \leftarrow c_\alpha(x); c_\alpha(y) \]

These laws justify the final refinement in the third column; by transitivity of refinement, it is also a refinement of the initial specification of insert.

2.1 Refinement of Abstract Datatypes

Fiat defines abstract data types \cite{11} (ADTs) as records of state types and computations implementing operations over states. Figure 4 gives a specification of a cache as an abstract data type. In the CacheSig type signature, rep stands for an arbitrary abstract implementation type, to be threaded through the methods; this type placeholder has a special status in signatures. The CacheSpec functional specification is a nondeterministic reference implementation of a cache. That is, it uses a simple data representation type and its associated method implementations to clearly express how any implementation of this ADT ought to behave. The representation type of CacheSpec does not even obviously lead to computable execution, since it is phrased in terms of mathematical sets. CacheSpec adds to our running example of insert a method for retrieving values from the cache, an update method for updating keys already in the cache, and a constructor called empty for creating a fresh cache.

ADTSig CacheSig :=

empty : () → rep,

insert : rep × Key × Value → rep,

update : rep × Key × (Value → Value) → rep,

lookup : rep × Key → Maybe Value

ADT CacheSpec implementing CacheSig :=

rep := Set of (Key × Value)

constructor empty := Return ()

method insert (r : rep, k : Key, v : Value) : rep :=

\{r' \mid \forall kv. kv \in r' \rightarrow kv = (k, v) \lor kv \in r\}

method update (r : rep, k : Key, f : Value → Value) : rep :=

\{r' \mid \forall kv. kv \in r \rightarrow \forall kv. kv \in r' \rightarrow kv = (k, f(kv)) \lor kv \in RemoveKey(k, r)\}

method lookup (r : rep, k : Key) : Maybe Value :=

\{vopt \mid \forall v. vopt = Some v → (k, v) \in r\}

Figure 4. An abstract data type for caches

While mathematical sets provide a clean way to specify the methods of a Cache, they are unsuitable for an ADT implementation, which requires a computational representation type for method implementations to operate on. Fiat uses abstraction relations \cite{9, 10} to enable refinement of representation types. An abstraction relation \( A \approx B \) between two ADTs implementing a common signature ASig is a binary relation on the representation types A.rep and B.rep that is preserved by the operations specified in ASig. In other words, the operations of the two ADTs take "similar" input states to "similar" output states. Since operations in Fiat are implemented as computations, the methods of B may be computational refinements of A. Thus, an ADT method B.m is a refinement of A.m if

\[ A.m \simeq B.m \equiv \forall r_A \forall r_B. r_A \approx r_B \rightarrow \forall i.A.m(i) \sim B.m(i) \]

The quantified variable \( i \) stands for the method's other inputs, beside the "self" value in the data type itself; and \( o \) is similarly the parts of the output value beside "self."
The statement of constructor refinement is similar:
\[ A . c \equiv B . c \equiv \forall i \ r^*_A, B . m(i) \sim r^*_B \]
\[ \exists \alpha, A . m(i) \sim r^*_A \land \exists \alpha, r^*_A \equiv r^*_B \]

B is a refinement of A if all the operations of B are refinements of the operations of A:

\[ A \simeq B \equiv \forall o \in A . o \sim B . o \]

To be completely formal, this relation \( \simeq \) should be indexed by the abstraction relation \( \sim \), so that we write \( A \simeq_{\sim} B \) to indicate that relation \( \sim \) demonstrates the compatibility between the representation types of A and B. Then we can define more general refinement as:

\[ A \simeq B \equiv \exists R. A \simeq_{R} B \]

Note that by picking equality as the abstraction relation, we can justify the refinement of the code of a particular method using any \( \subseteq \) proof. The transitivity of \( \simeq \) justifies chaining such steps with others that make representation changes, allowing us to decompose proofs of ADT refinement into applications of basic refinement facts and optimizations of the representation type.

### 3. Synthesis by Fiat

The core of the Fiat framework includes a Coq formalization of refinement that can be used to write machine-checked proofs certifying that an implementation is a valid refinement of an ADT specification. The implementation of a computation \( C_S \) can be expressed in Coq as a computation \( C_I \) paired with a proof that it is a valid refinement of \( C_S \):

\[ \text{SharpenedComputation } C_S \equiv \Sigma C_I, C_S \supseteq C_I \]

The derivation of an implementation of a computation in Fiat is simply a user-guided search for the two components of this dependent product. By applying transitivity of refinement, a user may take a single step towards an eventual implementation:

\[ \forall C_I, \text{SharpenedComputation } C_S \rightarrow C_S \supseteq C_I \rightarrow \text{SharpenedComputation } C_S \]

A user satisfied with an implementation of a computation can finish the derivation by reflexivity of refinement:

\[ \forall C_I, \text{SharpenedComputation } C_I \]

These two lemmas allow derivations to be decomposed into sequences of applications of basic refinement facts. The refinement proof in Figure 3 gives the recipe for such an optimization script. Beginning with an initial goal of SharpenedComputation (insert \( k \mapsto v \)), the user can progressively apply transitivity with a proof of each refinement step until arriving at

if noKey(\( k \mapsto v \)) then \text{ret } [(k,v)] \cup l \ else \text{ret } l

Moving the \text{ret} outside of the if and applying reflexivity to this goal finishes the derivation.

