**CSCI 4333**

**4/23/2025**

**Introduction to concurrency control and transaction management**

by K. Yue

**1. Concepts of Concurrency Control**

* Modern databases are multi-user, multi-tasking systems: many users access the system concurrently with many tasks.
* A task may not be completed in one continuous execution. It may be divided into many execution steps.
* There are many concurrent tasks.
* There are no guarantees of the relative orders of concurrent tasks in an execution *schedule*.
* Without proper concurrency control,
  1. Read-write anomaly and write-write anomaly can occur.
  2. Database may become inconsistent.
* Task schedules need to maintain data and transaction integrity.

***Example:***

Use case: transfer $200 from account 1000 to account 2000.

-- Task t1  
-- Assumption: account 1000: $1,000, account 2000: $500  
-- Initial consistent state: total of two accounts: $1,500  
  
-- Step [1]:  
UPDATE Account SET amount=amount-200 WHERE account\_number=1000;  
  
-- Between step [1] and step [2]:  
-- Inconsistent state at this point; total of two accounts: $1,300  
  
-- Step [2]:  
UPDATE Account SET amount=amount+200 WHERE account\_number=2000; -- step [2]  
  
-- After completion of step [2]: consistent state again; total of two accounts: $1,500

Intended sequence #1 for task #1:

(1) Task t1 step [1]  
(2) Task t1 step [2]

Sequence #2: read-write anomaly.

(1) Task t1: step [1]  
(2) Task t2 reads the inconsistent state to produce an account report: account 1000: $800, account 2000: $500  
(3) Task t1: step [2]

Sequence #3: system crash and recovery

(1) Task t1: step [1]  
(2) System crashes; task t1 aborts after step [1]

Sequence #4: write-write anomaly.

(1) Task t1: step [1]  
(2) Task t2 reads and account amounts, calculate interest and update accounts. Interests will be calculated based on account 1000: $800, account 2000: $500.  
(3) Task t1: step [2]

**1.1 ACID Properties**

* Thus, to avoid accessing inconsistent states, concurrency control is necessary.
* Concurrency control is mainly done by transaction management.
* A transaction is a logical unit of database processing that is *atomic*: either the entire transaction is performed, or none of the transaction action is performed. This is the 'all or nothing' property.
* This refers to the famous ACID properties in DBMS: e.g. <http://en.wikipedia.org/wiki/ACID>
* ACID properties:
  1. Atomicity: A transaction is an atomic unit of processing. It is either performed in its entirety or not performed at all. (all or nothing property)
  2. Consistency preservation: A correct execution of a transaction must take the database from one physically consistent state to another. This is known as physical consistency.
  3. Isolation: A transaction should not make its updates visible to other tasks and transactions until it is committed.
     + In the example above, isolation disallows task t2 to access the inconsistent states of accounts 1000 and 2000 within task t1.
     + This property, when enforced strictly, solves the temporary update problem and makes cascading rollbacks of transactions unnecessary.
  4. Durability or permanency: Once a transaction changes the database and the changes are committed, these changes must never be lost because of subsequent failure.
* Implementing ACID can bring performance degradation. Thus, for example, some NoSQL DB provide only 'eventual consistency'.
* Many NoSQL databases support the BASE model instead: Basic Availability, Soft-State, Eventual Consistency.
* Many DBMS support ACID by means of locking or multi-versioning.
* Basically, in locking, a transaction may have the exclusive access to selected data until the transaction is terminated.
* SQL support of transaction management depends on the vendor. It usually includes:
  1. The execution of a single SQL statement is atomic.
  2. The commands START TRANSACTION (or similar) and END TRANSACTION (or similar) are available to specify the boundary of transactions.
  3. COMMIT makes all data changes in the transaction to become permanent.
  4. ROLLBACK undoes all data changes in the transaction (or since the last COMMIT or ROLLBACK).

***Example:***

Use case: transfer $200 from account 1 to account 2000.

START TRANSACTION;  
  UPDATE Account SET amount=amount-200 WHERE account\_number=1000;  
  UPDATE Account SET amount=amount+200 WHERE account\_number=2000;  
  
IF ERRORS=0 COMMIT;  
IF ERRORS<>0 ROLLBACK;

**1.2 Application programmer's responsibility in terms of ACID**

1. Atomicity: the transaction is either fully committed, or fully rollback. The DB developer needs to define the scope and action of the transaction.
2. Consistency: the execution of transaction should keep data consistent. It is the programmer's responsibility to ensure logical consistency: that the logic of the code is consistent with the problem requirements.

