Geometry in Noncommutative Algebra

Sean Grate

January 14, 2021

Let's start with some preliminary notions.

Definition 1. Let S be a set (sometimes called an *alphabet*) and call the elements of S *letters*. A *word* is any finite concatenation of letters from S.

Example 1. Suppose $S = \{a, b, c\}$. Then a, b, c are letters from S and acb is a word.

For simplicity of notation, for any letter s, we can let denote $ss = s^2$ and so on. Thus the word $accbbbcca$ is the same as the word $ac^2b^3c^2a$. It is important to note that the concatenation operation may not be commutative, i.e. the order of letters in a word is *very* important.

Definition 2. The *discrete Heisenberg group* $H(\mathbb{Z})$ is the group of unipotent upper-triangular matrices with integer entries under matrix multiplication, i.e. matrices of the form

$$\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \quad \text{where} \quad x, y, z \in \mathbb{Z}.$$

1 Working in the Heisenberg Group

Matrices can be complicated so identifying a matrix group with something that is easier to understand is good. This can be accomplished via an *isomorphism*.

Note. Let

$$x = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, z = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then

$$H(\mathbb{Z}) = \left\{x, y \ : \ z = xyx^{-1}y^{-1}, xz = zx, yz = zy\right\} = \{x, y \ : \ xy = yxz, xz = zx, yz = zy\}.$$

Because of the last presentation, this is why $H(\mathbb{Z})$ is the nicest noncommutative group one could ask for.

Definition 3. Let G, H be groups. A *group homomorphism* is a function $\varphi\colon G \to H$ s.t. φ is well-defined and $\varphi(xy) = \varphi(x)\varphi(y)$. Basically, it is a function between groups which respects group multiplication. A *group isomorphism* is a bijective group homomorphism. This is useful since it allows us to work with "the same" group, but under a different lens.

Theorem. There is a bijection given by

$$\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \longleftrightarrow (x, y, z).$$

This can be extended to an isomorphism on $H(\mathbb{Z})$ computed as

$$\begin{gathered}\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + x' & z + z' + xy' \\ 0 & 1 & y + y' \\ 0 & 0 & 1 \end{bmatrix} \\ \updownarrow \\ (x, y, z)(x', y', z') = (x + x', y + y', z + z' + xy').\end{gathered}$$

Through this isomorphism, we can see that $H(\mathbb{Z})$ is basically integral vectors under addition, except there is a twist in the last component. This twist yields the noncommutative nature of $H(\mathbb{Z})$. Moreover, this isomorphism allows us to visualize elements and subsets of $H(\mathbb{Z})$ as points in $\mathbb{Z}^3 \subset \mathbb{R}^3$.

1.1 Translating Words to Groups

Suppose we have a set S that takes its letters from some group G. We can form words from S and send them to group elements of G naturally: If w is a word, i.e. a product of letters from S, our evaluation map simply multiplies the letters together via the group operation. For example, in the context of $H(\mathbb{Z})$, the word xy^2zy is reduced to

$$\begin{aligned} xy^2zy &= (1,0,0)(0,1,0)(0,1,0)(0,0,1)(0,1,0) \\ &= (1,1,1)(0,1,0)(0,0,1)(0,1,0) \\ &= (1,2,2)(0,0,1)(0,1,0) \\ &= (1,2,3)(0,1,0) \\ &= (1,3,4). \end{aligned}$$

So for any word formed from letters of S, there is a corresponding element in $H(\mathbb{Z})$ given by multiplying the letters according to the group operation.

We are also going to impose some additional constraints when looking at these words to make them easier to study. In particulay, we are going to restrict words based on their *word length*, or the number of letters in a word. For instance, the word x^2zy has a word length of 4 since there are 4 letters in it. In doing so, we are now able to iteratively examine what happens to the number of group elements we get from words of length k. In general, one would expect that as k gets larger, the possible group elements one might get also increases.

2 Minkowski Dilates

Let S be a finite set with letters taken from $H(\mathbb{Z})$. Define $P_k(S) \subset H(\mathbb{Z})$ to be the set of all group elements obtained from evaluating all of the words of length k formed from S. We are going to call $P_k(S)$ the k-th dilate of S. More formally, we can realize $P_k(S)$ as

$$P_k(S) = \left\{ \prod_{i=1}^{k} \ : \ s_i \in S \right\}.$$

Because our group operation is noncommutative, we must make sure to evaluate all possible orderings of letters that form words of length k. Thus if $|S| = n$, to compute $P_k(S)$, we must evaluate all n^k possible words. This becomes a very expensive operation very quickly. Compare this to the commutative setting where we would only need to evaluate $\binom{n+k-1}{k} \leq n^k$.