The core of Fiat includes a collection of proofs of basic refinement facts to use in derivations. One example lemma is \textsc{RefinePickDecides}, which can be used to justify the first refinement step in the third column of Figure 3.

\[ \forall P_c, P_e, \{ x \mid P_c \rightarrow P_e x \land \neg P_e \rightarrow P_e x \} \supseteq b \leftrightarrow \{ b \mid \text{if } b \text{ then } P_c \text{ else } \neg P_e \}; \]

Users can freely augment the set of refinements available by writing their own refinement lemmas. These facts are safe to use in any derivation without any expansion of the trusted code base and without breaking the guarantees of refinement. Fiat automates applying these facts using Coq’s setoid rewriting tactics, which extend Coq’s rewriting machinery with support for partial-order relations other than Leibniz equality.

A synthesis goal involving an ADT is expressed as an ADT \( B \) paired with a proof that it is a valid refinement of a reference ADT \( A \):

\[ \text{Sharpened } A \equiv \Sigma B. A \simeq B \]

A user can interactively derive a Sharpened ADT implementation in a similar manner as above, by transitivity applying basic ADT refinement facts. Once a satisfactorily refined ADT has been derived, users can transform it into a version suitable for extraction to OCaml by refining its method bodies to \text{rets}.

In addition to the definitions making up the refinement framework discussed so far, Fiat includes a library of honing tactics to help automate the derivation of Sharpened ADTs. As an illustration of these honing tactics, we consider a derivation of an implementation of the cache specified by CacheSpec. Figure 5 shows this derivation, with single-bordered boxes framing honing tactics and double-bordered boxes framing the goals they produce.

**Honing Data Representations** One of the key design choices when implementing a bounded cache is the policy used to evict entries from a full cache. Many selection algorithms depend on more information than the reference implementation provides. Conceptually, these algorithms associate an index with each key in the cache, which the insertion algorithm uses to select a key for eviction when the cache is full. By augmenting the reference type with an additional set holding the indexes that are assigned to active keys, we are able to refine toward a whole family of cache algorithms. The particular abstraction relation we will use is

\[ r_v \approx_i (r'_v, r'_v) \equiv r_v \approx \forall k . (k, i) \in r'_v \leftrightarrow (k, i) \in r'_v \]

Importantly, it is always possible to build a default (very non-deterministic!) implementation for any abstraction relation:

\[ \text{default}_v^= \text{CacheSpec} \approx \{ (r'_v, o) \mid \forall k . r_v \approx r'_v \rightarrow \exists \alpha, A.m(r_v, i) \sim r'_v \rightarrow \exists \alpha, A.m(r_v, i) \sim r'_v \rightarrow \exists \alpha, A.m(r_v, i) \sim r'_v \approx r'_v \} \]

Fiat includes a honing tactic “honing representation using \( R \)” which, when given an abstraction relation \( R \), soundly changes the refinement goal from Sharpened \( A \) to Sharpened \( A' \), where \( A' \) is an ADT with the new representation type and with methods and constructors built by the \text{default}_v^= and \text{default}_v^= functions, respectively. Applying honing representation to CacheSpec produces the Cache2 ADT in Figure 5.

**Honing Operations** After honing the representation of CacheSpec, we can now specify the key replacement policy of a bounded cache as a refinement of the insert method. Fiat includes a honing tactic “hone method \( m \)” that generates a new subgoal for interactively refining \( m \). Figure 5 shows the result of using “hone method insert” to sharpen Cache2. We can refine the initial specification of insert in this goal to

\[ \{ f' \mid \exists k_{opt}, f' = [(k, v)] \cup \text{RemoveKey}(k_{opt}, l) \} \]

by rewriting with the \text{refineReplaceUsedKeyAdd} refinement fact, as in Figure 3. We then use a sequence of rewrites to select the key with the smallest index in \( r_v \) once \( r_v \) is full.