***Example:*** The following transaction can be atomic but *inconsistent*.

START TRANSACTION;  
  UPDATE Account SET amount=amount-200 WHERE account\_number=1000;  
  UPDATE Account SET amount=amount+400 WHERE account\_number=2000;  
  
IF ERRORS=0 COMMIT;  
IF ERRORS<>0 ROLLBACK;

1. Isolation: As a result, concurrent access will leave the database consistent. Usually not a concern for the application programmers.
2. Durability: Once committed, the transaction is finalized. Usually no concern for the application programmers.

**2. MySQL Transaction Management**

* MySQL Manual on TM statements: <https://dev.mysql.com/doc/refman/8.1/en/sql-transactional-statements.html>
* Autocommit mode: after the execution of a SQL statement, the result is automatically committed.
* START TRANSACTION disables the autocommit mode.
* MySQL supports COMMIT and ROLLBACK.
* It also supports LOCK TABLES and UNLOCK TABLES.

***Example:***

This is not a realistic example but it shows you an example of transaction management.

Suppose we have an ActiveStudent table on top of the Student table in toyu. The column numCourses is the number of courses a student has enrolled in. It is a derived column obtained by counted the number of classId the student in the enroll table.

CREATE TABLE IF NOT EXISTS activeStudent(  
    stuId        INT NOT NULL,  
    fname        VARCHAR(30) NOT NULL,  
    lname        VARCHAR(30) NOT NULL,  
    numCourses   INTEGER(4) DEFAULT 0  
);  
  
SELECT \* FROM activeStudent;  
  
-- Populating activeStudent initially.  
INSERT INTO activeStudent(stuId, fName, lName, numCourses)  
SELECT s.stuId, s.fName, s.lName, COUNT(e.classId) as numCourses  
FROM Student AS s LEFT JOIN Enroll AS e ON (s.stuId = e.stuId)  
GROUP BY s.stuId, s.fName, s.lName;  
  
SELECT \* FROM activeStudent;  
  
When we add the enrollment (100000, 10006, NULL, 0), we need to perform two tasks:

1. insert the row (100000, 10006, NULL, 0) into enroll.
2. increment numCourses for student 100000 by 1 in activeStudent

We can write a procedure to do so:

DROP PROCEDURE IF EXISTS enroll;  
  
DELIMITER //  
  
CREATE PROCEDURE enroll  
   (IN stuid VARCHAR(6),  
    IN classId VARCHAR(8),  
    IN grade VARCHAR(2),  
    IN n\_alerts INT)  
BEGIN  
  
DECLARE EXIT HANDLER FOR SQLEXCEPTION  
BEGIN  
   ROLLBACK;  
   RESIGNAL; -- pass on the error with no change.  
END;  
  
START TRANSACTION;  
  
INSERT INTO enroll  
VALUES (stuid, classId, grade, n\_alerts);  
  
UPDATE activestudent AS a  
SET a.numCourses = a.numCourses + 1  
WHERE a.stuid = stuid;  
  
COMMIT;  
  
END //  
  
DELIMITER ;  
  
SELECT \* FROM Enroll;  
SELECT \* FROM ActiveStudent;  
  
CALL enroll(100000, 10006, NULL, 0);  
CALL enroll(100009, 10006, NULL, 0);  
  
SELECT \* FROM Enroll;  
SELECT \* FROM ActiveStudent;  
  
DROP TABLE ActiveStudent;  
DROP PROCEDURE enroll;  
  
DELETE FROM enroll WHERE stuId = 100000 AND classId = 10006;  
DELETE FROM enroll WHERE stuId = 100009 AND classId = 10006;  
  
SELECT \* FROM Enroll;

