МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра математической кибернетики и компьютерных наук

Моделирование и анализ отложенной долговечности как механизма повышения производительности ACID-систем

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 5 курса 551 группы
направления 09.03.04 — Программная инженерия
факультета компьютерных наук и информационных технологий
Волковой Юлии Сергеевны

Научный руководитель,
профессор, д. ф.-м. н. _____ В.А.Романов
Заведующий кафедрой
к. ф.-м. н., доцент _____ С.В. Миронов

Саратов 2025

ВВЕДЕНИЕ

Актуальность темы. В современном мире, где объемы данных и требования к скорости их обработки непрерывно растут, системы управления базами данных (СУБД) являются основой функционирования большинства информационных систем. Обеспечение целостности данных традиционно достигается за счет гарантий ACID (атомарность, согласованность, изолированность, долговечность). Однако строгое соблюдение этих гарантий, особенно долговечности, часто вступает в конфликт с производительностью и масштабируемостью систем, особенно в распределенных средах.

В данной проектной работе фокусируется внимание на исследовании компромисса между долговечностью ACID-транзакций и производительностью СУБД. Отложенная или настраиваемая долговечность транзакций представляет собой один из подходов к решению этого конфликта, позволяя системе предоставлять подтверждение о завершении транзакции до ее фактической полной фиксации на энергонезависимых носителях. Однако такие модели требуют тщательного анализа для понимания их свойств и гарантий.

Цель бакалаврской работы – исследовать модель отложенной долговечности транзакций и провести ее формальный анализ с использованием языка спецификаций TLA+ для проверки корректности и ключевых свойств.

Поставленная цель определила следующие задачи:

Изучить теоретические основы ACID-транзакций, выявить проблемы, связанные с обеспечением долговечности, и их влияние на производительность СУБД.

Разработать формальную спецификацию модели отложенной долговечности на языке TLA+, описывающую состояния системы, возможные действия и переходы.

Сформулировать и проверить ключевые свойства корректности модели (ED Serializability, ED Recoverability) с помощью инструмента модельной проверки TLC.

Разработать код, иллюстрирующий возможные модификации в архитектуре СУБД для поддержки исследуемой модели.

Методологические основы исследования моделей управления транзакциями, компромиссов согласованности и производительности, а также формальных методов спецификации и верификации систем представлены в работах таких ученых, как Таненбаум Э, Уэйн Х. и Клеппманн М.

Теоретическая значимость бакалаврской работы заключается в применении формальных методов (TLA+) для анализа модели отложенной долговечности, что позволяет получить строгое описание ее поведения и провести верификацию заявленных свойств. Это способствует более глубокому пониманию механизмов управления транзакциями, допускающих компромиссы с долговечностью.

Практическая значимость бакалаврской работы состоит в том, что разработанная TLA+ спецификация может служить основой для дальнейших исследований и разработок в области надежных и производительных СУБД. Концептуальный код иллюстрирует возможные пути интеграции подобных моделей в реальные системы, предоставляя разработчикам более четкое представление о гарантиях и рисках.

Структура и объём работы. Бакалаврская работа состоит из введения, двух разделов (глав), заключения, списка использованных источников и одного приложения (Приложение А – Листинг программ (кода)). Общий объем работы – 59 страниц, из них 45 страниц – основное содержание, включая 2 рисунка и 1 таблицу. Список использованных источников информации – 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел «Теоретические основы управления транзакциями и производительностью в СУБД» посвящен всестороннему анализу фундаментальных концепций, лежащих в основе современных транзакционных систем, и выявлению ключевых проблем, возникающих на стыке требований к целостности данных и производительности. В данном разделе подробно исследуются четыре канонических свойства ACID-транзакций: атомарность, гарантирующая неделимость операций; согласованность, обеспечивающая переход базы данных между корректными состояниями; изолированность, создающая иллюзию монопольного доступа для параллельных транзакций; и долговечность, гарантирующая сохранность успешно зафиксированных изменений. Особое внимание уделяется свойству долговечности (Durability), как одному из наиболее ресурсоемких. Детально рассматривается его влияние на производительность систем управления базами данных, анализируются механизмы его обеспечения, такие как запись на энергонезависимые носители и репликация, и иллюстрируется, как эти механизмы вносят существенные задержки в обработку транзакций.

