Using Formal Methods To Reason About Semantics-Based Decompositions Of Transactions[*]

Paul Ammann[†] Sushil Jajodia[‡] Indrakshi Ray[§]
Center for Secure Information Systems &
Department of Information and Software Systems Engineering
George Mason University Fairfax, VA 22030-4444

Abstract

Many researchers have investigated the process of decomposing transactions into smaller pieces to increase concurrency. The research typically focuses on implementing a decomposition supplied by the database application developer, with relatively little attention to what constitutes a desirable decomposition and how the developer should obtain such a decomposition. In this paper, we argue that the decomposition process itself warrants attention. A decomposition generates a set of proof obligations that must be satisfied to show that a particular decomposition correctly models the original collection of transactions. We introduce the notion of semantic histories to formulate and prove the necessary properties. Since the decomposition impacts not only the atomicity of transactions, but isolation and consistency as well, we present a technique based on formal methods that allows these properties to be surrendered in a carefully controlled manner.

1 Introduction

Key to the success of the transaction model are the *atomicity*, *consistency*, and *isolation* properties. Atomicity ensures that either all actions of a transaction complete successfully or all of its effects are absent. Consistency ensures that a transaction when executed by itself, without interference from other transactions, maps the database from one consistent state to another consistent state. Isolation ensures that no transaction ever views the partial effects of other transactions even when transactions execute concurrently.

Sometimes performance requirements force a transaction to be decomposed into *steps*, especially if the transaction is long-lived. Consider the simple example of making a hotel reservation. The reserve transaction might ensure there are still rooms vacant, select a vacant room that matches the customer's preferences, and record billing information. Since the reserve transaction might last a relatively long time – for example, when the customer makes reservations by phone – an implementation might force the three steps in the reserve transaction to occur separately.

Breaking transactions into steps not only sacrifices atomicity (since atomicity of the single logical action is lost), but impacts consistency and isolation as well. Execution of a step may leave the database in an inconsistent state, which may be viewed by other transactions or steps. Thus it is necessary to reason about the interleavings of the steps of different transactions. Even if the step-by-step decomposition of a single transaction is understood in isolation, reasoning about the interleaving of these steps with other transactions, possibly also decomposed into steps, is difficult.

To reason about interleavings, we introduce the notion of *semantic* histories which not only list the sequence of steps forming the history, but also convey information regarding the state of the database before and after execution of each step in the history. We identify properties which semantic histories must satisfy to show that a particular decomposition correctly models the original collection of transactions.

The paper is organized as follows. Section 2 reviews related research. Section 3 presents a motivating example. Section 4 describes our model and applies it to the motivating example. Section 5 outlines an implementation. Section 6 concludes the paper.

We adopt the Z specification language [Spi89] for expressing model-based specifications. Z is based on set theory, first order predicate logic, and a *schema calculus* to organize large specifications. Knowledge of Z is helpful, but not required, for reading this pa-

[*]The text of this paper appears in VLDB '95, Proceedings of the Twenty-First International Conference on Very Large Databases, Zurich, Switzerland, September, 1995. In addition, the appendices of this report contain proofs that space constraints precluded from the VLDB paper.

[†]Partially supported by National Science Foundation under grant number CCR-9202270.

[‡]Partially supported by a grant from ARPA, administered by the Office of Naval Research under grant number N0014-92-J-4038, by National Science Foundation under grant number IRI-9303416, and by National Security Agency under contract number MDA904-94-C-6118.

[§]Partially supported by a George Mason University Graduate Research Fellowship Award.

per, since we narrate the formal specification in English. We explain conventions peculiar to Z as necessary. Table 1 briefly explains the Z notation used in our examples.

2 Related Work

Most transaction-oriented models enforce a very low level, syntactic notion of consistency, namely serializability with respect to read/write conflicts [BHG87]. An expansion is the atomic transactions work [Her87, HW91, LMWF94, Lyn83, Wei84, Wei88], in which access operations are given by the particular abstract data type. We relax the requirement that transactions in correct executions histories appear atomic.

Many researchers have broken transactions into steps and developed semantics-based correctness criteria for decompositions [AAS93, BR92, FO89, GM83, JM87]. In [SSV92] correctness for chopped-up transactions is defined such that any stepwise serial history is equivalent to a serial history. We disallow some stepwise serial histories based on semantic considerations. Some have weakened the notion of serializability. For example, quasi-serializability defines global correctness for transactions distributed over heterogeneous systems [DE90]. Researchers have introduced the notions of transaction steps, countersteps, allowed vs. prohibited interleavings of steps, decomposed databases as well as transactions [SLJ88], and implementations in locking environments. Our focus is on the front-end activities of defining desirable transaction decompositions and aiding the developer in deriving such decompositions.

The idea of specifying transactions with preconditions and postconditions has been elaborated in the NT/PV model [KS94, KS88], which is based on nested transactions, multiple versions and explicit predicates. A transaction, denoted by (T, P, I, O), is characterized by the set of subtransactions T of the transaction, the partial order P among subtransactions, the input conditions or preconditions I, and the output conditions or postconditions O. An execution of a transaction is correct if it begins in a state that satisfies the preconditions, the subtransactions execute consistently with the partial order, and the state after execution satisfies the postconditions. An execution of an interleaved set of transactions is NT/PV correct if every transaction in the set executes correctly. In [KS94, KS88], the application developer has the burden of correctly specifying the preconditions and postconditions and of determining the partial order of subtransactions in a transaction. Our work focuses on a subset of what is covered by the NT/PV model; we help the application developer decompose transactions into steps and reason about the resulting interleavings.

The ACTA framework for specifying models of extended transactions [CR94] requires extension to accommodate our work, just as ACTA requires extension to accommodate NT/PV [KS94]. Specifically, ACTA conditions cannot express preconditions and postconditions of transactions in our semantic histories.

$\mathbb{N}$	Set of Natural Numbers
$\mathbb{P}\,A$	Powerset of Set A
$\#A$	Cardinality of Set A
$\setminus$	Set Difference
$A \mathbin{;} B$	A Composed with B
$x \mapsto y$	Ordered Pair $(x,\ y)$
$A \rightarrow\!\!\!\!+ B$	Partial Function from A to B
$A \rightarrowtail\!\!\!\!+ B$	Partial Injective Function from A to B
$B \lhd A$	Relation A: Set B Removed from Domain
$A \rhd B$	Relation A: Range Restricted to Set B
dom A	Domain of Relation A
ran A	Range of Relation A
$A \oplus B$	Function A Overridden with Function B
$x?$	Variable $x?$ is an Input
$x!$	Variable $x!$ is an Output
x	State Variable x before an Operation
x'	State Variable x' after an Operation
ΔA	Before and After State of Schema A
ΞA	ΔA with No Change to State

Table 1: Z Notation

3 The Hotel Database

We illustrate our ideas with a hotel database example. A Z specification of the example appears in figure 1. The hotel database has a set of objects, two integrity constraints on these objects, and three types of transactions, which we identify and explain below.

The two types, *Guest* and *Room*, enumerate all possible guests and all possible hotel rooms, respectively. The global variable *total* is the size of the hotel.

In Z states are described with a two-dimensional graphical notation called a *schema*, in which declarations for the objects in the state appear in the top part and constraints on the objects appear on the bottom part. Objects in the hotel database are listed in the schema *Hotel*, which defines the state of the hotel.

The object *res* is a natural number that records the total number of reservations, *RM* is a partial injection that relates guests to rooms, *ST* is a partial function that records the status of each room in *Hotel*, and *guest* records the set of guests.

The integrity constraints on the objects in hotel database appear in the bottom part of *Hotel*. There are two integrity constraints:

1. $\#RM = res$. The number of guests who have been assigned rooms (the size of the RM function) equals the total number of reservations (res).

