1 Monday, February 16

Reading: Rosen 5.1, 5.2. LLM 5.1, 5.2, 5.3. Ducks 8.2, 8.3

1.1 Rosen 5.1 – Mathematical Induction

1.1.1 More Examples

Here are a few examples of statements you can prove using induction.

Thm: Every natural number $n \in \mathbb{N}$ is either even or odd.

Proof. Case $n = 0$: $0 = 2 \cdot 0$, so 0 is even.

(Induction Hypothesis) Now suppose for some integer $n \geq 0$, n is even or n is odd.

Case $n + 1$: By the induction hypothesis, n is even or n is odd. If n is even, then there exists an integer k such that $n = 2k$ and $n + 1 = 2k + 1$, so $n + 1$ is odd. If n is odd, then there exists an integer k such that $n = 2k + 1$ and $n + 1 = 2k + 1 + 1 = 2(k + 1)$, so $n + 1$ is even. □

Thm: Let $a_0 = 1$ and for $n \geq 1$ let $a_n = 5a_{n-1} + 1$. For all $n \geq 2$, $a_n < 6^n$.

Note: Since $a_0 = 1 = 6^0$ and $a_1 = 6 = 6^1$, the statement $a_n < 6^n$ is false for $n \in \{0, 1\}$. So, our "base case" is actually $n = 2$.

Proof. Case $n = 2$: $a_2 = 5(6) + 1 = 31 < 36 = 6^2$. Therefore $a_2 < 6^2$.

(Induction Hypothesis) Assume that for some $n \geq 2$ we have $a_n < 6^n$.

Case $n + 1$: $a_{n+1} = 5a_n + 1 < 5(6^n) + 1 = 5(6^n) + \frac{1}{6^n}(6^n) = (5 + \frac{1}{6^n})6^n$. Note that since $n \geq 2$, $\frac{1}{6^n} < 1$ and thus $5 + \frac{1}{6^n} < 6$. Therefore, $a_{n+1} < (5 + \frac{1}{6^n})6^n < 6(6^n) = 6^{n+1}$.

By induction, $a_n < 6^n$ for all $n \geq 2$. □

Ex: Let $b_0 = e$ and $c_0 = 1$, and for $n \geq 1$, $b_n = e^{c_{n-1}}$ and $c_n = \ln(b_{n-1})$. Prove that for all $n \geq 1$, $b_n = e$ and $c_n = 1$.

1.2 Rosen 5.2 – Strong Induction and the Well-Ordered Property

1.2.1 Strong Induction

The Principal of (Strong) Mathematical Induction: Let $(P(n))_{n=0}^{\infty}$ be a sequence of propositions. To prove $\forall n P(n)$, it suffices to demonstrate the following:

1. $P(0)$ is true.

2. If $P(m)$ is true for $0 \leq m < n$, then $P(n)$ is true.

(Alternatively, (2) can be stated as "For all n, $[P(0) \wedge P(1) \wedge \cdots \wedge P(n)] \rightarrow P(n + 1)$.")

Def: Recall the definitions of *Fibonacci numbers* F_n and *Lucas numbers* L_n:

$$\begin{aligned} F_0 &= 0 & L_0 &= 2 \\ F_1 &= 1 & L_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} & L_n &= L_{n-1} + L_{n-2} \end{aligned}$$

Since the recurrence relation depends on multiple previous values, regular mathematical induction does not suffice to prove facts about these sequences!

Thm: For all $n \geq 1$, $L_n = F_{n-1} + F_{n+1}$.

Proof. We will prove this by strong induction.

Case $n = 1$: $L_1 = 1 = 0 + 1 = F_0 + F_2$.

Case $n = 2$: $L_2 = 3 = 1 + 2 = F_1 + F_3$.

(Induction Hypothesis) Now let $N > 2$ and assume that for all n where $1 \leq n < N$ we have $L_n = F_{n-1}+F_{n+1}$.

Case N: By the recurrence relation of Lucas numbers, $L_N = L_{N-1} + L_{N-2}$. By the induction hypothesis, $L_{N-1} = F_{N-2} + F_N$ and $L_{N-2} = F_{N-3} + F_{N-1}$. Therefore, $L_N = F_{N-2} + F_N + F_{N-3} + F_{N-1} = (F_N + F_{N-1}) + (F_{N-2} + F_{N-3})$. By the recurrence relation of Fibonacci numbers, $F_N + F_{N-1} = F_{N+1}$ and $F_{N-2} + F_{N-3} = F_{N-1}$. Therefore, $L_N = F_{N-1} + F_{N+1}$.

