# Tutorial 5 Problems

## Problem 1 Computing GCDs

Consider the following procedure for computing the greatest common divisor (gcd) of a non-empty list of positive integers $(x_1, x_2, \ldots, x_n)$.

If all entries in the list are equal, then the procedure outputs the common value and terminates. Otherwise, the procedure selects two entries with different values and replaces the larger one by the difference.

**(a)** Model this procedure as a state machine.

**Solution:**

The set of states $Q$ consists of all lists of $n$ positive integers.

The set of start states $Q_0$ consists of the single state $(x_1, x_2, \ldots, x_n)$.

The set $\delta$ contains all transitions of the form $(y_1, y_2, \ldots, y_i, \ldots, y_j, \ldots, y_n) \to (y_1, y_2, \ldots, y_i - y_j, \ldots, y_j, \ldots, y_n)$, for $1 \leq i, j \leq n, i \neq j$ and $y_i > y_j$.

**(b)** Prove that the procedure terminates.

**Solution:**
We construct a non-negative, decreasing derived variable. This implies that the machine reaches at state with no outgoing transitions. All such states are terminating states of the procedure.

Define the derived variable $S$ to take on the value $y_1 + y_2 + \ldots + y_n$ in the state corresponding to the list $(y_1, y_2, \ldots, y_n)$. This derived variable is non-negative, since all $y_i$ are positive. The derived variable is decreased by each transition, since the list entry $y_i$ is decrease by $y_j$ (a positive quantity) and all other list entries are unchanged.

**(c)** Prove that the procedure computes the gcd of $x_1, x_2, \ldots, x_n$.

**Solution:**
We prove that the predicate

$$\gcd(y_1, y_2, \ldots, y_n) = \gcd(x_1, x_2, \ldots, x_n)$$

is an invariant for the state machine. The predicate holds trivially in the start state. Now given that the invariant holds prior to a transition, we have

$$\begin{aligned}\gcd(y_1, \ldots, y_i - y_j, \ldots, y_j, \ldots, y_n) &= \gcd(y_1, y_2, \ldots, y_i, \ldots, y_j, \ldots, y_n) \\ &= \gcd(x_1, x_2, \ldots, x_n)\end{aligned}$$

To justify the first step, let $p$ be a divisor of $\gcd(y_1, \ldots, y_i - y_j, \ldots, y_j, \ldots, y_n)$. Since $p|y_j$ and $p|y_i - y_j$, it follows that $p|y_i$. Therefore $p|\gcd(y_1, y_2, \ldots, y_i, \ldots, y_j, \ldots, y_n)$. Conversely, suppose $q$ is a divisor of $\gcd(y_1, y_2, \ldots, y_i, \ldots, y_j, \ldots, y_n)$. By an analogous argument, it follows that $q|\gcd(y_1, \ldots, y_i - y_j, \ldots, y_j, \ldots, y_n)$. Since both quantities have the same divisors, they must be equal.

Since the predicate holds in the start state and it is preserved by all transitions, it is an invariant of the state machine. By the invariant theorem, the invariant holds at termination.

**Problem 2 Strange motions**

You are standing in the bottom left square of a $2n \times 12$ grid. It is 5 minutes before the hour and you are in a rush to get to your 6.042 tutorial room which is located in the bottom right square of the grid. Unfortunately, you are only allowed to move to another square if the distance between the centers of the squares is precisely $\sqrt{r}$. Can you make it to tutorial if:

**(a)** $r$ is divisible by 2?

**Solution:**
Let's model this as a state machine $M$. The set of states $Q$ consists of all pairs $(x, y)$, where $0 \le x < 2n$ and $0 \le y < 12$. The only start state is $(0, 0)$. The transitions are $(x, y) \to (x+x', y+y')$ with $x'^2 + y'^2 = r$. The tutorial room is in state $(2n - 1, 0)$.

Let $r$ be even. We show that "$x + y$ is even" is an invariant on the states of $M$. It holds for the start state. Now consider a transition $(x, y) \to (x + x', y + y')$. For $x'^2 + y'^2$ to be even, $x'$ and $y'$ must have the same parity, so $x + x' + y + y'$ has the same parity as $x + y$. Therefore transitions preserve the parity of the sum.