2. $\mathrm{dom}(ST \rhd \{\mathit{Unavailable}\}) = \mathrm{ran}\, RM$. The set of unavailable rooms ($\mathrm{dom}(ST \rhd \{\mathit{Unavailable}\})$) is exactly the set of rooms reserved by guests

$$
\begin{array}{l}
[\mathit{Guest}, \mathit{Room}] \\
\mathit{Status} ::= \mathit{Available} \mid \mathit{Unavailable} \\
\quad \mathit{total} : \mathbb{N}
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{Hotel} \\
\mathit{res} : \mathbb{N};\ \mathit{RM} : \mathit{Guest} \pinj \mathit{Room} \\
\mathit{guest} : \mathbb{P}\,\mathit{Guest};\ \mathit{ST} : \mathit{Room} \pfun \mathit{Status} \\
\hline
\#\mathit{RM} = \mathit{res};\ \mathrm{dom}(\mathit{ST} \rhd \{\mathit{Unavailable}\}) = \mathrm{ran}\,\mathit{RM} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{Reserve} \\
\Delta \mathit{Hotel};\ g? : \mathit{Guest};\ r! : \mathit{Room} \\
\hline
\mathit{res} < \mathit{total};\ g? \notin \mathit{guest} \\
\mathit{ST}(r!) = \mathit{Available};\ \mathit{res}' = \mathit{res} + 1 \\
\mathit{ST}' = \mathit{ST} \oplus \{r! \mapsto \mathit{Unavailable}\} \\
\mathit{RM}' = \mathit{RM} \cup \{g? \mapsto r!\} \\
\mathit{guest}' = \mathit{guest} \cup \{g?\} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{Cancel} \\
\Delta \mathit{Hotel};\ g? : \mathit{Guest} \\
\hline
g? \in \mathit{guest};\ \mathit{res}' = \mathit{res} - 1 \\
\mathit{ST}' = \mathit{ST} \oplus \{\mathit{RM}(g?) \mapsto \mathit{Available}\} \\
\mathit{RM}' = \{g?\} \ndres \mathit{RM};\ \mathit{guest}' = \mathit{guest} \setminus \{g?\} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{Report} \\
\Xi \mathit{Hotel};\ \mathit{currentstatus}! : \mathit{Room} \pfun \mathit{Status} \\
\mathit{currentassignments}! : \mathit{Guest} \pinj \mathit{Room} \\
\hline
\mathit{currentstatus}! = \mathit{ST} \\
\mathit{currentassignments}! = \mathit{RM} \\
\hline
\end{array}
$$

Figure 1: Initial Specification of the Hotel Database

(ran RM). In other words, every unavailable room must be associated with some guest.

The three types of transactions in the hotel database are *Reserve*, *Cancel*, and *Report*. *Reserve* takes as input a guest $g?$ and produces as output a room assignment $r!$. *Reserve* has a precondition that there must be fewer than *total* reserved rooms and $g?$ must be a new guest. (Our particular example does not allow guests to register multiple times). *Reserve* has a postcondition that room $r!$ with status *Available* is chosen, the total number of reservations *res* is incremented, the status of $r!$ is changed to *Unavailable*, the ordered pair $g? \mapsto r!$ is added to the function RM, and $g?$ is added to the set *guest*.

Cancel cancels the reservation for guest $g?$. *Cancel* has a precondition that the $g?$ is in *guest*. *Cancel* has a postcondition that *res* is decremented, the status of the room assigned to $g?$ is changed to *Available*, $g?$ is removed from the domain of the function RM, and $g?$ is removed from the set *guest*.

Report has no precondition, and merely produces the state components ST and RM as outputs.

Since the role of initialization is peripheral to our analysis, we omit it here. Instead, we assume that the database has been initialized in a consistent state.

4 The Model

In our model, a *database* is specified as a (database) *state*, along with some *invariants* or *integrity constraints* on the state. At any given time, the *state* is determined by the values of the objects in the database. A change in the value of a database object changes the state. The invariants are predicates defined over the objects in the state. A database state is said to be *consistent* if the set of values satisfies the given invariants.

A *transaction* is an operation on a database state. Associated with each transaction is a set of *preconditions* and a set of *postconditions* on the database objects. A precondition limits the database states to which a transaction can be applied. For example, a *Reserve* transaction has a precondition that the hotel have at least one room available. A postcondition constrains the possible database states after a transaction completes. For example, a *Reserve* transaction has a postcondition that there be some room available before the reservation that is unavailable after the reservation. Preconditions and postconditions must be strong enough so that if a transaction executes on a consistent state, the result is again a consistent state.

Instead of executing a transaction as an atomic unit, we break a transaction into steps, and execute each step as an atomic unit. The decomposition exploits the semantic information associated with the transaction. Although such a decomposition process is application specific, we identify necessary properties that must be satisfied by any valid decomposition.

Definition 1 [Transaction Decomposition] A *decomposition* of a transaction T_i is a sequence of two or more atomic *steps* $< T_{i1}, T_{i2}, \ldots, T_{in} >$. In place of T_i, these steps are executed in the given order as atomic operations on a database state.

To show that the decomposition has been performed correctly, we must check that the steps, when executed in the correct sequence and without interference from other transactions, model the original transaction.

One possible composition requirement is that the steps in a decomposition be treated exactly as transactions in the original system, in that the integrity constraints must hold after each step. As the decomposition below demonstrates, such a requirement is too strong in practice. After presenting a naive decomposition, we develop a more realistic composition property.

NaiveR1

$\Delta Hotel$

$res < total$
$res' = res + 1$
$ST' = ST;\ RM' = RM$
$guest' = guest$

NaiveR2

$\Delta Hotel;\ r! : Room$

$ST(r!) = Available$
$ST' = ST \oplus \{r! \mapsto Unavailable\}$
$res' = res;\ RM' = RM$
$guest' = guest$

NaiveR3

$\Delta Hotel;\ r! : Room;\ g? : Guest$

$g? \notin guest$
$RM' = RM \cup \{g? \mapsto r!\}$
$guest' = guest \cup \{g?\}$
$res' = res;\ ST' = ST$

Figure 2: A Naive Decomposition

4.1 A Naive Decomposition of Reserve

Suppose we break up the *Reserve* transaction into the following three steps. A naive specification of these steps is given in figure 2.

Step 1: Increment the number of reserved rooms (*res*).

Step 2: Pick a room with status *Available* and change it to *Unavailable*.

Step 3: Add the guest to the set of guests and assign the room to the guest.

The decomposition in figure 2 has a serious flaw in that none of the proposed steps, considered by itself, maintains the invariants in *Hotel*. For example, *NaiveR*1 does not maintain the invariant $\#RM = res$ since *NaiveR*1 increments the value of *res*, but does not alter *RM*. Formally, the computed preconditions of all three steps simplify to **false**. Execution of any of the naive steps leaves the invariants unsatisfied, and other transactions are then exposed to the inconsistent state. For example, *Report* may produce an inconsistent output if executed in a state outside the invariants.

4.2 Modification of Original Invariants

The previous example demonstrates that not all decompositions are acceptable. Specifically, a decomposition may yield steps that leave the database in a state in which the invariants are not satisfied. This possibility is illustrated for the hotel example by the arrow labeled *NaiveR1* in figure 3. Once the invariants are violated, the formal basis for assessing the correctness of subsequent behavior collapses.

As noted earlier, one way to solve this problem is to allow only those decompositions that have the property that partial executions leave the database state consistent. Such an approach is exceedingly restrictive, and so we reject it. In the hotel example, the informal description of the steps into which *Reserve* is broken is perfectly satisfactory; what is unreasonable is the insistence that the invariants of *Hotel* hold at all intermediate steps. We need a formal model that can accommodate the notion that some – but not all – violations of the invariants are acceptable.

Figure 4 illustrates a model that allows inconsistent states – as defined by the invariants – that are nonetheless acceptable. The temporary inconsistency introduced by *R1* (specified below in figure 5) is allowed, and steps of some other transactions, e.g. *RefinedCancel*, can tolerate the inconsistency introduced by *R1*, and so are allowed to proceed. The general approach is to modify the original set of invariants and decompose transactions such that each step satisfies the new set of invariants. The model in figure 4 has many advantages, including greater concurrency among steps. We formalize the model as follows.