Thus, by strong induction, we have $L_n = F_{n-1} + F_{n+1}$ for all $n \geq 1$. □

Thm: There are F_{n+1} ways to tile the $2 \times n$ chessboard with dominoes.

Proof. Let d_n be the number of ways to tile the $2 \times n$ chessboard. We will prove "$d_n = F_{n+1}$" for all $n \geq 0$.

Case $n = 0$: There is 1 way to tile the 2×0 chessboard: no dominoes! $d_0 = 1 = F_1$.

Case $n = 1$: There is 1 way to tile the 2×1 chessboard: one vertical domino! $d_1 = 1 = F_2$.

Now let $N > 1$ and assume that for all $n < N$, $d_n = F_{n+1}$.

Case N: Consider a domino tiling, and consider the domino covering the $(1, 1)$ position. This tile is either horizontal or vertical.

If the domino is horizontal, then there is another horizontal domino covering the $(2, 1)$ position, and these dominoes cover the $(1, 1)$, $(1, 2)$, $(2, 1)$ and $(2, 2)$ positions. Since there are d_{n-2} ways to tile the rest of the positions, there are d_{n-2} domino tilings of the $2 \times n$ chessboard with a horizontal domino covering the $(1, 1)$ position.

If the domino is vertical, then it also covers the $(2, 1)$ position. Since there are d_{n-1} ways to tile the rest of the positions, there are d_{n-1} domino tilings of the $2 \times n$ chessboard with a vertical domino covering the $(1, 1)$ position.

Therefore, there are $d_{n-2} + d_{n-1}$ ways to tile the $2 \times n$ chessboard, so $d_n = d_{n-2} + d_{n-1} = F_{n-1} + F_n = F_{n+1}$. □

Note: We could prove the above using standard (incomplete) induction if we use the following parameterized statement: $P(n) =$ "$(d_n = F_{n+1}) \wedge (d_{n+1} = F_{n+2})''$.

1.2.2 Binary Representations

Thm: Every natural number n can be described as a sum of powers of 2. That is, there exists a $k \geq 0$ and a tuple $(a_k, a_{k-1}, \ldots, a_1, a_0) \in \{0, 1\}^{k+1}$ such that $n = \sum_{i=0}^{k} a_i 2^i$.

Proof. Case $n = 0$: Let $k = 0$ and $a_0 = 0$.

Case $n = 1$: Let $k = 0$ and $a_0 = 1$.

(Induction Hypothesis) Let $N > 1$ be a natural number and suppose that for all n where $0 \leq n < N$, the integer n can be described as a sum of powers of 2.

Case N: Let k be the maximum integer such that $2^k \leq N$. Then, $2^k \leq N < 2^{k+1}$. Since $N > 1$ we have $k \geq 1$. Let $n = N - 2^k$, so $0 \leq n < 2^k$. By the induction hypothesis, the number n can be described as a sum of powers of 2. Let $(a_\ell, \ldots, a_1, a_0) \in \{0,1\}^{\ell+1}$ be the tuple such that $n = \sum_{i=0}^{\ell} a_i 2^i$. Note: if $\ell < k$, then we can extend $\ell = k$ by adding leading zeroes to the tuple. Also, if $\ell \geq k$, then specifically $a_k = 0$ since $2^k > n$. (And in fact $a_i = 0$ for all $i \geq k$.)

Thus, let $(a'_k, a'_{k-1}, \ldots, a'_1, a'_0)$ be defined as $a'_i = \begin{cases} a_i & \text{if } i < k \\ 1 & \text{if } i = k \end{cases}$. Then, $\sum_{i=0}^{k} a'_i 2^i = 2^k + \sum_{i=0}^{\ell} a_i 2^i = 2^k + n = N$. □

1.2.3 Strong Induction and Well-Ordered Property

Def: The *well-ordered property* of the natural numbers is the statement "Every subset of the natural numbers has a least element."

Note: This is not true for integers (the whole set has no minimum) or even nonnegative rationals (the set of *positive* rationals has no least element).

This means we can prove Strong Induction.

Proof of Strong Induction. Let X be the set of values n such that $P(n)$ is false. Since $P(0)$ is true, $0 \notin X$.

If X is nonempty, then let $N = \min X$, the minimum value of X, which exists by the well-ordered property of the natural numbers. Since $0 \notin X$, $N > 0$. Therefore, since $N = \min X$ we have that $P(0), \ldots, P(N-1)$ are true statements (by definition of X). However, since $[P(0) \wedge P(1) \wedge \cdots \wedge P(N-1)] \to P(N)$, we have that N is not an element of X.

