A Random Walk on $\mathbb{Z}_n \times \mathbb{Z}_n$

Robert Davidson

What is a Random Walk?

A random walk at its simplest is a process that moves step by step, where each new step is the current position plus some random change. Random walks are used in a wide range of fields, from finance, where they model how stock prices move, to brain research, where they explore how neurons fire and interact, and even to computer science, where they're used to estimate the size of the World Wide Web[1].

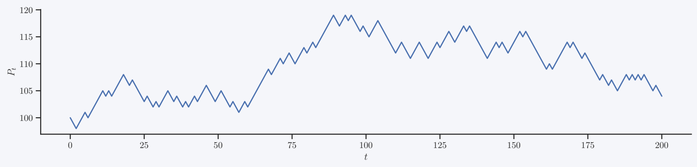


Figure 1. A simple stock price path (P_t at step t, with $x = 100$ and $t = 200$).

A simple example of a random walk is the walk on the integer line[1], $\mathbb{Z}$, we start at x and at each step, t, we randomly choose a move from the sample space:

$$\Omega = \{+1, -1\}$$

We let P_t denote our position at step t, then, following Lawler[2], we write:

$$P_t = x + X_1 + \cdots + X_t$$

where each X_i is an independent random variable with

$$P(X_i = 1) = P(X_i = -1) = 0.5$$

so our random variables dictate whether we move up or down the integer number line with equal probability.

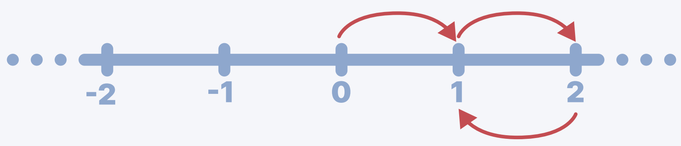


Figure 2. An example of a random walk on the Integers.

How does this relate to Group Theory?

From a group theory perspective, we see that our random walker walks on the set of integers $\mathbb{Z}$, equipped with the group operation of addition, and forms the infinite cyclic abelian group:

$$(\mathbb{Z}, +)$$

The group satisfies the group axioms, proven in Lecture 1. Every element of $\mathbb{Z}$ can be generated by repeatedly applying the group operation with the element 1:

$$\mathbb{Z} = \langle 1 \rangle = \{k \cdot 1 : k \in \mathbb{Z}\}$$

So, 1 is a generator of the group, and its inverse, -1, also generates the group.

Thus the set:

$$\langle S \rangle = \langle \{1, -1\} \rangle = \mathbb{Z}$$

forms a generating set for $(\mathbb{Z}, +)$.

We can describe our random walk entirely in group theory notation, starting at the identity element ($x = e$), each step corresponds to performing the group operation with some element from the generating set, and so after t steps:

$$P_t = e + s_1 + s_2 + \cdots + s_t, \quad s_i \in S$$

Since $x = e = 0$, rewriting gives:

$$P_t = \sum_{i=1}^{t} s_i \quad \text{where } s_i \in S \text{ is chosen uniformly at random}$$

What if we restrict our walker?

The question arises: what if instead of allowing our walker to walk on the entire integer number line, we restrict them to walking on a finite set of n positions, where moving past the end brings the walker back to the beginning?

More specifically, we want to walk on the finite cyclic abelian group:

$$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$$

with group operation addition modulo n. This group satisfies the group axioms:

- **Closed and Associative** $\Rightarrow a + (b + c) \equiv (a + b) + c \mod n \in \mathbb{Z}_n, \quad a, b, c \in \mathbb{Z}_n$
- **Identity** $e = 0$ $\Rightarrow a + 0 \equiv 0 + a \equiv a \mod n \quad a \in \mathbb{Z}_n$
- **Inverse** $a^{-1} = (-a \mod n)$ $\Rightarrow a + (-a) \equiv 0 \mod n \quad a \in \mathbb{Z}_n$