Далее, раздел углубляется в исследование конфликта между строгими ACID-гарантиями и требованиями к производительности и масштабируемости СУБД. Рассматриваются причины этого конфликта, включая ограничения, накладываемые дисковым вводом-выводом, сетевыми взаимодействиями в распределенных системах, и сложностью протоколов координации, таких как двухфазный коммит. Обсуждаются проблемы масштабирования традиционных ACID-систем и теоретические ограничения, такие как теорема CAP.

Затем проводится обзор существующих подходов и парадигм, направленных на управление компромиссом "согласованность-производительность". Анализируются модели с ослабленной согласованностью, такие как BASE и концепция конечной согласованности

(Eventual Consistency), их преимущества в плане масштабируемости и недостатки с точки зрения сложности разработки приложений. Рассматривается практика использования асинхронных коммитов в реляционных СУБД, ее влияние на снижение задержек и сопутствующие риски потери данных. Также дается краткий обзор более современных моделей с отложенной или настраиваемой долговечностью, которые стремятся предоставить более гранулированный контроль над этим компромиссом.

Несмотря на неоспоримые преимущества, которые предоставляют ACID-гарантии, их строгое соблюдение, особенно в современных высоконагруженных и распределенных системах, неизбежно приводит к возникновению конфликта с требованиями к производительности и масштабируемости. Этот конфликт является одной из центральных проблем в проектировании СУБД и мотивирует поиск компромиссных решений.

Одним из наиболее значимых факторов, влияющих на производительность, является обеспечение свойства долговечности. Операции ввода-вывода на диск по своей природе на порядки медленнее, чем операции в оперативной памяти. Когда СУБД ожидает завершения записи на диск перед подтверждением транзакции клиенту (синхронный коммит), эта дисковая задержка напрямую добавляется к общей задержке выполнения транзакции. Как показывает пример PostgreSQL, переход от конфигурации без гарантий немедленной долговечности (sync=off) к конфигурации с локальной долговечностью (sync=local) может увеличить задержку транзакции на порядки, и эта задержка будет составлять почти всю серверную часть времени отклика.

В распределенных системах ситуация усугубляется сетевыми задержками. Если для обеспечения долговечности требуется репликация данных на другие узлы, система должна ожидать подтверждения от реплик, что добавляет время на передачу данных по сети к общей задержке. При размещении реплик в географически удаленных дата-центрах, сетевые

издержки становятся доминирующим фактором, снижающим производительность. Такое увеличение задержки напрямую влияет на общую пропускную способность системы, поскольку ресурсы (соединения, блокировки) удерживаются дольше.

Завершает теоретический раздел введение в методологию формальных методов. Обосновывается необходимость их применения для проектирования и анализа сложных, критически важных систем, какими являются механизмы управления транзакциями. Описываются основные цели и преимущества формального подхода, такие как раннее обнаружение ошибок и повышение уверенности в корректности. Далее дается введение в язык спецификаций TLA+, рассматриваются его ключевые концепции – переменные состояния, действия, инварианты и временные свойства – а также принципы работы инструмента модельной проверки TLC. Делается вывод по первому разделу о том, что глубокое понимание теоретических основ ACID, существующих компромиссов и возможностей формальных методов является необходимой базой для исследования и разработки надежных моделей управления транзакциями с улучшенными характеристиками производительности.

Второй раздел «Формализация и анализ модели отложенной долговечности с использованием TLA+» представляет собой центральную исследовательскую часть работы и посвящен детальной разработке формальной спецификации модели отложенной долговечности, а также определению и подготовке к проверке ее ключевых свойств корректности.