Therefore, X is empty and $P(n)$ is true for all $n \geq 0$. □

We can also use Well-Ordered Property *directly.*

Recall that the integer division algorithm takes an integer n and a divisor n and will return values q and r such that $n = qd + r$, and $0 \leq r < d$.

Thm: Let d be a positive number. For integer n there exist integers q and r such that $n = qd + r$ and $0 \leq r < d$.

Proof. Fix n. Let $S = \{n - dq : q \in \mathbb{Z}, n - dq \geq 0\} \subseteq \mathbb{N}$. S is nonempty since $n - d(d|n|) = 1n + d^2|n| \geq 0$. Let $r = \min S$. By definition of S, $r = n - dq$ for some q, and $r \geq 0$. Observe that $r < d$ since otherwise $r - d = n - d(q+1)$ is also in S but smaller than r. Therefore, $n = dq + r$ and $0 \leq r < d$. □

1.2.4 Examples to Try Strong Induction

Ex: Define a sequence $\{a_n\}_{n=0}^{\infty}$ by $a_0 = 1$ and the recurrence relation $a_n = a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 + 1 = 1 + \sum_{i=0}^{n-1} a_i$. Prove that $a_n = 2^n$ for all $n \geq 0$.

Ex: Define a sequence $\{a_n\}_{n=0}^{\infty}$ by $a_0 = 1$ and the recurrence relation $a_n = 2a_{n-1} + 2a_{n-2} + \cdots + 2a_1 + 2a_0 + 1 = 1 + 2\sum_{i=0}^{n-1} a_i$. Prove that $a_n = 3^n$ for all $n \geq 0$.

Ex: Prove that every integer $n \geq 2$ has a factorization into prime numbers.

Ex: Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. Prove that for all $n \geq 0$ the Fibonacci number F_n is equal to $\frac{\phi^n - \psi^n}{\phi - \psi}$.

1.2.5 Suggested Homework

Rosen 5.1:

Rosen 5.2:

2 Wednesday, February 18

This day, we spent 50 minutes talking about Exam 1, then spent 10 minutes on the following proof.

2.0.6 Example from Computational Geometry

Def: A polygon with n sides is *simple* if its edges do not cross (i.e. intersect at points other than vertices (corners)).

Thm: Every simple polygon with n sides for $n \geq 3$ can be triangulated into $n-2$ triangles.

Lma: Every simple polygon with at least four sides has an interior diagonal.

(This very "simple" lemma is actually very subtle and can be difficult to prove. Many incorrect proofs were thought to hold.)

Proof of Lemma. Let P be a polygon and select a point p in the polygon (including boundary) by first minimizing the x coordinate and among those points minimize the y coordinate. (This is called an "extremal choice.") The point p is necessarily on the boundary, or else it does not minimize the x coordinate. The point p is necessarily a vertex, or else it either does not minimize the x coordinate (edge is angled) or it does not minimize the y coordinate (edge is straight up-and-down). Now that p is a vertex, there are two vertices a and b on either side of p in the polygon, where the angle $\angle apb$ is the interior angle at p. Note: Due to the extremal choice of p, the angle $\angle apb$ is at most π radians (or at most 180 degrees) or else p does not minimize the x coordinate in P.

Consider the triangle $\triangle pab$. If this triangle does not intersect any other edges of P, then the line ab is a diagonal.

Otherwise, there is at least one vertex in the interior of the triangle $\triangle pab$. (Here we must be careful! We cannot select just ANY vertex, nor can we select the CLOSEST vertex.) Among these points, select the vertex v that minimizes the angle $\angle pav$ (a second extremal choice). We claim that the line segment pv is a diagonal of P. Note, that if pv crosses an edge ij, then since P is simple, one of the vertices i or j (w.l.o.g i) is in the triangle $\triangle pav$. Then the angle $\angle pai$ is smaller than the angle $\angle pav$, contradicting our extremal choice of v. □

Proof of Theorem. Case $n = 3$: Every simple polygon with three sides is a triangle, which is triangulated into $1 = 3 - 2$ triangles.

(Induction Hypothesis) Let $N > 3$ and assume that for all n where $3 \leq n < N$ every simple polygon with n sides can be triangulated into $n - 2$ triangles.

Case N: Let P be a polygon with N sides. By the lemma, there exists a diagonal ab of P. Split the polygon P into two parts given by using ab on the boundary of each. Thus, we have two polygons P_1 and P_2 each using n_1 or n_2 sides, where $n_1 + n_2 = N + 2$ (two "new" sides are from the line segment ab). By the induction hypothesis, P_1 has a triangulation into $n_1 - 2$ triangles. Also by the induction hypothesis, P_2 has a triangulation into $n_2 - 2$ triangles. Combining these triangulations forms a triangulation of P into $n_1 + n_2 - 4$ triangles. Since $n_1 + n_2 - 4 = N + 2 - 4 = N - 2$, the statement holds.