Let I denote the original invariants. Let $\mathbf{ST}$ denote the set consisting of all consistent states; i.e., $\mathbf{ST} = \{ST : ST \text{ satisfies } I\}$. A transaction T_i always operates on a consistent $ST \in \mathbf{ST}$. If ST_i denotes the state after the execution of T_i, then ST_i is also in $\mathbf{ST}$. However, when T_i is broken up into steps $< T_{i1}, T_{i2}, \ldots, T_{in} >$, each step T_{ij} is executed as an atomic operation. If ST_{ij} represents the partial execution of T_i, it is possible that after execution of step T_{ij}, the resulting database state ST_{ij} no longer satisfies the invariants I and, therefore, lies outside $\mathbf{ST}$.

In our approach, we define a new set of invariants, $\hat{I}$, by relaxing the original invariants I. We decompose each transaction such that execution of any step results in a database state that satisfies $\hat{I}$; if all the steps of a transaction are executed serially on a consistent initial state, the final state satisfies the original set of invariants. Let $\widehat{\mathbf{ST}} = \{ \text{ST} : \text{ST satisfies } \hat{I}\}$. The relationship between $\mathbf{ST}$ and $\widehat{\mathbf{ST}}$ is shown in figure 4. The inner circle denotes $\mathbf{ST}$ and the outer circle denotes $\widehat{\mathbf{ST}}$ (signifying that $\mathbf{ST} \subset \widehat{\mathbf{ST}}$). The ring denotes the set of all states that satisfy $\hat{I}$ but not I. The important part about figure 4 is that the set of inconsistent but acceptable states is formally identified and distinguished from the states that are unacceptable. The advantage is that formal analysis can be used to investigate activities in $\widehat{\mathbf{ST}}$.

To reason about the correctness of decomposing transactions into steps, and avoid the problems of a naive decomposition, we use *auxiliary variables* to generalize the invariants. Auxiliary variables are a standard method of reasoning about concurrent executions

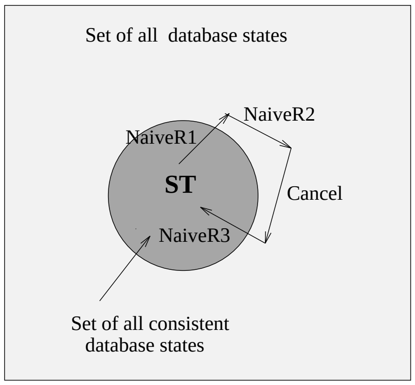
Set of all database states
NaiveR1
NaiveR2
ST
Cancel
NaiveR3
Set of all consistent database states

Figure 3: General classification of database states

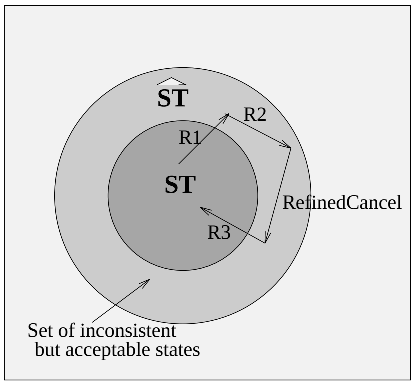

Figure 4: Database states as classified in our model

[OG76], and, in particular, have been applied to the problem of semantic database concurrency control [GM83]. Since our work focuses more on the decomposition process, we emphasize the role of auxiliary variables.

In the hotel example, we generalize the invariant $\#RM = res$ by introducing an auxiliary variable to express the fact that number of guests with rooms might differ from total reservations by the number of reserve transactions in progress. We generalize the invariant $\text{dom}(ST \rhd \{Unavailable\}) = \text{ran}\, RM$ by introducing another auxiliary variable to express the fact that the unavailable rooms might differ from the rooms assigned to guests by those rooms selected by reserve transactions in progress. Before we show these changes to the example, we present two properties that a decomposition must possess. We note that the auxiliary variables are introduced for purposes of analysis, and are eliminated in our implementation.

4.3 Composition Property

With the notion of generalized invariants in place, we can state the property relating steps in a decomposition to the original transaction. We call this requirement the *composition property*. Formally:

Composition Property Let T_i denote the original transaction and $T_{i1}, T_{i2}, \ldots, T_{in}$ denote the corresponding steps. T_i and its steps are related as follows:

$$T_i \Leftrightarrow (T_{i1} \mathbin{⨾} T_{i2} \mathbin{⨾} \ldots \mathbin{⨾} T_{in}) \wedge I$$

Executing the steps $T_{i1}, T_{i2}, \ldots, T_{in}$ serially on a state satisfying the original invariants I, changes the original database objects in the same way as executing the original transaction T_i on the same state.

From an implementation perspective, the composition property is similar to requiring that the stepwise execution of the steps be view equivalent to that of the original transaction. A complicating factor is that the decomposition may introduce additional database objects; the composition property does not limit the values of these objects. For example, compare *Hotel* in figure 1 with *ValidHotel* in figure 5.

4.4 Sensitive Transaction Isolation

In our model, we allow steps or transactions to see database states that do not satisfy the original invariants (i.e., states in $\widehat{\mathbf{ST}} - \mathbf{ST}$). But some transactions may output data to users; these transactions are referred to as *sensitive* transactions in [GM83]. We require sensitive transactions to appear to have generated outputs from a consistent state.

Sensitive Transaction Isolation Property All output data produced by a sensitive transaction T_i should have the appearance that it is based on a consistent state in $\mathbf{ST}$, even though T_i may be running on a database state in $\widehat{\mathbf{ST}} \Leftrightarrow \mathbf{ST}$.

In our model, we ensure the sensitive transaction isolation property by construction. For each sensitive transaction, we compute the subset of the original integrity constraints, I, relevant to the calculation of any outputs. This subset of I is included as an explicit precondition for the sensitive transaction.

4.5 A Valid Decomposition

In this section, we provide a valid decomposition of the hotel database. The problems of the naive decomposition are avoided, and the properties identified so far hold. After presenting the example, we derive additional properties required of valid decompositions.

To make the invariants more general, we add auxiliary variables and define a new state *ValidHotel*. We add the auxiliary variable *tempreserved*, which is a natural number, to denote the reservations that have been partially processed. We also add the auxiliary variable *tempassigned*, which is a set of rooms, to denote the rooms that have been reserved but which have not yet been assigned to guests. The invariants are modified accordingly. The schema *ValidHotel* together with the modified invariants is shown in figure 5.

$R1$, $R2$ and $R3$ are the steps of the reserve transaction. The steps satisfy the composition property. Although *Reserve* is a sensitive transaction, it turns out that no additional preconditions are needed to ensure that the output $r!$ reflects a consistent state. Space limitations preclude proofs of these properties; see the appendix of [AJR95].

The refined version of the single step *Cancel* transaction is nearly identical to the unrefined version, except that the auxiliary variables *tempassigned* and *tempreserved* are not changed.

Report is a sensitive transaction, and we establish the sensitive transaction isolation property by construction. Informally, *Report* transaction outputs values of ST and RM. ST and RM involve the original invariant $\mathrm{dom}(ST \rhd \{Unavailable\}) = \mathrm{ran}\, RM$ which can be derived from $\mathrm{dom}(ST \rhd \{Unavailable\}) = \mathrm{ran}\, RM \cup tempassigned$ if the variable *tempassigned* satisfies $tempassigned = \varnothing$. The refined version of *Report* is shown in figure 5.

4.6 Semantic Histories

Since we modify the invariants, several questions must be answered. In particular, we would like to know if and when the database state returns to a consistent state. We will answer these questions after we give some definitions.

