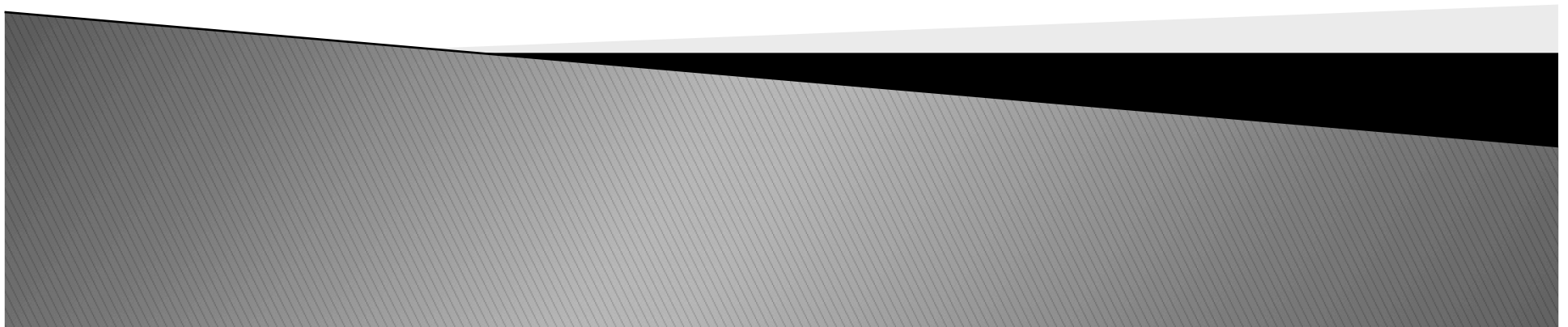


The discrete Log Problem

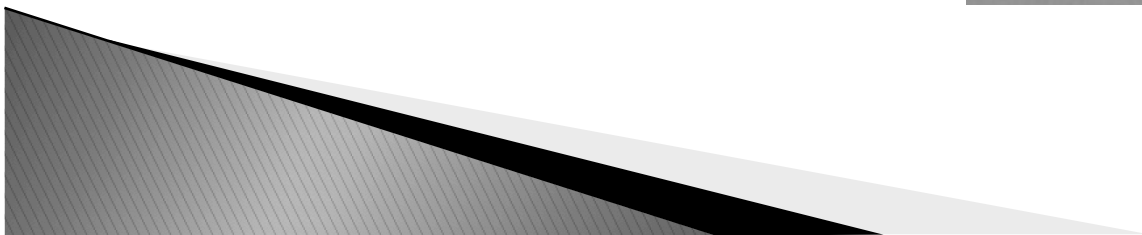
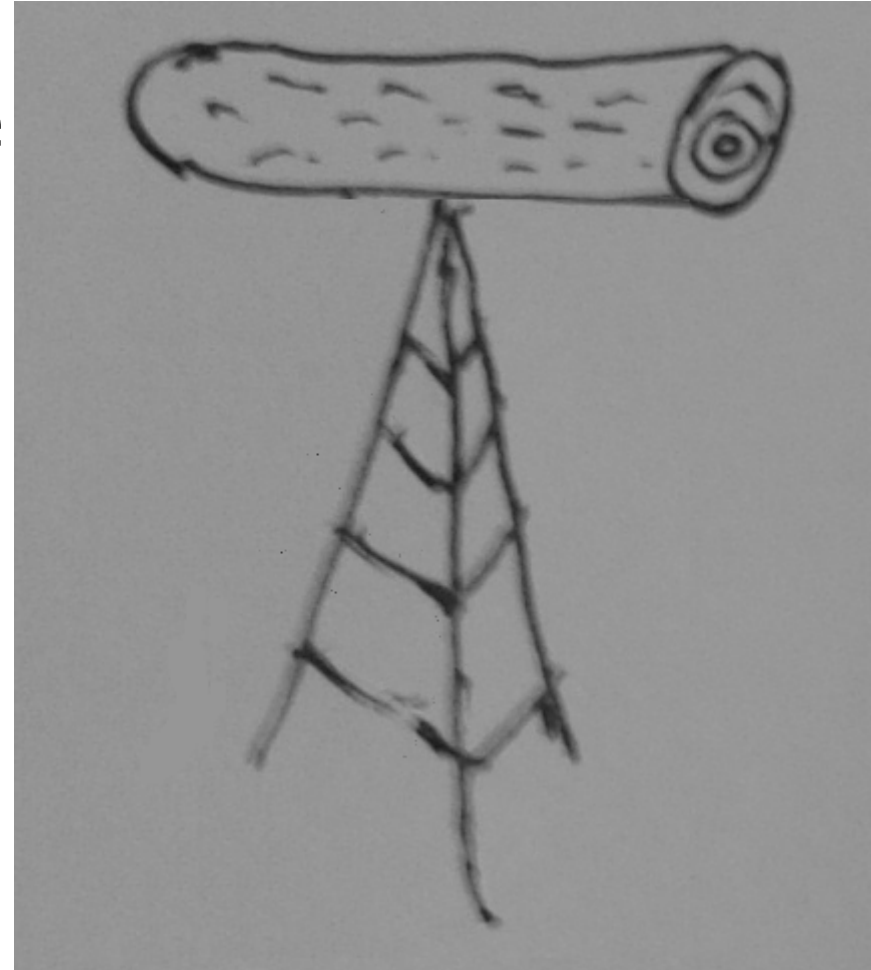
Speaker: Lil Maria Rodríguez