Therefore, by strong induction every simple polygon with n sides has a triangulation into $n - 2$ triangles when $n \geq 3$. □

3 Friday, February 20

3.1 LLM 5.4 — State Machines

Reading: LLM 5.4.

This topic does NOT appear in the Rosen textbook! However, the idea of a *state machine* is very important to computer science and the study of algorithms!

We will consider some examples of state machines before we rigorously define them.

The Collatz $3n + 1$ Problem

Suppose n is a number. If $n = 1$, then do nothing. However, if $n > 1$, then either: consider $\frac{n}{2}$ if n is even, or consider $3n + 1$ if n is odd.

Ex: Start at $n = 7$. We will list the values that we consider, in order:

$$7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.$$

Ex: Start at $n = 15$. We will list the values that we consider, in order:

$$15, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1.$$

Collatz Conjecture: Let n be any number at least 1. The process above will eventually terminate at $n = 1$.

See `http://en.wikipedia.org/wiki/Collatz_conjecture` for more information.

The Farmer and the River

A farmer is traveling with his Lettuce, Goat, and Wolf. The Wolf would eat the Goat if the farmer was not watching. The Goat would eat the Lettuce if the farmer was not watching. The group comes to a river and there is a canoe that can fit the farmer and one other item. The farmer would like to get across the river without losing the Lettuce or the Goat. How should the farmer use the canoe?

Bishops Moves

Consider the *infinite chessboard* $\mathbb{Z} \times \mathbb{Z}$. That is, every square is associated with an ordered pair (i, j) where $i, j \in \mathbb{Z}$.

A *bishop* can move diagonally. That is, if the bishop is in the position (i, j), then the bishop can move to the position $(i \pm k, j \pm k)$ where k is a positive integer.

Thm: If a bishop starts at position $(0, 0)$, then the bishop cannot reach the position $(1, 0)$.

Domino Tilings

Suppose that B is a chessboard (with some squares removed, possibly). We want to create a domino tiling of B. We say a *partial tiling* of B is an arrangement of dominoes such that every square is covered by *at most one* domino.

Given a partial tiling of B, we may attempt to place a domino on the board such that it does not cover a square already covered by a domino. This creates another partial tiling. The partial tiling may be a full domino tiling (if no squares remain uncovered) or may be a "maximal partial tiling" if no two uncovered squares are adjacent (so no domino can be placed!).

Note: B has a domino tiling if and only if there exists a list of domino placements that creates partial tilings leading to a complete tiling.

Thm: If B has a domino tiling, then B has an even number of squares.

GCD Algorithm

Recall Euclid's algorithm for computing the *greatest common divisor.*

```
**Input:** Integers $a$ and $b$ where $a \geq b \geq 0$.
If $b \equiv 0$, then return $a$.
Otherwise, let $q, r$ be integers such that $a = qb + r$ and $0 \leq r < b$.
Assign $a \leftarrow b$ and $b \leftarrow r$, then repeat the algorithm.
```

We may prove that this algorithm is correct later, but instead let's prove that this algorithm will terminate in a finite number of steps.

Thm: If a and b are integers with $a \geq b \geq 0$, the above algorithm will halt in a finite number of steps.

Proof. Observe that every time a and b are reassigned, b decreases by at least one (as the value r is guaranteed to be in the range $0 \leq r < b$). Therefore, the values a and b are reassigned at most b times (and the if statement is tested at most $b+1$ times). □

Mandlebrot Set

Consider a complex number $c \in \mathbb{C}$. Follow this process: Start with $z_1 = c$. Then for $n \geq 1$, let $z_{n+1} = z_n^2 + c$. Define a subset $M \subset \mathbb{C}$ as the set of values c where there exists a real number $x_c > 0$ where $|z_n| < x_c$ for all $n \geq 1$. The set M is called the *Mandlebrot set.*

See `http://en.wikipedia.org/wiki/Mandelbrot_set`.

3.1.1 State Machine Definition

Def: A *state machine* is a triple (S, T, s_0) where S is a set of *states*, T is a set of *transitions* between states (so T is a subset of $S \times S$), and $s_0 \in S$ is an *initial state.* A state machine *executes* by constructing a sequence $s_0, s_1, \ldots, s_n, \ldots$ where s_0 is the initial state, and for all $n \geq 0$, when s_n is a state in S, the sequence value s_{n+1} is a state in S such that the pair (s_n, s_{n+1}) is in T (that is, we can transition from s_n to s_{n+1}).