**NoSQL Databases**

by K. Yue

**1. Introduction**

* NoSQL:
  + “Not Only SQL” or “Not SQL.” Relatively new kinds of non-relational database systems.
  + A loose category of many diverse database systems with different data models.
* Some common NoSQL features:
  + Non-relational
  + Distributed
  + High scalability
  + High availability
  + High performance and parallelism
  + No or flexible schema
  + Weaker support of ACID properties
  + Oriented towards semi-structured or non-structured data.
  + Weaker support of data integrity and constraints.
  + Usually more object-oriented.
  + More analysis-oriented than transaction-oriented.
  + Simpler APIs for database interaction.
* Major non-relational database systems as in top db-engines ranking, <https://db-engines.com/en/ranking> (rankings as of 9/1/2023):
  + Document models: e.g. *MongoDB* (rank #5), CouchBase (32), Firebase Realtime Database (38), CouchDB (44), Realm (56)
  + Key-value models: e.g. Redis (6), Memcached (33), etcd (52), HazelCast (55), LevelDB (111).
  + Wide-column models: e.g. Cassandra (12), Hive (17), HBase (26), Datastax Enterprise (60)
  + Graphical models:*Neo4J (22)*
* Some observations:
  + Search engines (not really a data model): ElasticSearch (8; document model), Splunk (14; key-value), Solr (24; document model)
  + Still dominated by relational databases.
  + Many DB support multiple models.
* Read:
  + A simple introduction to NoSQL database: <https://www.guru99.com/nosql-tutorial.html>
  + Introduction to NoSQL: <https://www.geeksforgeeks.org/introduction-to-nosql/>

**2. Advantages and Disadvantages**

* Some advantages of NoSQL databases in general:
  1. Distributed
  2. High scalability: horizontal scalability, as opposed to vertical scalability.
     1. Horizontal scalability (scaling out): add more machines to the distributed system.
     2. Vertical scalability (scaling up): add more power to existing machines; replace existing machines by more powerful one.
  3. High availability
  4. High performance
  5. Flexibility: flexible schema or schemaless
  6. More object-oriented:
     1. Better abstraction model
     2. Better interoperability with programming language. No need of object-relational mapping.
* Some disadvantages of NoSQL databases in general:
  1. Weaker data integrity support
  2. Weaker transaction support
  3. Weaker theoretical and design methodology support
  4. Relative lack of standards
  5. Relative lack of tools and interoperability
  6. Complexity

**3. ACID versus BASE Transaction Models**

**3.1 ACID**

* Relational database support ACID properties to support data consistency and integrity of transactions under concurrent access: e.g., <http://en.wikipedia.org/wiki/ACID>
* ACID properties (review):
  1. Atomicity: A transaction is an atomic unit of processing. It is either performed in its entirety or not performed at all.
  2. Consistency preservation: A correct execution of a transaction must take the database from one physically consistent state to another. This is known as physical consistency.
  3. Isolation: A transaction should not make its updates visible to other tasks and transactions until it is committed.
  4. Durability or permanency: Once a transaction changes the database and the changes are committed, these changes must never be lost because of subsequent failure.
* Supporting ACID limits other desirable features: scalability, availability, and performance.

**3.2 BASE**

* To enhance scalability, availability and performance, most NoSQL DB do not fully support ACID.
* NoSQL supports different transaction models.
* The Basic Availability, Soft-State, Eventual Consistency (BASE model) for distributed database is the most popular one.
  1. Basic available: data is basically available across nodes of the distributed database, despite network failures.
  2. Soft-state: There is no immediate consistency. As a result, different replicas may have different values across the distributed systems at a given time. Thus, the state of the database is soft.
  3. Eventual consistency: eventually, data replicas will have the same value across the distributed database.

**3.3 CAP Theorem**

* Since NoSQL databases are mostly distributed, it is important to have some understanding of the famous CAP theorem for distributed data stores.
* See, for example, <https://en.wikipedia.org/wiki/CAP_theorem>.
* There are three *desirable* guarantees of *distributed* data stores, CAP:
  1. Consistency: the return value is always the same for the same data across the distributed systems.
  2. Availability: every request will return a response, either the data or an error. (Note that the return data may or may not always be the same).
  3. Partition tolerance: the database continues to operate in case of network partitions (one partition of the network cannot communicate with another partition because of message drops).
* The CAP theorem states that any distributed database can provide only two out of the three guarantees.
* Different databases based their designs on prioritizing two out of the three C-A-P.
* For a more detailed discussion, one may see:  <https://www.instaclustr.com/blog/cassandra-vs-mongodb/> (optional read):
  1. It contains a discussion how Cassandra and Mongo trade-off CAP.
  2. It also includes a discussion of a more refined CAP theorem: PACELC Theorem: "PACELC is summarized as follows: In the event of a partition failure, a distributed system must choose between Availability (A) and Consistency (C), else (E) when running normally it must choose between latency (L) or consistency (C)."

**4. Major NoSQL data models**

**4.1 Key-value model**

1. Data is stored as key-value pairs.
2. Values can possibly be JavaScript Object Notation (JSON) strings, which store serialized objects.
3. Some key-value databases support rich JSON queries.