Artist: Andrés Cortes



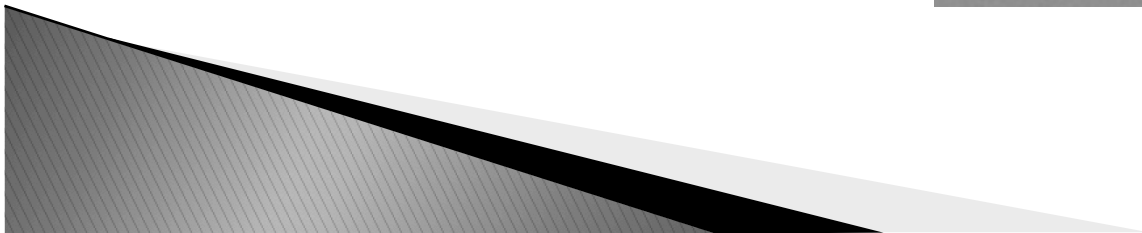
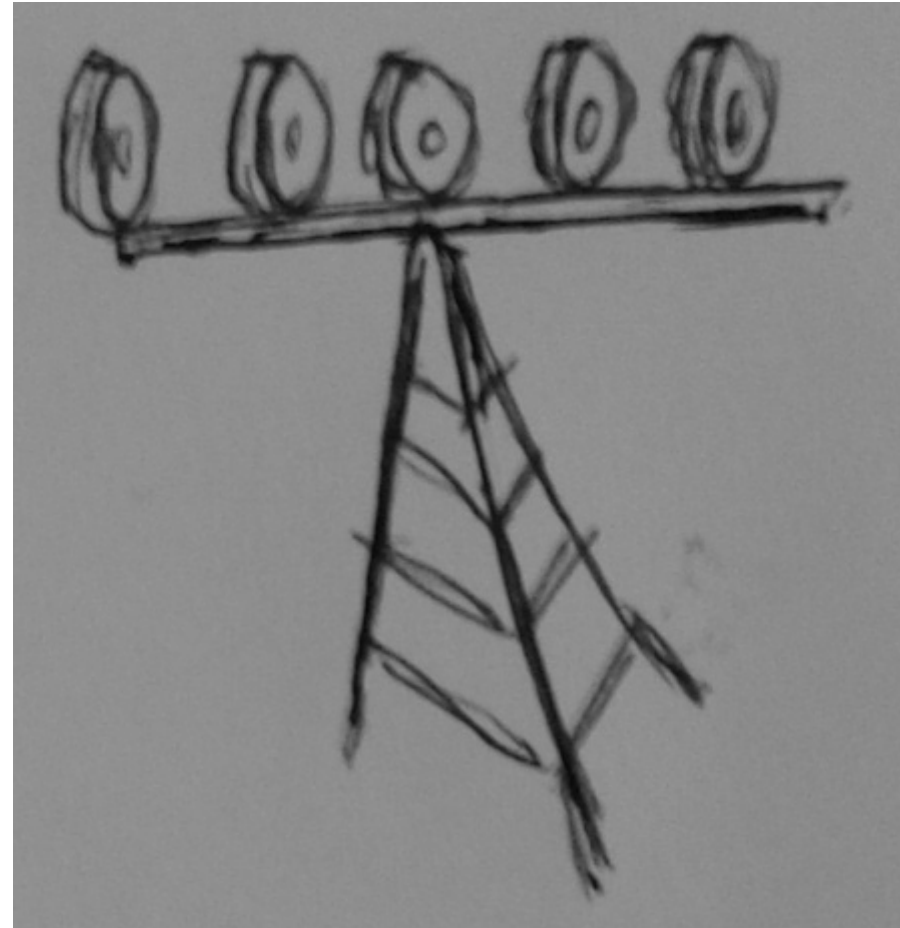
The log problem