Since $2n - 1$ is not even, $(2n - 1, 0)$ is not a reachable state.

**(b)** $r$ is divisible by 3 and $2n \not\equiv 1 \pmod 3$?

**Solution:**
Here we show that "$x$ and $y$ both divide 3" is an invariant of the state machine. It holds for the start state. Given a transition $(x, y) \to (x + x', y + y')$, with $x'^2 + y'^2 = 3k$, we want to show that $3|x'$ and $3|y'$. Note that if for any integer $n$, $n^2 \equiv 0$ or $1 \pmod 3$. If $3|x'^2 + y'^2$, it follows that $x'^2 \equiv y'^2 \equiv 0 \pmod 3$. Therefore $3|x'$ and $3|y'$. Hence $x + y \equiv x + x' + y + y' \pmod 3$, and the invariant is proved.

As $2n \not\equiv 1 \pmod 3$, the state $(2n - 1, 0)$ does not satisfy the invariant.

**(c)** $n = 20$ and $r = 73$?

**Solution:**
Yes, for example $(0, 0) \to (3, 8) \to (11, 5) \to (3, 2) \to (0, 10) \to (8, 7) \to (0, 4) \to (8, 1) \to (5, 9) \to (13, 6) \to (5, 3) \to (13, 0) \to (16, 8) \to (19, 0)$

**(d)** $r = 97$?

**Solution:**
No. First note that $97 = 4^2 + 9^2$ is the only representation of 97 as a sum of squares of natural numbers. Consequently, there are only 8 possible transitions: translations by $(\pm 4, \pm 9)$ and translations by $(\pm 9, \pm 4)$.

The trick of this problem is to realize that the state machine representation from part (a) is insufficient to prove anything useful in this case. We need to extend our specification of the state machine to keep track of the particular types of transitions that have been performed so far. We extend each state $q$ to a 10-tuple $(x, y, n_{(-4,-9)}, \ldots, n_{(9,4)})$, where $(x, y)$ is the position on the board, and $n_{(i,j)}$ is the number of translations by $(i, j)$.

Let

$$\begin{aligned} r &= n_{(4,9)} + n_{(-4,9)} - n_{(4,-9)} - n_{(-4,-9)} \\ s &= n_{(9,4)} + n_{(-9,4)} - n_{(9,-4)} - n_{(-9,-4)} \end{aligned}$$

Note that $y = 9r + 4s$. The following observations lead to the solution.

**Lemma 0.1.** *The predicate "$0 \le r \le 3$" is an invariant of the state machine.*

**Proof.** The statement is satisfied by the start state. For transitions, first note that $r \equiv y \pmod 4$. Now each transition either preserves $r$ or modifies $r$ by $\pm 1$. If $r = 3$, then $y \equiv 3 \pmod 4$ so no translations of type $(\pm 4, 9)$ can happen; hence $r$ cannot grow any further. Finally, $r \ge 0$ because the $y$-coordinate of each state is positive. ■

**Lemma 0.2.** *The predicate "If $y = 0$, then $x$ is even" is an invariant of the state machine.*

**Proof.** If $y = 0$, then $9r + 4s = 0$, so $r \equiv 0 \pmod 4$. By the previous lemma, $0 \le r \le 3$, from where $r = 0$. $s = 0$ follows from here. Now

$$\begin{aligned} x &= 4(n_{(4,9)} + n_{(4,-9)} - n_{(-4,9)} - n_{(-4,-9)}) + 9(n_{(9,4)} + n_{(9,-4)} - n_{(-9,4)} - n_{(-9,-4)}) \\ &= 4(n_{(4,9)} + n_{(4,-9)} - n_{(-4,9)} - n_{(-4,-9)}) + 9s + 2(n_{(9,-4)} - n_{(-9,4)}) \end{aligned}$$

since $s = 0$, this quantity is even. ■

The state $(2n - 1, 0)$ does not satisfy the predicate from the previous lemma. Therefore this state is not reachable.