The Collatz $3n+1$ Problem

Let k be a positive integer. Let $S = \mathbb{Z}^+$, the set of positive integers. Define the transition set T as

$$T = \underbrace{\left\{(2n, n) : n \in \mathbb{Z}^+\right\}}_{\text{even transitions}} \cup \underbrace{\left\{(2n+1, 3(2n+1)+1) : n \in \mathbb{N}\right\}}_{\text{odd transitions}}.$$

Define the Collatz machine $M_k = (S, T, k)$, so the initial state of M_k is the integer k. The state machine M_k follows the Collatz process.

Conjecture: For every $k \geq 1$, the Collatz machine M_k will reach 1.

The Farmer and the River

A farmer is traveling East with his Lettuce, Goat, and Wolf. The Wolf would eat the Goat if the farmer was not watching. The Goat would eat the Lettuce if the farmer was not watching. The group comes to a river and there is a canoe that can fit the farmer and one other item. The farmer would like to get across the river without losing the Lettuce or the Goat. How should the farmer use the canoe?

We can model the situation using a state machine. Let $\mathcal{U} = \{F, L, G, W\}$ be a universe containing the Farmer, Lettuce, Goat, and Wolf. Our states will be pairs $(A, \overline{A})$ where A is a subset of $\mathcal{U}$ corresponding to which animals are on the West side of the river. A state is *acceptable* if it does not result in the Goat eating the Lettuce or the Wolf eating the Goat. Thus, if $\{L, G\} \subseteq A$ but $F \in \overline{A}$, then $(A, \overline{A})$ and $(\overline{A}, A)$ are not acceptable states. Thus, if $\{G, W\} \subseteq A$ but $F \in \overline{A}$, then $(A, \overline{A})$ and $(\overline{A}, A)$ are not acceptable states.

Therefore, let S be the set of acceptable states. Our initial state is $(\{F, L, G, W\}, \varnothing)$ and we want to reach the state $(\varnothing, \{F, L, G, W\})$. We need to describe our transitions!

Suppose $(A, \overline{A})$ is an acceptable state. If $F \in A$, then for each subset $B \subset A \setminus \{F\}$, we can transition to $(A \setminus (B \cup \{F\}), \overline{A} \cup B \cup \{F\})$, if the resulting state is acceptable. If $F \in \overline{A}$, then for each subset $B \subset \overline{A} \setminus \{F\}$, we can transition to $(A \cup B \cup \{F\}, \overline{A} \setminus (B \cup \{F\}))$, if the resulting state is acceptable.

We can now explore the space of reachable states. (Draw a picture, starting at $(FLGW, \varnothing)$, following transitions.)

Bishops Moves

Let $B = (S, T, s_0)$ be the state machine where $S = \mathbb{Z} \times \mathbb{Z}$, $s_0 = (0, 0)$, and the transition set T is defined as

$$T = \left\{ \big((i, j), (i + (-1)^a k, j + (-1)^b k)\big) : i, j, k \in \mathbb{Z}, a, b \in \{0, 1\} \right\}.$$

This machine B encodes all possible Bishop moves, starting at the position $(0, 0)$.

When talking about state machines, we will make use of the following concept.

Let $M = (S, T, s_0)$ be a state machine.

Preserved Invariant: A property $P : S \to \{\mathbf{T}, \mathbf{F}\}$ is a *preserved invariant* for M if "$\forall (s, t) \in T$, $P(s) \to P(t)$." That is, if a state has property P, then all states that are reachable from that state by one transition also have that property. **Invariant**

Principle: If a preserved invariant of a state machine is true for the start state, then it is true for all reachable states.

Observe that the above concept is equivalent to induction. If $s_0, s_1, s_2, \ldots, s_n, \ldots$ is a sequence of states given by a state machine, then let $Q(n) = P(s_n)$. The base case is that $Q(0)$ is true, which means the property is held by the initial state s_0. The preserved invariant property means that if $Q(n)$ is true, then $Q(n + 1)$ is true. So, you can use induction explicitly, or you can prove that a property is a preserved invariant.

Thm: If a bishop starts at position $(0, 0)$, then the bishop cannot reach the position $(1, 0)$.

Proof. Let $P(i, j)$ be the property "$i + j$ is even." We claim that P is a preserved invariant on the state machine B.

