香 港 中 文 大 學
The Chinese University of Hong Kong

Course Examination 1st Term, 2013-14

Course Code & Title: BMEG 3120 Database and Security for Biomedical Engineering

Time Allowed : 1.5 hours

Student ID : ..... Seat No. : .....

Problems 1-3 are based on the tables below:

- `author(aid, aname)`: This represents a table with name `author` whose attributes are as shown in the brackets. The underlined is the candidate key. Each tuple represents an author, whose id and name are given by `aid` and `aname`, respectively.
- `book(bid, title, category)`: Each tuple represents a book. The attribute `category` describes the genre of the book (e.g., novel, sci-fi, science, music, ...).
- `student(sid, sname, dept)`: Each tuple represents a student. The attributes' meanings should be self-explanatory.
- `write(aid, bid)`: A tuple means that book `bid` was written by author `aid`.
- `borrow(sid, bid, checkout-time, return-time)`: A tuple means that student `sid` checked out book `bid` at `checkout-time`, and returned it at `return-time`.

All attributes are strings, except `checkout-time` and `return-time`, which are integers. A smaller `checkout-time` represents an earlier timestamp (same for `return-time`).

Problem 1. Give relational algebra queries for the tasks below:

1. (6%) Find the `sid`s of the students that have never borrowed any book.
2. (12%) Find the `sid`s of all such students: all the books that s/he has ever borrowed belong to the same category (it does not matter which category it is).

Solutions.

1. $\Pi_{\text{sid}}(\text{student}) - \Pi_{\text{sid}}(\text{borrow})$
2. $T_1 \leftarrow \Pi_{\text{sid, category}}(\text{student} \bowtie \text{borrow} \bowtie \text{book})$
   $T_1 \leftarrow T_2$
   $T_3 \leftarrow \Pi_{\text{sid}}(\sigma_{T_1.\text{sid}=T_2.\text{sid} \wedge T_1.\text{category}\neq T_2.\text{category}}(T_1 \times T_2))$
   $\Pi_{\text{sid}}(\text{borrow}) - T_3$

Problem 2. Given SQL queries for the tasks below:

1. (6%) Find the category with at least 10000 books.
2. (12%) Define the *popularity* of a book as the number of distinct students that have ever borrowed it. Find the titles of the books with the highest popularity (note that multiple books may have the same popularity).

Solutions.

1. select category
   from book
   group by category
   having count (bid) >= 10000
2. select title
   from (select bid, count(distinct sid) as popularity
   from borrow
   group by bid) as T, book
   where popularity = (select max(popularity) from T) and T.bid = book.bid

Problem 3 (12%). Explain in English the task performed by the following query:

select sname, title
from student S, borrow, book
where S.sid = borrow.sid and borrow.bid = book.bid and
checkout-time <= all (select checkout-time from borrow where sid = S.sid)

Solutions. For each student that has borrowed at least one book, find her/his name and the title of the first book s/he borrowed.

Problem 4. We have a relation $R(A, B, C, D)$. In each of the following questions, you are given a set F of functional dependencies, and a decomposition of R into two tables R_1 and R_2. In each case, indicate whether the decomposition is lossy or lossless.

1. (5%) $F = \{BC \to D, C \to D\}$; decompose into $R_1(A, B, C)$ and $R_2(B, D)$.
2. (5%) $F = \{B \to C, C \to A, AC \to D\}$; decompose into $R_1(A, B, C)$ and $R_2(B, D)$.

Solutions.

1. Lossy
2. Lossless

Problem 5. We have a relation $R(A, B, C, D)$. In each of the following questions, you are given a set F of functional dependencies. In each case, indicate (i) all the candidate keys of R, (ii) whether R is in BCNF, and (iii) whether R is in 3NF (only if R is not in BCNF).

1. (5%) $F = \{AB \to C, B \to D, D \to A\}$.
2. (5%) $F = \{AD \to C, BD \to A\}$.

Solutions.

1. Candidate keys: B. Not in BCNF. Not in 3NF.
2. Candidate key: BD. Not in BCNF. Not in 3NF.

Problem 6. We have a relation $R(A, B, C, D)$. In each of the following questions, you are given a set F of functional dependencies. In each case, decompose R into BCNF tables; your design must preserve all the functional dependencies.

1. (6%) $F = \{B \to C, B \to D\}$.
2. (6%) $F = \{AB \to C, BC \to D, AB \to D\}$.

Solutions.

1. $R_1(BC), R_2(BD), R_3(AB)$.
2. $R_1(ABC), R_2(BCD)$.

Problem 7 (10%). We have a relation $R(A, B, C, D)$, and a set of functional dependencies $F = \{ABC \to D, AB \to D, B \to A\}$. Decompose R into 3NF tables. Your design must preserve all the functional dependencies.

Solutions. $R_1(BD)$, $R_2(AB)$, $R_3(BC)$.

Problem 8. Consider an RSA cryptosystem with $p = 17, q = 13$ (and hence, $n = 221$), and $e = 5$. Answer the following questions:

1. (6%) What is the value of d?
2. (4%) Let (e, n) be the public key. If we use it to encrypt a message $m = 15$, what is the encrypted message?

Solutions.

1. $d = 77$. Note that $\phi = (p-1)(q-1) = 192$. Hence, $ed = 1 \pmod{\phi}$.
2. $C = m^e \pmod{n} = 15^5 \pmod{221} = 19$.

-End-