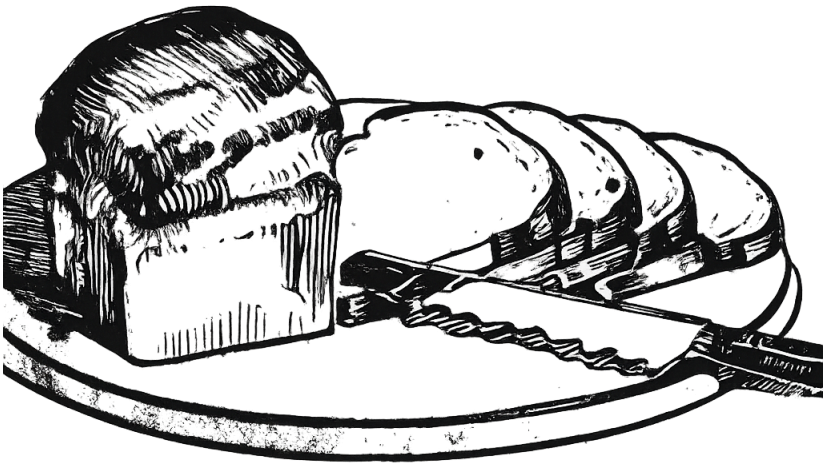
Math Meals:
Platters of Mathematics With Sides of Computer Science



As a math major, I think about math a lot. It includes the fifty hours of classes per week and the random times I spend hanging out in the math lounge. Now that I am nearing the end of my undergraduate years, I want a way to savor the topics I learned and look back at them. The following is a compilation of some of the projects along with my favorite ideas I have seen in classes and problem sets. Currently, the style is closer to raw notes instead of polished write-ups, though I have ideas of turning them into a blog later. Maybe some of them will resonate with you as they did with me :)

I am always open to questions/comments/mistakes you catch: henry.siegel17@gmail.com

On the Menu

Part I

Projects

1 Pebbling Around

1.1 Abstract

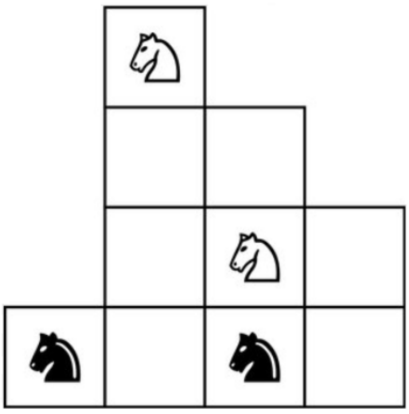
Given a chessboard, can a knight tour every square exactly once? Conrad (1994) showed that for square chessboards this problem can be determined in linear time, but for general chessboards with holes, McGown (2002) showed that it is NP-hard. It is natural to ask how the hardness of the problem changes with board restrictions. One of the main new results of this paper is showing that the problem remains NP-hard for connected chessboards. We also show that determining closed knight tours is NP-hard on connected chessboards, that is a tour that returns to the start.

The knight's tour and closed knight's tour are instances of the Hamiltonian Cycles and Hamiltonian Path problem for knights graph. We also study Pebble Motion Problems in the context of knight graphs, and look at a specific instance of the Pebble Motion Problem where two colors of pebbles are swapped. We present a short reduction from the Hamiltonian Cycle problem on bipartite graphs to the Pebble Swap Problem, showing that the problem is NP-hard. Then we apply the reduction when restricted to knight graphs generated by connected chessboards, proving that the Pebble Swap Problem is NP-hard for these graphs.

1.2 Introduction

Pebble Motion Problems ask how pebbles placed on vertices of a graph can move around constrained to some rules. They ask the question of whether one configuration of pebbles is reachable from another and, if it is possible, is there an optimal number of moves. These types of problem are important in distributed systems, where it is of interest to move packets over a network in an optimal way. Several variants of this problem have been studied, such as when each pebble is distinct. Kornhauser (1984) gave an algorithm that determines the feasibility of any two configurations and constructs a solution in $O(n^3)$ number of moves.

Variants of Pebble Motion Problems also appear as recreational puzzles. In the image below, can you swap the black and white knights and find an optimal sequence of moves? This specific puzzle appeared in a video game called



Goal: *Exchange the positions of the black and white knights*

The Eleventh Hour. The knights can be thought of as pebbles on a graph. There are two colors of unlabeled pebbles, and the goal is the swap the black and white colors in an optimal number of moves. This is a variant of the pebble motion problem, which I call the pebble swap problem, which we will study, and by the end of the paper, we will be able to classify the hardness of this problem.

Knights graphs have been studied extensively in the literature. Some classic problems are determining a knight's tour on the graph, which is a Hamiltonian Path on knight's graph. One can ask the analogous question for closed knight's tour, which is a Hamiltonian Cycle. This problem ranges from linear time to NP-hard depending on the graphs that are restricted. Conrad (1994) show that there is a linear time decider for square chessboards, and McGown (2002) show that it is NP-hard.

Definitions:

- **A Hamiltonian Path** is a path that visits every vertex in the graph exactly once.
- **A Hamiltonian Cycle** is a cycle in the path that includes every vertex exactly once.

1.3 The Pebble Swap Problem for General Graphs

We start with a formal definition of the problem.

Definitions:

- Given a graph with vertex set V, a **configuration** is a function $\mathcal{C} : V \to \{-1, 0, 1\}$ that can be thought of as the pebble assignment function where vertices mapped to -1 are occupied by a black pebble, vertices mapped to 1 are occupied by a white pebble, and vertices mapped to 0 are empty.
- A **move** is the ordered pair of configurations $(\mathcal{C}_1, \mathcal{C}_2)$ such that there exists $uv \in E$ such that $\mathcal{C}_1 \equiv \mathcal{C}_2$ on $V \setminus uv$, and $\mathcal{C}_1(v) = \mathcal{C}_2(u) = 0$ and $\mathcal{C}_1(u) = \mathcal{C}_2(v) \neq 0$.
  For brevity, we will denote a move as $u \to v$, where the pebble on u moves to v.
- A **plan** is a sequence of moves of the form $\langle(\mathcal{C}_0, \mathcal{C}_1), (\mathcal{C}_1, \mathcal{C}_2), \cdots, (\mathcal{C}_{k-2}, \mathcal{C}_{k-1}), (\mathcal{C}_{k-1}, \mathcal{C}_k)\rangle$. We say that the plan **transforms** $\mathcal{C}_0$ to $\mathcal{C}_k$.

Pebble Swap Problem: Given a graph G, a configuration $\mathcal{C}$ and a natural number k, is there a plan of length k that transforms $\mathcal{C}$ into $\mathcal{C}'$ so that $\mathcal{C} \equiv -\mathcal{C}'$ (the white and black pebbles have swapped places).

As shown in [**Akiyama**], determining if there is a Hamiltonian Cycle in a bipartite graph is NP-Hard. We will show that there is a polynomial time reduction from the Hamiltonian Cycle problem to the Pebble Swap Problem, showing that the Pebble Swap Problem is NP-hard.

Theorem 1.1. ***The Pebble Swap Decision Problem is NP-Hard.***

Proof. Suppose the input graph is $G = (V, E)$.

We will construct the modified graph $G' = (V', E')$ as follows: Set the new vertex set V' to include all the original vertices with two extra vertices: $V' = V \cup \{x, y\}$, where $x, y \notin V$. Fix an arbitrary $v_0 \in V^+$ and add edges v_0x and v_0y. The new edge set E' contains all the original edges in E in addition to these two extra edges:

Let V^-, V^+ be the two bipartite sets of V. Place black pebbles on all the vertices in V^- and white pebbles on all the vertices in V^+.

$$\mathcal{C}(v) = \begin{cases} 1 \text{ if } v \in V^+ \\ -1 \text{ if } v \in V^- \\ 0 \text{ if } v \in \{x, y\} \end{cases}$$

Then our transformation is $G \to (G', \mathcal{C}, n + 4)$.

Polynomial Time Reduction:

There are $O(n^2)$ edges to construct, and $O(n)$ vertices to construct in G'.

1.3.1 The existence of Hamiltonian Cycle $\implies$ There is a plan of n+4 moves to swap the pebbles.

Suppose $v_0v_1v_2\cdots v_{n-1}v_0$ is a Hamiltonian cycle in the input graph. (I counted up to $n-1$ because there are n vertices and we're starting at 0). Recall that v_0 is the "special" vertex that has edges v_0x and v_0y. Table 1 shows a plan of $n+4$ moves to swap the black and white pebbles on G'. For clarity, Figure 2 illustrates the plan if G is a four-cycle.

move #	move	Configuration
0	Initial	$\langle 0, 0, 1, -1, 1, \cdots, -1\rangle$
1	$(v_0 \to x)$	$\langle 1, 0, 0, -1, 1, \cdots, -1\rangle$
2 ... n	$(v_1 \to v_0)$ $(v_2 \to v_1)$, ..., $(v_{n-1} \to v_{n-2})$	$\langle 1, 0, -1, 1, -1, \cdots, 0\rangle$
n+1	$(v_0 \to y)$	$\langle 1, -1, 0, 1, -1, \cdots, 0\rangle$
n+2	$(x \to v_0)$	$\langle 0, -1, 1, 1, -1, \cdots, 0\rangle$
n+3	$(v_0 \to v_{n-1})$	$\langle 0, -1, 0, 1, -1, \ldots, 1\rangle$
n+4	$(y \to v_0)$	$\langle 0, 0, -1, 1, -1, \cdots, 1\rangle$

Table 1: The configurations are $\langle \mathcal{C}(x), \mathcal{C}(y), \mathcal{C}(v_0), \cdots, \mathcal{C}(v_{n-1})\rangle$. The white and black pebbles have swapped because the starting and ending configurations are opposite.

1.3.2 The Existence of a plan of n+4 moves to swap pebbles $\implies$ Existence of Hamiltonian Cycle

This is a careful counting argument. For any plan that swaps the black and white pebbles, we can analyze how the holes that start from x and y evolve after each move. We define the *ith* index of trajectories traj(x) (traj(y)) as the position of the hole starting from x (y) after it has moved i times as a result of moves.

traj$(x) := x_0x_1, \cdots x_j$

traj$(y) := y_0y_1, \cdots y_k$

Note that the length of the plan is $j + k$.

Lemma 1.2.