Definition 2 [History] A *history* H over a set of transactions $\mathbf{T} = \{T_1, T_2, \ldots, T_m\}$ is a sequence of steps $< T_{i_1j_1}, T_{i_2j_2}, \ldots, T_{i_pj_q} >$, $1 \leq i_1, \ldots, i_p \leq m$, $T_{i_rj_s}$ is a step in T_{i_r}, $1 \leq r \leq m$, $1 \leq s \leq n$, such that

1. for each $T_i \in \mathbf{T}$, a step of T_i either appears exactly once in H or does not appear at all,
2. for any two steps T_{ij}, T_{ik} of some $T_i \in \mathbf{T}$, T_{ij} precedes T_{ik} in H if T_{ij} precedes T_{ik} in T_i, and
3. if $T_{ij} \in H$, then $T_{ik} \in H$ for $1 \leq k < j$.

By Condition (1), we ensure that every step of a transaction should occur at most once in a history. Condition (2) ensures that the order of the steps in a transaction is preserved in the history. Condition (3) ensures that for every step in a history, all the preceding steps in the corresponding transaction are present in the history.

Example 1 $< R1, R3, Report, R2 >$ is not a history as it violates conditions (2) and (3). $< R1, R2, R3, R2 >$ is not a history since it violates condition (1). $< R1$, $Report, R2, R3 >$ is a history. □

To emphasize the fact that we view the database as an abstract data type and transactions as operations on this abstract data type, we define the term *semantic history* to distinguish it from the term history used in database literature (e.g., [BHG87]).

Definition 3 [Semantic History] A *semantic* history H is a history that is bound to

1. an initial state, and
2. the states resulting from the execution of each step in H.

Definition 4 [Complete Execution] An execution of a transaction $T_i = < T_{i1}, T_{i2}, \ldots, T_{in} >$ in a semantic history H is a *complete* execution if all n steps of T_i appear in H.

Example 2 An execution of the reserve transaction will be complete in a history H if all three steps $R1$, $R2$, and $R3$ of reserve appear in H. □

Definition 5 [Partial Semantic History] A semantic history H_p over $\mathbf{T}$ is a *partial* semantic history if the execution of some transaction T_i is not complete in H_p.

Definition 6 [Complete Semantic History] A semantic history H over $\mathbf{T}$ is a *complete* semantic history if the execution of each T_i in $\mathbf{T}$ is *complete.*

4.7 Consistent Execution Property

Similar to the consistency property for traditional databases, we place the following requirement on semantic histories:

Consistent Execution Property If we execute a complete semantic history H on an initial state (i.e., the state prior to the execution of any step in H) that satisfies the original invariants I, then the final state (i.e., the state after the execution of the last step in H) also satisfies the original invariants I.

Although consistent execution property is definitely desirable, it is not enough because it does not capture the cumulative effect of each transaction. For a semantic history to be correct, we require that all intermediate states be in $\widehat{\mathbf{ST}}$, which is formalized in following definitions. Note that the consistency of outputs is ensured by the sensitive transaction isolation property.

Definition 7 [Correct Partial Semantic History] A partial semantic history H_p is a *correct* partial semantic history if

1. the initial state is in $\mathbf{ST}$,
2. all states before and after the execution of each step in H_p are in $\widehat{\mathbf{ST}}$, and

$$\begin{array}{|l} \textit{ValidHotel} \\ \hline \textit{res}, \textit{tempreserved} : \mathbb{N} \\ \textit{ST} : \textit{Room} \pfun \textit{Status};\ \textit{RM} : \textit{Guest} \pinj \textit{Room} \\ \textit{guest} : \mathbb{P}\,\textit{Guest};\ \textit{tempassigned} : \mathbb{P}\,\textit{Room} \\ \hline \#\textit{RM} + \textit{tempreserved} = \textit{res} \\ \mathrm{dom}(\textit{ST} \rhd \{\textit{Unavailable}\}) = \mathrm{ran}\,\textit{RM} \cup \textit{tempassigned} \\ \hline \end{array}$$

$$\begin{array}{|l} \textit{R1} \\ \hline \Delta\,\textit{ValidHotel} \\ \hline \textit{res} < \textit{total};\ \textit{res}' = \textit{res} + 1 \\ \textit{tempreserved}' = \textit{tempreserved} + 1 \\ \textit{ST}' = \textit{ST};\ \textit{RM}' = \textit{RM};\ \textit{guest}' = \textit{guest} \\ \textit{tempassigned}' = \textit{tempassigned} \\ \hline \end{array}$$

$$\begin{array}{|l} \textit{R2} \\ \hline \Delta\,\textit{ValidHotel};\ r! : \textit{Room} \\ \hline \textit{ST}(r!) = \textit{Available} \\ \textit{ST}' = \textit{ST} \oplus \{r! \mapsto \textit{Unavailable}\} \\ \textit{tempassigned}' = \textit{tempassigned} \cup \{r!\} \\ \textit{res}' = \textit{res};\ \textit{tempreserved}' = \textit{tempreserved} \\ \textit{guest}' = \textit{guest};\ \textit{RM}' = \textit{RM} \\ \hline \end{array}$$

$$\begin{array}{|l} \textit{R3} \\ \hline \Delta\,\textit{ValidHotel};\ g? : \textit{Guest};\ r! : \textit{Room} \\ \hline \textit{tempreserved} > 0;\ r! \in \textit{tempassigned};\ g? \notin \textit{guest} \\ \textit{RM}' = \textit{RM} \cup \{g? \mapsto r!\};\ \textit{res}' = \textit{res} \\ \textit{guest}' = \textit{guest} \cup \{g?\};\ \textit{ST}' = \textit{ST} \\ \textit{tempassigned}' = \textit{tempassigned} \setminus \{r!\} \\ \textit{tempreserved}' = \textit{tempreserved} - 1 \\ \hline \end{array}$$

$$\begin{array}{|l} \textit{RefinedCancel} \\ \hline \Delta\,\textit{ValidHotel};\ g? : \textit{Guest} \\ \hline g? \in \textit{guest};\ \textit{res}' = \textit{res} - 1 \\ \textit{ST}' = \textit{ST} \oplus \{\textit{RM}(g?) \mapsto \textit{Available}\} \\ \textit{RM}' = \{g?\} \ndres \textit{RM};\ \textit{guest}' = \textit{guest} \setminus \{g?\} \\ \textit{tempreserved}' = \textit{tempreserved} \\ \textit{tempassigned}' = \textit{tempassigned} \\ \hline \end{array}$$

$$\begin{array}{|l} \textit{RefinedReport} \\ \hline \Xi\,\textit{ValidHotel} \\ \textit{currentstatus}! : \textit{Room} \pfun \textit{Status} \\ \textit{currentassignments}! : \textit{Guest} \pinj \textit{Room} \\ \hline \textit{tempassigned} = \varnothing \\ \textit{currentstatus}! = \textit{ST} \\ \textit{currentassignments}! = \textit{RM} \\ \hline \end{array}$$

Figure 5: A Correct Decomposition for the Hotel Database

3. preconditions for each step are satisfied before it is executed.

Definition 8 [Correct Complete Semantic History] A complete semantic history H is a *correct* complete semantic history if

1. H is a correct partial semantic history, and
2. the final state is in **ST**.

4.8 Complete Execution Property

The fourth property which we describe is the *complete execution property.* When transactions have been broken up into steps, the interleaving of steps may lead to deadlock (i.e., a state from which we cannot complete some partially executed transaction). The complete execution property ensures that deadlock is avoided; if a transaction has been partially executed, then it can eventually complete.

Complete Execution Property Every partial correct semantic history H_p is a prefix of some complete correct semantic history.

In the hotel database suppose we have a partial semantic history H where $H =< R1, \textit{Report}, R2 >$. where the reserve transaction executes with $g? = \text{John}$. Consider step $R3$. The precondition $g? \notin \textit{guest}$ of $R3$ requires that John not have a existing reservation, but it is possible that in the final state in H, John *is* an element of *guest*. We may cancel John's existing reservation, thereby allowing the reserve transaction to complete. First, the precondition of *Cancel*, $g? \in \textit{guest}$, is guaranteed to hold if the precondition of $R3$ does not hold. Second, the postcondition of *Cancel* establishes the precondition of $R3$. Thus the reserve transaction for John can complete.