Suppose that $(i, j) \to (i + (-1)^a k, j + (-1)^b k)$ is a transition in the machine B and that $i + j$ is even. Let $i + j = 2\ell$ for some integer ℓ. If $a \neq b$, then $i + (-1)^a k + j + (-1)^b k = i + j = 2\ell$, so the resulting state has an even coordinate sum. If $a = b$, then $i + (-1)^a k + j + (-1)^b k = (i + j) + (-1)^a (2k) = 2\ell + (-1)^a (2k) = 2(\ell + (-1)^a k)$, so the resulting state has an even coordinate sum. Therefore, P is a preserved invariant.

Also, $0 + 0 = 2(0)$ so $P(0, 0)$ is true.

Thus by the Invariant Principle, $P(i, j)$ is true for all reachable states. Since $P(1, 0)$ is false, $(1, 0)$ is not a reachable state! □

Domino Tilings

Suppose that B is a chessboard (with some squares removed, possibly). Let $M_B = (S, T, s_0)$ be the state machine with states S given by the set of partial domino tilings of B, transitions T given by ways to place a new domino onto a partial tiling to produce a new partial tiling, and initial state s_0 given by the empty tiling.

Thm: If B has a domino tiling, then B has an even number of squares.

Proof. For a partial tiling $t \in S$, we let $P(t)$ be the property "The tiles in t cover an even number of squares." Notice that $P(s_0)$ is true.

Suppose that $t \to t'$ is a transition given by placing a new domino onto the partial tiling t to form a partial tiling t'. If $P(t)$ is true, then t covers $2k$ squares for some $k \geq 0$. Then t' covers $2k + 2 = 2(k + 1)$ squares, so $P(t')$ is true.

Therefore, if a complete tiling t is reachable from the empty tiling s_0, then $P(t)$ is true. □

GCD Algorithm

Let $E = (S, T, s_0)$ be the machine where S is the set of pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ where $a \geq b$, $s_0 = (a_0, b_0)$ for some pair $(a_0, b_0) \in \mathbb{N} \times \mathbb{N}$, and the transition set T is given by

$$T = \big\{\big((a, b), (b, a\%b)\big) : a, b \in \mathbb{N}, a \geq b > 0\big\}.$$

(Recall that $a\%b$ returns the remainder after integer division of a by b.)

The theorem that the GCD Algorithm halts is equivalent to saying this machine will reach a state $(a, 0)$ (where there are no transitions out).

Let $M = (S, T, s_0)$ be a state machine.
Decreasing Functions: Let $f : S \to \mathbb{N}$ be a function[1] The function f is *decreasing* if $\forall (s, t) \in T(f(s) > f(t)$. That is, for every transition $s \to t$, the value of f decreases from $f(s)$ to $f(t)$ with $f(t) < f(s)$.

Monotonicity Principle: If $f : S \to \mathbb{N}$ is a decreasing function, then the time it takes for a machine to terminate starting at a state s is at most $f(s)$.

Thm: The GCD Algorithm will terminate in a finite number of steps.

Proof. Define $f(a, b) = a + b$. Note that if $(a, b) \to (b, r)$ is a transition, then $0 \leq r < b \leq a$. Therefore, $f(b, r) = b + r < a + b = f(a, b)$ and hence f is a decreasing function.

By the monotonicity principle, starting at (a, b) will result in a halt in at most $a + b$ steps. (This is a gross over-count!) □

Thm: Let $d \geq 1$ be a positive integer. Let $P_d(a, b)$ be the property "a and b are both multiples of d." $P_d(a, b)$ is a preserved invariant for the machine E.

Proof. Suppose that $P_d(a, b)$ is true and $(a, b) \to (b, r)$ is a transition (implying $b > 0$ and $r = a\%b$). Then there exist nonnegative integers i, j such that $a = di$ and $b = dj$.

By integer division with remainder, there exists an integer q such that $a = qb + r$. So, $di = qdj + r$, which implies that $r = d(i - qj)$. Therefore, r is a multiple of d, and hence $P_d(b, r)$ is true. □

Thm: The GCD algorithm outputs the correct value.

In order to prove this statement, we need to make a different state machine, one that is *reversible*.

Let $M = (S, T, s_0)$ be a state machine.
Reversible Transitions: The machine M is *reversible* (or *undirected*) if whenever a transition (s, t) is in T, the transition (t, s) is also in T. That is, if $s \to t$ is a transition, then also $t \to s$ is a transition.

Reversibility Principle: If M is a reversible machine and P is an invariant property, then P holds on the initial state if and only if P holds on all reachable states.