- ▶ Raise a big log on the top of power generator (transmission tower).
- ▶ Problem: Retrieve the log

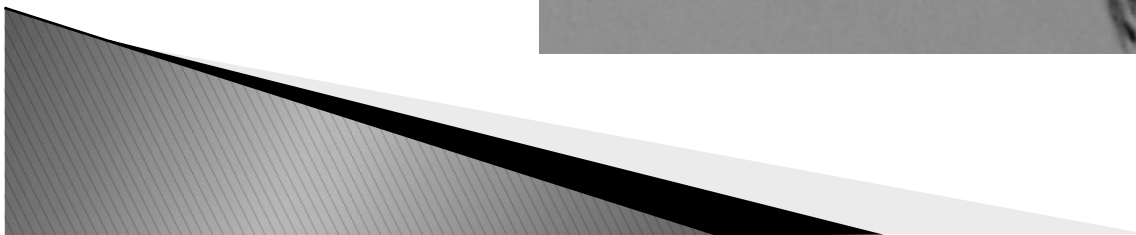
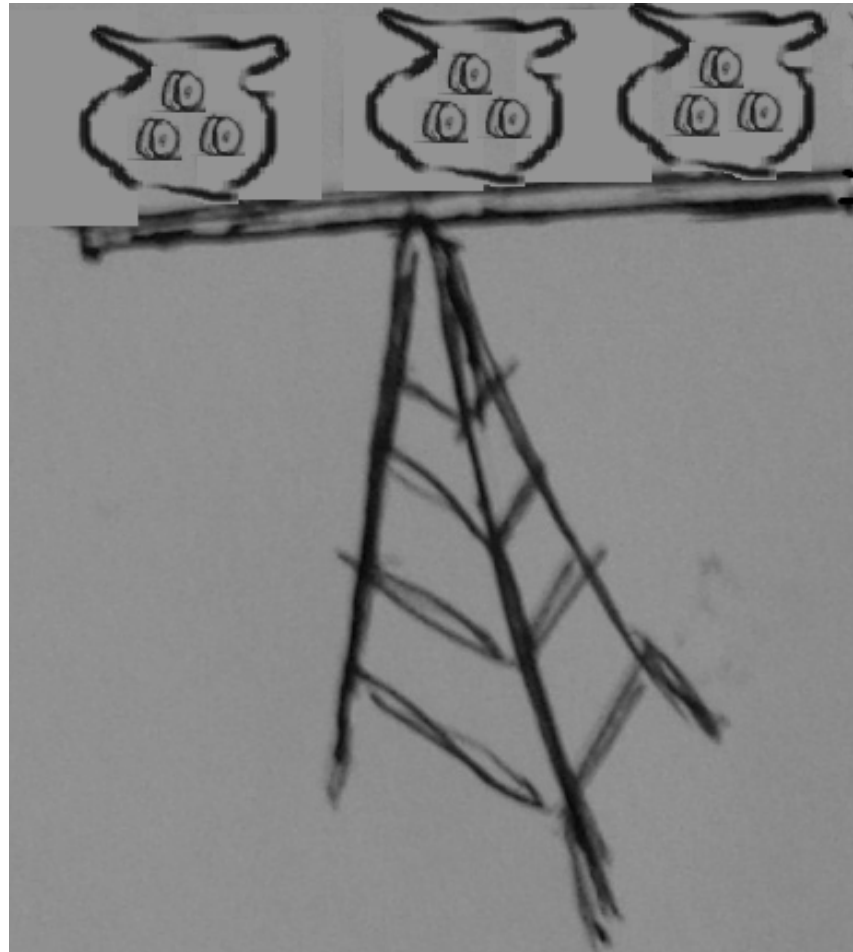


