Type your answers to the following questions and submit a PDF file to Blackboard. One page per problem.

Problem 1. [10pts] Let $M = (S, T, s_0)$ be the state machine where $S = \mathbb{N} \times \mathbb{N}$ and the transitions in T are given as $(m, n) \to (m-1, n+1)$ if $m \geq 1$, and $(m, n) \to (m, n-1)$ if $n \geq 1$. Define a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where f is decreasing with respect to M and use the Monotonicity Principle to prove that if the initial state is (m, n), then the machine will halt in at most $f(m, n)$ transitions. (Bonus 1pt for defining $f(m, n)$ to be *optimal*, predicting exactly the maximum number of steps from (m, n) to a halting state.) [Hint: Draw the points (m, n) in the plane and draw lines between points for possible transitions.]

Proof. Let $f(m, n) = 2m + n$. Consider a state (m, n). The transition $(m, n) \to (m, n - 1)$ satisfies $f(m, n) = 2m + n > 2m + n - 1 = f(m, n - 1)$. The transition $(m, n) \to (m - 1, n + 1)$ satisfies $f(m, n) = 2m + n > 2m + n - 1 = 2(m - 1) + (n + 1) = f(m - 1, n + 1)$. Therefore, $f(m, n)$ is a decreasing function and $f(m, n) \geq 0$ for all $m, n \in \mathbb{N}$. By the Monotonicity Principle, the state machine halts in at most $f(m, n)$ steps.

[Bonus] Starting at a state (m, n), use m transitions of the type $(m, n) \to (m - 1, n + 1)$ to arrive at the state $(0, n + m)$. Then use $m + n$ transitions of the type $(m, n) \to (m, n - 1)$ to arrive at the state $(0, 0)$. Therefore, (m, n) has a set of $2m + n$ transitions until reaching the halting state $(0, 0)$. $\square$

Problem 2. [10pts] Let $\Sigma = \{a^+, a^-, b^+, b^-\}$. Let $M = (S, T, s_0)$ be the state machine where $S = \Sigma^*$ and the transitions available in T from a string $x_1 \dots x_n \in \Sigma^*$ are as follows:

- If there exists $i \in \{1, \dots, n{-}1\}$ such that $x_i = a^+$ and $x_{i+1} = a^-$, then $x_1 \dots x_n \longrightarrow x_1 \dots x_{i-1}x_{i+2} \dots x_n$.
- If there exists $i \in \{1, \dots, n{-}1\}$ such that $x_i = a^-$ and $x_{i+1} = a^+$, then $x_1 \dots x_n \longrightarrow x_1 \dots x_{i-1}x_{i+2} \dots x_n$.
- If there exists $i \in \{1, \dots, n{-}1\}$ such that $x_i = b^+$ and $x_{i+1} = b^-$, then $x_1 \dots x_n \longrightarrow x_1 \dots x_{i-1}x_{i+2} \dots x_n$.
- If there exists $i \in \{1, \dots, n{-}1\}$ such that $x_i = b^-$ and $x_{i+1} = b^+$, then $x_1 \dots x_n \longrightarrow x_1 \dots x_{i-1}x_{i+2} \dots x_n$.

a. [5pts] Describe all of the possible state sequences when starting at the string $b^+a^+b^+b^-a^-b^+a^+b^-b^+$.

$b^+a^+b^+b^-a^-b^+a^+b^-b^+$ can transition to $b^+a^+a^-b^+a^+b^-b^+$ (collapsing b^+b^- in positions 3 and 4) or $b^+a^+b^+b^-a^-b^+a^+$ (collapsing b^-b^+ in positions 8 and 9).

$b^+a^+a^-b^+a^+b^-b^+$ can transition to $b^+b^+a^+b^-b^+$ (collapsing a^+a^- in positions 2 and 3) or $b^+a^+a^-b^+a^+$ (collapsing positions 6 and 7).

$b^+a^+b^+b^-a^-b^+a^+$ can transition to $b^+a^+ - a^-b^+a^+$ (collapsing b^+b^- in positions 3 and 4).

$b^+b^+a^+b^-b^+$ can transition to $b^+b^+a^+$ (collapsing b^-b^+ in positions 4 and 5).

$b^+a^+a^-b^+a^+$ can transition to $b^+b^+a^+$ (collapsing a^+a^- in positions 2 and 3).