1. $x_0, x_j, y_0, y_k \in \{x, y\}$.
2. $j, k > 0$.
3. *The union of trajectories x and y visits every vertex in V: $v_0, v_1, \cdots, v_{n-1}$.*

Proof. Recall $V = \{v_0, v_1, \cdots v_{n-1}\} = V' \setminus \{x, y\}$ and $v_0 \in V^+$.

1. Every $v \in V$ starts with a pebble, so the holes must start and return to x and y.
2. Without loss of generality, suppose a plan didn't use y. Then the pebble at v_0 can only shift between x and v_0. Both of these vertices aren't in V^-, which is where it needs to be after the plan.
3. For each $v \in V$, a different pebble starts and ends there. Thus, there must have been a hole there at some point, so a pebble could move there.

□

By the first two parts of lemma 1.3.2, trajectories x and y take the form: traj$(x) = xv_0P_xu$ and traj$(y) = yv_0P_yv$ where $u, v \in \{x, y\}$, and P_x and P_y are paths of even length that end with v_0 (they could be empty). If there was a plan of length $n+4$ that swapped the pebbles, then I claim that P_x or P_y is empty. Suppose not. Then the trajectories take the form: traj$(x) = xv_0P'_xv_0u$ and traj$(y) = yv_0P'_yv_0v$ where $P'_xv_0 = P_x$ and $P'_yv_0 = P_y$. By the third part of lemma 1.3.2, $P'_x \cup P'_y = \{v_1, \cdots v_{n-1}\}$, so $|P'_x| + |P'_y| \geq n-1$. The length of the plan is $j+k = |\text{traj}(x)| + |\text{traj}(x)| - 2$. Note that $|\text{traj}(x)| + |\text{traj}(y)| = 8 + |P'_x| + |P'_y|$ which includes the four total visits of v_0, and one visit each of x, y, u and v. Thus, $|P'_x| + |P'_y| \geq n-1$ implies that the sum of the lengths of the trajectories is greater than $n+4$. This is a contradiction, so P_x or P_y is empty.

We can assume without loss of generality that P_y is empty, and P_x visits $v_1, \cdots, v_{n-1}$. Each vertex appears exactly once in P_x because if a vertex occured more than once, P_x would be longer than $n-1$, contradicting the fact that the plan contains $n+4$ moves. Therefore, each vertex occurs exactly once and v_{n-1} is connected to v_0, so we have a Hamiltonian cycle. There is a small technicality when $n = 2$, but we can assume that all input graphs have at least four vertices. □

Remark:

There are certainly input graphs that do not have Hamiltonian Cycles, and it is possible to swap the black and white pebbles on the transformed graph using more than $n+4$ moves. Figure 1 shows an example.

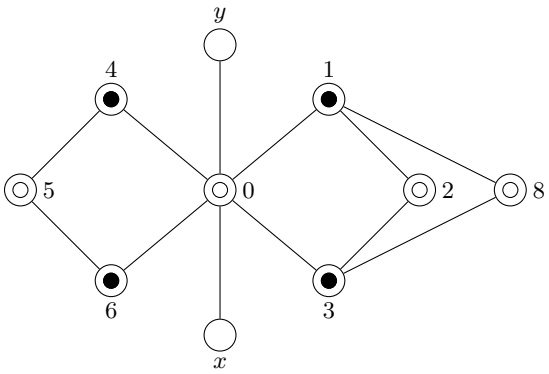


Figure 1: One can check that it is possible to swap the black and white pebbles on G', but there is no Hamiltonian Cycle in G. Note that traj(x) and traj(y) both have length more than 2 for any plan that swaps the colors, so the length of the plan must be longer than 12 moves.

1.4 NP hard problems on Knight Graphs

We now restrict our attention to knight graphs. One goal we have is proving that the Pebble Swap Problem on these restricted graphs is still NP-hard.

Definitions:

- **A chessboard with holes** is a rectangular lattice of squares with some subset of squares removed.
- **A connected chessboard** is a chessboard with holes with the property that a rook can travel between any two squares in some number of moves.
- The **knight graph** of a chessboard is a graph such that the vertices are the squares of the chessboard, and the edges are the pairs of squares so that a knight can move between them in one move.
- A **knight's tour** is a Hamiltonian path on a knight graph.
- A **closed knight's tour** is a Hamiltonian cycle on a knight graph.

Any knight graph is a bipartite graph, so if we can show that finding a closed knight tour is NP-hard, then we can consider applying the reduction in the previous section to show that Pebble Swap is NP-hard on knight graphs. This will be the direction we will take, but there is a caveat. For any connected chessboard, it is not true that we can apply the same transformation to the knight graph by attaching two vertices to a unique vertex because the structure of the knight graph depends on the geometry of the board. For some connected chessboards, in fact, it is impossible to add two squares a knights distance away from a unique square, as shown in figure 9, but this is not an issue. As we will show, all instances of connected chessboards that we build will have this nice property. Alas, we begin our analysis on knight's tours and closed knight's tours.

[**McGown et. al.**] show that the knight's tour problem with holes is NP-complete. They also conjecture that finding a knight's tour on a connected chessboard is NP-hard, a more restricted kind of chessboard. Inspired by their original construction, I offer a new construction that shows the hardness result for connected boards. The team reduced from the Hamiltonian Paths decision problem in grid graphs which was shown to be NP-hard by [**Itai et. al.**]. We will also reduce from the Hamiltonian paths decision problem in Grid Graphs to show that knight's tours in connected chessboards is NP-hard. To show that the closed knight tours in connected chessboards is NP hard, we will reduce the decision problem of finding Hamiltonian cycles in Grid Graphs, which was shown to be NP hard by [ML02]. (NOTE TO UPDATE CITATION)The same reduction will be used to prove the hardness of both problems.

1.5 The polynomial reduction from Grid Graphs

Given an input grid graph, each vertex in the grid is replaced by a chessboard in the transformation. Let's call this mapping $a \to g(a)$, where a is the vertex in the grid graph, and $g(a)$ is its corresponding chessboard. The precise shape of each chessboard depends on the edge set of the vertex and its position in the grid graph.

Here is how we will define $a \to g(a)$
Define the partition (A,B) on the vertex set as follows: Let (a, b) be the coordinates of a vertex in the grid graph. If $a + b$ is even, then put (a, b) in A, otherwise put (a, b) in B. First, consider v in A. Assign v a four bit string $b_1b_2b_3b_4$ denoting the edges among the four possible edges that are present. b_i is 1 if and only if the ith edge is present. The directions 1, 2, 3, and 4 are up, right, down, and left, respectively. If v is on the edge of the grid, say, direction i goes out of bounds, then assign $b_i \leftarrow 1$. This distinction for edge vertices is necessary for when we show that pebble swap is NP-hard on connected knight graphs. There are 16 total chessboards, and the edge string of v determines the board that v is mapped to. For the complete mapping, see tables 2 and 3.

Now consider $v \in B$. Its edge string is $b_2b_1b_4b_3$. More clearly, if there was a vertex $u \in A$ with edge string $b_1b_2b_3b_4$ and u and v have the same edges, then the edge string of v would be $b_2b_1b_3b_2$. Let Q be the chessboard from this bit string, in matrix form, where 1 is a square and 0 is a hole. Rotate the elements of Q about the center square halfway around (reverse the rows and columns of Q), and then apply the transpose operation. Map v with the resulting board.

We will glue the chessboards together so that if a shares a vertical edge with b in the grid graph (and a is higher than b), the center of $g(a)$ is situated 9 units above $g(b)$. Perform an analogous procedure for horizontal edges. Finally, we define the total chessboard to be all the glued together pieces. Then a and b share an edge if and only if $g(a)$ and $g(b)$ share a two square bridge in the total chessboard. Hence, the grid graph is connected if and only if the total chessboard is connected. We can assume that we are working with connected grid graphs because otherwise we can check in polynomial time that the grid graph is not connected, and there is no Hamiltonian cycle and path. For a concrete example of a grid graph with the transformation, see figure 3.

1.5.1 Hamiltonian Cycle in grid graph $\implies$ Closed Knight Tour.

Suppose that we have a Hamiltonian cycle in the grid graph. We want to show that there is a closed knight tour. For all adjacent edges in the cycle, xy and yz, there is one square in $g(y)$ that the knight can use to go from $g(x)$ to $g(y)$, and a different square that the knight can use to go from $g(y)$ to $g(z)$. We need to show that there is a knight's tour in $g(y)$ that starts and ends at these two transition squares. Figures 4, 5, 6, and 7 enumerate all the cases for the chessboards coming from the vertices in A. The chessboards coming from the vertices in B are reversed and transposed versions of type A chessboards, so they also have a knight tour between any two transition square. Glue all these knight's tours together and we get a closed knight's tour on the total chessboard.

1.5.2 Closed Knight Tour $\implies$ Hamiltonian Cycle in grid graph

We adapt a lemma used in [ML02].

Suppose that we have a closed knight tour. In order to show that there is a Hamiltonian Cycle in the grid graph, we need to argue two things: the closed knight tour visits every vertex in the grid graph, and it visits each vertex exactly once. The first claim is true because the knight needs to reach every chessboard to hit all the squares. To prove the second claim, note that for any vertex in the grid graph, the closed knight tour cannot pass through it twice. This is because every time a knight enters and leaves a vertex, it does so by passing through the same colored square, let us say a dark square (without loss of generality). Since a knight alternates between dark and light squares, for each pass through a board, the number of dark squares used by the knight is one more than the number of light squares. If a closed knight tour passed through a vertex at least twice, there would have to be at least two more dark vertices than light vertices. This is a contradiction because for every $g(v)$, there is exactly one more dark square than light square. Once the knight enters $g(v)$ it must traverse through every square there before leaving. The knight can travel from $g(v)$ to $g(w)$ if and only if there is an edge between v and w in the grid graph. We showed that the closed knight tour visits all the chessboards in the order $g(v_1)g(v_2)\dots g(v_n)g(v_1)$, so therefore $v_1v_2\dots v_nv_1$ is a Hamiltonian Cycle in the grid graph.