To make M reversible, we will make $M' = (S, T \cup T', s_0)$ where $T \cup T'$ is the set of transitions from T (of the kind $(a, b) \to (b, a\%b)$) along with the transitions T' given as:

$$T' = \big\{\big((a, b), (ia + b, a)\big) : a, b, i \in \mathbb{N}, a \geq b, i > 0\big\}.$$

For the transition $(a, b) \to (ia + b, a)$, note that $(ia + b)\%a = b$, so these transitions are reversals of the transitions from T.

Proof. Recall the property P_d is a preserved invariant for the transitions in T. We will show it is also a preserved invariant for the transitions in T'. Suppose $(a, b) \to (ia + b, a)$ is a transition in T' and $P_d(a, b)$ is true. Then $a = dk$ and $b = d\ell$ for integers k and ℓ. Then $ia + b = idk + d\ell = d(ik + \ell)$, so d is a divisor of both $ia + b$ and a. Hence $P_d(ia + b, a)$ is true and P_d is a preserved invariant for the transitions in T and T'. By the Reversibility Principle, $P_d(a, b)$ is true if and only if it holds for all reachable states (a', b').

Let d be the greatest common divisor of a and b. Then $P_d(a, b)$ is true, and $P_{d'}(a, b)$ is false for all $d' > d$. If we follow transitions from T, we will terminate in a state $(r, 0)$. By the Invariant Principal, $P_d(r, 0)$ is true, so d is a divisor of r, and $d \leq r$. However, r is a divisor of both r and 0, so by the Reversibility Principle $P_r(a, b)$ is true. Therefore, $r \leq d$ (since d is the greatest common divisor of a and b) and therefore $r = d$. □

Mandlebrot Set

Fix a complex number $c \in \mathbb{C}$. The *Mandelbrot machine* $M_c = (S, T, c)$ has states $S = \mathbb{C}$ and transition set T given by

$$T = \{(z, z^2 + c) : z \in \mathbb{C}\}.$$

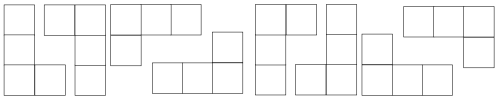
The *Mandlebrot set* M is the set of complex numbers c where the Mandlebrot maching M_c has all reachable states within a finite distance from 0.

3.1.2 Suggested Homework

LLM Problems 5.10, 5.28–38.

4 Extra Strong Induction Example

The *L-shaped Tetris piece* (or *tetromino*, see the Wikipedia page) consists of four squares: three of which are in a line and a fourth attached to one end of that line. See the figure below for all of the arrangements of the L-shaped Tetris piece (or L-piece).



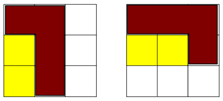
Thm: If k is odd, then the $3 \times 4k$ chessboard *cannot* be tiled using L-pieces.

Proof. We will use *strong* induction to prove that if $k \geq 1$ is odd, then the $3 \times 4k$ chessboard cannot be tiled using L-pieces. We first make a claim about any tiling:

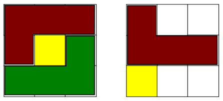
Claim: Any tiling of the $3 \times 4k$ chessboard using L-pieces must use an L-piece covering all three rows on the left-most and right-most edges.

Proof of Claim. Suppose there is a tiling that does not use an L-piece on an edge of length three (without loss of generality, we use the left edge). The top-left corner must be covered by some L-piece. Consider the possible placements, by how many squares of the L-piece are on the left edge.

Case 1: Exactly one square of the L-piece is on the left edge. In this case, the L-piece covers the three squares in the second column, leaving two squares on the left edge that cannot be covered by an L-piece!



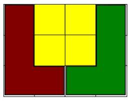
Case 1.



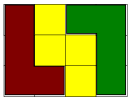
Case 2.

Case 2: Exactly two squares of the L-piece are on the left edge. There are two ways for the L-piece to cover two squares on the left edge. However, since the bottom-left corner must be covered by an L-piece, the top-left corner piece cannot cover three squares in the middle row. So, the top-left corner is covered by an L-piece that has three squares on the top edge. Finally, the bottom-left corner must be covered by an L-piece and the only way this can be placed is with three squares on the bottom edge. This leaves the square in the $(2, 2)$ position surrounded by squares already covered, so no L-piece can cover this square! □

Case $k = 1$: By the claim above, any tiling of the 3×4 chessboard must include an L-piece covering three squares of the left edge. Also, the tiling must include an L-piece covering three squares of the right edge. These L-pieces are either arranged such that they cover adjacent squares, or do not. When they cover adjacent squares, the four squares not covered by these two pieces form a 2×2 chessboard, which cannot fit an L-piece. When they do not cover adjacent squares, the four squares not covered by these two pieces form a 3×2 chessboard with two opposite corners missing, which cannot fit an L-piece. Therefore, there is no tiling of the 3×4 chessboard.