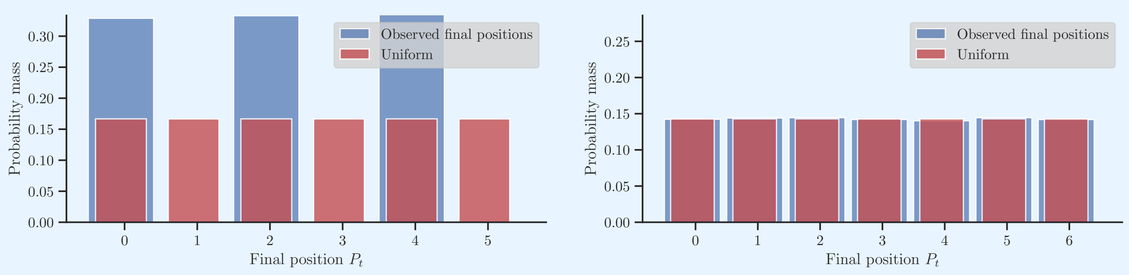
The element 1 still acts as a generator, with -1 as its inverse, so the generating set remains the same. Our walk, starting again at $e = 0$, after t steps is given by:

$$P_t = \sum_{i=1}^{t} s_i \mod n \quad s_i \in S$$

Since we've restricted our walker to a finite set of n positions, we might assume that after many steps, with many walkers, each position should be visited equally often and that the distribution of final positions should be uniform.

However, this isn't the case, even in this simple group, the group's structure constrains where the walker can be.

As we see below, the walkers' final positions can only reach a uniform distribution for odd n (right histogram), and for even n, they can only occupy half of $\mathbb{Z}_n$ (left histogram).



3.1: Final positions on $\mathbb{Z}_6$.

3.2: Final positions on $\mathbb{Z}_7$.

Figure 3. Histogram of final positions on even and odd n $(30,000$ walkers, $10,000$ steps).

Why can we only reach uniformity for odd n?

Intuitively, in $\mathbb{Z}$, after an even amount of steps from 0, the walker can only be on an even number. Similarly, if our walker takes an odd number of steps they must be on an odd number.

The same is only true on $\mathbb{Z}_n$ for even n.
More specifically, when n is even, the subset, H, of even residues:

$$H = \{0, 2, 4, \ldots, n-2\} \subset \mathbb{Z}_n$$

forms a subgroup of $\mathbb{Z}_n$.
Since half of $\mathbb{Z}_n$ is even, we have:

$$|H| = n/2$$

Then, by Lagrange's Theorem:

$$[\mathbb{Z}_n : H] = \frac{|\mathbb{Z}_n|}{|H|} = \frac{n}{n/2} = 2$$

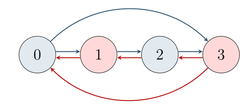


Figure 4. Parity of the random walk on $\mathbb{Z}_4$.

Thus, for even n, we see $\mathbb{Z}_n$ splits into two disjoint left cosets:

$$H = \{0, 2, 4, \ldots, n-2\} \quad \text{and} \quad 1 + H = \{1, 3, 5, \ldots n-1\}$$

Because each step is either ± 1, each move sends the walker from one coset to another, and thus, after even steps, the walker lies in H and after odd steps in $1 + H$.
Across many walkers, all are constrained to positions in one coset or the other, but never both, and so the distribution of final positions can never become uniform.

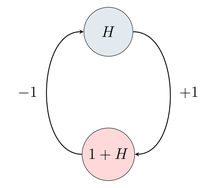


Figure 5. Movement between the cosets for even n.

However, when n is odd, the subset H no longer forms a subgroup of $\mathbb{Z}_n$. Since H is not a subgroup it has no cosets that partition $\mathbb{Z}_n$ and this parity breaks.
Wrapping around connects an even node to another even node, breaking the even-odd separation. Since this step links even and even residues, the parity between steps and position breaks.

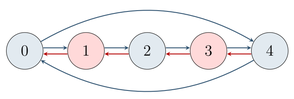


Figure 6. Break in parity of the random walk on $\mathbb{Z}_5$.

What if our walker could walk in two dimensions?

Now that we've studied the walk through the lens of group theory on the 1-Dimensional cyclic group, $\mathbb{Z}_n$, we ask what happens when we allow the walker to move in 2-Dimensions?

