Solutions for Final Test 2IT50 on Thu 05 Nov 2015

Tom Verhoeff

27 October 2015, 06 November 2015

Note

- These are not the only possible correct answers.

---

1. Give an example of a relation R on a finite set such that $R^* \neq (R\,;R)^*$.

   Example Consider the set $U = \{0, 1\}$, and define R on U by $x\ R\ y \Leftrightarrow x < y$.

   Observe that

   - $xR^*y \Leftrightarrow x \leq y$
   - $R\,;R = \emptyset$, and hence $(R\,;R)^* = I_U$.

   Thus, $0\ R^*\ 1$, but not $0\ (R\,;R)^*\ 1$. Hence, we have $R^* \neq (R\,;R)^*$.

   □

   Notes

   - The given R is in fact transitive.
   - If R has to be transitive, then we will have $(R\,;R)^* \subseteq R^*$.

2. Let R be a transitive relation on a set U. Prove that $R^{2n} \subseteq R^{n+1}$ for all $n \geq 1$.

Proof We prove this by induction on n. Observe that $R^2 = R\,;R \subseteq R$, because R is transitive.

Base: Let $n = 1$. We calculate: $R^{2n} = R^2 = R^{n+1}$.

Step: Let $n \geq 1$, and assume as induction hypothesis that $R^{2n} \subseteq R^{n+1}$. To prove: $R^{2(n+1)} \subseteq R^{n+1+1}$.

We calculate:

$$
\begin{array}{ll}
 & R^{2(n+1)} \\
= & \quad \{ \text{ algebra, prop. rel. exp. } \} \\
 & R^{2n}\,;R^2 \\
\subseteq & \quad \{ \text{ monotonicity of rel. composition, ind. hyp., given trans. of } R \text{ } \} \\
 & R^{n+1}\,;R \\
= & \quad \{ \text{ def. exp. } \} \\
 & R^{n+1+1}
\end{array}
$$

□

Notes

- If you prove separately (by induction) that relation exponentiation is monotonic, then the following direct proof is possible.

  Let $n \geq 1$. We calculate:

  $$
  \begin{array}{ll}
   & R^{2n} \\
  = & \quad \{ \text{ prop. rel. exp., using } n \geq 1 \text{ } \} \\
   & \left(R^2\right)^{n-1}\,;R^2 \\
  \subseteq & \quad \{ \text{ monotonicity of rel. exp., given trans. of } R \text{ } \} \\
   & R^{n-1}\,;R^2 \\
  = & \quad \{ \text{ prop. rel. exp., using } n \geq 1 \text{ } \} \\
   & R^{n+1}
  \end{array}
  $$

- More generally, we have that $m \geq n \geq 1$ implies $R^m \subseteq R^n$ for transitive endorelation R (by induction on $m - n$).

  In fact, this also holds for $m = n = 0$, but not for $m > n = 0$.

3. Let two non-empty sets A, B satisfy $A \cap B = \emptyset$. For a function $f : A \to B$. define undirected graph $G_f = (V, E)$ for which $V = A \cup B$ and

$$E \quad = \quad A \times A \cup \{(x, f(x))) \mid x \in A\}$$

Prove that G_f is connected if and only if f is surjective.

Proof We present a ping-pong proof.

- Assume that f is surjective; that is, for every $v \in A$ there exists a $u \in A$ with $f(u) = v$. To prove: G_f is connected.
  Let $x_1, x_2 \in A \cup B$. W.l.o.g.[1] (because of symmetry of the 'path between' relation), we distinguish three cases:
  (a) $x_1, x_2 \in A$
  Given is that (x_1, x_2) is an edge of G_f. Hence, there is a path (of length 1) between x_1 and x_2.
  (b) $x_1 \in A \wedge x_2 \in B$
  Since f is surjective and $x_2 \in B$, take $u \in A$ such that $f(u) = x_2$. By definition of G_f, we have edges (x_1, u) and (u, x_2) in G_f, establishing a path between x_1 and x_2.
  (c) $x_1, x_2 \in B$
  Because A is non-empty, take $u \in A$. From the preceding case we have paths between u and x_1, and between u and x_2. This establishes (by concatenation) a path between x_1 and x_2.
- Assume that f is not surjective. To prove: G_f is not connected.
  Take $v \in B$ such that there is no $u \in A$ with $f(u) = v$. By definition of G_f, the degree of v is zero.
  Since A is non-empty, take $u \in A$. Since $f(u) \neq v$, u and v belong to distinct connected components.

□

Notes

- The non-emptiness of both A and B is used explicitly.

[1] Without loss of generality

4. Consider the poset $(\mathbb{N}, |)$ and let $n > 0$. Define

$$A \quad = \quad \{x \in \mathbb{N} \mid n \leq x \leq 2n\}$$

Determine all minimal elements of A and prove that there are exactly n of them.

Solution Observe that for $n > 0$, we have $n \neq 2n$. Therefore, $\#A = 2n + 1 - n = n + 1$. Since, $n \mid 2n$, we have that $2n$ is not minimal in A. Thus, it is necessary that all elements in A less than $2n$ are minimal, in order to have exactly n minimal elements.

