A statistical look at maps of the discrete logarithm

Dr. Joshua Holden and Nathan Lindle
Mathematics and Computer Science, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803

Definitions

Functional Graph – A directed graph where the edges are determined by a transition function. In this case the function is $f: z = g^z \mod p$.

Binary Functional Graph – A functional graph where the in-degree of each node is either 0 or 2. All the graphs studied were binary functional graphs.

Component – A connected set of nodes. The average number of components is measured for each prime modulus (e.g. 1.75 for $p = 11$).

Cyclic Nodes – Nodes that are part of a cycle, including nodes which loop back on themselves. The average cyclic nodes are measured for each prime (e.g. 3.25 for $p = 11$).

Average Cycle – The average cycle size as seen from a random node in a functional graph divided by the number of nodes in all the functional graphs for a given prime (e.g. 2.05 for $p = 11$).

Average Tail – The average distance to the cycle as seen from a random node in the graph. Cyclic nodes have a distance of 0. Computation is similar to that of the average cycle (e.g. 1.225 for $p = 11$).

Max Cycle – The largest cycle in a graph. The average is taken over all bases for a given $p$ (e.g. 2.5 for $p = 11$).

Max Tail – The longest distance from a node to its cycle in a graph. Similar to max cycle (e.g. 2.75 for $p = 11$).

Example Graphs (mod 11)

- $g = 3$:
  - Components: 2
  - Cyclic nodes: 4
  - Average cycle: 2.2
  - Average tail: 0.8
  - Max cycle: 3
  - Max tail: 2

- $g = 4$:
  - Components: 1
  - Cyclic nodes: 2
  - Average cycle: 2
  - Average tail: 2
  - Max cycle: 2
  - Max tail: 4

- $g = 9$:
  - Components: 2
  - Cyclic nodes: 4
  - Average cycle: 2.6
  - Average tail: 0.8
  - Max cycle: 3
  - Max tail: 2

Results

<table>
<thead>
<tr>
<th>$p$</th>
<th>Predicted</th>
<th>Observed</th>
<th>Predicted</th>
<th>Observed</th>
<th>$p$-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>99923</td>
<td>154.516</td>
<td>165.249</td>
<td>163.805</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>99961</td>
<td>154.737</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>99972</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>99999</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>100003</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>100019</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>100049</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>100069</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
<tr>
<td>100103</td>
<td>154.899</td>
<td>165.343</td>
<td>163.809</td>
<td>0.105</td>
<td></td>
</tr>
</tbody>
</table>

Summary

- Many of the statistics gathered do not provide sufficient evidence to question the theory that modular exponentiation graphs are similar to random functional graphs.
- The observed variance in the average cycle and the average tail were significantly lower than the expected variance for a random binary functional graph.
- A few tests had surprisingly low $p$-values, but the normality tests indicate that these were just outliers.

Future Work

- Get theoretical values for maximum tail and maximum cycle variance.
- Analyze lower variances in average cycle length and average tail length to try and come up with a reason.
- Find an explanation for the lower maximum tail.