Example 2. Let $S = \{x, y, z, 0\}$. Then for $k = 1$, we simply get

$$P_1(S) = \{x, y, z, 0\}.$$

For $k = 2$, $P_2(S)$ is the set of all words formed from S of length 2. So

$$P_2(S) = \left\{ \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\2\\0\end{bmatrix}, \begin{bmatrix}0\\0\\2\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix} \right\}.$$

Note that since $H(\mathbb{Z})$ is not commutative, we must evaluate 4^k words for the kth dilate versus $\binom{4+k-1}{k}$ in the commutative setting. For instance, when computing $P_{10}(S)$, this is the difference between $4^{10} = 1048576$ and $\binom{4+10-1}{10} = 286$ (see Figure 1). However, $|P_{10}(S)| = 781$ which is much smaller than 1048576 indicating that $H(\mathbb{Z})$ is a relatively nice noncommutative group (see Figure 2).

Now we get to the essence of what we want to inverstigate. Our goal is to show that given any basis with n elements, $|P_k(S)| = \mathcal{O}(n^4)$ for k sufficiently large, i.e. the asymptotic growth of the Heisenberg group is quartic. If we can do this, it might be possible to accomplish an ancillary objective: prove that the number of points in $P_k(S)$ can be counted by a polynomial of degree 4 or less.
This second objective has already been accomplished in the commutative setting through Ehrhart theory and Ehrhart polynomials. In fact, some of the coefficients in the Ehrhart polynomial of a polytope can actually be interpreted meaningfully. For example, the leading coefficient relates to the d-dimensional volume of the polytope and the constant term relates to the Euler characteristic. Extending these methods and their corresponding interpretations to the noncommutative setting is invaluable.

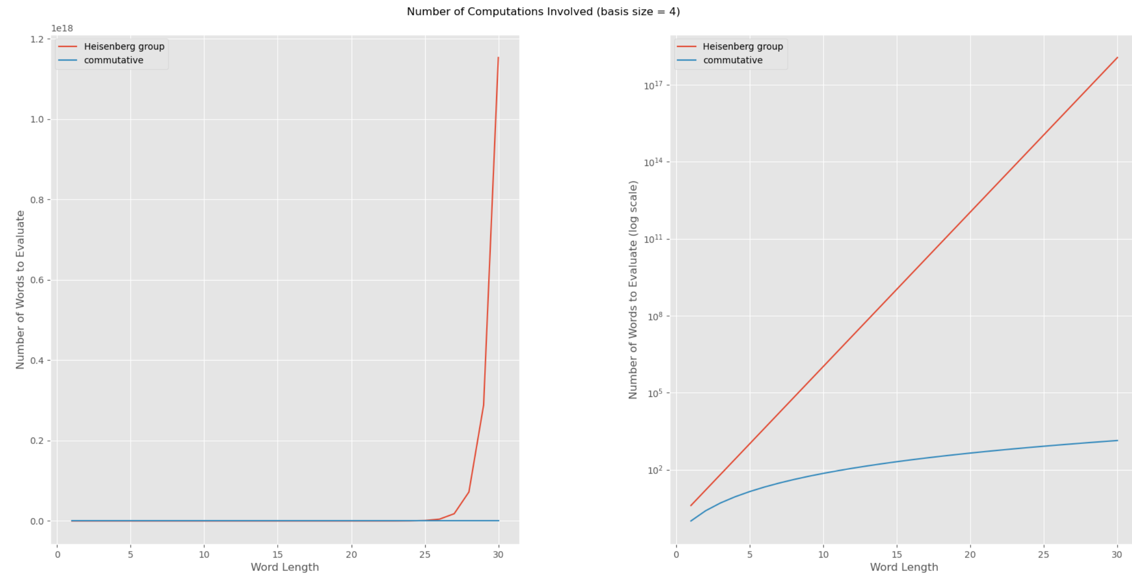

Figure 1: The number of computations needed in the commutative and Heisenberg group settings. The difference in evaluations becomes staggering very quickly.