**4.2 Document Model**

1. Document-oriented databases store data as documents.
2. Documents can be considered as semi-structured data.
3. Thus, XML databases can be considered as employing the document model.
4. Modern document-oriented databases commonly employ JSON. E.g., MongoDB and CouchDB.
5. The document model can be considered as a subclass of key-value model.
   1. The stored value of a key-value model can be a document.
   2. The stored value can be manipulated by operations based on the selected document model (mostly JSON).
6. MongoDB is likely the most popular document-oriented NoSQL DB. It will be covered in more details in this class.

***Example:*** In CouchDB, a key-value pair may be:

**Key:**"MBSEBaseModel~939c7672-5d2d-11ec-bf63-0242ac130002"  
  
**Value to be stored:**

{  
   "BCAssetId": "939c7672-5d2d-11ec-bf63-0242ac130002",  
   "BCAssetType": "MBSEBaseModel",  
   "BCAssetName": "Gateway-PPE-Base-Model",  
   "BaseModelDesc": "PPE project's model.",  
   "version": {  
      "version": "2.1",  
      "subversion": "4.6",  
      "startTime": "2021-12-08T17:25:23+06:00"  
   },  
   "storage": {  
      "isEncrypted": true,  
      "EncrypMethod": "AES256",  
      "EncrypKey": "q4t7w!z%C\*F-JaNdRgUkXp2r5u8x/A?D",  
      "useIPFS": true,  
      "IPFSCid": "QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX",  
      "IPFS\_HashHead": "A0Xa",  
      "payloadRaw": "raw PPE MBSE Base model description. V2.1.4.6.",  
   }  
}

Note:

* CouchDB adds two fields, \_id and \_rev, automatically if they are not supplied.
* The field \_rev is used for multi-version concurrency control (MVCC) to ensure 'eventual consistency.'
* Some may consider CouchDB as a document-oriented database. The boundary between key-value model and document model is not clear cut.

To query CouchDB, one may use many methods. Examples:

1. CouchDB RESTful API: <https://docs.couchdb.org/en/latest/api/index.html>
2. MapReduce-based views: <https://docs.couchdb.org/en/latest/ddocs/views/index.html>
3. Mango query

An example Mango query that returns all CouchDB key-value pairs for MBSEBaseModel.

{  
    "selector": {  
        "BCAssetType": { "$eq": "MBSEBaseModel" }  
    }  
}

See <https://docs.couchdb.org/en/latest/api/database/find.html> for more information about selector syntax.

**4.3 Wide-Column Model**

1. A columnar DBMS or column-oriented DBMS stores data tables grouped by columns, instead of grouped by rows (as in most relational DBMS).
   1. For example, related columns may be stored together in a file for faster performance.
   2. Benefits:
      1. Faster access for certain types of queries.
      2. Better chance for data compression.
   3. Disadvantages:
      1. Slower update.
      2. Slower access for certain types of queries.
2. Read introductions to the wide-column model. Examples:
   1. <https://dandkim.com/wide-column-databases/>
3. In wide column model, data is stored as keys and columns. Each column contains a column-name and a value.
4. Thus, to get a data value, use (key, column-name).
5. Cassandra is one of the most popular wide-column databases.

**4.4 Graphical Model**

1. "A graph database stores nodes and relationships instead of tables, or documents."
2. Quite object-oriented, using a directed graph model.
3. neo4j is the most popular graphical database.
4. Introduction: <https://neo4j.com/developer/graph-database/>.
5. To start learning Neo4j, download and install Neo4j desktop.
6. Neo4j Query Language: Cypher, <https://neo4j.com/developer/cypher/>.
7. Basic Cypher syntax: (nodes)-[:ARE\_CONNECTED\_TO]->(otherNodes).

**DB Security**

by K. Yue

**1. Database Security**

* Protect the database from unauthorized access, modification, or destruction.
* The CIA Model of Security (or AIC Triad)
  1. Confidentiality: accessed only by authorized users.
  2. Integrity: modified only by authorized users.
  3. Availability: accessible when needed.
* Information system *access control* must address:
  1. Authorization: Who have what privileges to which objects?
  2. Identification: E.g., Account names.
  3. Authentication: E.g., Password.
  4. Accountability: E.g., Who have done what actions?
* Some database security mechanisms:
  1. Views: define better access controls.
  2. Security log: journals storing attempted security violations.
  3. Audit trail: Information about SQL operations are stored, such as by using triggers.
  4. Encryption: especially sensitive information such as passwords.
* SQL authorization language:
  1. GRANT statement used for authorization
  2. REVOKE statement used to retract authorization
  3. MySQL directly supports ROLE, which can be used as the basis of a simple Role Based Access Control (RBAC) system.