Theorem 1.3. *The closed knight's tour problem in connected chessboards is NP-hard.*

Proof. All that is left is to prove that this reduction is polynomial time. For every v, $g(v)$ is a 9 by 9 tile, so the number of squares on the total chessboard is linear with the number of vertices on the grid graph. Checking for the position of a vertex and determining its edges can be done in polynomial time. □

Theorem 1.4. *The knight's tour problem in connected chessboards is NP-hard.*

Proof. Repeat the argument in [ML02] for this construction. With their nomenclature, the even squares refer to the dark squares, and the odd squares refer to the light squares. □

Theorem 1.5. *The pebble swap problem on knight graphs generated by connected chessboards is NP-hard.*

Proof. Let us use the terminology that a connected chessboard is nicely extendable if we can attatch two additional vertices to a unique vertex in the associated knight graph, in such a way that the resulting chessboard is still connected. Additional squares may also be added as long as they are isolated vertices in the knight's graph, since we can keep them as holes, and no pebbles can move there. All the chessboards in the reduction are nicely extendable due to the shape of $g(v)$ for the vertices v located on the right edge of the grid graph. The details are shown in figure 8. We can conclude that the closed knight's tour problem is NP-hard for nicely extendable connected chessboards. Thus, we can apply the analogous reduction from Hamiltonian Cycles on bipartite graphs to the pebble swap problem to show that the pebble swap problem is NP-hard on knight graphs for connected chess boards that are nicely extendable. The set of all connected chessboards is a superset of those that are nicely extendable, so the pebble swap problem is NP-hard for connected chessboards. □

Corollary 1.6. *This implies that the pebble Swap Problem on (all) knight graphs is NP-hard.*

Corollary 1.7. *All of the problems are also NP-complete on knight graphs because they are each NP.*

1.6 Possible Future Directions

1. Which other classical NP-hard problems are still NP-hard when restricted to knight graphs?
2. One can continue exploring the difficulty of the knight tour problem for more restrictive classes of graphs. For example, one natural extension is to define the area measuring map μ on connected chessboards as:

$$\mu(X) = \frac{\sum_{x\in X} \max\{Area(R) : R \subseteq X \text{ is a rectangle containing } x\}}{|X|^2}$$

   $\mu \leq 1$, and $\mu = 1$ if and only if X is a rectangular chessboard. μ is minimized when X is a staircase.
3. This relates to the last remark: Suppose that we change the way a knight moves, so that it jumps $(\pm x, \pm y)$ for some $x, y \in \mathbb{N}$. Would the problems we studied still be NP-hard on this modified knight graph? What if the knight's move took the form $(\pm x_1, \cdots, \pm x_k)$, so chess is played in k dimensions.

References

[1] T. Akiyama, T. Nishizeki, and N. Saito. *NP-completeness of the Hamiltonian cycle problem for bipartite graphs. Journal of Information Processing*, 3:73–76, 1980.

[2] K. McGown and A. Leininger. *Knight's Tour.* Oregon State University REU Proceedings, August 15, 2002.

[3] A. Itai, C. H. Papadimitriou, and J. L. Szwarcfiter. *Hamiltonian Paths in Grid Graphs.* SIAM Journal on Computing, 11(4):676–686, November 1982.

[4] E. D. Demaine and M. Rudoy. *Hamiltonicity is Hard in Thin or Polygonal Grid Graphs, but Easy in Thin Polygonal Grid Graphs.* arXiv preprint arXiv:1706.10046, June 2017.

[5] A. Conrad, T. Hindrichs, H. Morsy, and I. Wegener. *Solution of the knight's Hamiltonian path problem on chessboards. Discrete Applied Mathematics*, 50(2):125–134, 1994.

[6] D. M. Kornhauser, G. L. Miller, and P. G. Spirakis. *Coordinating Pebble Motion on Graphs, the Diameter of Permutation Groups, and Applications.* MIT Laboratory for Computer Science Technical Report MIT-LCS-TR-320, 1984.

1.7 Appendix

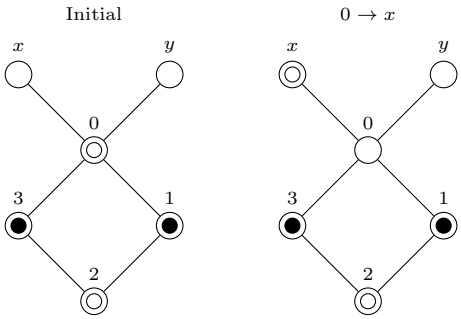
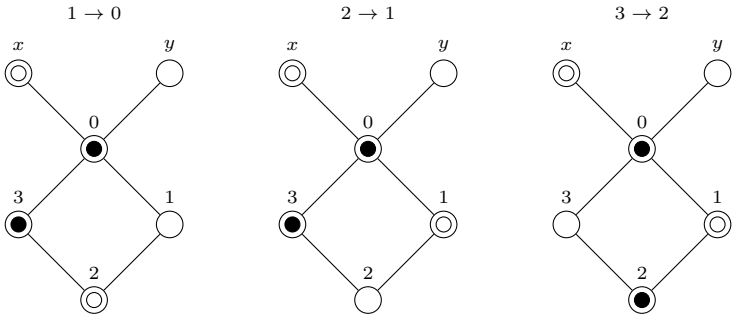
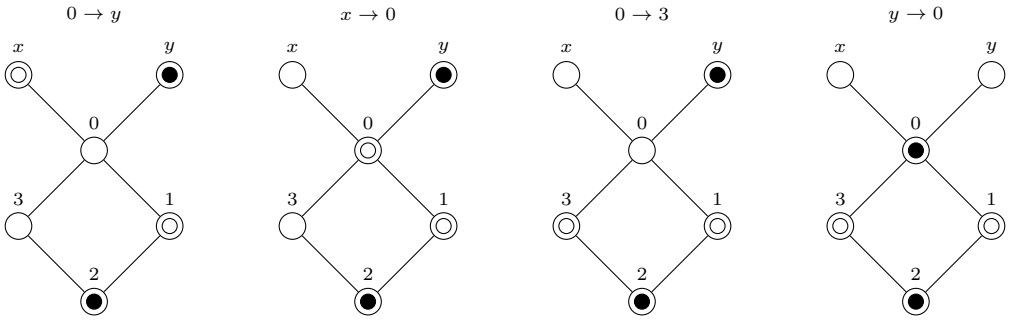
Move #	Picture
0 through 1:	
2 through n:	
n+1 through n+4:	

Figure 2: G is a four-cycle, and G' contains two additional vertices x and y attached to 0 as shown. In this example, $n = 4$.

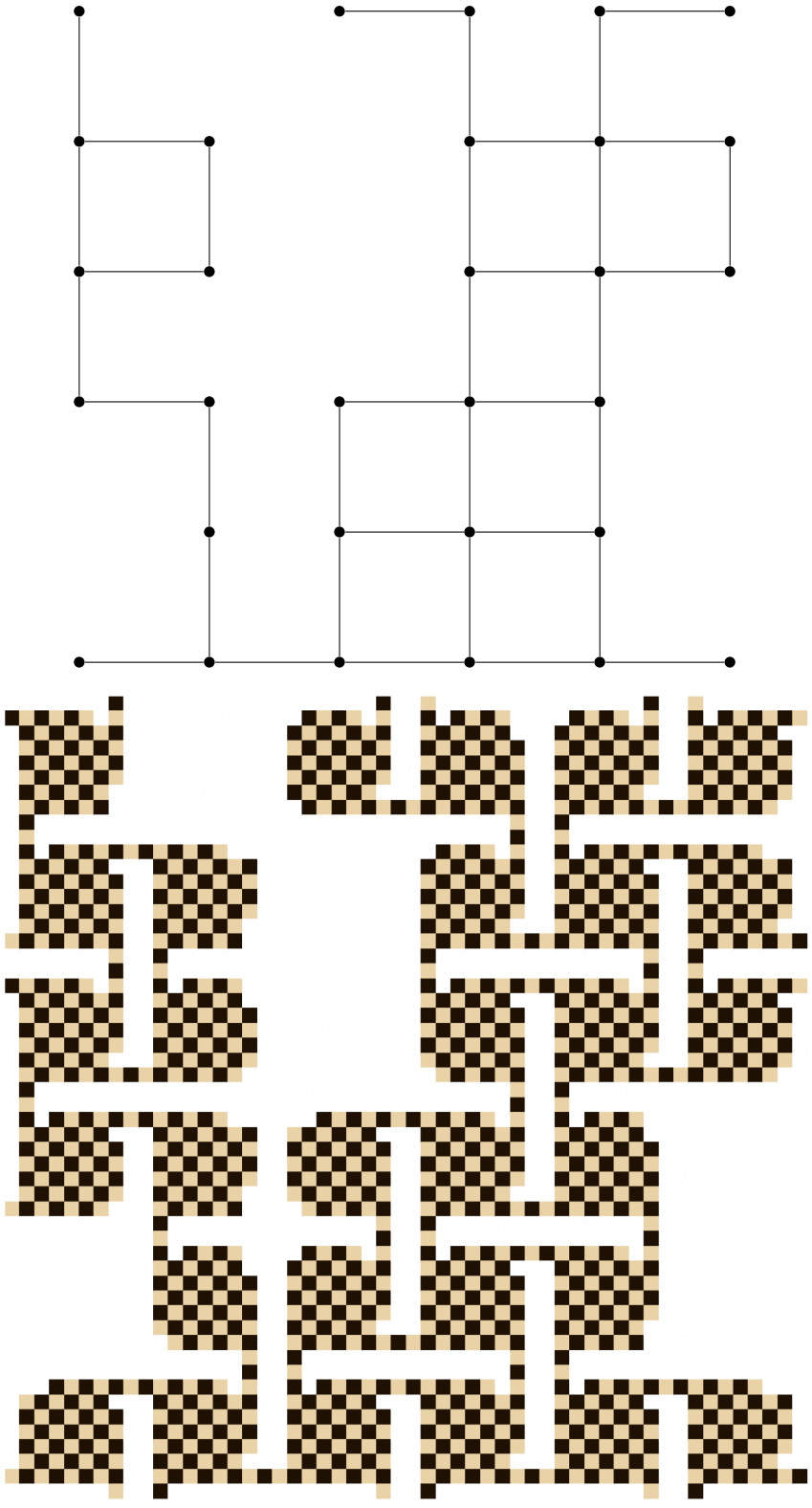


Figure 3: A grid graph and the resulting construction is shown. Each vertex in the grid graph gets mapped to a 9 by 9 chessboard with holes. There is only one way to get between any two adjacent chessboards that are connected by an edge in the grid graph, and there is no way to get between them if they are not connected. Also notice that all the transition squares are the same color, and the number of squares of this color is the majority by 1 for each chessboard.