For this, it suffices that $k \mid \ell$ for $n \leq k < \ell \leq 2n$ holds if and only if $k = n \wedge \ell = 2n$. Since, $n \leq k < \ell \leq 2n$ and $k \neq n \vee \ell \neq 2n$ implies $2k > \ell$, we have $\ell = k + r$ with $0 < r < k$. Thus, in that case, ℓ is not divisble by k.

□

Notes

- Similarly, n is not maximal, and the n maximal elements are $A \setminus \{n\}$.

5. Let $(G, *, I)$ be a group and let $a, b \in G$ such that $a * b$ has order 2. Prove that $b * a$ has order 2.

Proof Let $a * b$ have order 2 in group $(G, *, I)$. By definition of order, we thus have $a * b * a * b = I$ and $a * b \neq I$. From the latter, we infer that b is not the inverse of a. Hence, also $b * a \neq I$ (for otherwise b would be the inverse of a).

Furthermore, we calculate

$$\begin{array}{ll} & b * a * b * a \\ = & \quad \{\ b * b^{-1} = I\ \} \\ & b * a * b * a * b * b^{-1} \\ = & \quad \{\ \text{using } a * b * a * b = I\ \} \\ & b * I * b^{-1} \\ = & \quad \{\ \text{group axioms}\ \} \\ & I \end{array}$$

From $b * a * b * a = I$ and $b * a \neq I$ we conclude that $b * a$ has order 2.

□

Notes

- The group is not assumed to be commutative. Thus, we cannot use $a * b = b * a$.

6. Find a closed expression for a_n defined by $a_0 = a_1 = 1$, and

$$a_n = 2a_{n-1} + 15a_{n-2}$$

for $n \geq 2$.

Solution The characteristic equation is $x^2 = 2x + 15$. We have

$$x^2 - 2x - 15 = (x-5)(x+3).$$

Hence, the solution has the form $a_n = A5^n + B(-3)^n$. We obtain A and B from the initial conditions:

$$\begin{aligned} A5^0 + B(-3)^0 &= 1 \\ A5^1 + B(-3)^1 &= 1 \end{aligned}$$

This equivales

$$\begin{aligned} A + B &= 1 \\ 5A - 3B &= 1 \end{aligned}$$

which in turn equivales

$$\begin{aligned} A + B &= 1 \\ 8A &= 4 \end{aligned}$$

This finally yields

$$\begin{aligned} B &= 1/2 \\ A &= 1/2 \end{aligned}$$

Thus, a closed expression is $a_n = (5^n + (-3)^n)/2$ for $n \geq 2$.
□

7. Apply the extended Euclidean algorithm to find an integer number x such that

$$(17x \bmod 83) \quad = \quad 1.$$

Solution If we find x, y satisfying $17x + 83y = 1$, then x also solves the given problem. Apply the fast Euclidean algorithm:

$B = (B \operatorname{div} A) \cdot$	$A + (B \bmod A)$
$\mathbf{83} =$ $4 \cdot \mathbf{17} +$	15
$\mathbf{17} =$ $1 \cdot \mathbf{15} +$	2
$\mathbf{15} =$ $7 \cdot \mathbf{2} +$	1
$\mathbf{2} =$ $2 \cdot \mathbf{1} +$	0
$\mathbf{1} =$ $1 \cdot \mathbf{0} +$	0

Now we calculate x, y with $Ax + By = 1$, where A, B come from the table above:

A	B	x	y
0	1	0	1
1	2	$1 - 0 \cdot 2 = 1$	0
7	5	$0 - 1 \cdot 7 = -7$	1
15	17	$1 - (-7) \cdot 1 = 8$	-7
17	83	$-7 - 8 \cdot 4 = -39$	8

Thus, we find $x = -39$, which reduces to $x = 44$ module 83.

□

Notes

- For comparison, we also present an ad hoc solution that does *not* use the Euclidean algorithm.

  Observe that $5 \cdot 17 = 85 = 83 + 2$. Hence, $5 \cdot k \cdot 17 \equiv 2k \pmod{83}$. Solve for $2k = 83 + 1$, yielding $k = 42$. Thus, $x = 5 \cdot 42 = 210$ is a solution. Reducing this modulo 83, yields the smaller solution $x = 44$.

8. Let $n = 2k + 1 > 10$ and $(2^k \bmod n) = 3$. Prove that n is not a prime number.

   (Hint: note that $2^{n-1} = \left(2^k\right)^2$)

   Proof By contradiction. Assume that $n = 2k + 1 > 10$ is prime. Hence, $\neg(n \mid 2)$. Therefore, by Fermat's little theorem we have $2^{n-1} \equiv 1 \pmod{n}$. We calculate:

   $$\begin{array}{ll} & \mathsf{true} \\ \Leftrightarrow & \{ \text{ given } \} \\ & 2^k \equiv 3 \pmod{n} \\ \Rightarrow & \{ \text{ squaring both sides } \} \\ & 2^{2k} \equiv 9 \pmod{n} \\ \Leftrightarrow & \{ \ n = 2k + 1 \ \} \\ & 2^{n-1} \equiv 9 \pmod{n} \end{array}$$

   Since $n > 10$ is given, this contradicts the result of Fermat's little theorem above.

   Conclusion, n is not a prime number.

   □

   Notes

   - The statement also holds for $n = 2k + 1 > 2$, since $1 \not\equiv 9 \pmod{n}$ for prime $n > 2$.