$b^+b^+a^+$ is a halting state.

b. [5pts] For certain states in Σ^*, there may be more than one outgoing transition. Prove that for every string $\mathbf{x} \in \Sigma^*$, there is a unique halting state reachable from $\mathbf{x}$. [Hint: List the possible outgoing states $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(k)}$ and show that every pair $\mathbf{y}^{(i)}$ and $\mathbf{y}^{(j)}$ have a common outgoing state, so they have a common halting state.]

We claim that for every state $\mathbf{x}$, there is a unique halting state reachable from $\mathbf{x}$.

Proof. We will use proof by strong induction, using $n = |\mathbf{x}|$, the length of $\mathbf{x}$.

Case $n = 0$: If $|\mathbf{x}| = 0$, then $\mathbf{x}$ is the empty word. There are no transitions from $\mathbf{x}$, so $\mathbf{x}$ is its own unique halting state.

Case $n = 1$: If $|\mathbf{x}| = 1$, then $\mathbf{x}$ has exactly one letter. There are no transitions from $\mathbf{x}$, so $\mathbf{x}$ is its own unique halting state.

(Strong Induction Hypothesis) Let $N > 0$ and suppose that for all $0 \le n < N$, the statement holds for all words of length n.

Case N: Let $\mathbf{x}$ have length N. If $\mathbf{x}$ has no transitions, then $\mathbf{x}$ is its own unique halting state and $k = 0$. Now suppose that $\mathbf{x}$ has transitions $\mathbf{x} \to \mathbf{y}^{(i)}$ for $i \in \{1, \dots, k\}$ for some $k \ge 1$. If $k = 1$, then $\mathbf{x}$ has a unique outgoing transition, and $\mathbf{y}^{(1)}$ has a unique halting state, so $\mathbf{x}$ has a unique halting state. Thus, we can suppose that $k \ge 2$. (Note that $|\mathbf{y}^{(i)}| = N - 2$, so the induction hypothesis holds for each $\mathbf{y}^{(i)}$. Since $\mathbf{x}$ transitions to each $\mathbf{y}^{(i)}$, there is a value $c_i \in \{1, \dots, N-1\}$ where the positions $x_{c_i}x_{c_i+1}$ are deleted from $\mathbf{x}$ to form $\mathbf{y}^{(i)}$. We can order the transitions such that when $i < j$, $c_i < c_j$ ($c_i \neq c_j$ since equality would create the same word). Thus, $\mathbf{y}^{(i)} = x_1 \dots x_{c_i-1}x_{c_i+2} \dots x_n$.

Note: If $c_j = c_i + 1$, then observe that $x_{c_i} = x_{c_i+2}$ and hence $\mathbf{y}^{(i)} = \mathbf{y}^{(j)}$. This is a very subtle point and students will not lose points if they do not mention this point. Therefore, since $\mathbf{y}^{(i)} \neq \mathbf{y}^{(j)}$, we have $c_i + 2 \leq c_j$ when $i < j$.

For $1 \leq i < j \leq k$, we will prove that the halting state for $\mathbf{y}^{(i)}$ is the same as the halting state for $\mathbf{y}^{(j)}$. If suffices to show that $\mathbf{y}^{(i)}$ and $\mathbf{y}^{(j)}$ have a common outgoing transition $\mathbf{w}$, and by the induction hypothesis, $\mathbf{w}$ has a unique halting state $\mathbf{z}$, which is the unique halting state for both $\mathbf{y}^{(i)}$ and $\mathbf{y}^{(j)}$. In $\mathbf{y}^{(j)}$, the letters in the c_i and c_i+1 positions are the same as those in the word $\mathbf{x}$ (as $c_i < c_j$ so there were two letters removed *after* the c_i position), so there is a transition out of $\mathbf{y}^{(j)}$ to the word $\mathbf{w} = x_1 \dots x_{c_i-1} x_{c_i+2} \dots x_{c_j-1} x_{c_j+2} \dots x_n$. In $\mathbf{y}^{(j)}$, the letters in the $c_j - 2$ and $c_j - 1$ positions are the same as the c_j and $c_j + 1$ positions in the word $\mathbf{x}$ (as $c_i < c_j$ so there were two letters removed *before* the c_j position), so there is a transition out of $\mathbf{y}^{(j)}$ to the word $\mathbf{w} = x_1 \dots x_{c_i-1} x_{c_i+2} \dots x_{c_j-1} x_{c_j+2} \dots x_n$. By Strong Induction, $\mathbf{w}$ has a unique halting state $\mathbf{z}$, which is equal to the unique halting state of $\mathbf{y}^{(i)}$ and $\mathbf{y}^{(j)}$. Thus, for all $i \in \{1, \dots, k\}$, the halting state from $\mathbf{y}^{(i)}$ is the halting state $\mathbf{z}$. Finally, this halting state $\mathbf{z}$ is the unique halting state reachable from $\mathbf{x}$. $\square$