After selecting the replacement policy, the refined insert method still has dangling nondeterministic choices, with constraints like

1 The Coq documentation\cite{coq} has a full explanation of the machinery involved.
2 As the keywords refine, replace, and change are already claimed by standard Coq tactics, Fiat uses the keyword hon in many of the tactics it provides hence the name of the Sharpened predicate.
\{ r'_n | r'_n \approx r''_n \}, arising from the defaultₗ implementations. Determining these picks in every method amounts to selecting the particular replacement key policy. Initializing the index of a key to zero after insert and incrementing the index of a key after each lookup, for example, implements a least frequently used policy. Alternatively, we can use these indexes as logical timestamps by initializing the index of a key to a value greater than every index in the current map and having lookup leave indexes unchanged, implementing a least recently used policy. Once we have rewritten the goal further to select the latter policy, the “finish honing” tactic presents the original sharpened goal updated with the refined method body. Figure 6 presents the full optimization script for Figure 5.

**Invariants via Abstraction**  The idea of abstraction relations turns out to subsume the idea of representation invariants that must always hold on an ADT’s state. Consider that an LRU implementation can “cache” the value of the greatest timestamp in its representation and use it in insert to select the next timestamp efficiently. In order to justify this refinement, however, we must maintain the invariant that this cached value holds the latest timestamp. To do so, we can include the invariant in the abstraction relation:

\[ r_{vi} \approx_i \{ r'_{vi}, r''_{vi} \} \equiv r_{vi} \approx r_{vi} \land r''_{vi} = \max_{(k,i) \in r_{vi}} i \]

Now when honing insert, we can exploit the invariant on \( r'_{vi} \) from \( r_{vi} \approx r_{vi} \) to implement the selection of the timestamp. Since the abstraction relation formalizes the requirements on the saved index, the default implementation of insert automatically keeps the new piece of state up-to-date, albeit in a nondeterministic way that needs further refinement.

**Implementing the Cache**  Once we are satisfied that the cache is sufficiently specified, we can implement it by honing the representation type to a data structure efficiently implementing the remaining nondeterministic operations on sets. For this example, we choose the finite maps implementation in Coq’s standard library. We have proven a library of lemmas showing that the operations provided by finite maps correctly implement mathematical set operations used to specify the cache behaviors. The refinement lemmas can be used to implement a number of different high-level specifications. Conversely, since intermediate specifications (such as Cacheₗ) are independent from the implementation data structure, a library of refinement facts about a different data structure can be used to synthesize a different implementation. As an example, we could implement Cacheₗ with a single map of keys to pairs of values and timestamps, or as two separate maps, one from keys to values and another from timestamps to keys. The former implementation uses less memory, but looking up the key to evict takes \( O(n) \) time, whereas the latter can use the second map to do this lookup in \( O(1) \) time.

**Taking Stock**  We pause here to put the last two sections in context. Fiat provides a number of simple concepts for organizing the refinement of specifications into efficient code, where abstract data types are a central idea for packaging methods with private data. We apply refinements step-by-step with optimization scripts, which apply to sharpened goals in Coq. These scripts are implemented in Ltac, Coq’s Turing-complete tactic language, so it is possible to implement arbitrarily involved heuristics to choose good refinement sequences, packaged as callable tactic functions. The Coq kernel ensures that only semantically valid refinements will be admitted, providing a kind of enforced modularity that allows users to write their own refinements to use in optimization scripts. This idea is simple but powerful, supporting decomposition of programming tasks into uses of separate encapsulated components for functionality and optimization.

The next section shows how to automate the synthesis of ADTs in a domain with a well-known functionality/optimization split.
complete automating derivations in this domain with a set of honing tactics that act like database query planners.

4. Query Structures
This section presents a library for writing specifications of ADTs using reference implementations called query structures and with SQL-like query and insert operations. The library also provides tactic support for automatically refining those specifications into correct and efficient implementations, allowing users to generate custom database-like ADTs. Figure 1 from the introduction. This code is taken almost verbatim from the QueryStructure library.

4.1 Specification of Query Structures
The Fiat query structure library includes a DSL for specifying reference query structures implemented in convenient notation, thanks to Coq’s extensible parser. Figure 7 presents the grammar of this embedded DSL; the types, terms, and propositions are exactly those of Coq itself. The grammar also draws on an infinite set of identifiers.

Query structures are designed to align with the conceptual abstraction of SQL databases as sets of named relations (i.e. tables) containing tuples. The query structure library defines tuples as functions from attributes (i.e. column names) to values; the type of each value is described by a heading mapping attributes to types. Tuple projection is denoted using the ! notation:

\[
\text{Author:: } \text{string, Title:: string, ISBN:: nat}
\]

To align with the standard SQL notion of tables, relations are multisets (mathematical sets that can have repeated elements) of tuples. We implement that concept more concretely by pairing each tuple with a unique numeric index, storing these pairs as sets. Subsection 4.2 discusses how these indexes can be dropped for query structure implementations that only have SQL-like operations. A relation (S) schema specifies the heading of the tuples contained in a relation and also a set of constraints describing properties that included tuples must satisfy. Relations themselves are implemented as records, with a field for a mathematical set containing the relation’s tuples, and a field for a proof that the schema constraints hold for every pair of tuples in the relation. A query structure is similarly described by a query structure (Q) schema that contains a set of schemas and a set of cross-relation constraints describing properties that must hold between tuples of different tables. A query structure is implemented as a record that contains a list of relations and proofs that each pair of relations satisfies its cross-relation constraints. The relations of a query structure are accessed using the ! notation: qs[i].

