Massachusetts Institute of Technology
6.042J/18.062J, Spring '10: Mathematics for Computer Science — March 3
Prof. Albert R. Meyer — revised March 1, 2010, 826 minutes

Solutions to In-Class Problems Week 5, Wed.

By now you are very familiar with the 6.042 icon that appears on the course webpage and lecture slides. This icon is a picture of a game called the **Fifteen Puzzle**. The following problem may help you appreciate why this icon was chosen as the course logo.

Problem 1.
In this problem you will establish a basic property of a puzzle toy called the *Fifteen Puzzle* using the method of invariants. The Fifteen Puzzle consists of sliding square tiles numbered $1, \ldots, 15$ held in a 4×4 frame with one empty square. Any tile adjacent to the empty square can slide into it.

The standard initial position is

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

We would like to reach the target position (known in my youth as "the impossible" — ARM):

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

A state machine model of the puzzle has states consisting of a 4×4 matrix with 16 entries consisting of the integers $1, \ldots, 15$ as well as one "empty" entry—like each of the two arrays above.

The state transitions correspond to exchanging the empty square and an adjacent numbered tile. For example, an empty at position $(2, 2)$ can exchange position with tile above it, namely, at position $(1, 2)$:

$$\begin{array}{|c|c|c|c|}\hline n_1 & n_2 & n_3 & n_4 \\ \hline n_5 & & n_6 & n_7 \\ \hline n_8 & n_9 & n_{10} & n_{11} \\ \hline n_{12} & n_{13} & n_{14} & n_{15} \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline n_1 & & n_3 & n_4 \\ \hline n_5 & n_2 & n_6 & n_7 \\ \hline n_8 & n_9 & n_{10} & n_{11} \\ \hline n_{12} & n_{13} & n_{14} & n_{15} \\ \hline \end{array}$$

We will use the invariant method to prove that there is no way to reach the target state starting from the initial state.

We begin by noting that a state can also be represented as a pair consisting of two things:

1. a list of the numbers $1, \ldots, 15$ in the order in which they appear—reading rows left-to-right from the top row down, ignoring the empty square, and

2. the coordinates of the empty square—where the upper left square has coordinates $(1, 1)$, the lower right $(4, 4)$.

(a) Write out the "list" representation of the start state and the "impossible" state.

Solution. start: $((1\ 2\ \ldots\ 15), (4, 4))$,

impossible: $((15\ 14\ \ldots\ 1), (4, 4))$.

■

Let L be a list of the numbers $1, \ldots, 15$ in some order. A pair of integers is an *out-of-order pair* in L when the first element of the pair both comes *earlier* in the list and *is larger*, than the second element of the pair. For example, the list $1, 2, 4, 5, 3$ has two out-of-order pairs: (4,3) and (5,3). The increasing list $1, 2 \ldots n$ has no out-of-order pairs.

Let a state, S, be a pair $(L, (i, j))$ described above. We define the *parity* of S to be the mod 2 sum of the number, $p(L)$, of out-of-order pairs in L and the row-number of the empty square, that is the parity of S is $p(L) + i \pmod 2$.

(b) Verify that the parity of the start state and the target state are different.

Solution. The parity of the start state is

$$(0 + 4) \bmod 2 = 0.$$

The parity of the target is

$$((15 \cdot 14/2) + 4) \bmod 2 = 1.$$

■

(c) Show that the parity of a state is preserved under transitions. Conclude that "the impossible" is impossible to reach.

Solution. To show that the parity is constant, consider how moves may affect the parity. There are only 4 types of moves: a move to the left, a move to the right, a move to the row above, or a move to the row below.

Note that horizontal moves change nothing, and vertical moves both change i by 1, and move a tile three places forward or back in the list, L. To consider how the parity is changed in this case, we need to consider only the 3 pairs in L that are between the tile's old and new position. (The other pairs are not effected by the tile's move). This reverses the order of three pairs in L, changing the number of inversions by 3 or 1, but always by an odd amount.