Covering Adjacent Squares



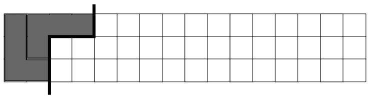
Not Covering Adjacent Squares

(Induction Hypothesis) Suppose that the statement is true for all odd values of k with $k < K$ for some $K > 1$.

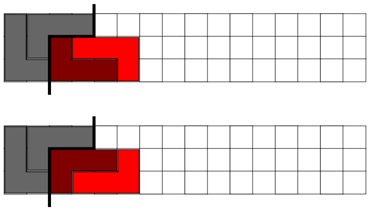
Case K: Suppose that we have a tiling of the $3 \times 4K$ chessboard using L-pieces. If an L-piece is placed vertically so it covers all three rows of the chessboard, then the tiling of the $3 \times 4K$ chessboard partitions into tilings of a $3 \times m$ chessboard and a $3 \times (4K - m)$ chessboard, for some m. Since L-pieces cover 4 squares each, these tilings cover a multiple of 4 squares, so $3m$ is a multiple of 4 and therefore $m = 4n$ for some integer n. Finally, this implies that the $3 \times 4n$ chessboard and the $3 \times 4(K - n)$ chessboard are tiled using L-pieces. Since K is odd, one of n or $K - n$ is odd. Suppose without loss of generality, n is odd, but by the induction hypothesis the $3 \times 4n$ chessboard cannot be tiled using L-pieces.

Therefore, no L-piece is placed vertically to cover all three rows of the chessboard, except for the left-most edge and the right-most edge.

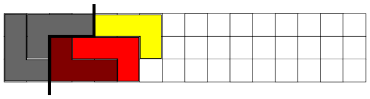
We now investigate our tiling, starting on the left edge. As claimed, all three squares on this edge are covered by the same L-piece. Since the square in the (2,2) position must be covered by an L-piece, the only arrangement of an L-piece covering this square without immediately making a tiling impossible is to have that L-piece cover the other open position in the second column. Therefore, we definitely have a tiling that looks like the below (or its vertical mirror).



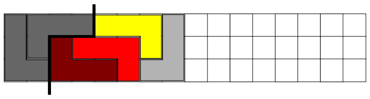
We now consider how the (3,3) position is covered. Note that if it is covered by an L-piece without also covering the (2,3) position, the (2,3) position cannot be covered by an L-piece. Thus, both the (3,3) and (3,2) positions are covered by the same L-piece. There are two options to cover these two by a single L-piece, and they each "force" another L-piece, as in the pictures below.



Observe that both options cover the same set of squares, so we can take either option. We now consider how the (1,5) position is covered, and there is exactly one option.

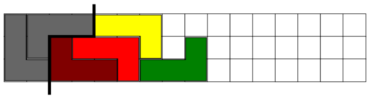


Given this set of covered squares, we can now consider the (3,7) position. This cannot be covered by an L-piece that covers all three rows (as below) because that would create a vertical L-piece, which we demonstrated does not exist.

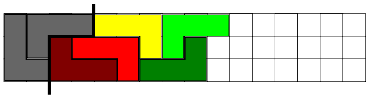


Bad example!

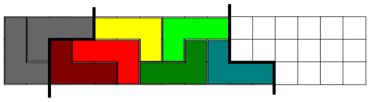
Therefore, the L-piece covering the (3,7) position covers three squares on the bottom edge.



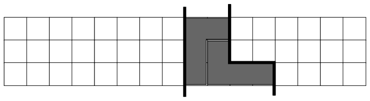
This forces the (2,8) position to be covered by an L-piece that has three squares on the top edge.



Now consider how the (2,10) position is covered by an L-piece. If it is covered by an L-piece that does not have three squares on the bottom row, observe that the tiling cannot continue in one or two more placements of L-pieces [I know this is sketchy, but its' getting late]. Thus, the (2,10) position is covered by an L-piece covering three squares on the bottom row, as in the picture below.



Now, see the two thick black lines. If we remove all of the L-pieces between them and take the two L-pieces on the left, flip them vertically, they fit nicely with the rest of the tiling to the right. See the picture below.



Therefore, our tiling of the $3 \times 4K$ chessboard gives us a way to tile the $3 \times 4(K-2)$ chessboard. However, our induction hypothesis claims this is impossible, so we have a contradiction! □