Data-Integrity Constraints
The constraints contained in relation and query structure schemas are familiar to SQL programmers in the form of data-integrity properties like functional dependencies and foreign-key constraints. In our library, these constraints are simply representation invariants over the state of query structures, enforced by the proof fields of the relation and query structure records. Fiat’s query structure library includes notations for these common SQL constraints (listed in Figure 7), but S and Q schema constraints are not limited to them: query structures can include arbitrary predicates over tuples. It is possible to specify that the population of a nation is always equal to the sum of the populations of its cities, for example. Since query structure notations are simply an embedded DSL for writing ADTs, it is possible to write non-SQL-like operations for these ADTs – in addition to conforming with the standard data-integrity properties SQL programmers are familiar with, explicitly including these constraints allows users to be sure that they cannot write operations that go wrong.

4.2 Specification of Operations
The query structure library also provides a set of definitions and notations for specifying query and insertion operations mimicking standard SQL queries. Note that ADTs using query structures as reference implementations can support a mix of these operations and operations with arbitrary specifications, and can furthermore use SQL-style notations in the specifications of nonstandard operations. The most basic definition is empty, which returns a query structure containing only empty relations. All the operation specifications provided by the library have two implicit arguments: qs, the Q schema of the reference implementation; and q, the rep argument used by each method.

Querying Query Structures Figure 9 presents the notations the query structure library provides for specifying query operations.

Figure 6. Complete optimization script for Figure 5

| hone method | insert. | { | StartMethod | setoid rewrite refine_ReplaceUsedKeyAdd. | setoid rewrite refine_SubEnsembleInsert. | autowrite with monad laws. | setoid rewrite refine_pick_KeyToBeReplaced_min. | setoid rewrite refine_IfThenElse_Bind. | autowrite with monad laws. | setoid rewrite refine_IfOpt_ThenElse_Bind. | autowrite with monad laws. | setoid rewrite refine_pick_CacheADTwLogIndex_AbsR. | setoid rewrite refine_pick_KVEnsembleInsertRemove with (1 := EquivKeys_H). | setoid rewrite refine_pick_KVEnsembleInsert with (1 := EquivKeys_H). | autowrite with monad laws; simpl. | finish honing. | } | 1 | 2 |
empty \equiv \{ q \mid \forall i \in qs. qli = \emptyset \}

For \( b \equiv \text{result} \leftarrow b; \{ l [\text{Permutation} l \text{result}] \} \):

\( \langle x \in i \rangle \ b \equiv \text{table} \leftarrow \{ l [\text{qli} \sim l]; \text{fold_right} (\lambda a. l \leftarrow x; l' \leftarrow b; \text{ret} (l + l')) \} \left( \langle x \rangle \right) \left( \langle \lambda x. b \rangle \right) \left( \langle \text{table} \rangle \right) \)

Where \( P \ b \equiv \{ l \mid \exists t \rightarrow l \wedge \neg P \rightarrow l = \emptyset \} \)

Return \( a \equiv \text{ret} [a] \)

Count \( b \equiv \text{results} \leftarrow b; \text{ret} \left( \text{length} (\text{results}) \right) \)

Query Structure Inserts

Figures 9. Notations for initializing a query structure and defining query operations.

Queries specified by the For notation compute any permutation of a list of result tuples generated by a body expression. We use permutations in order to avoid fixing a result order in advance. Since queries are specified over relations implemented as mathematical sets, the definitions of these operations are a straightforward lifting of the standard interpretation of queries using comprehensions [3] and the list monad to handle computations. The in notation picks a result list that is equivalent (\(~\)) to the mathematical set of relation \( i \); this is a placeholder for an enumeration method that is filled in by an implementation. This equivalence relation ignores the indexes of the tuples and only considers their multiplicities, and result thus disregards the indexes of the tuples in \( i \). The body \( b \) is a function that is mapped over each tuple in result, producing a list of computations of query results for each element. This list of computations is then flattened into a single list of query results. Finally, Where clauses are allowed to use arbitrary predicates. Decision procedures for these predicates are left for an implementation to fill in.

