Problem Set 5 Solutions

2:35pm in lecture, Thursday, October 12, 2000

Be sure to indicate your TA's name clearly on the solutions your turn in.

Self-study: Simple algorithms and pseudocode Read: Rosen Section 2.1 Self-study problems (not to be handed in): 1, 3, 5, 7, 9, 11, 19

Reading: Lecture notes; Rosen 2.1, 3.5 (skim)

Policy on collaboration If you collaborated with someone on the problem sets, you should mention their names on top of the problem set. If you did not collaborate with anyone, you should explicitly say so. As a reminder, the write-up of your solutions should be entirely your own.

Problem 1 In ancient times, the downtown section of Verona was laid out in a 1000 by 1000 meter square. Romeo lived at grid point $(0, 0)$ of the square, and Juliet lived at grid point $(0, 1000)$. Of course, Romeo and Juliet wanted to meet, at *exactly* the same point in the square. However, both were restricted by their rather strange families to move according to very particular rules: Romeo could only move 3 units, parallel to either the x axis or y axis or at a 45 degree angle to both axes. Juliet could only move 3 units, and only parallel to either the x axis or y axis.

(a) Model Romeo and Juliet and their possible moves as a (single) state machine. That is, define the states Q, the start state Q_0, and the transitions δ.

Solution:

$Q = \{(R_x, R_y, J_x, J_y) | R_x, R_y, J_x, J_y \in \{0, \dots, 1000\}\}$, where (R_x, R_y) and (J_x, J_y) are the positions of Romeo and Juliet, respectively.

$Q_0 = \{(0, 0, 0, 1000)\}$

$\delta : (R_x, R_y, J_x, J_y) \to (R_x + 3a, R_y + 3b, J_x + 3c, J_y + 3d))$, where
$(a, b, c, d) \in \{(1, 0, 0, 0), (-1, 0, 0, 0), (0, 1, 0, 0), (0, -1, 0, 0), (1, 1, 0, 0), (1, -1, 0, 0),$
$(-1, 1, 0, 0), (-1, -1, 0, 0), (0, 0, 1, 0), (0, 0, -1, 0), (0, 0, 0, 1), (0, 0, 0, -1)\}$

(b) Can Romeo and Juliet meet by some sequence of moves? If yes, then give such a sequence of moves. If no, then prove formally (using an invariant) that no sequence of moves can yield a meeting.

Solution: We show that for all reachable states $q = (R_x, R_y, J_x, J_y)$,

$$R_x + R_y - J_x - J_y \equiv 2 \pmod 3.$$

For notational convenience, let $r(q) = R_x + R_y - J_x - J_y$. For the only possible initial state q_0, $r(q_0) = -1000$, so $r(q_0) \equiv 2 \pmod 3$. For any transition from state q to state q', we note that $r(q') - r(q)$ is always a multiple of 3. Hence $r(q') \equiv 2 \pmod 3$ implies $r(q) \equiv 2 \pmod 3$.

Suppose, for a contradiction, that Romeo and Juliet can meet in some state q. That would imply that $r(q) = 0$. However, we just showed that $r(q)$ can never be 0, which yields a contradiction.

Problem 2 In the late 1960s, the military junta that ousted the government of the small republic of Miranda outlawed multiplication and division by any number other than 3. When democracy was reinstated 30 years later, people were interested in rediscovering the lost art of multiplication. A young inventor came up with the following algorithm to multiply any two natural numbers x and y using only multiplication and division by 3:

procedure *multiply*(x, y: natural numbers)
$r := x;$
$s := y;$
$a := 0;$
do until $s = 0$
    if $s \equiv 0 \pmod 3$ **then**
        $r := 3r;$
        $s := s/3;$
    else if $s \equiv 1 \pmod 3$ **then**
        $a := a + r;$
        $r := 3r;$
        $s := (s - 1)/3;$
    else
        $a := a + 2r;$
        $r := 3r;$
        $s := (s - 2)/3;$
return a;

(a) Model the algorithm as a state machine (Q, Q_0, δ).

Solution:

$$Q = \{(r, s, a, x, y) | r, s, a, x, y \in \mathbb{N}\}$$

$$Q_0 = \{(x, y, 0, x, y)\}$$

$\delta : (r, s, a, x, y) \to (3r, s', a', x, y)$, where
If $s \equiv 0 \pmod 3$: $s' = s/3$, and $a' = a$
If $s \equiv 1 \pmod 3$: $s' = (s-1)/3$, and $a' = a + r$
If $s \equiv 2 \pmod 3$: $s' = (s-2)/3$, and $a' = a + 2r$

(b) List the sequence of steps that appears in the execution of the algorithm for inputs $x = 5$ and $y = 10$.