To confirm this last remark, note that if the 3 pairs were all out of order or all in order before, the amount is changed by 3. If two pairs were out of order and 1 pair was in order or if one pair was out of order and two were in order, this will change the amount by 1. So the sum of i and the number of out-of-order pairs changes by an even amount (either 1+3 or 1+1), which implies that its parity remains the same. Since the initial state has parity 0 (even), all states reachable from the initial state must have parity 0, so the target state with parity 1 can't be reachable. ■

By the way, if two states have the same parity, then in fact there *is* a way to get from one to the other. If you like puzzles, you'll enjoy working this out on your own.

Problem 2.
The most straightforward way to compute the bth power of a number, a, is to multiply a by itself b times. This of course requires $b-1$ multiplications. There is another way to do it using considerably fewer multiplications. This algorithm is called *fast exponentiation*:

Given inputs $a \in \mathbb{R}, b \in \mathbb{N}$, initialize registers x, y, z to $a, 1, b$ respectively, and repeat the following sequence of steps until termination:

- if $z = 0$ **return** y and terminate
- $r := \text{remainder}(z, 2)$
- $z := \text{quotient}(z, 2)$
- if $r = 1$, then $y := xy$
- $x := x^2$

We claim this algorithm always terminates and leaves $y = a^b$.

(a) Model this algorithm with a state machine, carefully defining the states and transitions.

Solution. 1. The set of states is $\mathbb{R} \times \mathbb{R} \times \mathbb{N}$,

2. The start state is $(a, 1, b)$,
3. the transitions are defined by the rule

$$(x, y, z) \rightarrow \begin{cases} (x^2, y, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and even,} \\ (x^2, xy, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and odd.} \end{cases}$$

■

(b) Verify that the predicate $P((x, y, z)) ::= [yx^z = a^b]$ is a preserved invariant.

Solution. We show that P is preserved, namely, assuming $P((x, y, z))$, that is,

$$yx^z = a^b \tag{1}$$

holds and $(x, y, z) \rightarrow (x_t, y_t, z_t)$ is a transition, then $P((x_t, y_t, z_t))$, that is,

$$y_t x_t^{z_t} = a^b$$

holds.

We consider two cases:

If $z > 0$ and is even, then we have that $x_t = x^2, y_t = y, z_t = \text{quotient}(z, 2)$. Therefore,

$$\begin{aligned} y_t x_t^{z_t} &= yx^{2\cdot\text{quotient}(z,2)} \\ &= yx^{2\cdot(z/2)} \\ &= yx^z \\ &= a^b && \text{(by (1))} \end{aligned}$$

If $z > 0$ and is odd, then we have that $x_t = x^2, y_t = xy, z_t = \text{quotient}(z, 2)$. Therefore,

$$\begin{aligned} y_t x_t^{z_t} &= xyx^{2\cdot\text{quotient}(z,2)} \\ &= yx^{1+2\cdot(z-1)/2} \\ &= yx^{1+(z-1)} \\ &= yx^z \\ &= a^b && \text{(by (1))} \end{aligned}$$

So in both cases, $P((x_t, y_t, z_t))$ holds, proving that P is a preserved invariant. ■

(c) Prove that the algorithm is partially correct: if it halts, it does so with $y = a^b$.

Solution. P holds for the start state $(a, 1, b)$ since $1 \cdot a^b = a^b$. So by the Invariant Theorem, P holds for all reachable states. But a terminal state must have $z = 0$, so if any terminal state $(x, y, 0)$ is reachable, then $y = yx^0 = a^b$ as required. ■

(d) Prove that the algorithm terminates.

Solution. Just notice that z is a natural-number-valued variable that gets smaller at every transition. So by the Well-Ordering Principle, when this variable reaches its minimum value, the algorithm terminates. ■

(e) In fact, prove that it requires at most $2\lceil\log_2(b+1)\rceil$ multiplications for the Fast Exponentiation algorithm to compute a^b for $b > 1$.

Solution. The value of z is initially b and gets at least halved at every step. So it can't be halved more than $\lceil\log_2(b+1)\rceil$ times before hitting zero. We need $(b+1)$ because for $b = 2^p$, a power of two, it takes $(p+1)$ halves to get zero. Since each of the transitions involves at most two multiplications, the total number of multiplications until $z = 0$ is at most $2\lceil\log_2(b+1)\rceil$. ■