## Problem 3 A Puzzle

Math Moose has been given a new puzzle: a $3 \times 3$ grid of squares, where each square contains one of the digits in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, each digit appearing exactly once in the puzzle. Each row can be rotated right or left and each column can be rotated up or down. The effects of such rotations are demonstrated in the following figure.

The first picture shows the initial configuration of the puzzle. The leftmost column is then rotated downward to give the middle picture. The 2 and 7 move down and the 5 rotates back up to the top. Then, the middle row is rotated leftward to produce the final picture. The 8 and 9 move left and the 2 rotates back around to the right.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 6 | | 5 | 3 | 6 | | 5 | 3 | 6 |
| 7 | 8 | 9 | → | 2 | 8 | 9 | → | 8 | 9 | 2 |
| 5 | 4 | 1 | | 7 | 4 | 1 | | 7 | 4 | 1 |

**Figure 1**: Examples of puzzle row and column rotations.

Since discovering the puzzle, Math Moose has spent hours trying to obtain the following configuration, starting of course from the initial configuration of Figure 1 and using legal row and column rotations.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Sad to say, Math Moose has failed miserably. He is beginning to suspect that the puzzle might be designed in a way that makes this configuration impossible, no matter what sequence of row and column rotations one attempts.

Given the initial configuration of the puzzle indicated above, namely 236 789 541, prove that Math Moose can never obtain the configuration 123 456 789.

**Solution:**
The idea is to keep track of the number of digit pairs that are out of order relative to the desired configuration 123 456 789. For example, in the initial configuration, 2 appears before 1; this pair of digits is out of order, because 1 appears before 2 in the desired configuration 123 456 789. We will refer to an out-of-order digit pair as an *inversion*. In the initial configuration, there are 17 inversions:

| | | | | |
|---|---|---|---|---|
| 21 | 31 | 65 | 64 | 61 |
| 75 | 74 | 71 | 85 | 84 |
| 81 | 95 | 94 | 91 | 54 |
| 51 | 41 | | | |

The key observation is that a rotation always changes the number of inversions by an even amount. Since the puzzle initially has an odd number of inversions, no sequence of rotations can reduce the number of inversions to 0, an even number. Consequently, there will always be at least one pair of digits out of order.

The main challenge is to prove that a rotation always changes the number of inversions by an even amount. We prove this claim in a sequence of lemmas.

**Lemma 0.3.** *Swapping an adjacent pair of digits changes the number of inversions by an odd amount.*

**Proof.** If the digits were initially in the same order as in 123 456 789, then the number of inversions is increased by 1, an odd number. Otherwise, the digits were initially in the wrong order, and the number of inversions is decreased by 1, also an odd number. ■

**Lemma 0.4.** *Swapping any pair of digits changes the number of inversions by an odd amount.*

**Proof.** We will show how to swap any pair of digits using an odd number of swaps of adjacent digits. Suppose that we are swapping digits $x$ and $y$, where $x$ is on the left, $y$ is on the right, and there are $k$ stray digits between the two. First, we swap $x$ with its right neighbor $k$ times. This leaves $x$ directly left of $y$ and leaves all the stray digits shifted one place to the left. Then we swap $x$ and $y$, putting $x$ into $y$'s original positions. Finally, we swap $y$ with its left neighbor $k$ times. This puts $y$ into $x$'s original position and shifts the stray digits back to their original position. The total number of swaps of adjacent digits is $k + 1 + k = 2k + 1$, which is odd for all $k \geq 0$. ■

**Lemma 0.5.** *Rotating any row or column changes the number of inversions by an even amount.*

**Proof.** We show below that any row or column rotation can be obtained by two swaps. The preceding lemma says that every swap changes the number of inversions by an even amount. Since the sum of two odd numbers is even, any row or column rotation changes the number of inversions by an even amount.

Here is how to obtain a rotation from two swaps. Suppose that the digit sequence $xyz$ appears in some row or column. Swapping $x$ with $y$ and then swapping $x$ with $z$ creates the sequence $yzx$, which corresponds to a leftward or upward rotation. Swapping $z$ with $y$ and then $z$ with $x$ creates the sequence $zxy$. This corresponds to a rightward or downward rotation. ■