4.9 Decomposition with Deadlock

In this section, we show that some otherwise plausible decompositions do *not* satisfy the complete execution property, which is clearly undesirable. To illustrate the possibility, we modify the *Hotel* database as shown in figure 6.

In the example specification, the cancel transaction is decomposed into steps C1 and C2. We introduce the auxiliary variable *tempcanceled* which keeps count of the cancel transactions that have completed step $C1$ but not step $C2$. The invariant $\#RM = res \Leftrightarrow tempreserved$ in the original *ValidHotel* is changed to $\#RM = res \Leftrightarrow tempreserved + tempcanceled$.

Moreover, we introduce a new structure *clist* which keeps track of the guests whose cancellations are in progress. The guest whose reservation is being canceled is added to the *clist* in step $C1$ and is removed from the *clist* in step $C2$. We impose an additional constraint that a room cannot be reserved for a guest whose cancellation is in progress; note the precondition $g? \notin \textit{clist}$ in step $\textit{Res}3$. The reserve transaction is broken into steps $\textit{Res}1$, $\textit{Res}2$ and $\textit{Res}3$, similar to $R1$, $R2$ and $R3$ of the *ValidHotel* specification.

Consider the partial history $H_p =< C1, \textit{Res}1, \textit{Res}2 >$.

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{DeadlockHotel}} \\ \hline
\mathit{res}, \mathit{tempreserved}, \mathit{tempcanceled} : \mathbb{N} \\
\mathit{RM} : \mathit{Guest} \rightarrowtail \mathit{Room};\ \mathit{ST} : \mathit{Room} \nrightarrow \mathit{Status} \\
\mathit{guest}, \mathit{clist} : \mathbb{P}\,\mathit{Guest};\ \mathit{tempassigned} : \mathbb{P}\,\mathit{Room} \\ \hline
\#\mathit{RM} = \mathit{res} - \mathit{tempreserved} + \mathit{tempcanceled} \\
\operatorname{dom}(\mathit{ST} \rhd \{\mathit{Unavailable}\}) = \operatorname{ran} \mathit{RM} \cup \mathit{tempassigned} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Res1}} \\ \hline
\Delta \mathit{DeadlockHotel} \\ \hline
\mathit{res} < \mathit{total};\ \mathit{res}' = \mathit{res} + 1;\ \mathit{ST}' = \mathit{ST} \\
\mathit{tempreserved}' = \mathit{tempreserved} + 1;\ \mathit{RM}' = \mathit{RM} \\
\mathit{tempcanceled}' = \mathit{tempcanceled};\ \mathit{clist}' = \mathit{clist} \\
\mathit{tempassigned}' = \mathit{tempassigned};\ \mathit{guest}' = \mathit{guest} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{C1}} \\ \hline
\Delta \mathit{DeadlockHotel};\ g? : \mathit{Guest} \\ \hline
\mathit{res} > 0;\ \mathit{res}' = \mathit{res} - 1 \\
\mathit{clist}' = \mathit{clist} \cup \{g?\};\ \mathit{ST}' = \mathit{ST} \\
\mathit{tempcanceled}' = \mathit{tempcanceled} + 1 \\
\mathit{tempreserved}' = \mathit{tempreserved};\ \mathit{guest}' = \mathit{guest} \\
\mathit{tempassigned}' = \mathit{tempassigned};\ \mathit{RM}' = \mathit{RM} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Res2}} \\ \hline
\Delta \mathit{DeadlockHotel};\ r! : \mathit{Room} \\ \hline
\mathit{ST}(r!) = \mathit{Available};\ \mathit{res}' = \mathit{res};\ \mathit{guest}' = \mathit{guest} \\
\mathit{ST}' = \mathit{ST} \oplus \{r! \mapsto \mathit{Unavailable}\} \\
\mathit{tempassigned}' = \mathit{tempassigned} \cup \{r!\} \\
\mathit{RM}' = \mathit{RM};\ \mathit{tempreserved}' = \mathit{tempreserved} \\
\mathit{tempcanceled}' = \mathit{tempcanceled};\ \mathit{clist}' = \mathit{clist} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{C2}} \\ \hline
\Delta \mathit{DeadlockHotel};\ g? : \mathit{Guest} \\ \hline
g? \in \mathit{guest};\ g? \in \mathit{clist};\ \mathit{tempcanceled} > 0 \\
\mathit{ST}' = \mathit{ST} \oplus \{\mathit{RM}(g?) \mapsto \mathit{Available}\} \\
\mathit{RM}' = \{g?\} \lhd \mathit{RM};\ \mathit{guest}' = \mathit{guest} \setminus \{g?\} \\
\mathit{clist}' = \mathit{clist} \setminus \{g?\};\ \mathit{res}' = \mathit{res} \\
\mathit{tempcanceled}' = \mathit{tempcanceled} - 1 \\
\mathit{tempreserved}' = \mathit{tempreserved} \\
\mathit{tempassigned}' = \mathit{tempassigned} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Res3}} \\ \hline
\Delta \mathit{DeadlockHotel};\ g? : \mathit{Guest};\ r! : \mathit{Room} \\ \hline
\mathit{tempreserved} > 0;\ r! \notin \operatorname{ran} \mathit{RM} \\
g? \notin \mathit{guest};\ g? \notin \mathit{clist} \\
\mathit{guest}' = \mathit{guest} \cup \{g?\};\ \mathit{clist}' = \mathit{clist} \\
\mathit{RM}' = \mathit{RM} \cup \{g? \mapsto r!\};\ \mathit{res}' = \mathit{res} \\
\mathit{tempreserved}' = \mathit{tempreserved} - 1 \\
\mathit{tempassigned}' = \mathit{tempassigned} \setminus \{r!\} \\
\mathit{tempcanceled}' = \mathit{tempcanceled};\ \mathit{ST}' = \mathit{ST} \\ \hline
\end{array}$$

Figure 6: Example Specification Lacking Complete Execution Property

Let the reserve and cancel transactions in H_p have the same $g?$ as their input. Also assume that $g? \notin \mathit{guest}$. We try to complete the reserve and cancel transactions. *Res*3 cannot be executed because the precondition $g? \notin \mathit{clist}$ is not satisfied because step $C1$ has inserted $g?$ in *clist*. $C2$ cannot be executed because the precondition $g? \in \mathit{guest}$ is not satisfied. It is possible to execute any number of steps of other transactions, but the reserve and cancel transactions in H_p still cannot complete.

The deadlock could be avoided by including the invariant $\mathit{clist} \subseteq \mathit{guest}$ in *DeadlockHotel*. Omission of this constraint allows the database to enter an undesirable state where $c? \in \mathit{clist} \wedge c? \notin \mathit{guest}$, from which neither *Res*3 nor $C2$ can complete.

5 Implementation

5.1 Successor Set Mechanism

Decomposing transactions into steps yields improved performance, but the interleaving of these steps must be constrained so as to avoid inconsistencies. In the decomposition we have given so far, which is based on generalizing invariants with auxiliary variables, the interleaving is constrained by additional preconditions on the auxiliary variables. Although the generalized invariants facilitate analysis, it is expensive to implement the auxiliary variables and to check the additional preconditions.

To avoid implementing auxiliary variables and to avoid checking additional preconditions, we propose two mechanisms: a *queuing mechanism* to ensure that steps of a transaction execute in order and a *successor set* mechanism. The specification of a queuing mechanism is straightforward and is therefore omitted.

Although our successor set mechanism is somewhat similar to the the notion of *compatibility sets* in [GM83] and *breakpoint sets* in [FO89], the semantics of these concepts are substantially different. Also, via specific decomposition steps and corresponding proof obligations, we assist the specifier in verifying the correctness of successor sets with respect to the original specification; in [FO89] and in [GM83], the burden of arguing correctness rests entirely with the application developer.

