UNDERSTANDING WORD METRICS: PATTERNS IN NUMBERS AND GEOMETRY

CALEB LEE

1. Introduction

How do we measure distance? Distance is a concept we encounter daily, whether measuring the length of a road, the separation between cities, or the space between stars. In these scenarios, distance is typically measured in meters, miles, or light-years—quantities that represent how far apart two points are in physical space. These measurements rely on straightforward rules, like using a ruler or calculating using coordinates and formulas from geometry.

But what happens when we think about distance in a more abstract sense? Consider navigating a maze. Here, "distance" might represent the number of turns or steps required to reach the exit. Each choice—turning left or right, moving forward or backward—can be thought of as a step toward your goal. This way of thinking about distance involves counting actions rather than measuring lengths, and it reflects a more abstract notion of distance.

Mathematics is often seen as a tool for solving practical problems, but it also provides a way to explore abstract ideas. One such concept is the *word metric*, which combines algebra and geometry to measure distances in mathematical groups. This paper explores two specific cases: the group of integers $\mathbb{Z}$ and the 4-dimensional Heisenberg group $H(4)$. While these structures may seem esoteric, they have surprising connections to cryptography, quantum mechanics, and robotics.

Our goal is to understand how these groups behave geometrically by developing algorithms to compute the shortest "paths" within them. These paths are not physical but represent combinations of basic elements, or *generators*, that form the group.

2. What is a Word Metric?

A *word metric* measures how many steps it takes to move from one element of a group to another using a specific set of tools (called *generators*). For example:

- In $\mathbb{Z}$, if your tools are $\{2, 3\}$, you might ask, "How many steps are needed to build the number 11?".

Date: December 6, 2024.

- In the Heisenberg group $H(4)$, which models multi-dimensional systems, the challenge is more complex because the tools operate in multiple directions.

The word metric helps us explore how groups are structured and how their elements interact.

3. The Integer Group $\mathbb{Z}$

The group of integers $\mathbb{Z}$ is the simplest example of a group. It consists of all whole numbers and is typically generated by the number 1 (and its negative, -1). However, what happens if we use other generators, like $\{2, 3\}$? Say we are attempting to find the word metric of the number n = 11 with the aforementioned generators.

One method to build 11 might be $2+3+3+3 = 11$. In this case, we used four numbers to build 11, making the distance equal to 4. The reader can check that this is the minimum possible steps to make 11, thus marking its appropriate distance of 4.

3.1. Defining the lower-bound M.

When considering large target numbers, n. At a certain point, it will be sufficient to take the largest possible step forwards toward our target number until we hit a threshold where smaller steps start to matter more. Say instead of trying to find the *word metric* of $n = 11$, we are instead trying to find the metric of $n = 1000$.

In this case, it makes sense that the number of big steps of 3 will far outnumber the number of smaller steps of 2 as the distance is very far away from 0 in comparison to our largest generator. In the case of 1000, we have 332 steps of 3 and only 2 steps of 2. To save time in our algorithm, it makes sense to always take the largest possible step when we are pass this threshold until we are able to get to a more manageable distance that is less than or equal to M. From here, we know that there is a possibility that smaller steps will lead to a faster solution. We call this lower-bound M.

3.2. Algorithm for $\mathbb{Z}$.

We developed an algorithm to compute the word metric for any integer n using a finite set of generators $X = \{x_1, x_2, \ldots, x_k\}$:

(1) Check that $\gcd(X) = 1$ to ensure X generates all integers (Bézout's Lemma) [1], when $\gcd(X)$ is the greatest common denominator of the set X.

(2) Compute a threshold M based on the generators [3]:

$$M = \sum_{i=1}^{k-1} \left(\frac{x_i + x_{i+1}}{2} x_i \right) + x_k.$$

(3) Precompute the word lengths for all integers $|n| \leq M$.

(4) For $|n| > M$, use the recursive formula:

$$|n|_X = |n - x_k|_X + 1.$$

This method guarantees efficiency because the precomputed values allow us to break down large numbers into simpler steps.

4. The Heisenberg Group $H(4)$

The Heisenberg group $H(4)$ is more complex than $\mathbb{Z}$ because its elements are 4x4 matrices. These matrices have the form:

$$H = \begin{pmatrix} 1 & x_1 & x_2 & z \\ 0 & 1 & 0 & y_1 \\ 0 & 0 & 1 & y_2 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where x_1, x_2, y_1, y_2, z are integers. The group is *nilpotent*, meaning its structure reflects certain constraints on how its elements combine. The reader can find more information on nilpotent groups here [7].

4.1. Algorithm for $H(4)$.

To compute the word metric in $H(4)$, we used the following approach:

(1) Given the generators of $H(4)$:

$$X_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$Y_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(2) Split the computation into two simpler problems using commutative subgroups:
   - One subgroup generated by X_1, Y_1.
   - Another subgroup generated by X_2, Y_2.

(3) Apply known formulas for smaller Heisenberg groups to compute distances. This was proven by Blachere [6].

(4) Combine the results to optimize the overall path.

This algorithm reduces the complexity of $H(4)$ by leveraging its internal symmetries and breaking it into manageable parts.

5. Why Does This Matter?

The algorithms developed in this project have implications for both theoretical and practical applications:

- **Cryptography**: Word metrics can help secure data by analyzing group structures used in encryption [2].
- **Robotics**: Robots navigating multi-dimensional spaces rely on similar mathematical principles [4].

- **Physics**: The Heisenberg group plays a key role in quantum mechanics, describing uncertainty in particle systems [5].

6. Conclusion

Exploring word metrics has deepened our understanding of how algebraic and geometric concepts intersect. From the simplicity of $\mathbb{Z}$ to the complexity of $H(4)$, these algorithms provide tools for uncovering hidden structures in mathematics and beyond. The journey doesn't end here—future research could explore even more intricate groups and their applications. As a further step, we have turned our attention to solving an open problem on the large scale structure of Rough Isometries of $\mathbb{Z}$.

Acknowledgments: This work was made possible through the mentorship of Professor Yanlong Hao and contributions from our collaborative team.

References

[1] Étienne Bézout. *Théorie générale des équations algébriques*. Ph.-D. Pierres, 1779.

[2] Benjamin Dörr, Stefan Frei, Kimmo Järvinen, and Thomas Schneider. Efficient privacy-preserving secure multiparty computation for modular exponentiation, 2023. https://eprint.iacr.org/2023/046.pdf.

[3] Yanlong Hao. Personal communication, 2024. In-person meeting on geometric group theory.

[4] Jens Kober, J. Andrew Bagnell, and Jan Peters. Reinforcement learning in robotics: A survey. *Autonomous Robots*, 40(5):789–825, 2016. https://link.springer.com/article/10.1007/s10514-016-9587-8.

[5] David Morin. Waves and quantum mechanics, n.d. https://scholar.harvard.edu/files/david-morin/files/waves_quantum.pdf.

[6] Blachère Sébastien. *Word Distance on the Discrete Heisenberg Group*. Colloquium Mathematicum, 2003.

[7] Marcos Zyman, Stephen Majewicz, and Anthony E. Clement. *The Theory of Nilpotent Groups*. Birkhäuser, 2017.