Query Structure Inserts

Whereas queries are observers for the query structure, insertion operations are mutators returning modified query structures, which by definition must satisfy the data-integrity constraints specified by their \( Q \) schema. The naive specification of insertion always inserts a tuple into a query structure:

\[
\text{Insert} \ t \ into \ i \equiv \{ q' \mid \forall u. u \in qli' \leftrightarrow u \in (qli \cup \{ t \}) \}
\]

This specification is unrealizable in general, however, as there does not exist a proof of consistency for a query structure containing a tuple violating its data-integrity constraints.

The specification of Insert given in Figure 10 thus only specifies insertion behavior when the tuple satisfies both the \( S \) and \( Q \) schema constraints. This definition highlights Fiat's ability to specify method behavior at a high level without regard for implementation concerns. The specification delays the decision of how to handle conflicts (i.e., ignore the insertion, drop conflicting tuples, etc.) to subsequent refinements.

As we shall see in the following section, this specification can be transformed automatically into a more readily implementable form.

4.3 Honing Query Structures

Figure 1 contains the specification of an ADT using a query structure with the bookstore schema from Figure 8 and insert and query operations specified with the notations from the query structure library. As an initial step in implementing this specification, the library provides a fully automated tactic for removing the data-integrity constraints from the representation type of the ADT, building an ADT that uses unconstrained query structures, i.e.

\[ \text{Count} (\text{For} (\text{book} \in \text{Books}) \text{bookISBN} = \text{orderISBN}) \]

\[ \text{Count} (b \mid b \text{decides} (\exists \text{book} \in \text{Books}. \text{bookISBN} = \text{orderISBN})) \]

Similarly, functional-dependency checks are refined from

\[ \text{Count} (\text{For} (\text{book} \in \text{Books}) \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \land \text{bookTitle} = \text{book1Title}) \]

\[ \text{Count} (b \mid b \text{decides} (\forall \text{book} \in \text{Books}. \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \land \text{bookTitle} = \text{book1Title})) \]

\[ \text{Count} (\text{For} (\text{book} \in \text{Books}) \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \lor \text{bookTitle} = \text{book1Title}) \]

\[ \text{Count} (b \mid b \text{decides} (\forall \text{book} \in \text{Books}. \text{bookISBN} = \text{book'ISBN}) \land \text{bookAuthor} = \text{book1Author} \lor \text{bookTitle} = \text{book1Title})) \]

\[ \text{Count} (\text{For} (\text{book} \in \text{Books}) \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \leftrightarrow \text{bookTitle} = \text{book1Title}) \]

\[ \text{Count} (b \mid b \text{decides} (\forall \text{book} \in \text{Books}. \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \leftrightarrow \text{bookTitle} = \text{book1Title})) \]

\[ \text{Count} (\text{For} (\text{book} \in \text{Books}) \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \leftrightarrow \text{bookTitle} = \text{book1Title})) \]

\[ \text{Count} (b \mid b \text{decides} (\forall \text{book} \in \text{Books}. \text{bookISBN} = \text{book'ISBN} \rightarrow \text{bookAuthor} = \text{book1Author} \leftrightarrow \text{bookTitle} = \text{book1Title})) \]
on a container must return the same results, modulo permutation, as
filtering the container’s elements using the `bfind_matcher` function
(including this function allows us to retain maximal generality
by allowing different bag instances to provide widely varying
types of find functions). Finally, for performance reasons, a bag
implementation is required to provide a `bcount` method (elided here),
used to count elements matching a given search term instead of
enumerate all.

Class Bag (TContainer TItem TSearchTerm : Type) :=

- `bempty` : TContainer;
- `bfind_matcher` : TSearchTerm → TItem → bool;
- `benumerate` : TContainer → list TItem;
- `bfind` : TContainer → TSearchTerm → list TItem;
- `binsert` : TContainer → TItem → TContainer;
- `binsert_enumerate` :
  ∀ inserted container,
  Permutation
  (benumerate (binsert container inserted))
  (inserted :: benumerate container);
- `benumerate_empty` : benumerate bempty = [];
- `bfind_correct` :
  ∀ container search_term,
  Permutation (filter (bfind_matcher search_term)
  (benumerate container))
  (bfind container search_term).

4.5 Bag Implementations

Fiat provides two instances of the Bag interface, one based on lists
and the other based on AVL trees through Coq’s finite map interface.
The definitions making up the list instance are extremely simple and
can thus be reproduced in their entirety below:

```
Instance ListAsBag (TItem TSearchTerm : Type)
  (matcher : TSearchTerm → TItem → bool) :
Bag (list TItem) TItem TSearchTerm := {
  bempty := nil;
  bfind_matcher := matcher;
  benumerate := lambda container.
  filter (matcher search_term) container;
  binsert_container item := item :: container}.;
```

The tree-based implementation, though lengthier, is also readily
explained: it organizes elements of a data set by extracting a key
from each element and grouping elements that share the same key
into smaller bags. The smaller bags are then placed in a map-like
data structure, which allows for quick access to all elements sharing
the same key. Tree-based bags can thus be used to construct a nested
hierarchy of bags, with each level representing a further partition
of the full data set (in that case, smaller bags are tree-based bags
themselves). In practice, tree bags are implemented as AVL trees
mapping projections (keys) to sub-trees whose elements all project
to the key under which the sub-tree is filed.