Solution: $(5, 10, 0, 5, 10) \to (15, 3, 5, 5, 10) \to (45, 1, 5, 5, 10) \to (135, 0, 50, 5, 10)$

(c) Prove that the algorithm gives the correct answer if it terminates, that is, that $s = 0$ implies $a = xy$. (*Hint*: Use induction on the number of steps in the execution. You will have to strengthen the inductive hypothesis.)

Solution: We prove the following invariant.

$P(r, s, a, x, y) =$ "$xy = rs + a$".

Base case: For any initial state we have $P(x, y, 0, x, y)$ which is true.

Inductive step: Consider a transition from (r, s, a, x, y) to (r', s', a', x', y'). We need to prove that $P(r, s, a, x, y) \to P(r', s', a', x', y')$. We consider three cases:

If $s \equiv 0 \pmod 3$, then $r's' + a' = (3r)\frac{s}{3} + a = rs + a = xy = x'y'$.

If $s \equiv 1 \pmod 3$, then $r's' + a' = (3r)\frac{s-1}{3} + (a + r) = rs + a = xy = x'y'$.

If $s \equiv 2 \pmod 3$, then $r's' + a' = (3r)\frac{s-2}{3} + (a + 2r) = rs + a = xy = x'y'$.

In all three cases, the last equality was derived by applying the inductive hypothesis, and in all cases $P(r', s', a', x', y')$ holds. When $s = 0$, the we get that $a = xy$. We also know that the algorithm terminates when $s = 0$. It follows, therefore, that if the algorithm terminates, then the correct answer is produced.

(d) Prove that the algorithm terminates.

Solution:

We first notice that $s \geq 0$ for any reachable execution state. We prove that this is an invariant by showing it is true for the base case, $y \geq 0$, and furthermore, no transition exists from a state with $s \geq 0$ to $s < 0$ in all cases.

Now consider the value of s during any valid execution. Since $s \geq 0$, as shown above, no transition increases s. Furthermore, for $s > 0$, all transitions decrease s by at least 1. Thus for any values of $x, y \in \mathbb{N}$, s decreases to 0 in a finite number of steps, and thus the program terminates in a finite number of steps.

Problem 3 Shah Shahryar's wife betrays him with a slave and he vows revenge on all women. Each night, he will marry a new bride and the next morning have her beheaded. One night comes beautiful Sheherezade and presents the Shah with a game:

You have three numbers: 1, 1 and 2. At each time, you are allowed to replace any two numbers x, y with $\frac{x+y}{\sqrt{2}}$, $\frac{x-y}{\sqrt{2}}$, but you must not change your third number. You will win only if, using this rule, you can obtain the numbers a, b and c.

(a) Model Sheherezade's game as a state machine. (*Note*: The representation is a little tricky because the numbers are not ordered.)

Solution:

$Q = \mathbb{R}^3$

$Q_0 = \{(1, 1, 2)\}$

$\delta : (x, y, z) \to (\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}, z)$ or $(x, y, z) \to (x', y', z')$, where (x', y', z') is a permutation of (x, y, z).

For each of the following choices of a, b and c, say whether or not the Shah can win the game. If yes, show a sequence of winning steps. If no, provide a proof using an invariant.

(b) $(a, b, c) = (\frac{3\sqrt{2}}{2}, \frac{\sqrt{2}+1}{2}, \frac{\sqrt{2}-1}{2})$

Solution: Yes. $(1, 1, 2) \to (2, 1, 1) \to (\frac{3\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 1) \to (\frac{3\sqrt{2}}{2}, \frac{\sqrt{2}+1}{2}, \frac{\sqrt{2}-1}{2})$.

(c) $(a, b, c) = (\frac{\sqrt{3}-1}{2}, \frac{\sqrt{3}+1}{2}, 7)$

Solution: No. The predicate

$$P(x, y, z) : x, y, z \in \{p + q\sqrt{2} | p, q \in \mathbb{Q}\}$$

is an invariant for the state machine. For the base case and the permutation transitions, the claim is evident. For the transitions of type $(x, y, z) \to (x', y', z')$ where $(x', y', z') = (\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}, z)$, let $x = p+q\sqrt{2}, y = r+s\sqrt{2}, z = u+v\sqrt{2}$. Then $x' = 2(q+s)+(p+r)\sqrt{2}, y' = 2(q-s)+(p-r)\sqrt{2}, z' = z$, so $P(x, y, z) \to P(x', y', z')$. Since $P(\frac{\sqrt{3}-1}{2}, \frac{\sqrt{3}+1}{2}, 7)$ is false, this state is not reachable.