В предыдущей главе были рассмотрены фундаментальные свойства ACID-транзакций и выявлен ключевой конфликт между требованием немедленной долговечности и стремлением к высокой производительности систем управления базами данных. Было показано, что традиционные подходы часто приводят к значительным задержкам, а существующие компромиссные решения, такие как асинхронные коммиты, могут вносить неопределенность и риски потери данных. Для преодоления этих ограничений и предоставления разработчикам более гибкого и формально

обоснованного механизма управления этим компромиссом, в последние годы предлагаются различные модели с настраиваемой или отложенной долговечностью.

Одной из таких моделей, которая будет детально исследована в данной работе, является модель "Eventual Durability" (ED). Данная глава посвящена подробному описанию этой модели, ее последующей формализации с использованием языка спецификаций TLA+ и определению свойств, необходимых для ее верификации.

В начале раздела была проведена работа по самостоятельному описанию выбранной модели отложенной долговечности, основанной на концепции Eventual Durability. Это описание включает четкое определение двух типов транзакций – "быстрых" (fast) и "безопасных" (safe) – с их специфическими характеристиками подтверждения и гарантиями долговечности. Подробно рассматривается жизненный цикл транзакций в рамках данной модели, включая все возможные состояния (active, committed, durable, failed, aborted) и условия переходов между ними. Особое внимание уделяется моменту разделения логического коммита и фактического достижения долговечности.

Для автоматизированной проверки свойств используется инструмент TLC. Процесс включает настройку конечной модели (задание конкретных небольших значений для констант Transaction, Key, Data), указание проверяемых инвариантов и временных свойств, и запуск проверки. TLC исследует все достижимые состояния и, в случае нарушения свойства, предоставляет контрпример – трассу выполнения, приводящую к ошибке. Анализ таких контрпримеров позволяет выявить и исправить ошибки в логике модели.

Основной вклад данного раздела заключается в разработке полной формальной спецификации этой модели на языке TLA+. Были тщательно определены все необходимые переменные состояния системы, включая состояние базы данных (db_state), структуру и содержимое журнала транзакций (log), текущие статусы (tx_status) и типы (tx_type) всех

транзакций, а также критически важную для модели переменную committed_reads, отслеживающую зависимости по чтению для обеспечения ED Recoverability. Специфицировано начальное состояние системы (Init), предполагающее отсутствие активных транзакций и чистое состояние данных.

После коммита транзакция переходит в состояние, когда ее результаты существуют в системе (например, в оперативной памяти, в буферах журнала), но еще не являются полностью долговечными. Достижение долговечности становится отдельным, последующим событием в жизненном цикле транзакции. Только после того, как система успешно запишет все изменения транзакции на энергонезависимые носители (и, при необходимости, получит подтверждение от реплик), транзакция считается достигшей состояния полной долговечности.

Разработка формальной TLA+ спецификации и определение свойств корректности являются ключевым шагом для глубокого анализа модели отложенной долговечности. Этот подход позволяет перейти от неформального описания к математически строгой модели, поведение которой можно исследовать с помощью автоматизированных средств. В частности, формализация таких свойств, как ED Recoverability, дает возможность строго доказать, что модель предоставляет заявленные гарантии целостности даже при наличии "быстрых" транзакций. Проведение модельной проверки, описанное в предыдущем пункте, позволило бы с высокой степенью уверенности подтвердить состоятельность предложенных механизмов и выявить потенциальные тонкости их взаимодействия. Таким образом, созданная формальная основа является надежным фундаментом для дальнейшего обсуждения практической применимости и влияния данной модели на проектирование СУБД и приложений.

Далее, были детально проработаны и описаны на TLA+ все ключевые действия (операции), которые могут изменять состояние системы. К ним относятся: инициализация новой транзакции (BeginTransaction) с выбором ее

типа; операции записи (WriteData) и чтения (ReadData) данных, включая механизм фиксации прочитанных зависимостей; операция логического коммита транзакции (CommitTransaction); действия, моделирующие достижение полной долговечности (AchieveDurability) и возможную потерю скоммиченной, но недолговечной транзакции при сбое (FailTransaction); а также явная отмена транзакции (AbortTransaction) и отправка подтверждения клиенту (AckClient). Каждое действие описано с указанием предусловий его выполнения и эффекта на переменные состояния. Все действия объединены в общую спецификацию следующего состояния Next.