Definition 9 [Successor Set] The *successor set* of a step T_{ij}, denoted $SC(T_{ij})$, is the set of steps that can appear after step T_{ij} and before step $T_{i(j+1)}$ in any correct semantic history.

Example 3 Successor set descriptions are obtained by examining the preconditions with auxiliary variables. Some of these preconditions will always be satisfied if the steps in each transaction are executed in order; the queuing mechanism guarantees the satisfaction of these preconditions. In the hotel example, the only remaining precondition with auxiliary variables is

$\textit{tempassigned} = \varnothing$ in *RefinedReport*. We observe that this precondition will always be satisfied as long as *RefinedReport* is not executed between steps $R2$ and $R3$ of a reserve transaction. Thus we specify the successor sets as follows.
$SC(R1) = \{R1, R2, R3, \textit{RefinedCancel}, \textit{RefinedReport}\}$
$SC(R2) = \{R1, R2, R3, \textit{RefinedCancel}\}$

The successor set for $R1$ includes every other possible step; after an $R1$ any of another $R1$, an $R2$ (of the same or of a different reserve transaction), an $R3$ (of a different reserve transaction), a *RefinedCancel*, or a *RefinedReport* may execute. The successor set for $R2$ is more restrictive. $\textit{RefinedReport} \notin SC(R2)$ means that the *RefinedReport* step cannot execute after step $R2$. In other words, *RefinedReport* is not allowed to the see the inconsistencies with respect to the original invariants that are introduced by step $R2$.

Note that with the queuing mechanism and the successor set description, the auxiliary variables themselves need not be implemented, and all constraints on the auxiliary variables may be ignored. □

Any complete semantic history generated using successor sets must meet an additional requirement to those given in Definition 8:

> Consider every pair of steps T_{ij} and $T_{i(j+1)}$ of transaction T_i. For every step T_{kl} of a different transaction T_k appearing between T_{ij} and $T_{i(j+1)}$ (if any), $T_{kl} \in SC(T_{ij})$.

Successor set descriptions are intended to allow the removal of predicates that reference auxiliary variables, and ultimately the variables themselves. Thus, with respect to the specifications given with generalized invariants and auxiliary variables, not all successor set descriptions are correct. Informally, a successor set is correct with respect to a generalized invariant specification if any semantic history generated using successor sets can also be generated by the generalized invariant specification. Although desirable, the converse property does not hold in general since first-order logic preconditions have more expressive power than the successor set mechanism. Formally, we describe correct successor set descriptions with the *valid successor set property*:

Definition 10 [Valid Successor Set Property] A specification S_2 that employs a successor set description is *valid* with respect to specification S_1 with generalized invariants if

1. Any correct semantic history generated by S_2 is also a correct semantic history generated by S_1.
2. S_2 satisfies the complete execution property.

Note that since the correct semantic histories of S_2 might be a proper subset of those of S_1, the complete execution property needs to be explicitly verified with respect to S_2.

5.2 Two-Phase Locking Mechanism

The notions of interleaving described in [FO89] and [GM83] are both implemented in a locking environment. Since our interleaving mechanism differs, we sketch a two-phase locking implementation of our mechanism. Other implementations are possible, as are various optimizations.

By treating steps as complete transactions, two-phase locking can guarantee that any history is stepwise conflict serializable (i.e., conflict serializable with steps as primitive operations). However, stepwise serializability is not sufficient, since some stepwise serial histories violate the successor set description. Specifically, step T_{ij} of one transaction might serialize between steps T_{km} and $T_{k(m+1)}$ of another transaction, even if the T_{ij} is not in the successor set of T_{km}.

To ensure that the successor set descriptions are met, we introduce a control mechanism for dispatching of steps to the data manager, which is responsible for implementing two-phase locking. We assume that the data manager produces an explicit prefix of a serialization order for all steps that commit.

Consider a set of steps under the control of the data manager. Since the data manager may serialize these steps in any order, we require that the concatenation of the committed prefix of the serialization order and any order of the steps in the data manager follow the successor set rules. Additional steps can be submitted to the data manager only if doing so maintains this constraint. The constraint can be checked by ensuring that each active step is an element of the intersection of the successor sets of all other active steps and also of all committed steps of incomplete transactions. Note that completed transactions do not affect the interleaving of active transactions.

6 Conclusion

In this paper, we have provided the database application developer conceptual tools necessary to reason about systems in which transactions that ideally should be treated as atomic – for reasons of analysis – must instead be treated as a composition of steps – for reasons of performance. The developer begins with a specification produced via standard formal methods, transforms some transactions in the specification into steps, and assesses the properties of the resulting system. The formal analysis at each step of this process guarantees that the resulting system possesses the desired properties.

As we have indicated, the syntactic aspect of the implementation given in section 5.2 (i.e., stepwise conflict-serializability via two-phase locking), is preliminary. We anticipate developing a more efficient implementation, as was done in [GM83] and [FO89]. We also must address the problem of reliably transmitting parameters between steps of a transaction, a problem that is considered in [GMS94, WR92]. However, the semantic aspects of our implementation have been thoroughly addressed.

We can easily permit ad hoc transactions to be dynamically added in our model, although they will require some special intervention. An ad hoc transaction could be executed as an atomic, sensitive transaction, which means that all integrity constraints relevant to the calculation of any output will have to be included as explicit preconditions for the transaction (see section 4.4). Alternatively, an ad hoc transaction could be included at the successor set stage by simply excluding it from all successor set descriptions. Deletion of a transaction in our model is somewhat problematic since deletion may impact the complete execution property, which ensures that any transaction that has been partially executed can eventually complete.

An important question is how well our model scales to real-world applications. There are two major issues - identification of necessary properties and verification of these properties. The paper's major contribution is the identification of necessary properties, such as composition, complete execution, valid successor set, and so on. If the properties do not hold, the application may behave unexpectedly and undesirably. The demonstration of these properties is a separate issue. Fortunately, demonstration methods covering a spectrum of formality are possible, depending on the application. Less formal methods trade a degree of assurance in return for feasibility and ease of use. Possible methods are informal argument, inspection, paper and pencil proof, and formal machine-level verification. In this paper, we have used a specification language approach in which the analysis is carried out by hand. Researchers are developing Z tools that can automate some aspects of our analysis, although at present none are industrial-grade tools.

References

[AAS93] D. Agrawal, A. El Abbadi, and Ambuj K. Singh. Consistency and orderability: Semantics-based correctness criteria for databases. *ACM TODS*, 18(3):460–486, September 1993.

[AJR95] P. Ammann, S. Jajodia, and I. Ray. Using formal methods to reason about semantics-based decomposition of transactions. Technical Report ISSE-TR-95-1XX, ISSE Dept., GMU, MS 4A4, Fairfax, VA 22180, 1995.

[BHG87] P.A. Bernstein, V. Hadzilacos, and N. Goodman. *Concurrency Control and Recovery in Database Systems.* Addison-Wesley, Reading, MA, 1987.

[BR92] B. R. Badrinath and Krithi Ramamritham. Semantics-based concurrency control: Beyond commutativity. *ACM TODS*, 17(1):163–199, March 1992.

[CR94] P. K. Chrysanthis and K. Ramamritham. Synthesis of extended transaction models using ACTA. *ACM TODS*, 19(3):450–491, September 1994.

[DE90] W. Du and A.K. Elmagarmid. Quasi serializability: A correctness criterion for global concurrency control in interbase. In *Proc. 16th VLDB*, pages 347–355, 1990.

[FO89] A. A. Farrag and M. T. Ozsu. Using semantic knowledge of transactions to increase concurrency. *ACM TODS*, 14(4):503–525, December 1989.

[GM83] H. Garcia-Molina. Using semantic knowledge for transaction processing in a distributed database. *ACM TODS*, 8(2):186–213, June 1983.

[GMS94] H. Garcia-Molina and Kenneth Salem. Services for a workflow management system. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, 17(1):40–44, March 1994.

