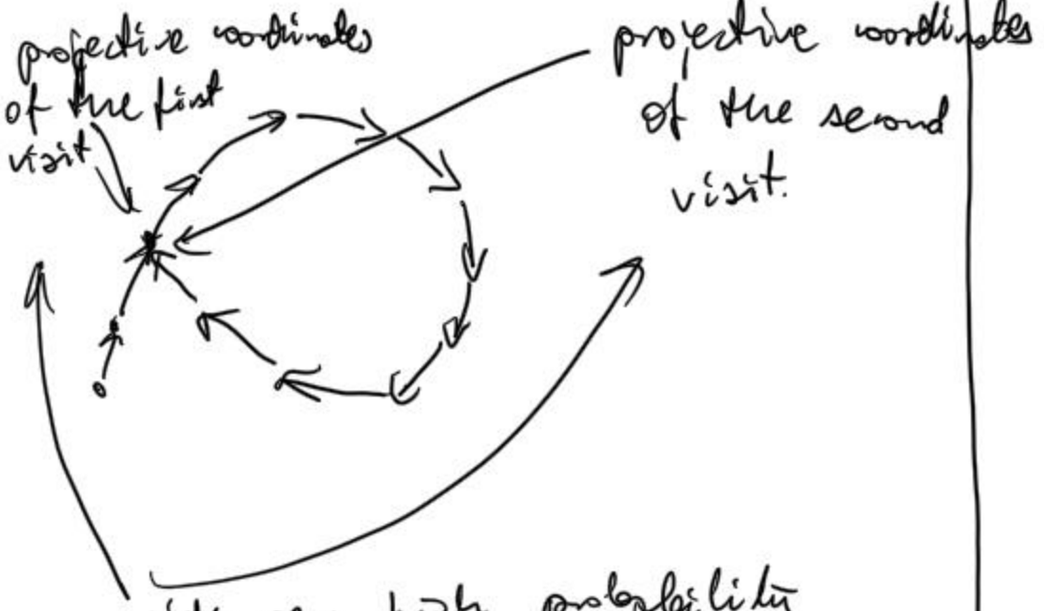
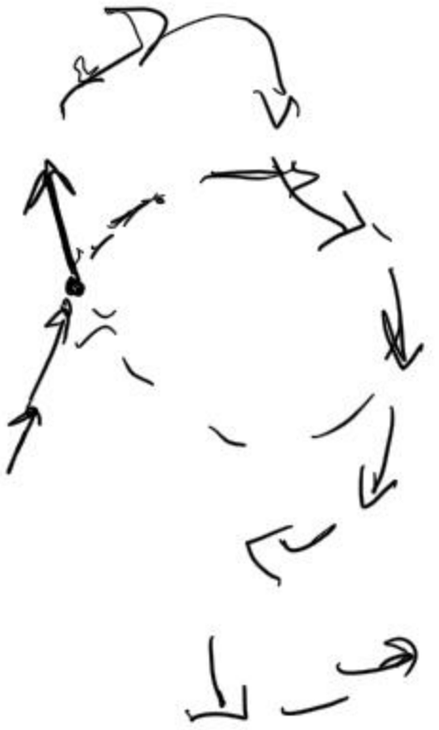
List nr 4.

Projective coordinates :)



with very high probability the representations of the same point in the projective coordinates will be different!

So, in consequence, the next step is not the same as previously



Instead of the loop we have a pseudo-random walk.

The number of steps we may visit is in fact:

$$|G| \cdot (p-1)$$

so instead of $O(\sqrt{|G| \cdot (p-1)})$ steps we need $O(\sqrt{|G|})$ steps