Note on the baby-step giant-step algorithm

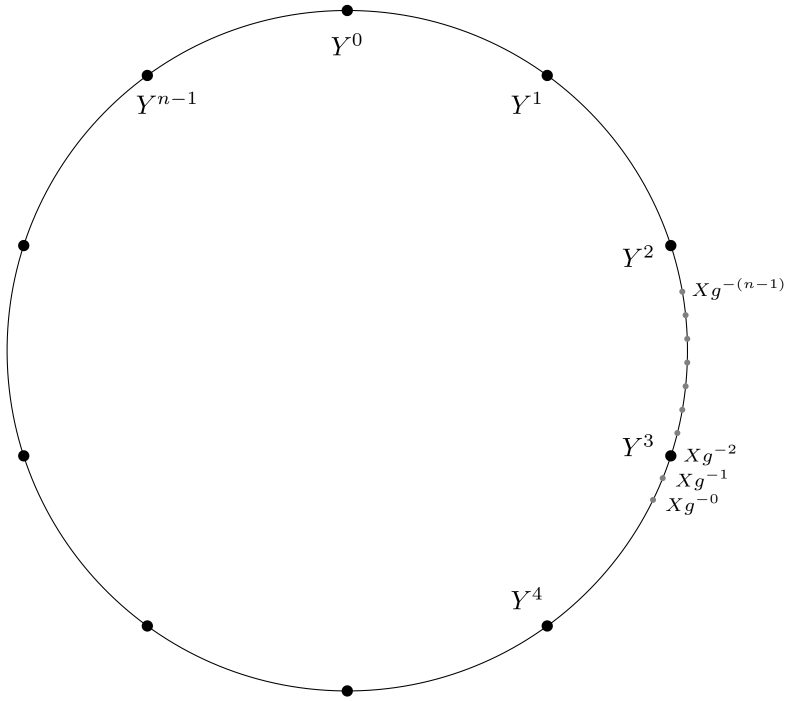

Figure 1: The baby-step giant-step algorithm

Let G be a cyclic group with generator g. The baby-step giant-step algorithm works as follows to compute the discrete logarithm of a value $X = g^x \in G$. First, it computes $n \leftarrow \left\lceil \sqrt{|G|} \right\rceil$ and $Y \leftarrow g^n$. Then it computes two tables:

$$T_0 \leftarrow \{Xg^0, Xg^{-1}, Xg^{-2}, \ldots, Xg^{-(n-1)}\}$$
$$T_1 \leftarrow \{Y^0, Y^1, Y^2, \ldots, Y^{n-1}\}$$

and looks for a "collision" between T_0 and T_1, i.e., an element from each table such that $Xg^{-i} = Y^j$. Then the discrete logarithm of X is simply $x = nj + i$.

Here's how to think about the values Xg^{-i} and Y^j. First, imagine arranging all the elements of G on a circle. Then, the Y^j values represents n evenly spaced out values on this circle, each having a "distance" of at most n elements between them (see Fig.1). These are the "giant steps". The value X is thus guaranteed to land in exactly one interval Y^j to Y^{j+1}. In Fig. 1 the X $(= Xg^{-0})$ value landed inside the interval between Y^3 and Y^4.

The Xg^{-i} values represents n elements, each one g-multiplication apart, starting at X. These are the "baby steps". Note that in Fig. 1 we step counter-clockwise because we're multiplying with g^{-1}. Since we do n baby steps, we're guaranteed to hit exactly one Y^i value during our baby steps. In Fig. 1 we have $Xg^{-2} = Y^3$. Thus, the baby-step giant-step algorithm is guaranteed to work.