CS21001 Discrete Structures, Autumn 2006

End-semester examination

Total marks: 100 November 20, 2006 (AN): S-302 (B) **Duration:** 3 hours

---

[*Answer <u>all</u> questions*]

1 *Consider the following C function:*

```
unsigned int f ( unsigned int n )
{
   if (n == 0) return 0;
   if (n % 2 == 1) return 0;
   return 1 + f(n*(n+1)/2);
}
```

Denote by $f(n)$ the value returned by the above function upon input n.

(a) *Derive the values of $f(2), f(3), f(4), f(5)$, and $f(6)$.* **(5)**

Solution

$$f(2) = 1 + f(3) = 1 + 0 = 1.$$
$$f(3) = 0.$$
$$f(4) = 1 + f(10) = 1 + 1 + f(55) = 2 + 0 = 2.$$
$$f(5) = 0.$$
$$f(6) = 1 + f(21) = 1 + 0 = 1.$$

(b) *Notice that if n is large, the computation of $n(n+1)/2$ (argument for the recursive call) may lead to an overflow. Assume that for some value of n, no overflow occurs during any of the recursive calls. Argue that in this case the function terminates after $\mathrm{O}(\log n)$ number of recursive calls, where n is the argument of f in the outermost call.* **(5)**

Solution Let $n = 2^s t$ with t odd. If $s = 0$, the function makes no recursive calls and returns 0. If $s > 0$, a recursive call is made on $n(n+1)/2$. Since n is even in this case, $n+1$ is odd, and so $n(n+1)/2 = 2^{s-1}t'$ for some odd t'. In other words, the exponent of 2 in the argument decreases by one in this case. After exactly s iterations, the exponent reduces to zero (i.e., the argument becomes odd), and no further recursive calls are made. So the number of recursive calls is s. But $n \geqslant 2^s$, that is, $s \leqslant \log_2 n$.

(c) *Suppose that your machine supports 32-bit unsigned integers and during a multiplication ab of unsigned integers a, b, the least significant 32 bits of the actual product is returned. This means that if there is no overflow during the multiplication, you get the correct product. In case of an overflow, you obtain the least significant 32 bits of the correct product. Justify that in this case too, the function makes $\mathrm{O}(\log n)$ number of recursive calls, where n is the argument of f in the outermost call.* **(5)**

Solution We concentrate only on the case when an overflow occurs during the computation of the product $n(n+1)$. Here $n = 2^s t$ with $s > 0$. Also since n fits in a 32-bit word, $s < 32$. (s cannot be 32, since n would be zero in that case.) But $n+1$ is odd and so the binary representation of $n(n+1)$ contains exactly s trailing 0's. The truncated product will, therefore, be of the form $2^s\tau$ for some odd integer τ. When this is divided by 2, the argument $2^{s-1}\tau$ is passed to the recursive call. That is, in this case too, the exponent of 2 in the argument reduces by exactly 1.

(d) *Describe (with proper justification) what $f(n)$ returns for a positive integer n.* **(5)**

Solution For $n = 2^s t$ with t odd, the function $f(n)$ returns s, since each recursive call contributes 1 and there are exactly s recursive calls.

(e) *Deduce that the running time of the above function is $\mathrm{O}(\log n)$.* **(5)**

Solution Each call of f on $n = 2^s t$ with t odd makes some constant work (checking whether $n = 0$ and $s = 0$). If $s > 0$, a recursive call is made. The argument $n(n+1)/2$ for the recursive call can be computed in constant time. Finally, there are exactly s recursive calls and $s \leqslant \log_2 n$.

2 *Argue (with proper justification) which of the following sets is/are countable.* **(5×5)**

(a) *The set $S_1 = \{n \in \mathbb{R} \mid 3^n + 2^n = 35\}$. (Here $\mathbb{R}$ is the set of real numbers.)*

Solution [Countable] $3^n + 2^n$ is a strictly increasing function of n and so we have

$$3^n + 2^n \begin{cases} = 35 & \text{if } n = 3, \\ < 35 & \text{if } n < 3, \\ > 35 & \text{if } n > 3. \end{cases}$$

It follows that $S_1 = \{3\}$, i.e., a finite (and so countable) set.

(b) *The set $S_2 = \{2, 3, 5, 7, \ldots\}$ of all (positive) prime integers.*

Solution [Countable] S_2 is a subset of the countable set $\mathbb{N}$.