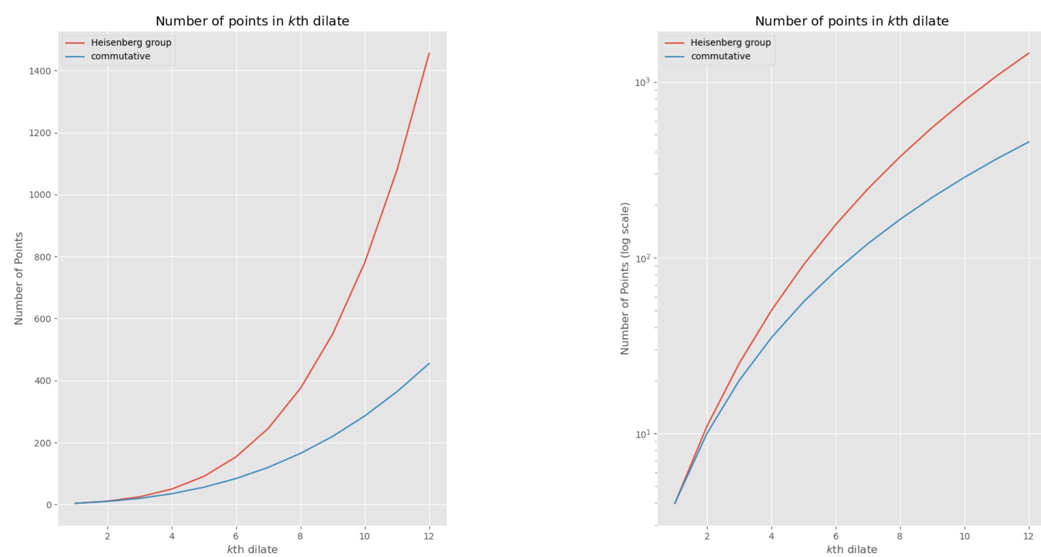

Figure 2: The actual number of computations (points) needed in the commutative and Heisenberg group settings. The difference is not very large compared to the worst case scenario, i.e. Figure 1.

3 Some Results

Example 3. Recall the basis set as given in Example 2: $S = \{x, y, z, 0\}$. A remarkable fact is that we can actually find a degree 4 polynomial that bounds the polytope $P_k(S)$ from above as well as $|P_k(S)|$. Through some work, this polynomial is given by

$$z = xy - x - y + k.$$

Integrating under this surface yields the volume of $P_k(S)$:

$$\begin{aligned}
V(k) &= \int_0^k \int_0^{k-x} xy - x - y + k \, dy \, dx \\
&= \int_0^k \int_0^{k-x} xy \, dy \, dx + \int_0^k \int_0^{k-x} k - x - y \, dy \, dx \\
&= \int_0^k \frac{x(k-x)^2}{2} \, dx + \int_0^k \frac{(k-x)^2}{2} \, dx \\
&= \frac{1}{24}k^4 + \frac{1}{6}k^3 \\
&= \frac{k^4}{4!} + \frac{k^3}{3!}.
\end{aligned}$$

Moreover, this will not be proven here (I do not remember if this is still conjecture), but

$$|P_k(S)| = \frac{1}{24}k^4 + \frac{1}{4}k^3 + \frac{23}{24}k^2 + \frac{3}{4}k + 1.$$

Example 4. Consider the basis set

$$S = \{0, x, y, yx\}.$$

Experimentally, it seems that for $x + y > k$,

$$\begin{aligned}
z_{roof} &= T_{x+y-k-1} + 2k(x+y) - x^2 - xy - y^2 - k^2 \\
z_{floor} &= T_{x+y-k-1}
\end{aligned}$$

and

$$|P_k(S)| = \frac{1}{6}k^4 + \frac{1}{6}k^3 + \frac{5}{6}k^2 + \frac{11}{6}k + 1.$$