The search terms used to query tree-based bags are pairs, each
consisting of an optional key and a search term for sub-bags. The
`bfind` operation behaves differently depending on the presence or
absence of a key: if a key is given, then `bfind` returns the results
of calling `bfind` with the additional search term on the smaller bag
whose elements project to the given key. If no key is given, then
`bfind` calls `bfind` on each smaller bag and then merges all results (a
process usually called a skip-scan, in the database world). Finally,
`benumerate` is implemented by calling `benumerate` on each sub-tree
and concatenating the resulting lists, and `binsert` is implemented by
finding (or creating) the right sub-bag to insert into and calling
`binsert` on it. This design is similar to that found in most database
management systems, where tuples are indexed on successive columns, with additional support for skip-scans. Figure 12 presents an example of such an indexed bag structure.

Figure 12. Indexed data is organized in a hierarchy of nested bags. In this example, the data set is first partitioned by column x, then by column y. Since our nested bags implementation supports skip-scanning, this same index can be used to answer queries related to x, to y, and to both x and y.

4.6 Automation

As an example of a very general optimization script, we implemented a tactic plan, which works automatically and is able to synthesize efficient implementations of a variety of query structures containing at most two tables, based on index structures backed by our bags library. Figure 13 shows an example of the code output by plan for our running Bookstore example. To produce this code from the reference implementation, the programmer only needs to specify a plan.

For our bags library. Figure 13 shows an example of the code output by plan for our running Bookstore example. To produce this code from the reference implementation, the programmer only needs to specify a plan.

The query heuristics run to refine default (nondeterministic) method bodies induced by choices of abstraction relations. Here a relevant abstraction relation connects each table to a bag-based index. Default query bodies will compute with table contents specified as mathematical sets, and we need to rewrite those operations to use the indexes efficiently. Every actual code transformation is implemented as a Coq setoid rewrite; we just need to determine a useful sequence of rules.

1. The starting point of refinement is expressions that work directly with mathematical sets. For example:

   \[ \text{For } (r \text{ in } T) \text{ Where } (r.c_1 = 7) \text{ Return } (r.c_2) \]

2. A concretization step replaces all references to sets with references to lists built by enumerating all members of index structures. For instance, the abstraction relation might declare that table T is implemented with index structure I, in which case we may rewrite the above to:

   \[ \{ \ell | \text{Permutation } \ell (\text{map } (\lambda r. r.c_2) \text{ (filter } (\lambda r. r.c_1 == 7) \text{ (benumerate } I))) \} \]

   That is, we convert set operations into standard functional-programming operations over lists, starting from the list of all table elements. Note that we use nondeterministic choice to select any permutation of the list that we compute. We do not want to commit to ordering this early, since we hope to find more efficient versions with different orders.

3. A rewriting-modulo-permutation step simplifies the list expression, possibly with rules that change ordering. Here we use standard algebraic laws, like \( \text{map } f (\text{map } g \ell) = \text{map } (f \circ g) \ell \). Less standard rules locate opportunities to apply our index structures. Our example query would be refined as follows, assuming the index structure only covers table column c1:

   \[ \{ \ell | \text{Permutation } \ell (\text{map } (\lambda r. r.c_2) \text{ (bfind } I (7, []))) \} \]

   Our tactic analyzes filter functions syntactically to figure out useful ways of applying index structures. In full generality, the heuristics of this phase apply to filter conditions over two tables, and they are able to decompose conjunctive conditions into some use of indexes and some use of less efficient filtering for conditions that do not map neatly to the indexes.

4. A commitment step accepts the current list expression as the final answer, committing to an ordering. Our example is refined in one simple step to:

   \[ \text{ret } (\text{map } (\lambda r. r.c_2) \text{ (bfind } I (7, []))) \]

   This basic three-step process can be extended quite flexibly. Our implementation handles aggregate functions (e.g., count or max) in the same way. A use of such an operation is concretized to a fold over a list, and we apply rewriting to incorporate chances to use index structures to compute folds more directly.