(c) *The set S_3 of all (finite) subsets of $\mathbb{N}$ whose sizes are odd.*

Solution [Countable] Let A_n be the set of all subsets of $\mathbb{N}$ of size n. But then S_3 is the (disjoint) union of countably many sets $A_1, A_3, A_5, \ldots$. Each member of A_n can be treated as an increasing n-tuple of integers, and under this identification A_n is embedded in $\mathbb{N}^n$. But $\mathbb{N}^n$ is countable and so each A_n is countable too. To sum up, S_3 is the union of countably many countable sets.

(d) *The set S_4 of all subsets of $\mathbb{N}$ containing no odd integers.*

Solution [Not countable] $S_4 = \mathcal{P}(\mathbb{E})$, where $\mathbb{E}$ is the set of all even natural numbers. Since $\mathbb{E}$ is a countably infinite set, its power set is not countable.

(e) *The set S_5 of all functions $f : \mathbb{N} \to \mathbb{Z}$ with the property that $f(n) = 0$ except for finitely many $n \in \mathbb{N}$.*

Solution [Countable] For each $f \in S_5$ define $\operatorname{supp} f = \{n \in \mathbb{N} \mid f(n) \neq 0\}$, and $\operatorname{maxsupp} f = \max(\operatorname{supp} f)$ provided that $\operatorname{supp} f$ is non-empty. If $\operatorname{supp} f = \emptyset$, we take $\operatorname{maxsupp} f = 0$. Also for $n \geqslant 0$ define $B_n = \{f \in S_5 \mid \operatorname{maxsupp} f = n\}$. Thus, S_5 is the (disjoint) union of countably many sets $B_0, B_1, B_2, \ldots$. Each B_n has a bijective correspondence with $\mathbb{Z}^{n-1} \times (\mathbb{Z} \setminus \{0\})$ (select the values $f(1), f(2), \ldots, f(n-1)$ arbitrarily from $\mathbb{Z}$ and the value $f(n)$ from $\mathbb{Z} \setminus \{0\}$). That is, each B_n is countable.

3 *In this exercise we work in the semigroup $\mathbb{N}$ under integer multiplication. Define a relation ρ on $\mathbb{N}$ as $a \ \rho \ b$ if and only if a has the same set of prime divisors as b. For example, 5 is related to $25 = 5^2$, $12 = 2^2 \times 3$ is related to $54 = 2 \times 3^3$, but 12 is not related to $16 = 2^4$ nor to $180 = 2^2 \times 3^2 \times 5$.*

(a) *Prove that ρ is a congruence relation on $\mathbb{N}$.* **(5)**

Solution I first show that ρ is an equivalence relation. Clearly, a has the same set of prime divisors as itself, so ρ is reflexive, Also if a has the same set of prime divisors as b, b too has the same set of prime divisors as a, i.e., ρ is symmetric. Finally, if a and b have the same set of prime divisors, and b and c have the same set of prime divisors, a and c too have the same set of prime divisors, i.e., ρ is transitive.

Next I prove the congruence property of ρ. Let $a \ \rho \ b$ and $c \ \rho \ d$. Let $\{p_1, \ldots, p_s\}$ be the common set of prime divisors of a and b, and $\{q_1, \ldots, q_t\}$ the common set of prime divisors of c and d. But then the set of prime divisors for both ac and bd is $\{p_1, \ldots, p_s\} \cup \{q_1, \ldots, q_t\}$, i.e., $(ac) \ \rho \ (bd)$.

(b) *Find the equivalence classes of $1, 2, 3, 4$ and 6.* **(5)**

Solution

$$[1] \ = \ \{1\},$$

$$
\begin{aligned}
[2] &= \{2^i \mid i \geqslant 1\},\\
[3] &= \{3^i \mid i \geqslant 1\},\\
[4] &= \{2^i \mid i \geqslant 1\},\\
[6] &= \{2^i 3^j \mid i, j \geqslant 1\}.
\end{aligned}
$$

(c) *A non-zero integer is called square-free if it is not divisible by the square of a prime number. Prove that each equivalence class in $\mathbb{N}/\rho$ contains a unique square-free integer, and that these unique square-free integers are different in distinct equivalence classes.* **(5)**

Solution Let $a \in \mathbb{N}$ have the prime factorization $a = p_1^{e_1} \cdots p_t^{e_t}$ with $t \geqslant 0$, pairwise distinct primes $p_1, \ldots, p_t$, and each $e_i > 0$. But then a is related to the square-free integer $p_1 \cdots p_t$. No other square-free integer can have the same prime divisors as $p_1 \cdots p_t$. Thus $[a]$ contains a unique square-free integer. Also if $[a] \neq [b]$, we have $[a] \cap [b] = \emptyset$ (ρ is an equivalence relation and so the equivalence classes partition $\mathbb{N}$), i.e., the square-free integers in $[a]$ and $[b]$ are distinct.

