

In this scenario shows an involvement of concurrency control in a database system, where three transactions (T1, T2, and T3) interact with shared data. **Transaction T1 A Successful Transaction:**

Transaction T<sub>1</sub> begins by acquiring an exclusive lock (Lock-X) on data item A in step 1. The exclusive lock ensures that no other transaction can read or modify A until T<sub>1</sub> releases the lock. After securing the lock, T<sub>1</sub> proceeds to read A in step 2 and then writes to A in step 3, updating its value. This sequence of operations indicates that T<sub>1</sub> has modified the data item.

In step 4, T<sub>1</sub> moves to acquire a shared lock (Lock-S) on data item B, reaching a lock point (LP). The lock point signifies a stage where T<sub>1</sub> has locked all necessary resources, preventing conflicts with other transactions. After locking B, T<sub>1</sub> reads the value of B in step 5 and then releases both locks on A and B in step 6. The successful unlocking of these resources indicates that T<sub>1</sub> has completed its operations and can commit its changes, thereby maintaining data consistency and integrity.

**Transaction T2 dirty read and rollback.** Transaction T<sub>2</sub> begins after T<sub>1</sub> has completed its operations. In step 7, T<sub>2</sub> attempts to acquire an exclusive lock on A. Once T<sub>2</sub> secures the lock, it reads the value of A in step 8. However, this is where the problem of a dirty read arises. The value that T<sub>2</sub> reads has been modified by T<sub>1</sub>, but the change has not yet been fully committed by T<sub>1</sub>. As a result, T<sub>2</sub> reads uncommitted data.

In step 9, T<sub>2</sub> tries to write to A, but the system detects that it has read uncommitted data, leading to a violation of concurrency control rules. To prevent data inconsistency, the system triggers a rollback for T<sub>2</sub>. The rollback ensures that any changes made by T<sub>2</sub> are undone, and the system is reverted to a consistent state. This rollback highlights the importance of handling dirty reads and the role of concurrency control mechanisms in ensuring database reliability.

**Transaction T3 Another Dirty Read and Rollback.** Transaction T<sub>3</sub> experiences a similar fate as T<sub>2</sub>. It begins by attempting to read the value of A after T<sub>1</sub> has modified it. In step 11, T<sub>3</sub> tries to acquire a shared lock (Lock-S) on A and subsequently reads the value of A. However, like T<sub>2</sub>, T<sub>3</sub> is also reading the uncommitted value of A from T<sub>1</sub>, which leads to another instance of a dirty read. The system again detects the problem and triggers a rollback for T<sub>3</sub> to prevent the propagation of inconsistent data.

**Dirty Reads and Rollbacks: Key Issues.** The term "dirty read" refers to a situation where a transaction reads data that has been modified by another transaction but not yet committed. This is a major issue in database concurrency because it can lead to inconsistencies if multiple transactions are allowed to operate on uncommitted data. In this scenario, both T<sub>2</sub> and T<sub>3</sub> fall victim to dirty reads caused by T<sub>1</sub>'s uncommitted write to A.

To address this, the system enforces strict concurrency control mechanisms. When it detects that T2 and T3 have read uncommitted data, it triggers a rollback for each transaction. Rollbacks are a safeguard in database systems, ensuring that any transaction that has operated on faulty data is undone, thus preserving the consistency of the overall system.