[Her87] M. Herlihy. Extending multiversion time-stamping protocols to exploit type information. *IEEE Transactions on Computers*, 36(4):443–448, April 1987.

[HW91] M. P. Herlihy and W. E. Weihl. Hybrid concurrency control for abstract data types. *Journal of Computer and System Sciences*, 43(1):25–61, August 1991.

[JM87] S. Jajodia and C. Meadows. Managing a replicated file in an unreliable network. In *Proceedings of 3rd IEEE International Conference on Data Engineering*, pages 396–404, Los Angeles, CA, February 1987.

[KS88] H. F. Korth and G. D. Speegle. Formal model of correctness without serializability. In *Proceedings of ACM-SIGMOD International Conference on Management of Data*, pages 379–386, June 1988.

[KS94] H. F. Korth and G. Speegle. Formal aspects of concurrency control in long-duration transaction systems using the nt/pv model. *ACM TODS*, 19(3):492–535, September 1994.

[LMWF94] N. Lynch, M. Merritt, W. Weihl, and A. Fekete. *Atomic Transactions.* Morgan Kaufmann Publishers, San Mateo, CA, 1994.

[Lyn83] Nancy A. Lynch. Multilevel atomicity—A new correctness criterion for database concurrency control. *ACM TODS*, 8(4):484–502, December 1983.

[OG76] S. Owicki and D. Gries. Verifying properties of parallel programs: An axiomatic approach. *Communications of the ACM*, 19(5):279–285, May 1976.

[PST91] B. Potter, J. Sinclair, and D. Till. *An Introduction to Formal Specification and Z.* Prentice-Hall, New York, 1991.

[SLJ88] L. Sha, J. P. Lehoczky, and E.D. Jensen. Modular concurrency control and failure recovery. *IEEE Transactions on Computers*, 37(2):146–159, February 1988.

[Spi89] J.M. Spivey. *The Z Notation: A Reference Manual.* Prentice-Hall, New York, 1989.

[SSV92] Dennis Shasha, Eric Simon, and Patrick Valduriez. Simple rational guidance for chopping up transactions. In *Proceedings ACM SIGMOD International Conference on Management of Data*, pages 298–307, San Diego, CA, June 1992.

[Wei84] William E. Weihl. *Specification and Implementation of Atomic Data Types.* PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 1984.

[Wei88] W.E. Weihl. Commutativity-based concurrency control for abstract data types. *IEEE Transactions on Computers*, 37(12):1488–1505, December 1988.

[WR92] Helmut Wachter and Andreas Reuter. The contract model. In Ahmed K. Elmagarmid, editor, *Database Transaction Models for Advanced Applications*, pages 219–263. Morgan Kauffman, 1992.

Appendix A – Properties of the Decomposition

We show that the decomposition as given in Section 4.5 has the necessary properties.

Composition Property

In the Hotel Database, the original invariants I are satisfied when the auxiliary variables *tempreserved* and *tempassigned* satisfy the following conditions:

$$tempreserved = 0 \wedge tempassigned = \varnothing$$

The reserve transaction is the only transaction in the Hotel Database that has been decomposed into multiple steps. For the reserve transaction the proof obligation is :

$$Reserve \Leftrightarrow tempschema \qquad \ldots(i)$$

where *tempschema* is given by,
$(R1 \mathbin{⨟} R2 \mathbin{⨟} R3) \wedge tempreserved = 0 \wedge tempassigned = \varnothing$

The right hand side of the equivalence ($\Leftrightarrow$) in the expression (i) obtained by schema composition [PST91] evaluates to:

$$\begin{array}{|l}
\multicolumn{1}{l}{tempschema} \\
\hline
\Delta RefinedHotel \\
g? : Guest \\
r! : Room \\
\hline
res < total \\
g? \notin guest \\
ST(r!) = Available \\
res' = res + 1 \\
guest' = guest \cup \{g?\} \\
ST' = ST \oplus \{r! \mapsto Unavailable\} \\
RM' = RM \cup \{g? \mapsto r!\} \\
tempreserved' = 0 \\
tempassigned' = \varnothing \\
\hline
\end{array}$$

The schema for the original *Reserve* transaction is given by:

$$\begin{array}{|l}
\multicolumn{1}{l}{Reserve} \\
\hline
\Delta Hotel \\
g? : Guest \\
r! : Room \\
\hline
res < total \\
g? \notin guest \\
ST(r!) = Available \\
res' = res + 1 \\
guest' = guest \cup \{g?\} \\
ST' = ST \oplus \{r! \mapsto Unavailable\} \\
RM' = RM \cup \{g? \mapsto r!\} \\
\hline
\end{array}$$

The constraints on *tempreserved*, *tempreserved'*, *tempassigned*, and *tempassigned'* are implied by the invariants in $\Delta Hotel$. The converse is also true. Thus the predicate parts of the schemas are equivalent, and hence the schemas are equivalent.

Sensitive Transaction Isolation Property

In the hotel database we have two sensitive transactions: the *Report* and *Reserve* transactions. In each case, the proof of the Sensitive Transaction Isolation Property is by construction.

First we consider the *Report* transaction. We compute the subset of the original invariants that must be satisfied as a precondition for *Report*. We obtain these from *Hotel* by hiding the state variables *not* involved in producing the outputs of *Report*. The state variables not involved in producing the output of *Report* are *res* and *guest*. Hiding the variables *res* and *guest* from *Hotel* produces the following schema:

$$\begin{array}{|l}
\multicolumn{1}{l}{Hotel \setminus (res, guest)} \\
\hline
RM : Guest \rightarrowtail Room \\
ST : Room \twoheadrightarrow Status \\
\hline
\exists\, res : \mathbb{N};\ guest : \mathbb{P}\, Guest \bullet \\
\#RM = res \wedge \\
\mathrm{dom}(ST \rhd \{Unavailable\}) \\
\qquad\qquad = \mathrm{ran}\, RM \\
\hline
\end{array}$$

The constraint simplifies to

$$\mathrm{dom}(ST \rhd \{Unavailable\}) = \mathrm{ran}\, RM$$

The constraint is implied by an invariant in $\hat{I}$, namely, $\mathrm{dom}(ST \rhd \{Unavailable\}) = \mathrm{ran}\, RM \cup tempassigned$ and $tempassigned = \varnothing$. Hence we include $tempassigned = \varnothing$ as a precondition for *RefinedReport*.

Next we consider the *Reserve* transaction. The output of a *Reserve* transaction is the room $r!$ assigned to the guest. The only constraint on $r!$ is that the function ST evaluated at $r!$ be *Available*. Therefore, to compute the subset of the original invariants that must hold as a precondition on *Reserve*, we hide all the state variables except *ST* in *Hotel.* The schema obtained by hiding all the variables but *ST* is as follows:

$$\begin{array}{|l}
\hline
\mathit{Hotel} \setminus (\mathit{res}, \mathit{guest}, \mathit{RM}) \\
\mathit{RM} : \mathit{Guest} \mathrel{\rightarrowtail\!\!\!\!\!+\,} \mathit{Room} \\
\mathit{ST} : \mathit{Room} \mathrel{\rightarrow\!\!\!\!\!+\,} \mathit{Status} \\
\hline
\exists\, \mathit{res} : \mathbb{N};\ \mathit{guest} : \mathbb{P}\, \mathit{Guest}; \\
\mathit{RM} : \mathit{Guest} \mathrel{\rightarrowtail\!\!\!\!\!+\,} \mathit{Room} \bullet \\
\# \mathit{RM} = \mathit{res} \land \\
\mathrm{dom}(\mathit{ST} \rhd \{\mathit{Unavailable}\}) \\
\qquad\qquad\qquad = \mathrm{ran}\, \mathit{RM} \\
\hline
\end{array}$$

The constraint simplifies to **true**, which means that no additional preconditions need be placed in the steps $R1$, $R2$, or $R3$ of the reserve transaction.