Edges	Board	Edges	Board
(0,0,0,0)	$\begin{pmatrix}0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}$	(1,0,0,0)	$\begin{pmatrix}0&0&0&0&0&0&0&1&0\\0&0&1&1&1&1&0&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}$
(0,0,0,1)	$\begin{pmatrix}0&0&0&0&0&0&0&0&0\\1&1&1&1&1&1&0&0&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}$	(1,0,0,1)	$\begin{pmatrix}0&0&0&0&0&0&0&1&0\\1&1&1&1&1&1&0&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}$
(0,0,1,0)	$\begin{pmatrix}0&0&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&1&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&0\end{pmatrix}$	(1,0,1,0)	$\begin{pmatrix}0&0&0&0&0&0&0&1&0\\0&0&1&1&1&1&0&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&1&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&0\end{pmatrix}$
(0,0,1,1)	$\begin{pmatrix}0&0&0&0&0&0&0&0&0\\1&1&1&1&1&1&0&0&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&1&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&0\end{pmatrix}$	(1,0,1,1)	$\begin{pmatrix}0&0&0&0&0&0&0&1&0\\1&1&1&1&1&1&0&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&1&0\\0&1&1&1&1&1&1&0&0\\0&1&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&0\end{pmatrix}$

Table 2: The mapping between edge strings and boards are shown above where the edge strings are in the order (up, right, down, left). For the edges, a 1 indicates the presence of an edge in that direction, and 0 indicates the absence of an edge. For the boards, a 1 indicates the presence of a square, and a 0 indicates the absence of a square. The (1,1,1,1) board has four transition squares. To construct the other boards whenever an edge isn't present we delete the square sticking out and one adjacent square next to it. That way, the number of dark and light squares are conserved, and there is no longer a transition square for that edge. No Hamiltonian Cycle or Path will include an isolated vertex, so (0,0,0,0) is mapped to the empty board. The mappings are continued in the next table.

Edges	Board	Edges	Board
(0,1,0,0)	$\begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}$	(1,1,0,0)	$\begin{pmatrix} 0&0&0&0&0&0&0&1&0 \\ 0&0&1&1&1&1&0&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}$
(0,1,0,1)	$\begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}$	(1,1,0,1)	$\begin{pmatrix} 0&0&0&0&0&0&0&1&0 \\ 1&1&1&1&1&1&0&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}$
(0,1,1,0)	$\begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&1&1&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0 \end{pmatrix}$	(1,1,1,0)	$\begin{pmatrix} 0&0&0&0&0&0&0&1&0 \\ 0&0&1&1&1&1&0&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&1&1&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0 \end{pmatrix}$
(0,1,1,1)	$\begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&1&1&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0 \end{pmatrix}$	(1,1,1,1)	$\begin{pmatrix} 0&0&0&0&0&0&0&1&0 \\ 1&1&1&1&1&1&0&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&0&0 \\ 0&1&1&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0 \end{pmatrix}$

Table 3: The rest of the mappings between edge strings and boards are shown above.

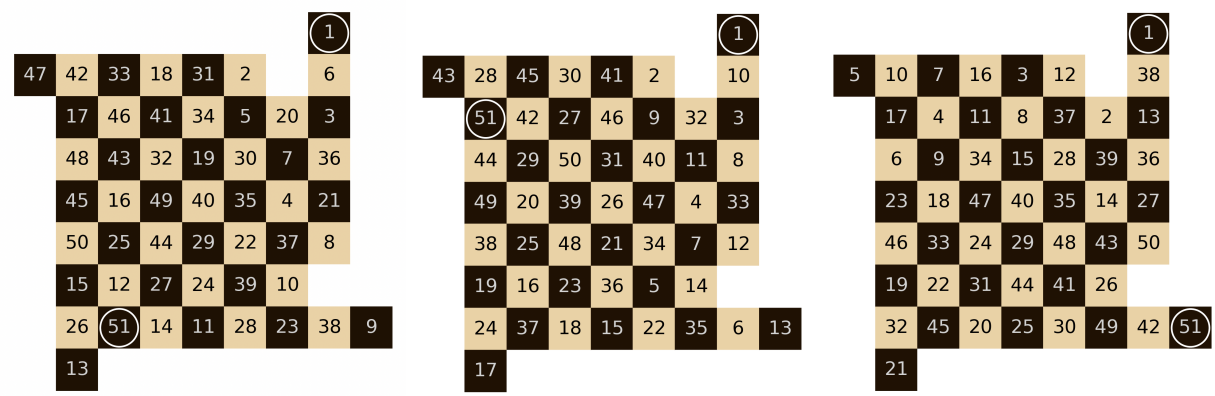


Figure 4: A board is $k-$connected if its vertex in the grid graph has k edges. Transition squares are entry/leaving points to other chessboards. For every pair of transition squares on the unique 4-connected board up to symmetry, there is a knight's tour. The visit times on each square is enumerated, and transition squares are circled.

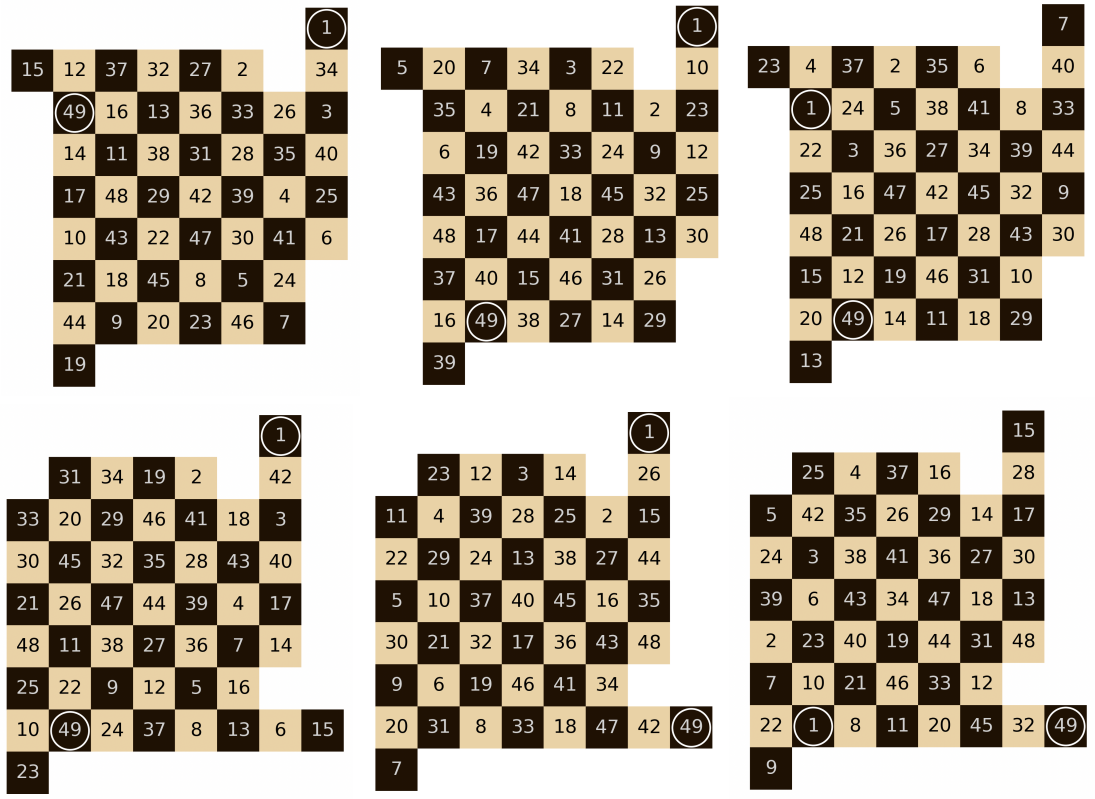


Figure 5: For every pair of transition squares on two 3-connected board up to symmetry, there is a knight's tour.

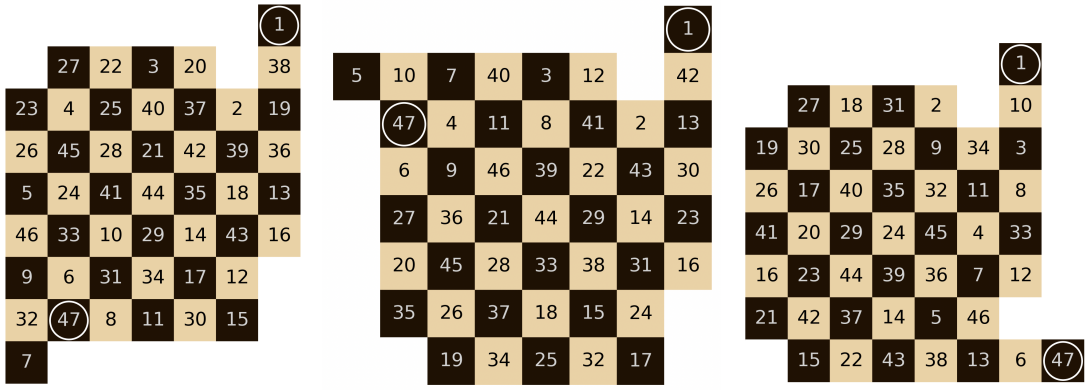


Figure 6: For every pair of transition squares on three 2-connected board up to symmetry, there is a knight's tour.

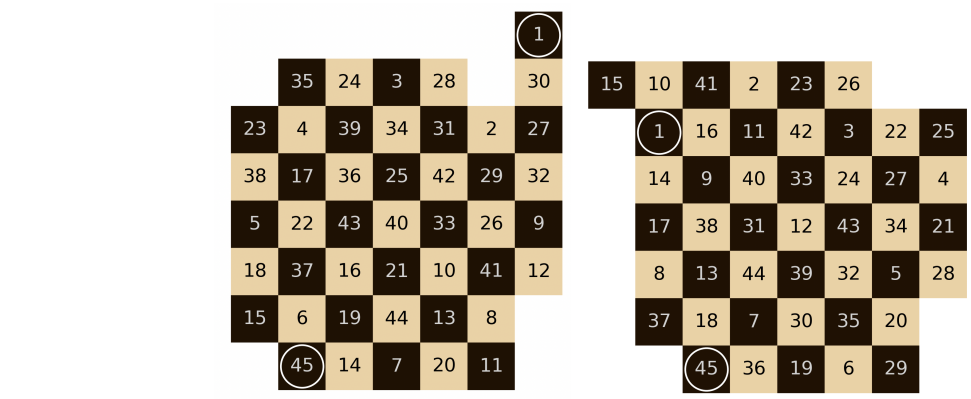


Figure 7: For both types of 1-connected boards, up to symmetry, there is a knight's tour starting on the transition square. For these boards, we only care about the starting square being a transition square because any knight tour that enters has to stay here.