(d) $(a, b, c) = (1, 2, 2)$

Solution: No. The predicate

$$P(x, y, z) : x^2 + y^2 + z^2 = 6$$

is an invariant for the state machine. For the base case and the permutation transitions, the claim is evident again. For the transitions of type $(x, y, z) \to (\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}, z)$, we have $x^2 + y^2 + z^2 = (\frac{x+y}{\sqrt{2}})^2 + (\frac{x-y}{\sqrt{2}})^2 + z^2$. Since $P(1, 2, 2)$ does not hold, the state $(1, 2, 2)$ is not reachable.

Problem 4 Consider the matching problem from lecture.

(a) For a particular value of n, give an example of a stable match between n boys and n girls where no person gets their first choice.

Solution:

Let $n = 3$. Call the boys $1, 2, 3$ and the girls a, b, c. Consider the following preference list:

choice	1st	2nd	3rd	choice	1st	2nd	3rd
1	a	b	c	a	2	3	1
2	b	c	a	b	3	1	2
3	c	a	b	c	1	2	3

The matching $(1, b), (2, c), (3, a)$ is stable even though no person gets their first choice.

(b) Can a stable match where no person gets their first choice be produced by the matching algorithm described in class? If yes, state an example and show why the example works. If not, prove using an invariant.

Solution:

Yes. For $n = 4$, for boys $1, 2, 3, 4$ and the girls a, b, c, d, the following preference list yields such a match (x choices don't matter):

choice	1st	2nd	3rd	4th	choice	1st	2nd	3rd	4th
1	a	c	x	x	a	3	2	1	4
2	b	a	x	x	b	1	4	3	2
3	b	d	x	x	c	x	1	x	x
4	a	b	x	x	d	x	3	x	x

The matching algorithm executes as follows:

Round 1 a picks 1. b picks 3. $2, 4$ are dropped.

Round 2 a picks 2. b picks 4. $1, 3$ are dropped.

Round 3 c picks 1. d picks 3.

Problem 5 Consider an instance of the matching problem with n boys and n girls. Call a person *unlucky* if he or she is matched up with one of his or her $\lfloor \frac{n}{2} \rfloor$ last choices. In this problem, we will prove the following:

Theorem The matching algorithm from class never produces a matching in which every person is unlucky.

Fix an execution of the matching algorithm. Define the variables $B_i, G_i, i \in \{1, 2, \ldots, n\}$ as follows:

$B_i = j$ if the i-th boy is currently courting the j-th girl on his list

G_i is the number of boys that the i-th girl has rejected.

(a) Show that $\sum_{i=1}^{n} B_i - \sum_{i=1}^{n} G_i$ is preserved at each step of the matching algorithm.

Solution: Let $S = \sum_{i=1}^{n} B_i - \sum_{i=1}^{n} G_i$. Suppose that at step t, boy b_i proposes to girl g_j. There are three possible outcomes:

If g_j has not had any previous proposals, she must accept. In this case, none of the B_is and none of the G_js change, so S is preserved.

If g_j rejects, then G_j increases by 1, B_i increases by 1, and the other Bs and Gs remain the same. S is preserved again.

If g_j accepts b_i because she likes him better than her current mate $b_{i'}$, then G_j increases by 1, $B_{i'}$ increases by 1, and the other Bs and Gs remain the same. S is preserved in this case as well.

(b) Formulate an invariant that you can use to prove the theorem, and show that your invariant is correct.

Solution: Let $P : S = n$. In the initial state, this is true because everyone is courting the first girl on their list. From part (a) it follows that all transitions preserve the truth value of P. Therefore P is an invariant.

(c) Use your invariant to prove the theorem.

Solution: We prove the statement by contradiction. Consider a match M in which every person is unlucky. Then:

For every $i \in \{1, \ldots, n\}$, $B_i \geq \lceil \frac{n}{2} \rceil + 1$, and

For every $i \in \{1, \ldots, n\}$, $G_i \leq \lfloor \frac{n}{2} \rfloor - 1$.

It follows that $\sum_{i=1}^{n} B_i - \sum_{i=1}^{n} G_i \geq 2n$. This violates the invariant P.