CS21201 Discrete Structures, Autumn 2021–2022

Second Test

Date: Oct 05, 2021 | Time: 10:15am–11:30am | Maximum marks: 40

---

1. Prove that the following C function terminates for all non-negative integer inputs a,b,c. Here, the divisions by 2 are to be considered as divisions of `int` variables. **(10)**

```
void wow ( int a, int b, int c )
{
   int r, s, t;

   while (1) {
      if ((a == b) || (b == c) || (c == a)) break;
      r = (a + b) / 2; s = (b + c) / 2; t = (c + a) / 2;
      a = r; b = s; c = t;
   }
}
```

Solution The loop in the function maintains the following two invariance properties.

(1) a,b,c always remain non-negative.
(2) $\max(a,b,c)$ decreases strictly from one iteration to the next.

The first invariance is obvious. In order to prove the second invariance, consider the situation $a > b > c$ (the other situations can be handled analogously). In this case, $\max(a,b,c) = a$. After the loop body is executed once, the maximum becomes $\lfloor (a+b)/2 \rfloor \leqslant \lfloor (a+(a-1))/2 \rfloor = \lfloor a - \frac{1}{2} \rfloor = a - 1 < a$.

Since $\max(a,b,c)$ is a non-negative integer by the first invariance, the second invariance implies that the loop cannot repeat forever.

2. 65 distinct integers are chosen in the range $1,2,3,\ldots,2021$. Prove that there must exist four of the chosen integers (call them a,b,c,d) such that $a-b+c-d$ is a multiple of 2021. **(10)**

Solution The total count of 2-subsets of the 65 chosen integers is $\binom{65}{2} = 2080 > 2021$. So we can find two distinct subsets $S = \{a,c\}$ and $T = \{b,d\}$ of the chosen integers such that $a+c \equiv b+d \pmod{2021}$, that is, $a-b+c-d \equiv 0 \pmod{2021}$. We need to show that $S \cap T = \emptyset$. Suppose not. Since S and T are distinct, we must have $|S \cap T| = 1$. Say, $a = b$ (but $c \neq d$). The condition $a+c \equiv b+d \pmod{2021}$ implies that $c \equiv d \pmod{2021}$. But c and d are chosen in the range $[1,2021]$, so they must be equal, a contradiction.

3. Let ρ and σ be two binary relations over the set $\mathscr{A}$. A *composite relation* $\rho \circ \sigma$ over $\mathscr{A}$ is defined as

$$\rho \circ \sigma = \big\{ (p,r) \mid \text{ there exists some } q \in \mathscr{A} \text{ such that } (p,q) \in \rho \text{ and } (q,r) \in \sigma \big\}.$$

Prove the following assertions with precise formal justifications.

(a) If ρ and σ are equivalence relations, then $\rho \circ \sigma$ is an equivalence relation if and only if $\rho \circ \sigma = \sigma \circ \rho$. **(6)**

Solution [$\Rightarrow$] Suppose that $(x,y) \in \rho \circ \sigma$ $(x,y \in \mathscr{A})$. Since $\rho \circ \sigma$ is an equivalence relation, we also have $(y,x) \in \rho \circ \sigma$ (symmetric property). This means that for some $\alpha \in \mathscr{A}$, we have $(y,\alpha) \in \rho$ and $(\alpha,x) \in \sigma$. Since ρ and σ are both equivalence relations, we further get $(\alpha,y) \in \rho$ and $(x,\alpha) \in \sigma$ (symmetric property) This means that $(x,y) \in \sigma \circ \rho$ (by definition). Therefore $\rho \circ \sigma \subseteq \sigma \circ \rho$. Similar arguments (in opposite direction) can be given to prove $\sigma \circ \rho \subseteq \rho \circ \sigma$, thereby establishing $\rho \circ \sigma = \sigma \circ \rho$.

[$\Leftarrow$] Since ρ and σ are both equivalence relations, $(x,x) \in \rho$ as well as $(x,x) \in \sigma$ (for all $x \in \mathscr{A}$). By the definition of composite relations, we immediately have $(x,x) \in \rho \circ \sigma$, proving that $\rho \circ \sigma$ is *reflexive*.

If $(x,y) \in \rho \circ \sigma$ $(x,y \in \mathscr{A})$, then for some $\alpha \in \mathscr{A}$, we have $(x,\alpha) \in \rho$ and $(\alpha,y) \in \sigma$. Since ρ and σ are both equivalence relations, we have $(\alpha,x) \in \rho$ and $(y,\alpha) \in \sigma$ (symmetric property). This means that $(y,x) \in \sigma \circ \rho$ (by definition). Finally, $\rho \circ \sigma = \sigma \circ \rho$ implies $(y,x) \in \rho \circ \sigma$. This proves that $\rho \circ \sigma$ is *symmetric*.