This is an exhaustive list for all chessboards up to symmetry. What we showed is that for all possible pairs of adjacent edges on a Hamiltonian Cycle/Path, there is a knight's tour between the two transition squares on the chessboard that came from the vertex the edges are incident to.

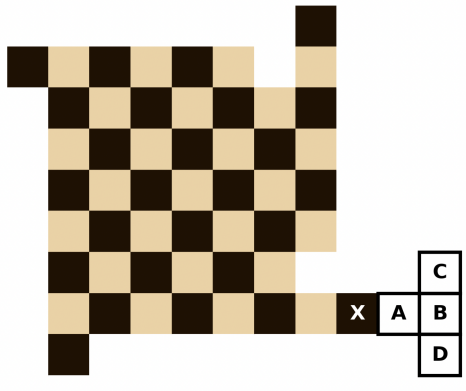


Figure 8: In our reduction, the chessboards coming from vertices on the right edge contain arm X, or a flipped version of it. When we reduce to pebble swap, we select one chessboard on the right edge and add squares A, B, C, and D. In this way, X is the only square that is a knight's distance away from C and D, while A and B are isolated vertices in the knight's graph, so their existence doesn't change the way the pebble swap reduction works: we leave A and B as holes (do not place any pebbles on them). The new chessboard is still connected. Finding vertex X can be done in polynomial time.

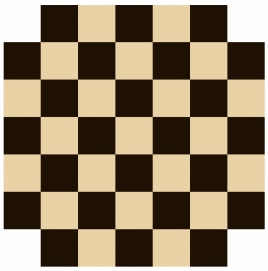


Figure 9: Shown above is an example of a chessboard that cannot be nicely extended. No matter how two additional squares are added, there are at least two squares in the original chessboard that are a knight's distance away from one of them. We don't build chessboards like this in our reduction, so this is not a problem.

1.8 My Burden of Dreams

I was introduced to this puzzle by my cousin who directed me to an interview by the Field Medalist June Huh, who explained how it related to his work on chromatic polynomials on graphs. It was the summer after high school, and I wanted a challenging problem to think about. After scribbling down a solution to the original puzzle above, I became curious about whether we could generalize the problem: given an arbitrary number of pairs of knights on a general graph, find an optimal solution. But finding such an algorithm eluded me for the summer. It just seemed like the problem was "impossibly difficult", but I could not formalize how at the time.

I don't know why, but this problem keeps drawing me back to it. It's just so...approachable yet annoyingly complicated at the same time. Having taken relevant courses in college, I also wanted to approach it with greater rigor and apply what I learned.

2 Mordell Curves - A Tourist Guide - And More

Introduction

Coined by the French mathematician Louis Mordell, Mordell curves refer to the broad family of integer equations of the form $a^2 = b^3 + k$ for some fixed non-zero integer k. Mordell was able to prove some remarkable properties, like for instance, there is only a finite number of solutions for any k. This was a two week-long project that I immersed myself in before taking a Number Theory course. I tried to make the following notes an honest transcription of what I found out then with some sprinkles on top.

2.1 Some specific values of k

2.1.1 Consider the case $k = 1$: $a^2 = b^3 + 1$

Theorem 2.1. *The only integral solutions (a, b) to $a^2 = b^3 + 1$ are $(\pm 1, 0), (0, -1), (\pm 3, 2)$*

Proof.

$$a^2 = b^3 + 1 \iff a^2 = (b+1)(b^2 - b + 1) = t(t^2 - 3t + 3) \text{ where } t = b + 1$$

If $a = 0$, we get the solution, $\boxed{(a, b) = (0, -1)}$ If $a \neq 0$, then a^2 has a unique prime factorization of the form $\prod p_i^{2\ell_i} \prod q_i^{2m_i} \prod r_i^{2n_i}$, where p_i are primes that only divide t, q_i are primes that only divide $(t^2 - 3t + 3)$, and r_i are primes that divide both of them. Setting $d = \prod q_i^{m_i}$, $x = \prod p_i^{\ell_i}$, and $y = \prod q_i^{m_i}$

$$\begin{cases} t = dx^2 \\ t^2 - 3t + 3 = dy^2 \end{cases}$$

Note that $d = \gcd(t, t^2 - 3t + 3)$ and x and y are coprime.

$$d^2x^4 - 3dx^2 + 3 = dy^2$$

d must divide 3, leaving $d = 1$, or $d = 3$ the only possibilities.

Suppose $d = 1$:
We want to find the integral solutions to the equation

$$x^4 - 3x^2 + 3 = y^2$$

At first glance it looks like we're heading in the wrong direction since we now have a quartic equation. However, it turns out that the transformed equations are easier to solve despite being of higher power.

Rearranging the equation and plugging it into the quadratic formula, we find

$$x^2 = \frac{3 \pm \sqrt{(2y)^2 - 3}}{2}$$

To make x^2 an integer, $\sqrt{(2y)^2 - 3}$ must be an integer, which means $(2y)^2 - 3 = k^2$. The only two perfect squares that are a difference of 3 apart are 1 and 4, so $2y = 4 \implies \boxed{(a, b) = (\pm 1, 0)}$

Suppose $d = 3$:
We want to find the integral solutions to the equation

$$9x^4 - 9x^2 + 3 = 3y^2 \iff 3x^4 - 3x^2 + 1 = y^2$$

This case is more challenging, but fortunately there's a lot of theory on more general elliptic curves that we can use. As you can perhaps tell, this is the place where I got stuck and sought external help :p

Lemma 2.2. ***(Dolan)****:*
The only positive integral solution (X, Y, Z) *to* $X^4 - 3X^2Y^2 + 3Y^4 = Z^2$ *such that* $\gcd(X, Y, Z) = 1$ *is* $(1, 1, 1)$. *Feel free to check out* https://www.jstor.org/stable/24497284?seq=1 *for more details. The proof isn't too technical.*

The equation $x^4 - 3x^2 + 1 = y^2$ is a special case of $X^4 - 3X^2Y^2 + 3Y^4 = Z^2$ in which $X = 1, Y = x, Z = y$. $\gcd(1, x, y) = 1$, so if (x, y) was a solution such that $x > 1$ or $y > 1$ it would contradict the lemma. The only positive integral solution (x, y) to $3x^4 - 3x^2 + 1 = y^2$ is $(1, 1)$, which corresponds to $\boxed{(a, b) = (\pm 3, 2)}$

□

2.1.2 Consider the case $k = -2$: $a^2 = b^3 - 2$

This particular case was posed as a challenge to his contemporaries by the genius French mathematician Pierre de Fermat, who came up with an incredibly elaborate argument. Fortunately, the tools available in modern mathematics, such as abstract algebra, make the problem more manageable.

Theorem 2.3. *The only integral solution* (a, b) *to* $a^2 = b^3 - 2$ *is* $(\pm 5, 3)$

Proof. $a^2 = b^3 - 2 \iff (a - \sqrt{2}i)(a + \sqrt{2}i) = b^3$.

Definition. *Let* $\mathbb{Z}[\sqrt{2}i] = \{A + B\sqrt{2}i : A, B \in \mathbb{Z}\}$ *i.e. the set of all integer linear combinations of* $1, \sqrt{2}i$.

Definition. *Define "norm function"* $N : \mathbb{Z}[\sqrt{2}i] \to \mathbb{N}$ *by* $N(a + b\sqrt{2}i) = a^2 + 2b^2$.

Lemma 2.4. *For all* $x, y \in \mathbb{Z}[\sqrt{2}i], N(xy) = N(x)N(y)$.

Proof. Let $x = a + b\sqrt{2}i$ and $y = c + d\sqrt{2}i$. Then

$$N(xy) = N(ac - 2bd + (ad + bc)\sqrt{2}i) = (ac - 2bd)^2 + 2(ad + bc)^2 = (a^2 + 2b^2)(c^2 + 2d^2) = N(x)N(y)$$

□

Let $d = \gcd((a - \sqrt{2}i), (a + \sqrt{2}i))$. In this setting d is defined as the factor in $\mathbb{Z}[\sqrt{2}i]$ with the largest possible value of $N(d)$. By definition, d divides $(a - \sqrt{2}i)$ and $(a + \sqrt{2}i)$, so it must divide their difference, namely $2\sqrt{2}i$. $2\sqrt{2}i = kd$ for some $k \in Z[\sqrt{2}i]$. So $N(2\sqrt{2}i) = N(kd) = N(k)N(d)$, and therefore $N(d)$ divides $N(2\sqrt{2}i) = (2\sqrt{2})^2 = 8 \implies N(d) \in \{1, 2, 4, 8\}$.

Lemma 2.5. *a is odd*

Proof. Assume for the sake of contradiction a was even. Then b must also be even. Setting $a = 2x$, $b = 2y$ gives $4x^2 = 8y^3 - 2 \implies 2x^2 = 4y^3 - 1$. The left-hand side is divisible by 2, while the right-hand side is not, a contradiction. □

Because d divides $a + \sqrt{2}i$, it must be the case that $N(d)$ divides $N(a + \sqrt{2}i) = a^2 + 2$, which is odd by the lemma. Hence $N(d)$ must also be odd, eliminating $2, 4, 8$ as a possibility.

$N(d) = 1$ tells us that $d = \pm 1, \pm i$, so $(a + \sqrt{2}i)$ and $(a - \sqrt{2}i)$ are coprime in $\mathbb{Z}[\sqrt{2}i]$. Now a remarkable fact is that all elements in $\mathbb{Z}[\sqrt{2}i]$ can be factored uniquely as a product of primes up to reordering and multiplication of units, just like how all integer numbers can be factored uniquely into a product of primes up to reordering and sign which we used in the $k = 0$ case. Then if b^3 is a perfect cube, it must also be the case that $(a - \sqrt{2}i)$ and $(a + \sqrt{2}i)$ are both perfect cubes as well.

$(a + \sqrt{2}i) = (x + y\sqrt{2}i)^3 \implies a = x^3 - 6xy^2 = x(x^2 - 6y^2)$ and $1 = 3x^2y - 2y^3 = y(3x^2 - 2y)$. How can a product of two factors be 1? Both factors must be 1 or -1. If $y = -1$, then $3x^2 - 2y$ cannot be -1, so $y = 1$, which means that $3x^2 - 2 = 1 \implies x = \pm 1$. Then $a = \pm 5$, and so the only solution is $\boxed{(a, b) = (\pm 5, 3)}$.