The discrete log problem

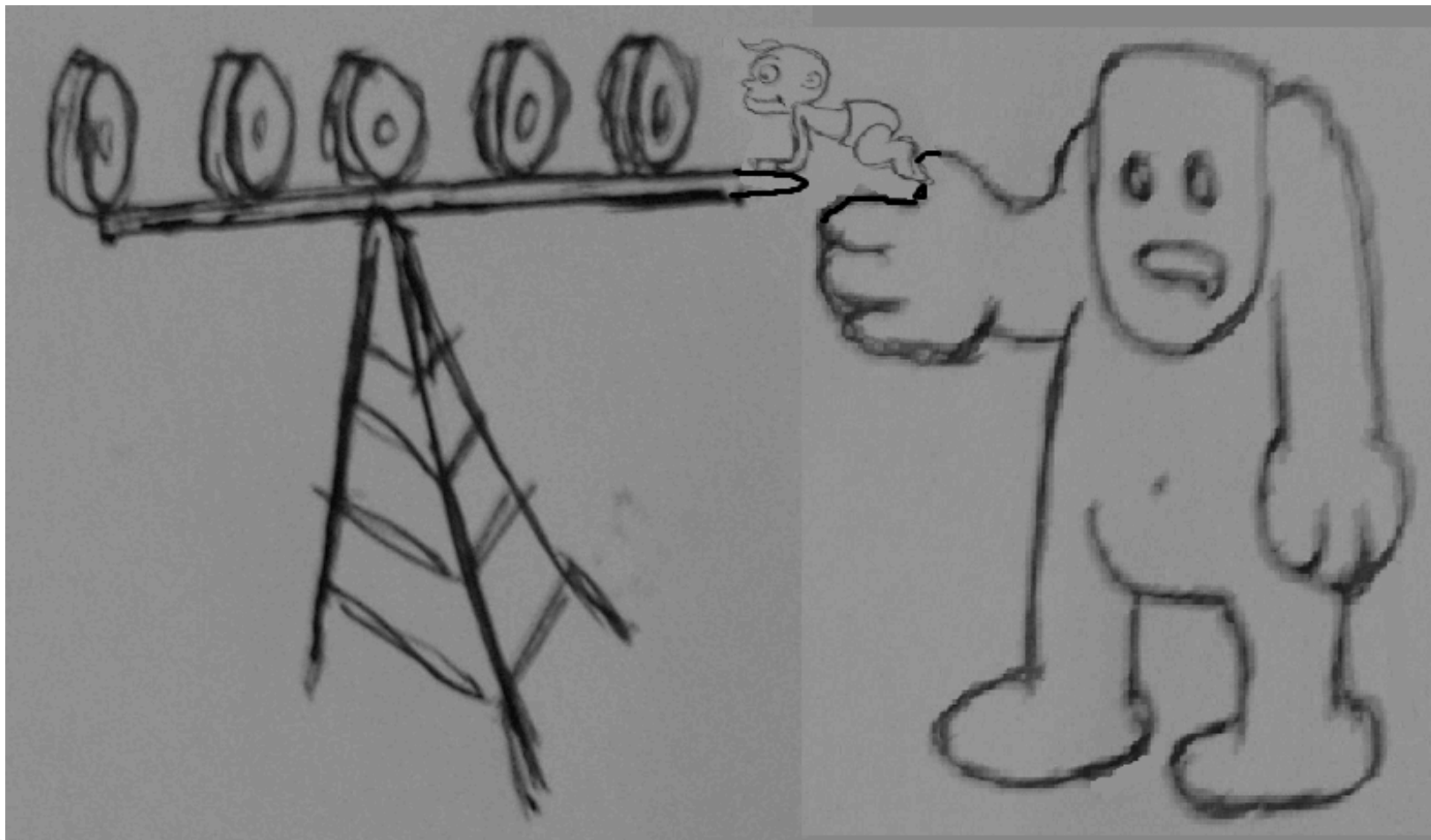
- ▶ In this case the log is discretized



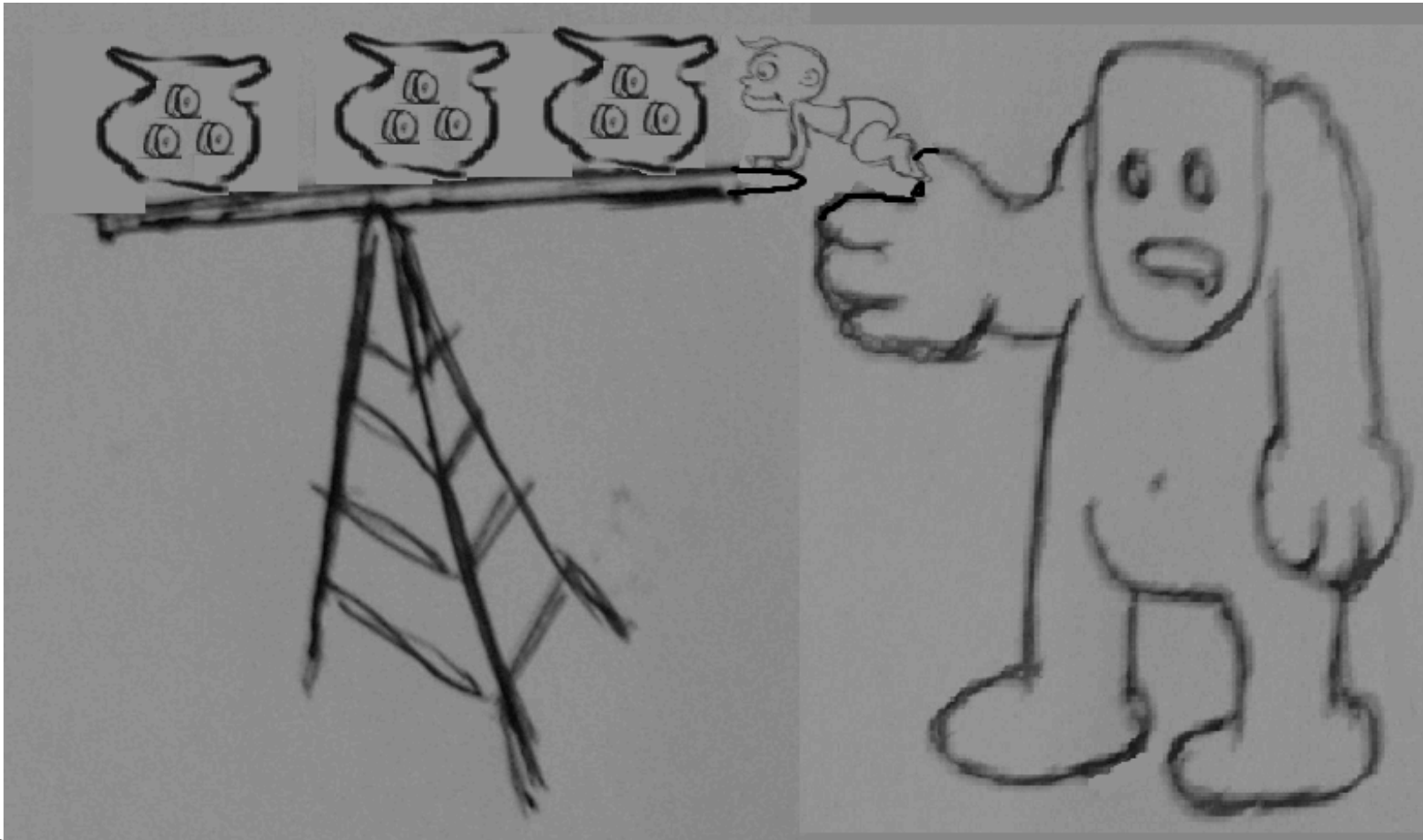
Discrete Log problem on groups