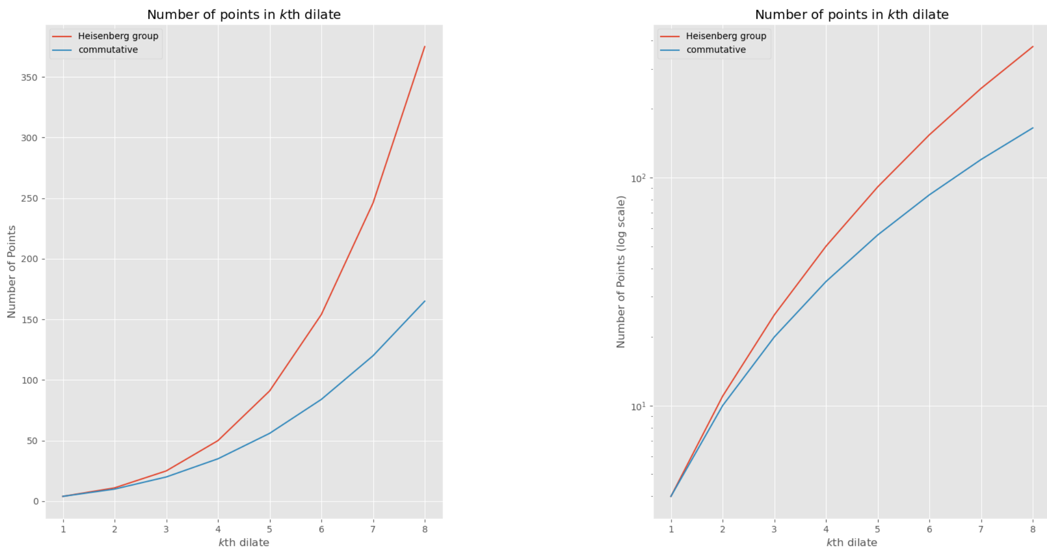

Figure 3: Using the tetrahedron generators.

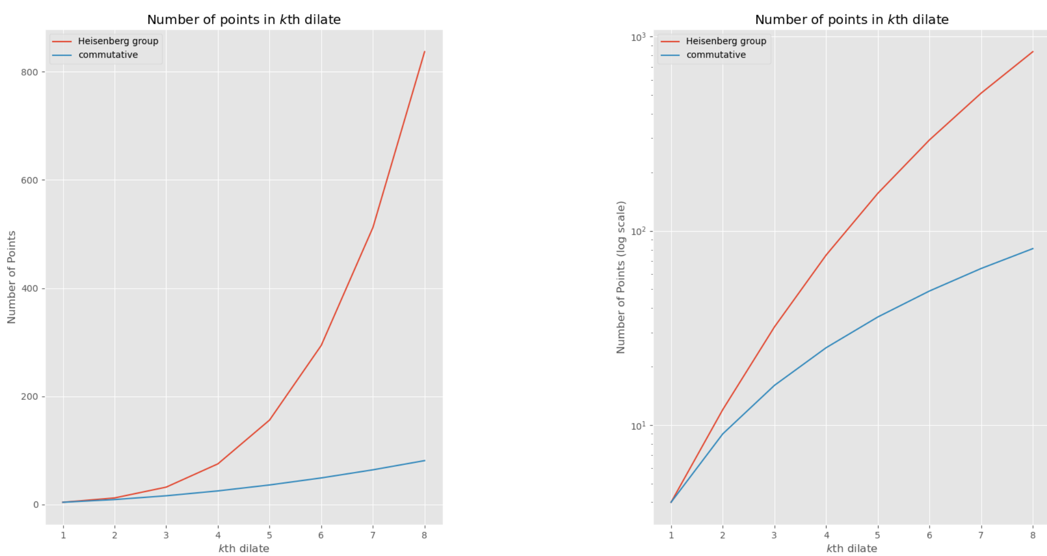

Figure 4: Using the vomit square generators.

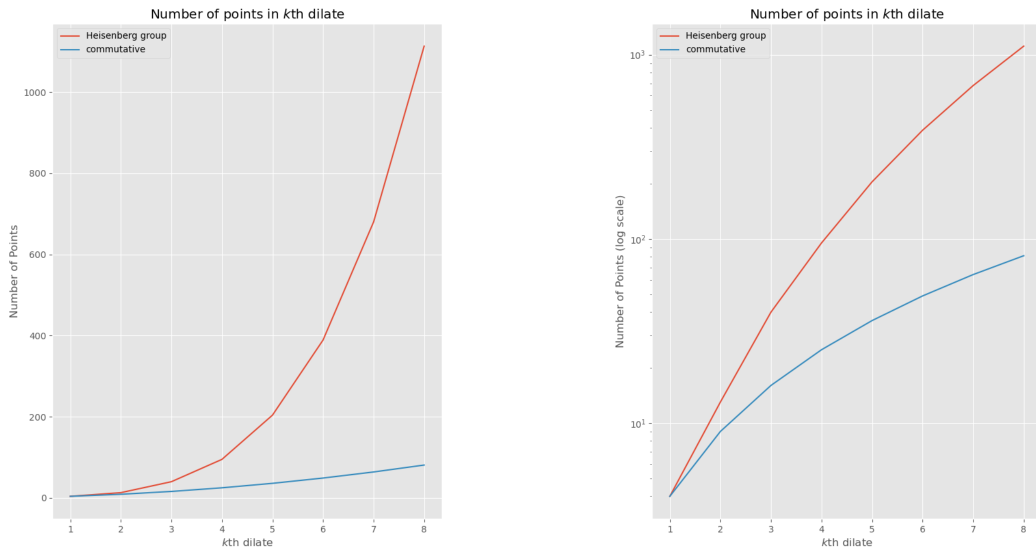

Figure 5: Using the standard $H(\mathbb{Z})$ generators.