   One further subtlety applies in the rewriting step for queries over multiple tables. Concretization rewrites a join of two tables into a Cartesian-product operation Join_Lists, defined as follows, where
We can use the cache consistency predicate to refine the query structure to include a cache ADT keyed on author names. The abstraction relation used to hone the representation maintains the invariant that the cache of the new representation only holds valid book counts for each author:

\[ r_{\ell_1} \equiv_{c} (r_{\ell_1}', r_{\ell_2}') \equiv r_{\ell_2} = r_{\ell_1} \wedge \forall k, v, (k, v) \in r_{\ell_2}' \rightarrow \text{NumTitles}(r_{\ell_2}, k) \sim v\]

We can use the cache consistency predicate to refine NumTitles so that it first nondeterministically picks a key in the cache using lookup, returns that value if it exists, and otherwise runs the query and adds a new key to the cache (this updated cache trivially satisfies the representation invariant). NumOrders and PlaceOrder are unchanged. Since AddBook can increase the number of books for an author in the cache, it needs to update the cache if the author of the new book is in the cache. Applying all these refinements to the bookstore ADT from Figure 11 yields the refined ADT in Figure 14.

Observe that the following refinement holds:

\[ f \left( \text{Count} (\text{For} (x \in R \cup \{a\}) b) \right) \rightarrow f' \left( \text{For} (x \in R + l') b' \right); \]

thus allowing us to refine the query in AddBook:

\[ \text{Count}(l \leftarrow \text{Count} (\text{For} (x \in R \cup \{a\}) b) \leftarrow l'; \]

\[ \text{Return} (l + l') \]

which can be further refined into:

\[ n \leftarrow \text{Count} (\text{For} (x \in R \cup \{a\}) b) \leftarrow n'; \]

\[ \text{Return} (n + n') \]

Due to the representation invariant in the abstraction relation, we know that the query bound to \( n' \) returns precisely the cache contents, allowing us to refine the update to simply increment the value of author currently in the cache:

\[ \text{mth AddBook} \left( r \leftarrow \text{Count} (\text{For} (x \in R \cup \{a\}) b) \leftarrow l'; \]

\[ \text{Return} (l + l') \]

This case is actually an example of the broader finite differencing [13] refinement for improving the performance of an expensive operation \( f \) whose input can be partitioned into two pieces, old \( y \) and new \( x \), such that \( f(x \oplus y) = f'(x) \oplus f(y) \). The representation invariant ensures that each value in the cache already stores \( f(y) \), allowing us to reduce the computation of \( f(x \oplus y) \) to computing \( f'(x) \) and updating the value in the cache appropriately. Note that Fiat’s refinement process supports finite differencing of any ADT operation, through the use of abstraction relations to express cache invariants and refinements to replace repeated computations. In particular, (2) allows us to easily cache \( \text{For} \) queries by partitioning their results into novel results and the portion already in the cache when performing \( \text{Insert} \) updates.
5. Evaluation

5.1 Extraction of the Bookstore Example

Once they have been fully refined, our data structures can be extracted to produce verified OCaml database management libraries. We performed such an extraction for the bookstore example and benchmarked it. The observed performance is reasonable, and the operations scale in a way that is consistent with the indexing scheme used, as demonstrated by Figure 15. Starting with an empty database, for instance, it takes about 480 ms on an Intel Core i5-3570 CPU @ 3.40GHz to add 10 000 randomly generated books filed under 1 000 distinct authors, and then 6.8 s to place 100 000 orders. Afterward, the system is able to answer about 350 000 GetTitles queries per second and about 160 000 NumOrders queries per second.

![Figure 15. Average query execution time, for increasingly large bookstores](image)

5.2 Further Examples

To demonstrate the generality of our automated refinement strategies, the code base also includes two more examples: a weather-data database and a stock-market database, both of which are included in the Fiat distribution.

The weather example includes two tables – one to hold information about the weather stations and one to log the measurements – and supports operations such as counting the number of stations in a given geographic area or computing the highest temperature on one day. The stock market example includes one table listing information about stocks and one table keeping track of transactions, and it allows clients to compute the total volume of shares exchanged on one day for a particular stock, plus the largest transaction for a given type of stock.

In both cases skip-scanning allowed for space-efficient indexing (in the weather case, stations could produce a small number of different measurement types: wind speed, temperature, air pressure, or humidity; in the stocks case, different types of stocks were distinguished), and in both cases nontrivial functional dependencies were expressed (for examples, two transactions occurring at the same time and concerning the same stock could differ in the number of shares exchanged but not in price). The plan tactic synthesizes correct, efficient implementation code in both cases.

6. Related Work

The concept of deriving implementations that are correct by construction via stepwise refinement of specifications has been around since at least the late sixties [7].