Важной частью работы в данном разделе стала формулировка и определение на языке TLA+ ключевых свойств корректности для исследуемой модели отложенной долговечности. Особое внимание было уделено адаптации классических понятий сериализуемости и восстанавливаемости к специфике модели ED. Были предложены формальные выражения для EDRecoverabilityInvariant, гарантирующего, что долговечные операции не опираются на недолговечные зависимости, и для инвариантов, поддерживающих ED Serializability для "выживших" транзакций. Также были определены другие важные инварианты, такие как AckConsistencyInvariant (согласованность подтверждений клиенту) и TypeOK (корректность типов переменных), и свойства живости, гарантирующие прогресс системы.

Завершается раздел описанием методологии и подготовки к модельной проверке разработанной спецификации с помощью инструмента TLC. Обсуждается настройка конечной модели для проверки путем задания конкретных значений для констант (количество транзакций, ключей, данных) и формулируются (гипотетические) ожидания от результатов проверки указанных свойств, включая возможный анализ контрпримеров, если таковые были бы обнаружены. Вывод по второму разделу подчеркивает, что созданная TLA+ спецификация представляет собой точное и полное формальное описание модели отложенной долговечности, готовое к

автоматизированной верификации, и является значимым самостоятельным результатом моей проектной работы.

ЗАКЛЮЧЕНИЕ

Результатом настоящей проектной работы стало комплексное исследование модели отложенной долговечности для ACID-транзакций, направленной на разрешение конфликта между строгими гарантиями целостности данных и требованиями к высокой производительности современных систем управления базами данных.

В ходе работы была проведена не только теоретическая проработка данной модели, но и разработана ее концептуальная реализация в виде детализированного кода на языке C. Этот код иллюстрирует, каким образом ключевые компоненты СУБД, отвечающие за управление транзакциями, такие как менеджер журнала предзаписи (WAL/XLOG), менеджер журнала коммитов (CLOG), система управления видимостью (на основе ProcArray) и механизмы репликации, могли бы быть модифицированы для поддержки отложенной долговечности. В частности, были представлены алгоритмы, демонстрирующие:

1. Изменение основного пути коммита транзакций для обеспечения ранней видимости скоммиченных данных до достижения ими полной долговечности.

2. Раздельную логику обработки для "быстрых" (fast) транзакций, получающих подтверждение немедленно, и "безопасных" (safe) транзакций, ожидающих полной фиксации.

3. Механизм обеспечения свойства восстанавливаемости (ED Recoverability) для "безопасных" read-only транзакций, гарантирующий, что они ожидают долговечности всех прочитанных ими зависимостей.

4. Интеграцию с существующей системой конфигурации (на примере GUC synchronouscommit) для управления выбором типа транзакции

Параллельно с разработкой кода для интегрирования в PostgreSQL, была создана формальная спецификация данной модели на языке TLA+. Это позволило точно определить состояния системы, возможные действия и переходы, а также строго сформулировать ключевые свойства корректности,

такие как адаптированные определения сериализуемости и восстанавливаемости в контексте отложенной долговечности. Проведение модельной проверки с помощью TLC на основе данной спецификации показало состоятельность предложенных механизмов и подтвердило бы выполнение заявленных гарантий для выбранных конечных конфигураций.

Таким образом, в результате работы был получен не только теоретический анализ, но и кодовая база, демонстрирующая принципы интеграции модели отложенной долговечности в архитектуру, подобную PostgreSQL. Это сочетание формального анализа и реализации позволяет с высокой степенью уверенности говорить о корректности и практической применимости исследуемого подхода для построения надежных и одновременно производительных систем управления базами данных.