Let $x,y,z \in \mathscr{A}$. Suppose that $(x,y) \in \rho \circ \sigma$ and $(y,z) \in \rho \circ \sigma$. Since $(x,y) \in \rho \circ \sigma$, there exists $\alpha \in \mathscr{A}$ such that $(x,\alpha) \in \rho$ and $(\alpha,y) \in \sigma$. Since $(y,z) \in \rho \circ \sigma$, there exists $\beta \in \mathscr{A}$ such that $(y,\beta) \in \rho$ and $(\beta,z) \in \sigma$. But then, since $(\alpha, y) \in \sigma$ and $(y, \beta) \in \rho$, we have $(\alpha, \beta) \in \sigma \circ \rho$ (by definition). It is given that $\sigma \circ \rho = \rho \circ \sigma$, so $(\alpha, \beta) \in \rho \circ \sigma$, that is, there exist $\delta \in \mathscr{A}$, such that $(\alpha, \delta) \in \rho$, and $(\delta, \beta) \in \sigma$. Since ρ is transitive, and (x, α) and (α, δ) are in ρ, we have $(x, \delta) \in \rho$. Moreover, since σ is transitive, and (δ, β) and (β, z) are in σ, we have $(\delta, z) \in \sigma$. By definition, we then have $(x, z) \in \rho \circ \sigma$, that is, $\rho \circ \sigma$ is *transitive*.

(b) The *inverse* of a relation τ over $\mathscr{A}$ is defined as $\tau^{-1} = \{(q, p) \mid (p, q) \in \tau\}$ $(p, q \in \mathscr{A})$. Prove that $(\rho \circ \sigma)^{-1} = (\sigma^{-1} \circ \rho^{-1})$. **(4)**

Solution Let $(y, x) \in (\rho \circ \sigma)^{-1}$ for $x, y \in \mathscr{A}$. By definition, $(x, y) \in (\rho \circ \sigma)$, that is, for some $\alpha \in \mathscr{A}$, we have $(x, \alpha) \in \rho$ and $(\alpha, y) \in \sigma$. This also implies that $(\alpha, x) \in \rho^{-1}$ and $(y, \alpha) \in \sigma^{-1}$. Therefore $(y, x) \in \sigma^{-1} \circ \rho^{-1}$, concluding that $(\rho \circ \sigma)^{-1} \subseteq (\sigma^{-1} \circ \rho^{-1})$.

On the other hand, let $(y, x) \in \sigma^{-1} \circ \rho^{-1}$ for $x, y \in \mathscr{A}$. Then, for some $\alpha \in \mathscr{A}$, we have $(y, \alpha) \in \sigma^{-1}$ and $(\alpha, x) \in \rho^{-1}$ (by definition). This also implies that $(\alpha, y) \in \sigma$ and $(x, \alpha) \in \rho$. Since $(x, y) \in \rho \circ \sigma$, we have $(y, x) \in (\rho \circ \sigma)^{-1}$, concluding that $(\sigma^{-1} \circ \rho^{-1}) \subseteq (\rho \circ \sigma)^{-1}$.

Together, we have proved that $(\rho \circ \sigma)^{-1} = (\sigma^{-1} \circ \rho^{-1})$.

4. Let $\mathscr{P}(S)$ denote the power set of S. For a function $f : X \to Y$, define two functions $g : \mathscr{P}(A) \to \mathscr{P}(B)$ and $h : \mathscr{P}(B) \to \mathscr{P}(A)$ as

$$
\begin{aligned}
g(A) &= \{b \mid \exists\, a \in A, f(a) = b\}, \text{ and} \\
h(B) &= \{a \mid f(a) \in B\}
\end{aligned}
$$

for all $A \subseteq X$ and $B \subseteq Y$. Prove the following assertions with precise formal justifications.

(a) f is injective if and only if $h(g(A)) = A$ for all $A \subseteq X$. **(5)**

Solution [If] To show that if $h(g(A)) = A$ for all $A \subseteq X$, then f is injective.

Let $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Then, $x_1 \in h(g(\{x_1\}))$. But $h(g(\{x_1\})) = h(\{f(x_1)\}) = h(\{f(x_2)\}) = h(g(\{x_2\})) = \{x_2\}$ (by taking $A = \{x_2\}$ in the hypothesis). It follows that $x_1 \in \{x_2\}$, that is, $x_1 = x_2$.

[Only if] To show that if f is injective, then $h(g(A)) = A$ for all $A \subseteq X$.

$[A \subseteq h(g(A))]$ $a \in A \Rightarrow f(a) \in g(A) \Rightarrow a \in h(g(A))$.

$[h(g(A)) \subseteq A]$ $a \in h(g(A)) \Rightarrow f(a) \in g(A) \Rightarrow \exists x \in A, f(x) = f(a) \Rightarrow x = a$ (since f is injective) $\Rightarrow a \in A$.

(b) f is surjective if and only if $g(h(B)) = B$ for all $B \subseteq Y$. **(5)**

Solution [If] To show that if $g(h(B)) = B$ for all $B \subseteq Y$, then f is surjective.

Take any $b \in Y$, and $B = \{b\}$. By hypothesis, $g(h(B)) = B = \{b\}$. This implies that there exists $a \in h(B)$ such that $f(a) = b$. Since $h(B) \subseteq X$, it follows that f is surjective.

[Only if] To show that if f is surjective, then $g(h(B)) = B$ for all $B \subseteq Y$.

$[g(h(B)) \subseteq B]$ Let $b \in g(h(B))$. By the definition of g, there exists $a \in h(B)$ such that $f(a) = b$. But then by the definition of h, we have $f(a) \in B$, that is, $b \in B$.

$[B \subseteq g(h(B))]$ Let $b \in B$. Since f is surjective, we have $b = f(a)$ for some $a \in X$. By the definition of h, we then have $a \in h(B)$. By the definition of g, we have $f(a) \in g(h(B))$, that is, $b \in g(h(B))$.