2.2 The Unpredictability of Mordell Curves

Is there a pattern to the number of solutions to Mordell Curves? Okay this question is extremely vague, so let's focus our question a bit. Let's investigate the number of solutions to Mordell Curves as we vary the constant term k. As we shall see, we can construct sequences of Mordell Curves that have arbitrarily many solutions as well as family of Mordell Curves without any solutions. All this maybe shows how unpredictable solutions to Mordell Curves are.

Let's consider family of Mordell curves of the form $a^2 = b^3 - 2^n$ for some $n \in \mathbb{N}$. Analyzing the number of solutions to this family will be fruitful to answering our main question. □

2.2.1 No Solutions

Lemma 2.6. *The number of integral solutions to the equation $a^2 = b^3 - 2^{6k+r}$ is the same as the number of integral solutions to the equation $a^2 = b^3 - 2^{6(k+1)+r}$. Furthermore, only the equations $a^2 = b^3 - 2$ or $a^2 = b^3 - 4$ have integral solutions such that a is odd.*

Proof. Let equation (1) be $a^2 = b^3 - 2^{6k+r}$ and equation (2) be $a^2 = b^3 - 2^{6(k+1)+r}$. (a', b') is an integral solution to (1) if and only if $(a, b) = (2^3a', 2^2b')$ is an integral solution to (2). It suffices to show that there are no odd solutions. Suppose a and b were both odd and (a, b) was a solution to (2). If r is even then $(a - 2^{3k+\frac{r}{2}}i)$ and $(a + 2^{3k+\frac{r}{2}}i)$ are coprime in $\mathbb{Z}[i]$, and if r is odd then $(a - 2^{3k+\frac{r-1}{2}}\sqrt{2}i)$ and $(a + 2^{3k+\frac{r-1}{2}}\sqrt{2}i)$ are coprime in $\mathbb{Z}[\sqrt{2}]$, which means they both have to be perfect cubes. Setting the factors to be squares of the form $(x + yi)^3$ or $(x + y\sqrt{2}i)^3$ and realizing that x must be odd in either case we obtain the equation of the form $3x^2 = 2^T \pm 1$

However because $\frac{2^T \pm 1}{3}$ is an odd square, it must be congruent to 1 mod 8, so $\frac{2^T \pm 1}{3} = 8n + 1 \implies T = 1$, or $T = 2$ and $n = 0$. I am brushing over some details here, but you would not get solutions for $T > 2$. This means that $a^2 = b^3 - 2$ and $a^2 = b^3 - 4$ are the only two equations of the form $a^2 = b^3 - 2^{6k+r}$ in which a can be odd.

Theorem 2.7. *There are no integral solutions (a, b) to the equations $a^2 = b^3 - 16$ and $a^2 = b^3 - 32$.*

Proof. By the lemma, if there are integral solutions (a, b) in either case, a and b must both be even. Assume for the sake of contradiction there are integral solutions. Let $a = 2a' = 4a'' = 8a'''$ and $b = 2b' = 4b''$. Consider the $k = -16$ case:

$$\begin{aligned}
&a^2 = b^3 - 16 \\
&\iff 4(a')^2 = 8(b')^3 - 16 \\
&\iff (a')^2 = 2(b')^3 - 4 \\
&\iff 4(a'')^2 = 2(b')^3 - 4 \\
&\iff 2(a'')^2 = (b')^3 - 2 \\
&\iff 2(a'')^2 = 8(b')^3 - 2 \\
&\iff (a'')^2 = 4(b')^3 - 1
\end{aligned}$$

However, $m^2 \not\equiv -1 \bmod 4$ for any $m \in \mathbb{N}$, so this is a contradiction.

Consider the $k = -32$ case:

$$\begin{aligned}
&a^2 = b^3 - 32 \\
&\iff 4(a')^2 = 8(b')^3 - 32 \\
&\iff (a')^2 = 2(b')^3 - 8 \\
&\iff 4(a'')^2 = 2(b')^3 - 8 \\
&\iff 2(a'')^2 = (b')^3 - 4 \\
&\iff 2(a'')^2 = 8(b')^3 - 4 \\
&\iff (a'')^2 = 4(b')^3 - 2 \\
&\iff 4(a''')^2 = 4(b')^3 - 2 \\
&\iff 2(a''')^2 = 2(b')^3 - 1
\end{aligned}$$

This is a contradiction because the left hand side is divisible by 2, but the right hand side is not.

□

Theorem 2.8. *We can fully classify the integral solutions (a, b) to all equations of the form $a^2 = b^3 - 2^{6k+r}$:*

$$\begin{cases}
r = 0 : (0, 2^{2k}) \\
r = 1 : (\pm 5 \cdot 2^{3k}, 3 \cdot 2^{2k}) \\
r = 2 : (\pm 2 \cdot 2^{3k}, 2 \cdot 2^{2k}), (11 \cdot \pm 2^{3k}, 5 \cdot 2^{2k}) \\
r = 3 : (\pm 2 \cdot 2^{3k}, 0) \\
r = 4 : \textit{No solutions} \\
r = 5 : \textit{No solutions}
\end{cases}$$

Corollary 2.9. *There are an infinite number of Mordell curves that have no integral solutions.*

2.2.2 Question I have:

Can you fully characterize the integral solutions of $a^2 = b^3 - p^{6k}$ for any prime p if you know $a^2 = b^3 - p$?

2.2.3 Arbitrarily many solutions

Now in the flip direction, we can show that Mordell Curves can have arbitrarily many integer solutions. I claim it suffices to show that some Mordell curve has infinitely many rational solution. Suppose that for some k, the equation $a^2 = b^3 + k$ has an infinite sequence of rational solutions $(\frac{a_n}{x_n}, \frac{b_n}{x_n})$. For any $N > 0$, we can construct a Mordell curve with at least N integer solutions as follows: Let $D_N := \prod_{i=1}^{N} x_i y_i$ (the product of the denominators of the rational solutions up to the Nth one.)

Then $\left(\frac{a_n}{x_n}\right)^2 = \left(\frac{b_n}{y_n}\right)^3 + k \iff \left(\frac{D_N^3 a_n}{x_n}\right)^2 = \left(\frac{D_N^2 b_n}{y_n}\right)^3 + k D_N^6$

$\left(\left(\frac{D_N^3 a_n}{x_n}\right)^2, \left(\frac{D_n^2 b_n}{y_n}\right)^3\right)$ is an integer pair, so we found N pairs of integral solutions to the Mordell Curve with constant term kD_N^6.

□

Lemma 2.10. *There are an infinite number of rational solutions to $a^2 = b^3 - 2$.*

Proof. Omitted for now. This involves knowing something about the group structure of rational solutions, which I don't know enough to include. □

Corollary 2.11. *Mordell Curves can have arbitrarily many integral solutions.*

What this means is pick your favorite natural number N. Then there is some Mordell Curve that has at least N many integral solutions. Cool, right!

2.3 References

- https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf
- https://www.cambridge.org/core/journals/mathematical-gazette/article/abs/9741-the-equation-py-2-x-4-x/998F0265A979
- https://www.jstor.org/stable/24497284?seq=1

3 Folding Paper and Totally Multiplicative Sequences

Take a rectangular sheet of printer paper. Fold it along the middle horizontal axis. In its folded state, fold the paper again along the middle horizontal axis and repeat.

Is your paper folded? Okay good. Now unfold everything and look at all the creases. Read them from the bottom to top of the paper as a sequence. Say each peak is 1 and each valley is a -1. After the first fold, we get one crease, which we will call a peak by convention. After two folds, we will get two peaks and a valley. Now, given a folding state, folding again keeps all the creases that were there previously, makes a new crease, and then copies all the creases that were there before but in reverse order and reverse orientation (all valleys become peaks, and all peaks become valleys). Mathematically, let S_k be the sequence after the kth fold. Then $S_k = S_{k-1}1\overline{(S_{k-1})^R}$ where $\overline{(S_{k-1})^R}$ is the reverse of the complement of the sequence. That is, S_k is S_{k-1} concatenated with 1 concatenated with the reverse of the sequence that flips all $1's$ with $-1's$ and vice versa.

When we do this an infinite number of times, we get an infinite sequence that is well defined. What's crazy is that this sequence is totally multiplicative. What that means is if $f(i)$ is the ith term in the sequence, then f is multiplicative. That is $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{N}^+$. We'll prove that right now.

Lemma 3.1. *$f(2^\ell) = 1$ for any $\ell \in \mathbb{N}$.*

Proof. Defining S_ℓ to be the sequence after ℓ folds, notice that $|S_\ell| = 2^\ell - 1$ ($|S_\ell|$ is the length of S_k). The $|S_\ell| + 1th$ element in the sequence is a 1 by construction. □

Lemma 3.2. *Let a_k be the kth odd natural number. That is, $a_k = 2k - 1$. Then $f(a_{2j}) = -1$ and $f(a_{2j-1}) = 1$*

Proof. Let 2^ℓ be the largest power of 2 not exceeding a_k. Let $a_k = 2^\ell + d$ and $a_j = 2^\ell - d$ for some odd d. Then $k = d + j$, and $f(a_k) = -f(a_j)$. The claim follows inductively. □

Lemma 3.3. *Let a, b be odd natural numbers. Then $f(ab) = f(a)f(b)$.*

Proof. Note that $(2k-1)(2j-1) = 2(2kj - k - j + 1) - 1$, so the product of the kth and the jth odd number is the $2kj - j - k + 1th$ odd number. If $k \equiv j \bmod 2$, then $2kj - j - k + 1 \equiv 1 \bmod 2$, so $f(2kj - j - k + 1) = 1$. Also, $f(2k-1) = f(2j-1)$, so $f(2k-1)f(2j-1) = 1$

Otherwise, $2kj - j - k + 1 \equiv 0 \bmod 2$ and $f(2kj - j - k + 1) = -1$. Because $f(2k-1) \neq f(2j-1)$ (k and j are different parity), then $-1 = f(2k-1)f(2j-1)$. □

Lemma 3.4. *$f(2)f(n) = f(2n)$ for any $n \in \mathbb{N}^+$*

Proof. Let (a_k) be the sequence of numbers so that $a_1 = n$, and a_{k+1} and a_k have the property that their average is the largest power of 2 not exceeding a_k. Let N be the smallest index such that a_N is a power of 2. Then a_j is a power of 2 for every $j \geq N$.

