Random Walk inside Expander Graph

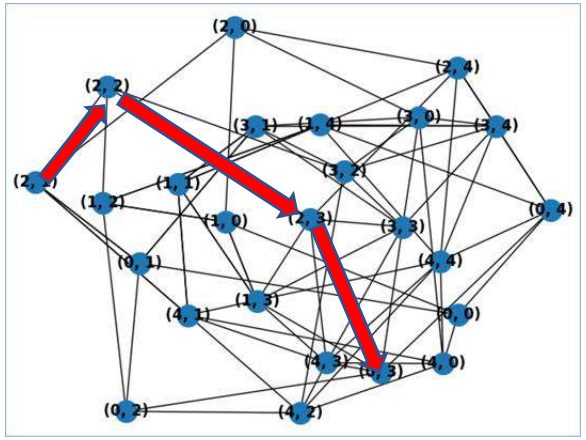
Fumihiro Tamada
Advisor: Dr. Takunari Miyazaki

Objective

Constructing a new and better random number generator by conducting random walk inside expander graph

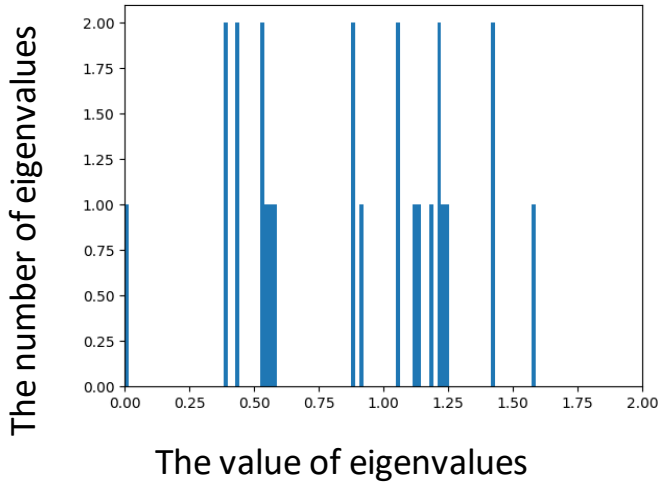
Method

1. Construct an expander graph by Margulis Method and confirm it by calculating the eigenvalues
2. Conduct a random walk inside it and create a random number generator
3. Test its correctness by counting how many consecutive values you get



Example of random walk

Result



The second highest eigen value is between 0.25 and 0.50 which is smaller than
2*sqrt((degree of the graph)-1).
Therefore, the graph is expander.

Consecutive runs	Expander Graph RNG with Margulis Method	Traditional RNG	Theoretical Result
12	3890	4319	4096 ± 64
13	1916	2175	2048 ± 45
14	933	1089	1024 ± 32

The table shows the comparison between a traditional RNG and the new RNG by counting how many consecutive runs of heads of tails more than n times in 256*65536 coin flips.

Technology

NETWORKX aws