Deductive Synthesis Specware [20] and its predecessors KIDS [16] and DTRE [2] are deductive synthesis tools for deriving correct-by-construction implementations of high-level specifications. Specware is accompanied by a library of domain theories that describe how to do iterative decomposition of high-level specifications into subproblems until an implementation can be constructed. At each step, Specware checks the validity of the refinement, although only recently have they begun generating Isabelle/HOL proof obligations justifying these transformations. Each of these proof obligation generators makes up part of Specware’s trusted code base; by implementing Fiat completely in Coq we rely on a considerably smaller trusted code base. At the end of refinement, Specware has a series of automated and quite sophisticated transformations that generate C code, though these final steps are currently unverified. In contrast, derivations of ADTs with Fiat are completely verified by Coq, and these derivations may be integrated within larger, more general proof developments. We have also demonstrated more automated refinement for more restrictive domains, as in our query structure examples.

Synthesis of Abstract Data Types There is also a philosophical difference between Fiat and Specware – Kestrel has focused on using Specware to develop families of complex algorithms, including families of garbage collectors [14], SAT solvers [17], and network protocols. In contrast, we envision Fiat being used to generate high-assurance code for algorithmically “simple” domains that are amenable to automation. A number of domains have been shown to have this property: Paige et. al [12] demonstrate how efficient implementations of ADTs supporting set-theoretic operations can be derived by applying fixed-point iteration [12] to generate initial implementations, using finite differencing [13] to further optimize the resulting implementation, before finally selecting data structure implementations. The generation of data types supporting query-like operations is another such domain. P2 [11] was a DSL extension to C that allowed users to specify the layout of container data structures using a library of structures implementing a common interface, akin to Fiat’s Bag interface. This interface included an iterator method for querying contents of the container – implementations of these iterators would dynamically optimize queries at runtime. More recently, Hawkins et. al [8] have shown how to synthesize the implementations of abstract data types specified by abstract relational descriptions supporting query and update operations. They also provide an autotuner for selecting the best data representation implementation in the space of possible decompositions. Our work with Fiat expands on these past projects by adding proofs of correctness in a general-purpose proof assistant, which also opens the door to sound extension of the system by programmers, since Coq will check any new refinement rules.

Constraint-Based Synthesis Constraint-based synthesis formulates the synthesis problem as a search over a space of candidate solutions, with programmers providing a set of constraints to help prune the search space. The Sketch [18] synthesis system, for exam-
ple, allows programmers to constrain the search space by encoding their algorithmic insight into skeleton programs with “holes” that a synthesizer automatically completes. Sketching-based approaches have been used to synthesize low-level data-structure manipulating algorithms [15], concurrent data structures [19], and programs with numeric parameters that are optimized over some quantitative metric [4]. These approaches fit into the broad decomposition of “functionality + optimization” proposed here, with the initial sketch representing the former and the synthesizer providing the optimization. Excitingly, Fiat enables opportunities for programmers to inject further insight into the synthesis process by chaining together honing tactics with various degrees of automation. Subsection 4.7 provides an example of such a development, with the user first automatically dropping data-integrity constraints via a honing tactic before manually specifying how to cache certain queries.

**Reasoning with Refinements** Cohen et al. rely on a similar foundation of refinement to verify an algebra library in Coq using data type refinement [5] by verifying algorithms parameterized over the data type and its operations. Verification is done using a simple, “proof-oriented” data type. The authors then show how to transport the proof of correctness to a version of the algorithm using a more efficient implementation that is related to the proof-oriented data type by a refinement relation. In contrast, Fiat is a system for (semi-) automatically deriving efficient ADTs that are valid refinements. The two approaches could certainly be combined to enable users to build and verify clients of ADTs synthesized by Fiat.

7. Future Work and Conclusion

We have reported here on the start of a project to explore the use of proof assistants to enable a new modularity pattern in programming: separating functionality from performance, where programmers express their functionality and then apply optimization scripts to refine it to efficient implementations. Special-case systems like SQL engines have provided this style of decomposition, but only for hardcoded domains of functionality. We explained how the design of Fiat allows programmers to define new functionality domains and new optimization techniques, relying on Coq to check that no optimization technique breaks program semantics. Programmers think of implementing a new database engine as a big investment, but they think of implementing a new container data structure as a reasonable component of a new project. The promise of the Fiat approach is to make the former as routine as the latter, by giving that style of optimization strategy more first-class status within a programming environment, with enforced modularity via checking of optimization scripts by a general-purpose proof kernel.

We plan to explore further applications of Fiat, both by identifying other broad functionality domains that admit effective libraries of optimization scripts, and by narrowing the gap with hand-tuned program code by generating low-level imperative code instead of functional code, using the same framework to justify optimizations that can only be expressed at the lower abstraction level.

**Acknowledgments**

We thank Eddy Westbrook, Arthur Charguéraud, and the anonymous reviewers for their feedback on earlier versions of this paper. The second author would like to thank École Polytechnique for allowing and supporting the internship during which his contributions were made. This work has been supported in part by NSF grant CCF-1253229 and by DARPA under agreement number FA8750-12-2-0293. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

**References**


