RANDOM WALKS ON EXPANDER GRAPHS

Yicheng Shao ‘16
Advisor: Takunari Miyazaki

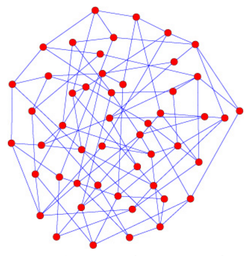
Abstract

The objective of this project is to improve pseudorandom number generation by performing random walks on expander graphs. Since pseudorandom numbers are not truly random, all sequences of pseudorandom numbers have repeating patterns. The length of repetition is called the period length, and the quality of pseudorandom numbers can be measured by such a length. In this project, we increase the period lengths of sequences of pseudorandom numbers by performing random walks on expander graphs.

Introduction

Expander Graphs

Expander graphs are graphs with high isoperimetric constants. The isoperimetric constant is a measure of connectedness within a graph.

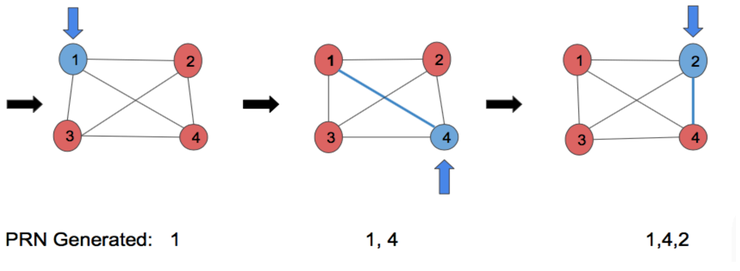


A family of expander graphs are a group of graphs with the same scheme of construction such that the isoperimetric constants of the members of the family is bounded away from zero as the graph size approaches infinity.

For the experiments in this project, we focus on 3-regular graphs (each node in the graph has three edges). More specifically, we consider two types of graph: Angluin graph[1][2] and 3-regular random graph[3].

- Angluin graph has explicit construction; its edges are selected due to fixed equations.
- 3-regular random graph has random construction; its edge selection involve some level of randomness.

Random Walk Process

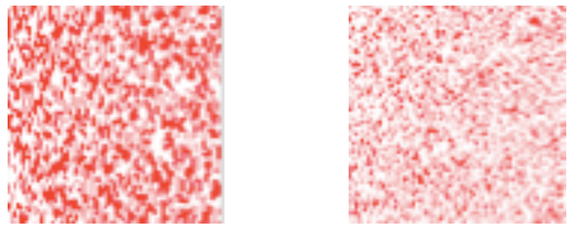


BitMap Visualization

- Bitmaps are binary images, each pixel is either colored or not.
- They can be used to see patterns.

In this experiment, we generate bitmaps to view the quality of the generated PRN, as well as the quality of the graph. In the bitmaps, whether each pixel is colored is based on whether each PRN generated is even or odd

Angluin Graph BitMap *3 Regular Random Graph BitMap*



- Observation: Angluin graph’s bitmap is more clustered 3 regular random graph’s bitmap.
- Conclusion: The PRN generated by the Angluin graph is less uniformly distributed than the 3 regular random graph, and 3 regular random graph has better quality.

Experiment

Methodology

- Define a simple PRNG with controlled period length.
- Apply random walks on expander graph to improve the quality of this PRNG.

Results

Angluin Graph	size 100, given period 10		
Walk Length	1000	10000	100000
Generated PeriodLength	120	60	100
	200	60	100
	60	200	200
	50	50	100
	200	100	300
Average	126	127	160

3 Regular Random Graph	size 100, given period 10		
Walk Length	1000	10000	100000
Generated PeriodLength	210	230	480
	100	90	360
	310	250	90
	90	200	310
	230	100	210
Average	188	174	290

- 3 regular random graphs produce better results than Angluin graphs.
- The results reflect previous observation that 3 regular random graphs have better connectivity.
- The better results in 3 regular random graphs may also due to the fact that its graph structure involves randomness.

More Comparisons

3 Regular Random Graph, size 100, given period length 10		
Walk Length	10000	100000
Generated Period Length	230	480
	90	360
	250	90
	200	310
	100	210
Average	174	290

- Longer walk lengths contribute to better results.

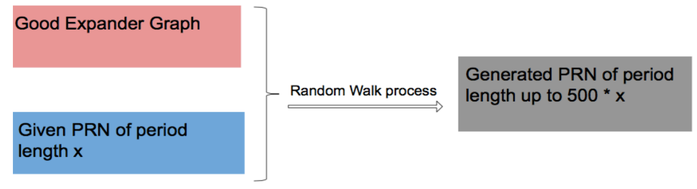
3 Regular Random Graph, size 100, walk length 10000		
Given Period Length	10	100
Generated Period Length	230	2300
	90	1200
	250	1200
	200	900
	100	2800
Average	174	1726

- Longer given PRN period lengths contribute to better results.

3 Regular Random Graph, given period length 10, walk length 10000		
graphs size	100	1000
Generated Period Length	230	3480
	90	4940
	250	910
	200	4130
	100	2190
Average	174	3130

- Larger graph sizes contribute to better results.

Conclusion



By performing random walks on expander graphs, we can improve the period length of pseudo random numbers up to 500 times.

References

[1]Angluin, D. A note on construction of Margulis. *Information Processing Letters, 8* (1). 17-19.
[2]Burca, V. ‘14 Construction Algorithms for Expander Graphs. *Computer Science Senior Thesis, Trinity College, (2014).*
[3]Chang, K. An experimental approach to studying Ramanujan graphs. *Math Junior Seminar Thesis, Princeton University,* (2001).