***Example:***

CREATE USER 'temp'@'%' IDENTIFIED VIA mysql\_native\_password USING ....;  
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, SHOW DATABASES, CREATE TEMPORARY TABLES ON \*.\*  
     TO 'temp'@'%' REQUIRE NONE WITH MAX\_QUERIES\_PER\_HOUR 0 MAX\_CONNECTIONS\_PER\_HOUR 0 MAX\_UPDATES\_PER\_HOUR 0 MAX\_USER\_CONNECTIONS 0;

**2. SQL Injection (SQLI)**

* A code injection method that takes advantages of dynamic SQL construction in database-driven Web applications.
* One of the most common Web hacking techniques.
* Originated from *improper filtering of special characters*in the target languages (SQL in this case).
* Attackers enter input through Web forms to modify the intention of the SQL statements in the backend Web applications.

***Example: adapted from the textbook and Wikipedia***

Consider a Web form that accepts user names and passwords:

The back-end page may include unsafe code dynamically constructing a query.

query = "SELECT \* FROM users WHERE name = '" + *username* + "' and password = '" + *password* + "';"

The variables username and password get their values from the users through the Web form through the CGI protocol.

Thus, if the user enters (not considering encryption issues here):

username = yue  
password = 1Bkm\*2ce

the variable query will have a value of

"SELECT \* FROM users WHERE name = '*yue*' and password = '*1Bkm\*2ce*';"

The query can be executed to get information about the user 'yue' if the right password is provided.

If someone enters:

username = yue  
password = 1Bkm\*2*'*ce

query becomes:

"SELECT \* FROM users WHERE name = 'yue' and password = '1Bkm\*2*'*ce';"

Executing the SQL query statements will result in a SQL syntax error in the server-side program since the single quote character ' is an escape character in SQL with special meanings.

For SQL injection, attacker may enter:

username = yue  
password = *' OR '1'='1*

query becomes:

"SELECT \* FROM users WHERE name = 'yue' and password = '*' OR '1'='1*';"

Note that the structure of the SQL statement has been changed. Since the and operator has a higher precedence than the or operator, this is equivalent to:

"SELECT \* FROM users WHERE (name = 'yue' and password = '') *OR* '1'='1';"

The condition in the WHERE clause will always be evaluated to true. The query will bypass the password checking and return information about *all* users, not just the user 'yue'.

For input:

username = yue  
password = ' OR '1'='1’; DELETE \* FROM student; --

query becomes essentially:

"SELECT \* FROM users  
 WHERE name = 'yue' and password = '*' OR '1'='1';  
 DELETE \* FROM student; --*'; "

For input:

username = yue  
password = ' OR '1'='1’; DROP TABLE users; SELECT \* FROM account; --

query becomes essentially:

"SELECT \* FROM users  
 WHERE name = 'yue' and password = '*' OR '1'='1';  
DROP TABLE users;  
SELECT \* FROM account; --* '; "

In all of these examples, the*intended structures* of the SQL statements are changed by the attackers.

**2.1 SQLI Mitigation**

[1] Input validation: validate input parameter values, properly escaping special characters.

In the minimum, replace one ' by two ':

username = username.replace("'", "''")  
password = password.replace("'", "''")

For input parameters:

username = yue  
password = ' OR '1'='1

after filtering query becomes:

"SELECT \* FROM users WHERE name = 'yue' and password = '*''* OR *''*1*''*=*''*1';"

The condition of the Where clause will be false (unless the password is really "*' OR '1'='1*".

* Besides possible SQLI, a Web page without proper input validation may result in syntax or runtime errors and reveals information about the back-end system.
* Input validation not only improves security. It has many other benefits.

[2] Using parameterized queries:

* Parameterized queries are usually *prepared and compiled* beforehand with placeholders for input parameters. The structure of the SQL statement cannot be changed. E.g., in Python, %s is a parameter placeholder.

query = "SELECT \* FROM users WHERE name = %s and password = %s;"  
cursor.execute(query,(username, password))

* Prepared statements provide many benefits and should always be considered as the first choice.

[3] Using intermediate mid-tiered objects instead of SQL for centralized checking.

* Example: instead of directly executing SQL statements, the Web applications can call methods of well-designed and well-tested classes to access the data.

[4] Use database security features and good practices

* Can be vendor specific.
* Apply the CIA principle to set up the database.