Problem 3. [10pts] Let $M = (\mathbb{Q}, T, s_0)$ be a state machine on the rational numbers with transitions $\frac{p}{q} \to \frac{p}{q} + \frac{1}{pq} = \frac{p^2+1}{pq}$, when $p > 0$ and $q > 0$.

a. [5pts] Let $P_d(\frac{p}{q})$ be the property "$d \leq \frac{p}{q} < d+1$." Prove that when d is an integer with $d \geq 3$, P_d is a reversible invariant for the state machine M. [Hint: Show that P_d is a preserved invariant for all $d \geq 2$. If $P_d(\frac{p}{q})$ is true, then $p = dq + r$ where r is an integer and $0 \leq r < q$. To show P_d is a reversible invariant for $d \geq 3$, use the fact that it is a preserved invariant for $d \geq 2$.]

Proof. Let $d \geq 2$. Suppose $P_d(\frac{p}{q})$ is true and $\frac{p}{q} \to \frac{p^2+1}{pq}$ is a transition. Since $d \leq \frac{p}{q} < d+1$, we have $dq \leq p < dq + q$ and hence $p = dq + r$ for an integer r with $0 \leq r < q$. Then, since $p \geq dq \geq 2$ we have $r + \frac{1}{p} \leq r + \frac{1}{2} < q$ and $rp + 1 = p(r + 1/p) < pq$ and hence

$$p^2 + 1 = p(dq + r) + 1 = dpq + rp + 1 < dpq + pq = (d+1)pq.$$

Therefore,

$$d \leq \frac{p}{q} < \frac{p^2+1}{pq} < d+1,$$

and P_d is a preserved invariant for $d \geq 2$.

Now let $d \geq 3$. For the sake of contradiction, suppose that P_d is not a reversible invariant, so there exists a fraction $\frac{p}{q}$ where $P_d(\frac{p}{q})$ is false but $P_d(\frac{p^2+1}{pq})$ is true. This means $d \leq \frac{p}{q} + \frac{1}{pq} < d+1$. Since $\frac{p}{q} < \frac{p}{q} + \frac{1}{pq}$, we know that $\frac{p}{q} < d+1$, so since $P_d(\frac{p}{q})$ is false it must be because $\frac{p}{q} < d$. If $\frac{p}{q} \geq 2$, then $P_e(\frac{p}{q})$ is true for some $e \geq 2$, but since P_e is a preserved invariant, it must be that $e = d$. Therefore, $\frac{p}{q} < 2$, implying that $1 < \frac{p^2+1}{pq} - \frac{p}{q} = \frac{1}{pq} \leq 1$, a contradiction. $\square$

b. [5pts] Use part (a) and the Reversibility Principle to say that if $\frac{p}{q}$ is the initial state with $\frac{p}{q} \geq 3$ and $\frac{i}{j}$ is a reachable state, then $\lfloor \frac{p}{q} \rfloor = \lfloor \frac{i}{j} \rfloor$. [You can get full points for this part if you assume (a), even if you have not proven (a) correctly.]

Proof. Let d be the integer where $P_d(\frac{p}{q})$ is true. Since $\frac{p}{q} \geq 3$, $d \geq 3$ and P_d is a reversible invariant. By the reversibility principle, $P_d(\frac{p}{q})$ is true if and only if $P_d(\frac{i}{j})$ is true. Thus, $d = \lfloor \frac{p}{q} \rfloor = \lfloor \frac{i}{j} \rfloor$. $\square$

c. [Bonus 1pt] Find a fraction $\frac{p}{q}$ such that $P_1(\frac{p}{q})$ is true but $P_1(\frac{p^2+1}{pq})$ is false.

d. [Bonus 1pt] Find a fraction $\frac{p}{q}$ such that $P_2(\frac{p}{q})$ is false but $P_2(\frac{p^2+1}{pq})$ is true.