More specifically, we want our walker to walk on the Direct Product:[3][4]

$$\mathbb{Z}_n \times \mathbb{Z}_n = \{(x, y) \mid x \in \mathbb{Z}_n, y \in \mathbb{Z}_n\}$$

where the group operation is defined by component-wise addition $\bmod n$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2 \bmod n,\ y_1 + y_2 \bmod n)$$

This group inherits group properties from $\mathbb{Z}_n$, specifically, it has:

- **Identity** $e = (0, 0)$
- **Inverse** $(-x, -y) \bmod n$

The group is a finite abelian group and has generating set S:

$$S = \{(1, 0), (0, 1), (-1, 0), (0, -1)\}$$

Starting at the identity, $(0, 0)$, we define our walker's position after t random steps the same as before:

$$P_t = \sum_{i=1}^{t} s_i \mod n \quad s_i \in S$$

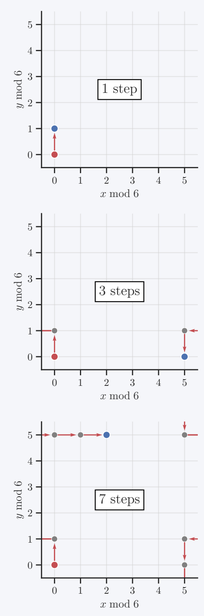
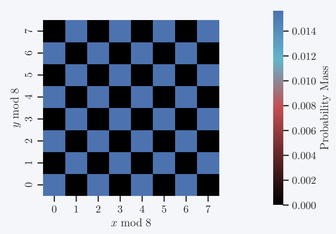


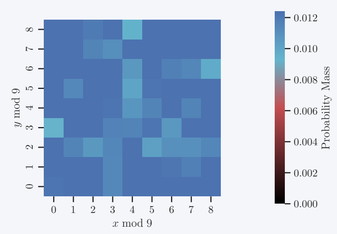
Figure 7. Example path on $\mathbb{Z}_6 \times \mathbb{Z}_6$.

Now, our walker is walking on the $n \times n$ grid, where stepping off one side returns the walker on the opposite side. An example path is shown above. We might ask the question, does the parity problem in the 1-Dimensional case still arise in this 2-Dimensional case?

As we see below, for even n, the same restriction occurs, and the walker can only reach half of the grid at any fixed time, so the final positions end up on the odd or the even half of the $n \times n$ grid (left heatmap). When n is odd, the restriction breaks, and the final positions are free to spread across all points, allowing the distribution to become uniform (right heatmap).



8.1: Final positions on $\mathbb{Z}_8 \times \mathbb{Z}_8$.



8.2: Final positions on $\mathbb{Z}_9 \times \mathbb{Z}_9$.

Figure 8. Heatmap of final positions on even and odd n $(30,000$ walkers, $10,000$ steps).

Summary and Applications

In this project we studied simple random walks through the perspective of Group Theory. We started by introducing a random walk on the integers, and viewed it as the walk on the group $(\mathbb{Z}, +)$. We then restricted the walk to $\mathbb{Z}_n$ and discussed why, for even n, the subgroup of even residues forces the walk to alternate between two disjoint cosets, and prevents us from reaching a uniform distribution for the final positions of our walkers. We then extended this to the direct product $\mathbb{Z}_n \times \mathbb{Z}_n$ and saw a similar restriction.

Random walks on groups appear in everyday examples. Shuffling cards is essentially taking random steps through the group, S_{52} all possible orders of the deck[5]. Scrambling a Rubik's Cube works the same way, where it corresponds to a random walk on a group containing 43 quintillion elements[6]. Some cryptographic methods also use repeated random steps through a group to search for hidden information[7].

References

[1] Wikipedia. Random walk. `https://en.wikipedia.org/wiki/Random_walk`, .

[2] Gregory F. Lawler. Simple random walk. `https://www.math.uchicago.edu/~lawler/reu1`. Page 1.

[3] Wikipedia. Direct product of groups. `https://en.wikipedia.org/wiki/Direct_product_of_groups`, .

[4] Bruce Ikenaga. Direct products. `https://sites.millersville.edu/bikenaga/abstract-algebra-1/product/product.pdf`, 2018. Page 1.

[5] Tuomas Sahlsten. Analysis, random walks and groups. `https://www.mv.helsinki.fi/home/sahlsten/documents/arg_notes.pdf`, 2023.

[6] Hillary Yang Yanlin Qu*, Tomas Rokicki. Rubik's cube scrambling requires at least 26 random moves. `https://arxiv.org/pdf/2410.20630`, 2024.

[7] Nolan Winlker. The discrete log problem and elliptic curve cryptography. `https://math.uchicago.edu/~may/REU2014/REUPapers/Winkler.pdf`, 2024.

Simulations and Figures implemented with Figma, TikZ and Python (NumPy, SciPy, Seaborn, Pandas, Matplotlib)

Project GitHub Repository