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\(^1\) 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.

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

<table>
<thead>
<tr>
<th>Angluin Graph size 100, given period 10</th>
<th>3 Regular Random Graph size 100, given period 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walk Length</td>
<td>1000</td>
</tr>
<tr>
<td>Generated</td>
<td>120</td>
</tr>
<tr>
<td>PeriodLength</td>
<td>200</td>
</tr>
<tr>
<td>60</td>
<td>200</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>Average</td>
<td>128</td>
</tr>
</tbody>
</table>

- 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

- Longer walk lengths contribute to better results.
- Longer given PRN period lengths contribute to better results.
- 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