Let $p = q = 1$. Then $1 \leq \frac{1}{1} < 2$ but $\frac{1^1+1}{1 \cdot 1} = \frac{2}{1} = 2$. Thus, this transition shows that P_1 is not a preserved invariant and P_2 is not a reversible invariant (although P_2 *is* a preserved invariant).

Problem 4. [10pts] Define a set $S \subseteq \mathbb{R}$ recursively using the Recursive Step "If $x \in S$, then $(x-1)(x+1) \in S$." Consider the following bases.

a. [3pts] Prove that if the basis step is "$0 \in S$" then $S = \{0, -1\}$.

Proof. By the basis step, $0 \in S$. Using 0 in the recursive step, $(0-1)(0+1) = -1$ and hence $-1 \in S$. Thus, $\{0, -1\} \subseteq S$.

Using -1 in the recursive step, $(-1-1)(-1+1) = 0$ and hence $0 \in S$. Therefore, no other elements are in the set. □

b. [3pts] Prove that if the basis step is "$1 \in S$" then $S = \{1, 0, -1\}$.

Proof. By the basis step, $1 \in S$. Using 1 in the recursive step, $(1-1)(1+1) = 0$ and hence $0 \in S$. Using 0 in the recursive step, $(0-1)(0+1) = -1$ and hence $-1 \in S$. Thus, $\{1, 0, -1\} \subseteq S$.

Using -1 in the recursive step, $(-1-1)(-1+1) = 0$ and hence $0 \in S$. Therefore, no other elements are in the set. □

c. [4pts] Prove that if the basis step is "$2 \in S$" then S is an infinite set.

Proof. We use proof by contradiction. Suppose that S is finite. Then there exists a maximum element $x = \max S$. Since $2 \in S$ by the basis step, $x \geq 2$.

Since $x \in S$, the element $(x-1)(x+1) = x^2 - 1$ is in S by the recursive step. Since $x \geq 2$, $x^2 > x + 1$, and hence $x^2 - 1 > x$, contradicting that x is the maximum element in S. □

Problem 5. [10pts] Define a set $S \subseteq \mathbb{R}$ recursively by (Basis Step) $\frac{1}{1} \in S$, and (Recursive Step) If $x \in S$, then $2x \in S$ and $\frac{x}{3} \in S$. Prove that $S = \{\frac{2^i}{3^j} : i, j \in \mathbb{N}\}$.

Proof. ($S \subseteq \{\frac{2^i}{3^j} : i, j \in \mathbb{N}\}$) We use structural induction.

(Basis) $\frac{1}{1} = \frac{2^0}{3^0}$.

(Recursive Step) Let $\frac{2^i}{3^i}$ be an element of S. The transition $\frac{2^i}{3^j} \to 2\frac{2^i}{3^j}$ implies the element $\frac{2^{i+1}}{3^j}$ is in S. The transition $\frac{2^i}{3^j} \to \frac{\frac{2^i}{3^j}}{3}$ implies the element $\frac{2^i}{3^{j+1}}$ is in S.

Therefore, by structural induction every element of S is of the form $\frac{2^i}{3^j}$.

($\{\frac{2^i}{3^j} : i, j \in \mathbb{N}\} \subseteq S$) We use induction on $i + j$ to show that $\frac{2^i}{3^j}$ is in S.

Case $i + j = 0$: $\frac{2^0}{3^0} = \frac{1}{1}$ which is in S by the basis step.

(Induction Hypothesis) Let $n \geq 0$ and suppose that for all $i, j \in \mathbb{N}$ with $i + j = n$ we have $\frac{2^i}{3^j} \in S$.

Case $i + j = n + 1$: If $i > 0$, then since $i - 1 \in \mathbb{N}$ and $(i - 1) + j = n$ we have $\frac{2^{i-1}}{3^j} \in S$. By the construction step, $2 \cdot \frac{2^{i-1}}{3^j} = \frac{2^i}{3^j}$ is in S. If $i = 0$, then since $j = n + 1 > 0$ we have $j - 1 \in \mathbb{N}$ and $\frac{1}{3^{j-1}}$ is in S. By the construction step, $\frac{\frac{1}{3^{j-1}}}{3} = \frac{1}{3^j}$ is in S.

By induction, every element $\frac{2^i}{3^j}$ with $i, j \in \mathbb{N}$ is in S. $\square$