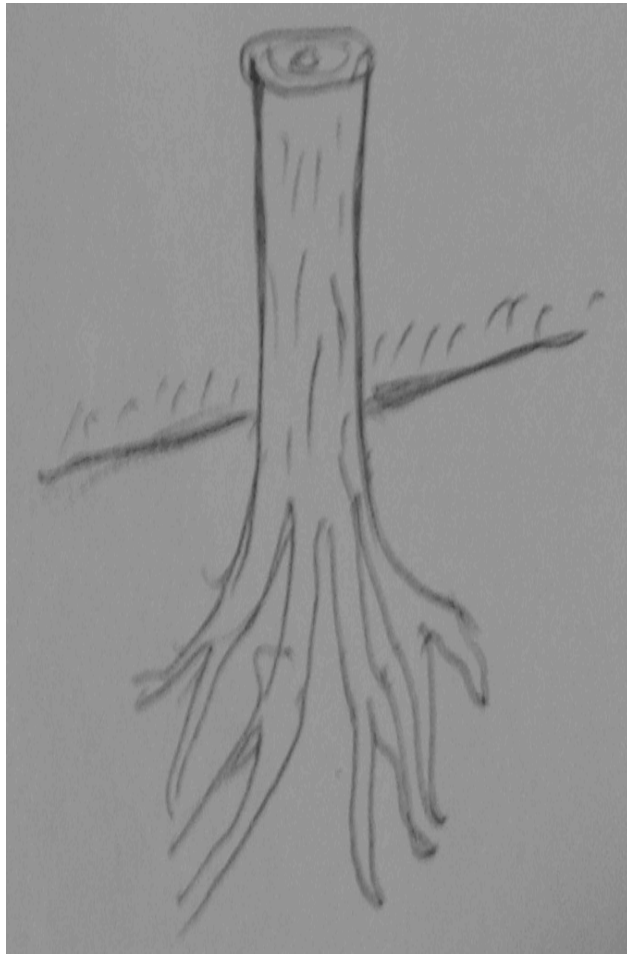
Baby step Giant step



Index Calculus



Square root method



1. Up root a big tree
2. Make a log out of it
3. Output the log in whole or discretized

On curves

- ▶ The index calculus does not work (as it is very dangerous for the baby)
- ▶ But the square root algorithm still works.