Let (b_k) be defined the same way but starting at $2n$ instead of n.

There's two key observations to note. First, $b_k = 2a_k$ for every k. This is easy to verify inductively. Second, N as defined before is the smallest index such that b_N is a power of 2.

Finally, noting that $f(a_k) = -f(a_{k+1})$ and $f(b_k) = -f(b_{k+1})$ for all $k < N$, and $f(b_N) = f(a_N) = 1$, it follows that $f(n) = f(2n)$. $f(2) = 1$, so $f(2)f(n) = f(2n)$. □

Theorem 3.5. *f is a totally multiplicative function.*

Proof. Let $m = 2^\ell a$ and $n = 2^j b$ where a and b are odd. By the previous lemma, only the odd component contributes to f, so $f(m) = f(a)$ and $f(n) = f(b)$. $f(mn) = f(2^{\ell+j}ab) = f(ab)$, so $f(mn) = f(ab) = f(a)f(b) = f(m)f(n)$ □

Part II

Snacks from Class

4 My Preparation for a Discrete Math Recitation

4.1 Parties

When people ask for examples of math, my discrete math professor Poh Shen Loh would give this one: Suppose that you want to host a party where 3 people all know each other, or 3 people are all strangers (Let's say for diversity purposes!). Say you're hosting the party at your small house that can't fit many people. What is the smallest possible size of the party?

A reasonable approach would be to study the types of relationships between every pair of people. Let's draw an edge between every person. If two people know each other, color their edge red. If two people don't know each other, color their edge blue. I guess there's an assumption here that if person A knows person B, then person B also knows person A. And if person A doesn't know person B, then person B doesn't know person A, but let's suppose this is the case (No internet stalking occured!!).

We rephrased the problem as: what is the minimum size of a fully connected graph to guarantee the existence of a monochromatic triangle (a red triangle or blue triangle)? We denote K_n as the fully connected graph with n vertices, and $R(3,3)$ as the smallest possible n such that any two-coloring of the edges of K_n admits a monochromatic triangle.

Finding $R(3,3)$ requires two steps. If we find a K_n such that **some** two-coloring does not admit a monochromatic triangle, it must be the case that $R(3,3) > n$ because $R(3,3)$ must be large enough to guarantee the existence of a monochromatic triangle. Now suppose that we find a K_n such that **any** possible two-coloring admits a monochromatic triangle. Then we can say that $R(3,3) \leq n$ because $R(3,3)$ is the smallest size in which this is true. This establishes a lower and upper bound, and we can trap the value of $R(3,3)$.

For the lower-bound there is a coloring on K_5 that does not admit a red or blue triangle as shown in 10. Thus, $R(3,3) > 5$.

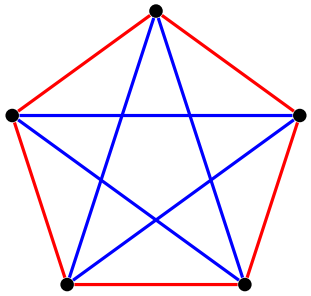


Figure 10: K_5 without a blue or red triangle

Now consider any two-coloring of the edges of K_6. Fix a vertex $v \in K_6$. Every vertex is connected to every other vertex, so v has 5 edges. One color must have been chosen for the majority of v's edges, so suppose vx, vy, and vz are blue edges. If there is a single blue edge among the triangle xyz, then that edge forms a blue triangle with vx, vy, or vz. In the other case, every edge in xyz is colored red, so we have a red triangle. Therefore, $R(3,3) \leq 6$. With the lower bound, we conclude that $R(3,3) = 6$.

More generally, we can define $R(s,r)$ to be the smallest n such that any two coloring of K_n admits a monochromatic K_s of color 1, or a monochromatic K_r of color 2. This is an extremely difficult problem in general: 4. Even for small cases like $R(4,10)$, we only have a range of possible values.

r \ s	1	2	3	4	5	6	7	8	9	10
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
2		**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
3			**6**	**9**	**14**	**18**	23	28	36	40–41
4				**18**	25	36–40	49–58	59–79	73–105	92–135
5					43–46	59–85	80–133	101–193	133–282	149–381
6						102–160	115–270	134–423	183–651	204–944
7							205–492	219–832	252–1368	292–2119
8								282–1518	329–2662	343–4402
9									565–4956	581–8675
10										798–16064

Table 4: Known values and bounding ranges for classical Ramsey numbers $R(r,s)$ (data from OEIS https://oeis.org/A212954). Note that $R(s,r) = R(r,s)$ so the table is symmetric.

Yet, even more generally, you can consider more than two colors and use the notation $R(n_1, n_2, \cdots, n_k)$ to be the minimum n such that in any k coloring of K_n, there is a monochromatic K_{n_i} with color i. We know that $R(n_1, n_2, \cdots, n_k)$ is finite, but a lot is still open! Extremal Graph Theory deals with these kinds of questions: If your graph has properties X, what is the smallest size you need to guarantee the existence of property Y.

4.2 A Striking Connection to...Number Theory?

Here's one unexpected application that popped up on my graph theory homework:

Theorem 4.1. *For every $k \in \mathbb{N}^+$, there is an $n \in \mathbb{N}$ such that, for every partition of $\{1, 2 \ldots, n\}$ into k sets, at least one of the subsets contains $x, y, z \in \{1, 2, \ldots, n\}$ such that $x + y = z$.*

The trick to this problem is to reframe it as a graph coloring problem. Let our vertex set be $V = \{1, \cdots, n\}$. Suppose that $X_1, \cdots, X_k$ partition V. We will use k colors when we color the edges of K_n. For each pair u and v, suppose that $|u - v| \in X_i$. Then color edge uv with color i. If there is a monochromatic triangle with color i, then there exists vertices u, v, w so that $|u - v|$, $|v - w|$, and $|u - w|$ are all in X_i. Without loss of generality, $u < v < w$, so $(v - u) + (w - v) = (w - u)$. Calling $x := v - u$, $y := w - v$, and $z := w - u$, we get exactly what we want because x, y, z are in X_i and $x + y = z$. How large should n be? It should be large enough to guarantee the existence of a monochromatic triangle, so it should be $\underbrace{R(3, \ldots, 3)}_{\text{there are } k \text{ 3's}}$

4.3 A Memorable Recitation

I remember preparing for my second discrete math recitation the night before, where I wanted to give interesting applications of the Pigeonhole Principle and Ramsey Theory. Then I remembered Poh Shen Loh's example and this cool graph theory homework problem, and my lesson was all set:) The party example works so well as an introduction because it is explained in simple English yet captures the essence of the math. 4.2 is very surprising when you see it the first time and is pretty difficult to see, so it complements the party example well.

5 A Bridge Between Discrete Math and Real Analysis

Here's my all-time favorite theorem, and an absolute classic. Seeing the proof for the first time almost felt like magic. I didn't expect a counting argument in a discrete math flavor to show something about the structure of rational numbers and real numbers.

For any real number α, there is a rational number that is arbitrarily close to it.

Lemma 5.1. ***Direchlet's Approximation Theorem:*** *Fix $\alpha \in \mathbb{R}$. For all integers $N > 0$, there exists $p \in \mathbb{Z}$ and $q \in \{1, 2, \cdots, N\}$ such that $|q\alpha - p| < \frac{1}{N}$.*

Proof. It suffices to assume that $\alpha, p > 0$.

For each $k \in \{0, 1, \cdots, N\}$, we express $k\alpha = \lfloor k\alpha \rfloor + \{k\alpha\}$, where $\lfloor k\alpha \rfloor$ is the floor i.e. the largest integer that is smaller than $k\alpha$ and $\{k\alpha\}$ is the fractional part of $k\alpha$. (So $0 \leq \{k\alpha\} < 1$).

Consider the N intervals $[0, \frac{1}{N}), [\frac{1}{N}, \frac{2}{N}), \cdots, [\frac{N-1}{N}, 1)$. Each $\{k\alpha\}$ lies in some interval. Moreover there are $N+1$ points in $\{0\alpha\}, \{1\alpha\}, \cdots, \{N\alpha\}$, so every point can't lie in different intervals. Two points must be in the same interval. That is, there exists $i, j \in \{0, 1, \cdots, N\}$ such that $\{i\alpha\} - \{j\alpha\} < \frac{1}{N}$. Without loss of generality, $i > j$.

Set $q = i - j$ and $p = \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor$. Then

$$|q\alpha - p| = |(i-j)\alpha - \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor| = |\{i\alpha\} - \{j\alpha\}| < \frac{1}{N}$$

□

Theorem 5.2. *For any $\alpha \in \mathbb{R}$, there exists infinitely many pairs of integers (p, q) such that $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.*

Proof. Set $N_0 = 3$. By Direchlet's Approximation, there exists $p_0 \in \mathbb{Z}$ and $q_0 \in \{1, 2, N_0\}$ such that $|q_0\alpha - p_0| < \frac{1}{N_0}$. Then

$$|\alpha - \frac{p_0}{q_0}| < \frac{1}{q_0 N_0} \leq \frac{1}{q_0^2}$$

Now suppose that inductively, the first $k \geq 0$ terms of the sequence are well defined. Choose N_{k+1} large enough so that

$$\frac{1}{N_{k+1}} < \min_{i,j \in \{1, \cdots, N_k\}} (\{i\alpha\} - \{j\alpha\})$$

Apply Direchlet's Approximation theorem again to get $p_{k+1} \in \mathbb{Z}$ and $q_{k+1} \in \{1, 2, N_{k+1}\}$ such that

$$|\alpha - \frac{p_{k+1}}{q_{k+1}}| < \frac{1}{q_{k+1} N_{k+1}} \leq \frac{1}{q_{k+1}^2}$$

Also,

$$|\alpha - \frac{p_{k+1}}{q_{k+1}}| < |\alpha - \frac{p_k}{q_k}| < \cdots < |\alpha - \frac{p_0}{q_0}|$$

Thus, (p_{k+1}, q_{k+1}) must be distinct from the previous pairs in the sequence. □

6 A Short Tale of Graphs and Inequalities

6.1 Introduction

In my Junior fall Semester, I remember being blown away by a problem in my Parallel and Sequential Algorithms and Data Structures Class. There was a crazy connection between finding a solution to a system of linear inequalities of a specific form and running a shortest path algorithm on a directed graph.