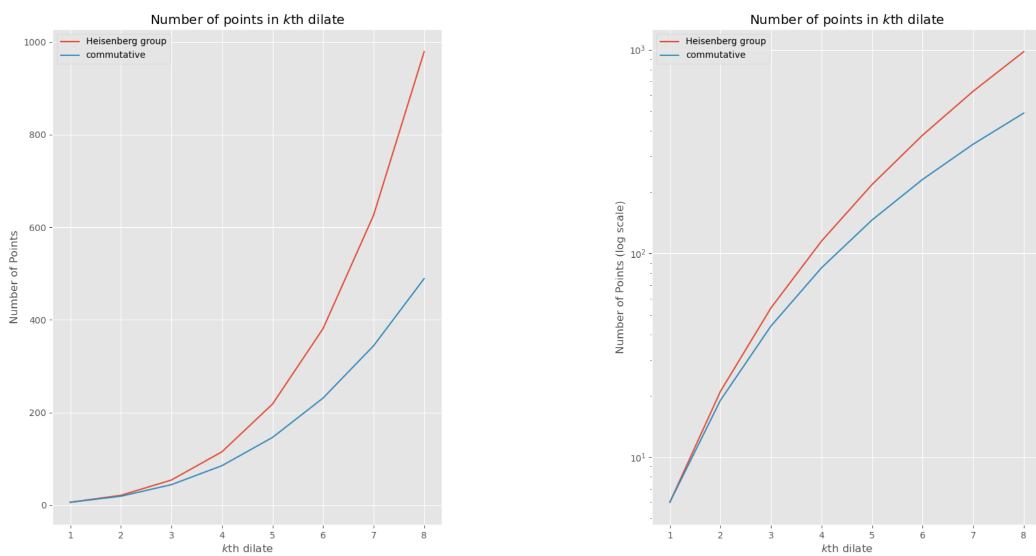

Figure 6: Using the half-octohedron generators.

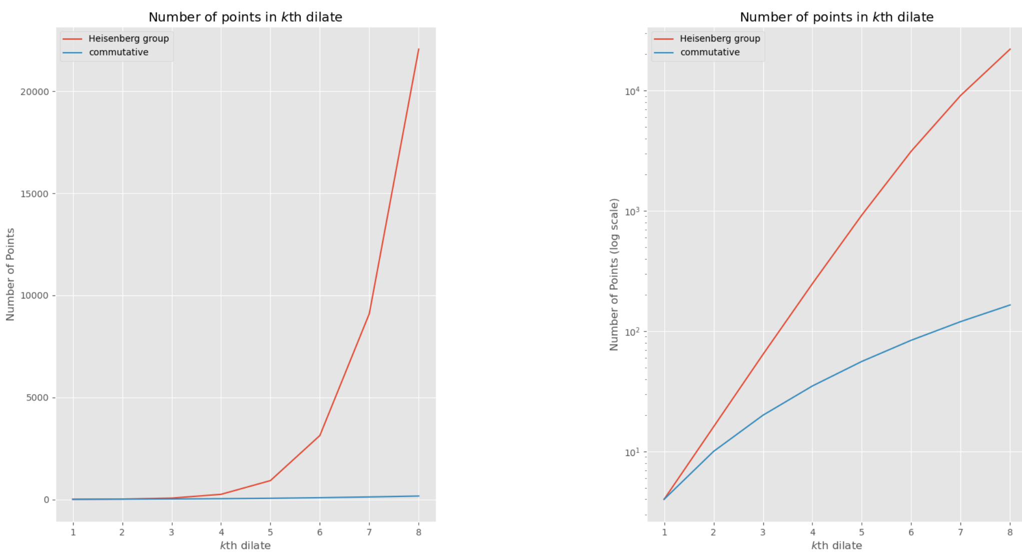

Figure 7: Using random generators.