4 (a) *Let G be the set of all invertible (i.e., non-singular) 2×2 matrices with real entries. Prove that G is a group under matrix multiplication.* **(5)**

Solution [Closure] The product of two invertible matrices is again invertible.
[Associativity] Matrix multiplication is associative.
[Identity] The identity matrix is invertible.
[Inverse] G contains invertible matrices only.

(b) *Define the center $Z(G)$ of G as:*

$$Z(G) = \{A \in G \mid AP = PA \ \text{ for all } \ P \in G\}.$$

Prove that $Z(G)$ is a normal subgroup of G. **(5)**

Solution First I show that $Z(G)$ is a subgroup of G. Let $A, B \in Z(G)$, i.e., $AP = PA$ and $BP = PB$ for all $P \in G$. But then for any $P \in G$ we have $(AB^{-1})P = A(B^{-1}P) = A(P^{-1}B)^{-1} = A(BP^{-1})^{-1} = A(PB^{-1}) = (AP)B^{-1} = (PA)B^{-1} = P(AB^{-1})$, i.e., $AB^{-1} \in Z(G)$.

For any $P \in G$ we have $PZ(G) = \{PA \mid A \in Z(G)\} = \{AP \mid A \in Z(G)\} = Z(G)P$, i.e., $Z(G)$ is a normal subgroup of G.

(c) *Derive that* $Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\}$. **(5)**

Solution Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an arbitrary member of $Z(G)$. The matrix $P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is invertible, and so $AP_1 = P_1A$ implies $\begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$, i.e., $b = c$, $a = d$, i.e., A must be of the form $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$. Now take $P_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. But then $AP_2 = P_2A$ gives $\begin{pmatrix} a+b & a \\ a+b & b \end{pmatrix} = \begin{pmatrix} a+b & a+b \\ a & b \end{pmatrix}$, i.e., $a = a + b$, i.e., $b = 0$. Therefore, A must be of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Since A is non-singular, we must have $a \neq 0$.

Conversely, note that for any $P \in G$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} P = aIP = aP = Pa = PaI = P \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, i.e., every matrix of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ commutes with every element of G.

(d) *A matrix $A \in G$ is said to be similar to a matrix $B \in G$ if $B = PAP^{-1}$ for some $P \in G$. Prove that similarity is an equivalence relation on G.* **(5)**

Solution [Reflexive] $A = IAI^{-1}$.
[Symmetric] If $B = PAP^{-1}$, $A = QBQ^{-1}$, where $Q = P^{-1}$.
[Transitive] If $B = PAP^{-1}$ and $C = QBQ^{-1}$, we have $C = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1}$.

(e) *Prove or disprove: Similarity is a congruence relation on G.* **(5)**

Solution [False] I prove the falsity of the assertion by contradiction. Suppose that similarity is a congruence relation on G. But then the equivalence classes under similarity are cosets of the normal subgroup $[I]$. If $A \in Z(G)$, $[A] = \{A\}$, i.e., the only matrix similar to A is A itself. In particular, $[I] = \{I\}$. On the other hand, if $A \notin Z(G)$, there exists at least one P for which $AP \neq PA$, i.e., $PAP^{-1} \neq A$, i.e., $[A]$ contains more than one element (A itself and PAP^{-1} as chosen above). This contradicts the fact that each coset of a subgroup has the same size as the subgroup.

(f) *For any fixed $P \in G$, define the map $f_P : G \to G$ as $f_P(A) = PAP^{-1}$. Prove that f_P is a group isomorphism.* **(5)**

Solution $f_P(AB) = P(AB)P^{-1} = PAIBP^{-1} = PA(P^{-1}P)BP^{-1} = (PAP^{-1})(PBP^{-1}) = f_P(A)f_P(B)$, i.e., f_P is a group homomorphism. Now suppose $f_P(A) = f_P(B)$, i.e., $PAP^{-1} = PBP^{-1}$, i.e., $P^{-1}(PAP^{-1})P = P^{-1}(PBP^{-1})P$, i.e., $A = B$. Thus f_P is injective. Finally, for every $B \in G$, we have $f(P^{-1}BP) = P(P^{-1}BP)P^{-1} = B$, i.e., f_P is surjective too.

(g) *Prove that f_P is the identity map on G if and only if $P \in Z(G)$.* **(5)**

Solution If $P \in Z(G)$, $f_P(A) = PAP^{-1} = APP^{-1} = A$ for all $A \in G$. Conversely, if $P \notin Z(G)$, $PA \neq AP$ for at least one $A \in G$. But then $f_P(A) = PAP^{-1} \neq A$.