6.2 The problem

Given n real-valued variables $x_1, \cdots, x_n$ and m linear inequalities of the form $x_i - x_j \leq c_{i,j}$, find an assignment of the variables that satisfies all the inequalities. For example, if $x_1 - x_2 \leq 2$, $x_1 - x_3 \leq 3$, and $x_2 - x_3 \leq -4$, then one possible satisfying assignment to x_1, x_2, x_3 would be $x_1 = -2$, $x_2 = -\pi$, and $x_3 = 0.5$.

6.2.1 Transforming the inequalities into a graph

Construct a dummy source variable s and construct a directed edge from s to x_j with edge weight 1 (the particular edge weight doesn't actually matter). Now for each inequality $x_i - x_j \leq c_{ij}$, build a directed edge from x_j to x_i of weight c_{ij}. Call the resulting graph G.

Theorem 6.1. *There is no negative weight cycle if and only if there is a satisfying variable assignment*

Proof. If there is no negative weight cycle, then the shortest path between s and any other vertex x_j is well defined. Let $d(s, x_j)$ be the distance of the shortest path between s and x_j (the sum of the edge weights of the shortest path). Then we claim that setting variable x_j to be $d(s, x_j)$ is a satisfying assignment. Why is this the case? For each inequality of the form $x_i - x_j \leq c_{i,j}$, consider the corresponding vertices. Note that it is possible to get to x_i by starting from s and going to x_j as an intermediate vertex and using edge $x_j x_i$. Thus, the shortest path to x_i must be bounded by the shortest path to x_j plus $w(x_i x_j)$-the weight of the edge $x_j x_i$. Therefore, $d(s, x_i) \leq d(s, x_j) + c_{i,j}$, and the inequality is satisfied.

Conversely, suppose that there is a negative weight cycle of size k: $y_1, \cdots, y_k$. Note that s is never part of a cycle. In order for the system to have a satisfying solution, the following inequalities must be satisfied:

$$\begin{cases} y_2 - y_1 \leq c_{2,1} \\ y_3 - y_2 \leq c_{3,2} \\ \vdots \\ y_k - y_{k-1} \leq c_{k,k-1} \\ y_1 - y_k \leq c_{1,k} \end{cases}$$

Adding up the k inequalities, we see that the left hand side is 0, so $0 \leq c_{2,1} + c_{3,2} + \cdots + c_{1,k}$, which contradicts the assumption that this is a negative weight cycle. □

6.2.2 Remark

What I like about this problem is that it is algorithmic in flavor. Choose your favorite shortest path graph algorithm that works with negative edge weights. You construct a graph, and the algorithm tells you whether there exists a solution by returning the shortest paths. If the algorithm fails, you know that there is no solution because the only time the algorithm fails is when there are negative weight cycles. As a bonus, you know how fast it takes to find a solution. Running Bellman Ford's Algorithm, for example takes $O(m^2 + nm)$ work.

7 The Magic of Error-Correcting Polynomials

On a warm Tuesday in April, I walked excitedly into my 15-451 (Algorithms Design and Analysis) Lecture, and I was surprised to hear my professor talk about Lagrange interpolating polynomials, a topic we covered in Linear Algebra. This was perhaps my favorite lecture from that class because it was so exciting to see the bridge between Linear Algebra and Theoretical Computer Science, specifically Error Correcting Codes. For example, when I took Linear Algebra for the first time, I remember learning that the set of real polynomials of degree n, $P_n(\mathbb{R})$, is a vector space over $\mathbb{R}$. This fact was always interesting to me from a theoretical perspective because it seemed to imply that the additive and multiplicative axioms of vector spaces are a lot more general than Euclidean Space.

7.1 The Setup

Suppose Alice wants to send Bob a message over a channel. We can think of the message as a stream of $d+1$ real numbers: $\langle c_0, c_1, \cdots, c_d \rangle$. However, the channel might be noisy, and $k \leq d$ numbers will be lost in translation. We denote these numbers by asterisks. As a concrete example, suppose that $d = 2$, $k = 2$, and Alice's message is $\langle 4, 5, 6 \rangle$. Suppose that 4 and 5 are lost in translation. If Alice were to send Bob $\langle 4, 5, 6 \rangle$, then Bob would see $\langle *, *, 6 \rangle$. Given just this information, Bob has no way to recover $\langle 4, 5, 6 \rangle$. Alice must send Bob a longer message, and the non-asterisked numbers in the message should give Bob enough information to deduce the missing numbers.

The trick is that we can construct a polynomial with the coefficients as Alice's original numbers.

$$P(x) = \sum_{i=0}^{d} c_i x^i$$

Now Alice sends Bob the message consisting of $d+k$ unique evaluations of this polynomial.

$$\langle P(x_0), P(x_1), \cdots, P(x_{d+k}) \rangle$$

To see why this helps, we take a short trip to Linear Algebra Land.

7.2 Results from Linear Algebra

Definition. *Suppose you're given $n+1$ distinct points: $x_0, \cdots, x_n$. For all $i \in \{0, \cdots, n\}$ define the Lagrange Polynomials as*

$$R_i(x) := \prod_{i \in \{0,\cdots,n\}, i \neq j} \frac{(x - x_j)}{(x_i - x_j)}$$

Notice that $R_i(x_i) = 1$, and $R_i(x_j) = 0$ for all $j \neq i$

Lemma 7.1. *$\beta := \{R_0(x), \cdots, R_n(x)\}$ is a basis for $P_n(\mathbb{R})$*

Proof.

$$\begin{aligned}
&\forall x \in \mathbb{R} : \sum_{i=0}^{n} c_i R_i(x) = 0 \\
&\implies \sum_{i=0}^{n} c_i R_i(x_j) = 0 \text{ for all } j \in \{1, \cdots, n\} \\
&\implies c_j = 0 \qquad \text{(because } R_j(x_j) = 1, \text{ and } R_i(x_j) = 0 \text{ for all } i \neq j)
\end{aligned}$$

Therefore β is a set of $n+1$ linearly independent vectors in $P_n(\mathbb{R})$, and the dimension of $P_n(\mathbb{R})$ is $n+1$, so β is a basis of $P_n(\mathbb{R})$ □

Corollary 7.2. *Given $n+1$ distinct points: $x_0, \cdots, x_n$, there is a unique degree n polynomial that passes through the points $(x_0, y_0), \cdots, (x_n, y_n)$*

Proof. Consider $p(x) = \sum_{i=0}^{n} y_i R_i(x)$. Then $p(x_j) = \sum_{i=0}^{n} y_i R_i(x_j) = y_j R_j(x_j) = y_j$. Now suppose polynomial q has the property such that $q(x_j) = y_j$. Write q in terms of the basis vectors: $q = \sum_{i=0}^{n} c_i R_i(x)$. Then $q(x_j) = p(x_j) \implies c_j = x_j$. Thus, $p = q$, which proves uniqueness. □

Definition. *Given $n+1$ points $x_0, \cdots, x_n$ we define the Vandermonde matrix via*

$$V := \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & \cdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix}$$

The Vandermonde Matrix helps us find the unique degree n polynomial that passes through $(x_0, y_0), \cdots, (x_n, y_n)$ because we can obtain the coefficients of the polynomial $p(x) = \sum_{i=0}^{n} c_i x^i$ by solving a system of linear equations.

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & \cdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

We know that the Vandermonde polynomial is invertible by 7.2 because solving the equation is equivalent to finding the unique degree n polynomial that passes through $(x_0, y_0), \cdots, (x_n, y_n)$.

7.3 Polynomials to the Rescue

Let's return to our problem at hand. Recall that Alice sends the message $\langle P(x_0), P(x_1), \cdots, P(x_{d+k}) \rangle$, where the coefficients of $P(x) = \sum_{i=0}^{d} c_i x^i$ are Alice's original numbers. Let $S = \{y_{i_0}, \cdots, y_{i_d}\}$ be the set of all numbers that Bob sees in Alice's message that have not been lost in translation. The size of S is at least $d+1$ because Alice sends $k+d+1$ numbers and at most k have been lost in translation. If the size of S is more than $d+1$, we can discard some of them because we only need $d+1$ points. Now Bob interpolates by solving the matrix equation:

$$\begin{pmatrix} 1 & x_{i_0} & x_{i_0}^2 & \cdots & x_{i_0}^d \\ 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^d \\ \vdots & & \cdots & & \vdots \\ 1 & x_{i_d} & x_{i_d}^2 & \cdots & x_{i_d}^d \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{pmatrix} = \begin{pmatrix} y_{i_0} \\ y_{i_1} \\ \vdots \\ y_{i_d} \end{pmatrix}$$

There is a unique solution to this equation, so Bob will be able to obtain the coefficients of Alice's polynomial, which is her intended message. Note that this method hinges on the assumption that Bob and Alice communicated ahead of time, so Bob knows the precise points that Alice evaluated the polynomial. But in practice, if the message Alice sends contains $d+k+1$ numbers, Bob and Alice can establish the convention that the polynomial is evaluated at points $0, 1, \cdots, d+k+1$.

7.4 Generalization

In our error correcting code, we used the fact that the Vandermonde Matrix is invertible. What if we had some other matrix instead of the Vandermonde Matrix. In fact, we can generalize to a broader class of error correcting codes. Suppose Alice's list of $d+1$ numbers is the vector x, and she sends Ax to Bob, where A is a $d+k+1$ by $d+1$ matrix. Our original set-up with the noisy channel remains: k entries in Ax are replaced with asterisks. Bob still hopes to recover x given Ax after d entries have been asterisked.

Theorem 7.3. *If Bob and Alice both know A ahead of time, then Bob can recover Alice's original $d+1$ numbers if and only if every $d+1$ by $d+1$ submatrix of A defined by selecting $d+1$ rows of A is invertible.*

Proof. ($\Longrightarrow$)

Assume that every $d+1$ by $d+1$ submatrix of A defined by selecting $d+1$ rows of A is invertible. Let $i_0, \cdots, i_d$ be the indices of the d entries in Ax that are not asterisks. Let A' be the submatrix by selecting these rows, and let y be the $d+1$ vector by selecting these elements in x. Then $A'x = y$. We assumed A' is invertible, so $x = A^{-1}y$, and therefore x is recoverable.

($\Longleftarrow$)

Fix some $d+1$ square submatrix A' defined by choosing the rows $i_0, \cdots, i_d$. By our assumption, Bob can recover x from Ax, so he can recover x when indices $i_0, \cdots, i_d$ are those that are not asterisks. Let y be the subvector of Ax defined by choosing these indices. Then $A'x = y$ has a unique solution by our assumption, so A' must be invertible.

□