ISCAS 中国科学院软件研究所学术年会'2023 暨计算机科学国家重点实验室开放周
学术论文

基于差分语句执行的数据库逻辑缺陷检测方法

宋建森，窦文生，崔紫玉，戴千旺，王伟，魏峻，钟华，黄涛

Testing Database Systems via Differential Query Execution

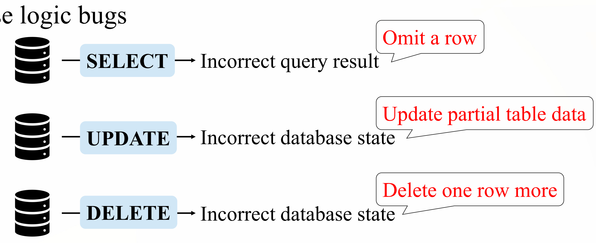
The 45th IEEE/ACM International Conference on Software Engineering (ICSE'23)

联系方式：宋建森，18730619983，songjiansen20@otcaix.iscas.ac.cn

Database Management Systems Suffer from Logic Bugs

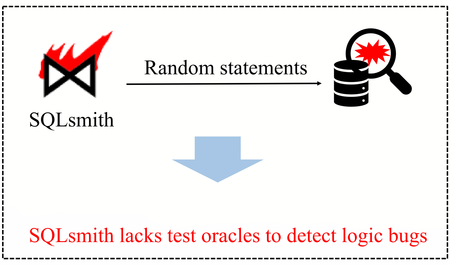
- Database Management Systems (DBMSs) are widely used to store, retrieve and manipulate data
- Incorrect implementations of DBMSs can cause logic bugs

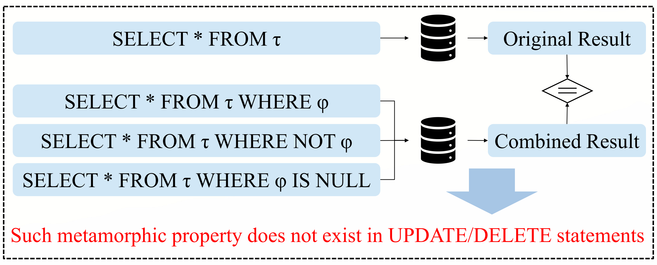
MySQL MariaDB SQLite PostgreSQL CockroachDB TiDB



Existing Approaches Focus on Detecting SELECT-related Logic Bugs

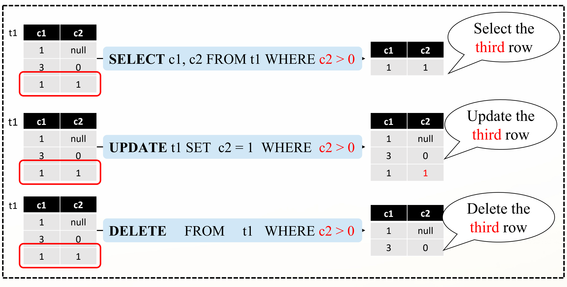
- Existing approaches either detect crash bugs or detect logic bugs in SELECT statements
- These approaches cannot detect logic bugs in UPDATE/DELETE statements

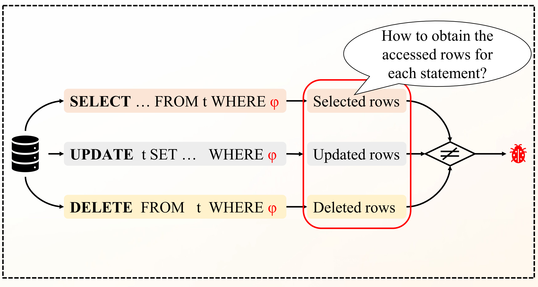




Differential Query Execution (DQE)

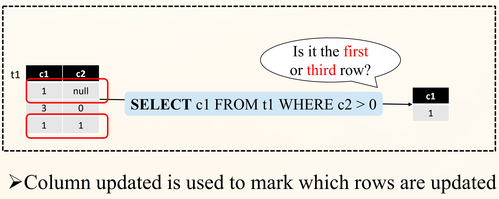
- We observe that SQL statements utilize predicates to specify which rows to manipulate
- We propose DQE to detect logic bugs in SELECT, UPDATE and DELETE statements



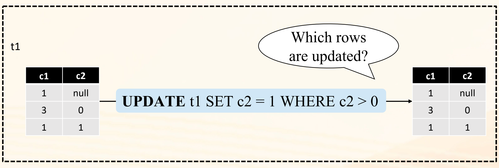


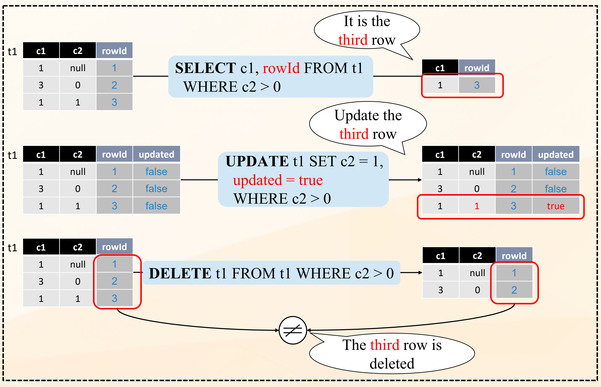
Obtain the Accessed Rows for Each Statement

- Column rowId is used to uniquely identify each row



- Column updated is used to mark which rows are updated





Experimental Results

DBMS	DB-Engines Ranking	GitHub Stars	Type	Submitted	Confirmed	Fixed	Duplicate	Not a bug
MySQL	2	9.0K	Traditional	7	1	1	0	6
SQLite	9	3.9K	Embedded	1	1	0	0	0
MariaDB	13	4.9K	Traditional	4	2	0	0	0
CockroachDB	60	26.9K	NewSQL	1	0	0	1	0
TiDB	107	34.4K	NewSQL	37	37	10	0	0
			Total	**50**	**41**	**11**	**1**	**6**