Consistent Execution Property

For the hotel database system, the original invariants in I are satisfied when $\mathit{tempassigned} = \emptyset$ and $\mathit{tempreserved} = 0$. Thus we have to prove that if the initial state of a complete semantic history satisfies $\mathit{tempassigned} = \emptyset$ and $\mathit{tempreserved} = 0$, the final state of the history will also satisfy $\mathit{tempassigned} = \emptyset$ and $\mathit{tempreserved} = 0$.

Let n_1, n_2 and n_3 be the number of $R1$s, $R2$s and $R3$s respectively present in any complete history. The variable *tempreserved* is modified by steps $R1$ and $R3$ of a reserve transaction. *tempreserved* is incremented in step $R1$ and is decremented in step $R3$. Thus *tempreserved* is given by the following expression

$$\mathit{tempreserved} = n_1 \Leftrightarrow n_3$$

The variable *tempassigned* is modified in steps $R2$ and $R3$ of the reserve transaction. In step $R2$ a room is added to the set *tempassigned* and in step $R3$ of the reserve transaction the room is taken out from the set *tempassigned.* Thus we can write,

$$\mid \mathit{tempassigned} \mid = n_2 \Leftrightarrow n_3$$

In a complete history since all the reserve transactions have completed, the number of $R1$s, $R2$s and $R3$s that have been executed are equal, and so

$$n_1 = n_2 = n_3$$

Therefore, in a complete history,

1. $\mathit{tempreserved} = 0$ and
2. $\mid \mathit{tempassigned} \mid = 0$ or $\mathit{tempassigned} = \emptyset$.

Hence we can conclude that the hotel database has the consistent execution property.

Complete Execution Property

To prove that the Hotel Database System has the complete execution property, we take any partial correct semantic history and show that it is the prefix of some complete correct semantic history.

In the Hotel Database, only the reserve transactions have been broken into steps. So in any partial semantic history the only incomplete transactions are reserve transactions. Suppose we have n incomplete reserve transactions in the correct partial semantic history. We show how an incomplete reserve transaction can be completed, thereby decreasing the number of incomplete reserve transactions from n to $n \Leftrightarrow 1$. By repeated applications of our argument, it is possible to reduce the number of incomplete reserve transactions to zero, at which point the history is a complete correct semantic history.

Consider an incomplete reserve transaction. If the reserve transaction has completed step $R1$, the preconditions of $R2$ is always satisfied and so $R2$ can be executed. If the reserve transaction has completed step $R2$, the precondition of step $R3$ ($g? \notin \mathit{guest}$) may or may not be satisfied. If the precondition of $R3$ is not satisfied, the precondition of another transaction, *RefinedCancel* ($g? \in \mathit{guest}$), is satisfied. Moreover the postcondition of *RefinedCancel* establishes the precondition of $R3$, and so $R3$ can complete. Thus all reserve transactions can complete.

Appendix B – Properties of the Histories Generated using Queuing and Successor Set Mechanism

Valid Successor Set Property

Part 1

In the first part, we prove that the set of correct semantic histories generated using successor set and queuing mechanism is a subset of the set of correct histories generated using invariants and precondition checks.
Let
$\mathbf{H_1}$ = set of correct semantic histories generated by decomposition of transactions and
$\mathbf{H_2}$ = set of correct semantic histories generated by the queuing and successor set mechanism.
The proof obligation is $\mathbf{H_2} \subseteq \mathbf{H_1}$, i.e. we have to show that for any correct semantic history in $\mathbf{H_2}$, there is a corresponding correct semantic history in $\mathbf{H_1}$.

Let H_2 be any correct semantic history generated using the queuing and successor set mechanism. From H_2 we construct a semantic history H_1 as follows:

1. make the initial state of H_1 the same as that of H_2,

2. for any step in H_2, include the same step in H_1,
3. add the preconditions *tempreserved* > 0 and $r! \notin$ *tempassigned* to any and all occurrence(s) of the step $R3$ in H_1,
4. add the precondition *tempassigned* $= \varnothing$ to any and all occurrence(s) of *RefinedReport* in H_1.

Clearly H_1 is the history corresponding to H_2, which uses precondition checks to control the ordering instead of using queuing and successor set mechanism as done in H_2. It remains to be shown that $H_1 \in \mathbf{H_1}$, i.e. the semantic history H_1 is a correct semantic history. Note that the only way in which history H_1 differs from H_2 is that, some preconditions present in the steps *RefinedReport* and $R3$ in H_1 are not present in the corresponding steps in H_2.

First let us consider the preconditions that were added in H_1 because of step $R3$.

1. *tempreserved* > 0
2. $r! \in$ *tempassigned*

Note that the only time the precondition, *tempreserved* > 0 in $R3$, will not be satisfied, is when an $R3$ is executed before its corresponding $R1$. However, the queuing mechanism used in the generation of history H_2 ensures that the three steps of *Reserve*, $R1$,$R2$ and $R3$, are executed in the proper sequence. Also the order of steps in H_1 and H_2 is the same. Since the step $R3$ in the history H_1 occurs only after the corresponding $R1$, the precondition *tempreserved* > 0 is satisfied by any $R3$ appearing in the history H_1.

Next we consider the precondition $r! \in$ *tempassigned*. This is always satisfied in history H_1. The step $R2$ adds a room $r!$ to the set *tempassigned* and step $R3$ removes the same room from the same set. In addition, the queuing mechanism ensures that $R2$ always precedes $R3$ in the history H_2. Since the ordering of steps is maintained in H_1, the precondition $r! \in$ *tempassigned* is satisfied.

Finally, let us consider the precondition, *tempassigned* $= \varnothing$, that was added to *RefinedReport* in H_1. From the specifications of $R1$, $R2$, $R3$, *RefinedCancel*, and *RefinedReport* we see that the only situation in which the precondition of *RefinedReport* is not satisfied, is when at least one $R2$ have been executed but the corresponding $R3$ has not yet been executed. However, as *RefinedReport* $\notin SC(R2)$, *RefinedReport* will never be allowed to execute between an $R2$ and a $R3$. Thus in H_2 *tempassigned* $= \varnothing$ is always satisfied before *RefinedReport* is executed.

Note that the set of operations that modify the database state are the same for steps in H_1 and H_2. The initial states are the same for both the histories. So the state obtained by applying a step in H_1 is the same as that obtained by applying H_2.

Summing up, for the semantic history H_1, the following observations can be made.

1. The initial state is in $\mathbf{ST}$ because it is the same as that of the correct semantic history H_2.
2. The state obtained by applying each step of the history is in $\widehat{\mathbf{ST}}$ because it is the same as applying the corresponding step in the correct semantic history H_2.
3. Preconditions are satisfied for each step.

Thus the history H_1 is a correct semantic history, i.e. $H_1 \in \mathbf{H_2}$. Therefore for any history $H_2 \in \mathbf{H_2}$, we have a corresponding $H_1 \in \mathbf{H_1}$.

For the Hotel Database example, we can also show that corresponding to any history in $\mathbf{H_1}$ we can generate a corresponding history in $\mathbf{H_2}$ using the successor set and queuing mechanisms. In any correct history in $\mathbf{H_1}$, the preconditions are satisfied at each step and *RefinedReport* can never appear between an $R2$ and the corresponding $R3$. The successor set mechanism ensures that *RefinedReport* does not occur between an $R2$ and an $R3$ and does not impose any further restrictions. Thus for any history in $\mathbf{H_1}$, we have a corresponding history in $\mathbf{H_2}$.

Thus for the hotel database example, the set of histories in $\mathbf{H_1}$ is equivalent to the set of histories in $\mathbf{H_2}$.

Part 2

In the second part of the valid successor set property, it is required to show that all partially correct semantic histories will eventually complete. For the Hotel Database the set $\mathbf{H_1}$ is equivalent to the set $\mathbf{H_2}$. Since we have proved earlier that the set of histories in $\mathbf{H_1}$ has the complete execution property, it is implied that the set of histories in $\mathbf{H_2}$ has the complete execution property.