The Discrete Lambert Map

J. Chen[1] M. Lotts[2]

[1]Pomona College
[2]Randolph-Macon College

MD-DC-VA MAA Spring Section Meeting
Stevenson University
April 14th, 2012

The problem of inverting the discrete exponentiation map, $x \mapsto g^x \bmod p$, is called the Discrete Logarithm Problem.

$$x \longmapsto y \equiv g^x \bmod p$$

This is thought to be hard.

The security of several cryptographic protocols relies on this assumption.

- Diffie-Hellman Key Agreement
- Blum-Micali Cryptographically Secure Pseudorandom Number Generator
- ElGamal Encryption
- ElGamal Digital Signature Scheme
- (Elliptic Curve DLP) Elliptic Curve Cryptography

We are interested in another map that is related to the ElGamal Digital Signature Scheme.

Traditionally, the ElGamal Digital Signature Scheme is attacked by calculating discrete logarithms.

However, the attacker could instead try to invert the map $x \mapsto xg^x \bmod p$, which we call the Discrete Lambert Map.

We are investigating the functional graph induced by the DLM.

Much like the discrete exponentiation map, the difficulty of inverting this map is essential to the security of the ElGamal DSS.

Question How much do the Discrete Lambert Map-induced graphs look like “random graphs"?

We are investigating the functional graph induced by the DLM.

Much like the discrete exponentiation map, the difficulty of inverting this map is essential to the security of the ElGamal DSS.

Question How much do the Discrete Lambert Map-induced graphs look like “random graphs"?

The more nonrandom the graphs appear, the easier it could be to invert the DLM.

We are investigating the functional graph induced by the DLM.

Much like the discrete exponentiation map, the difficulty of inverting this map is essential to the security of the ElGamal DSS.

Question How much do the Discrete Lambert Map-induced graphs look like “random graphs"?

The more nonrandom the graphs appear, the easier it could be to invert the DLM.

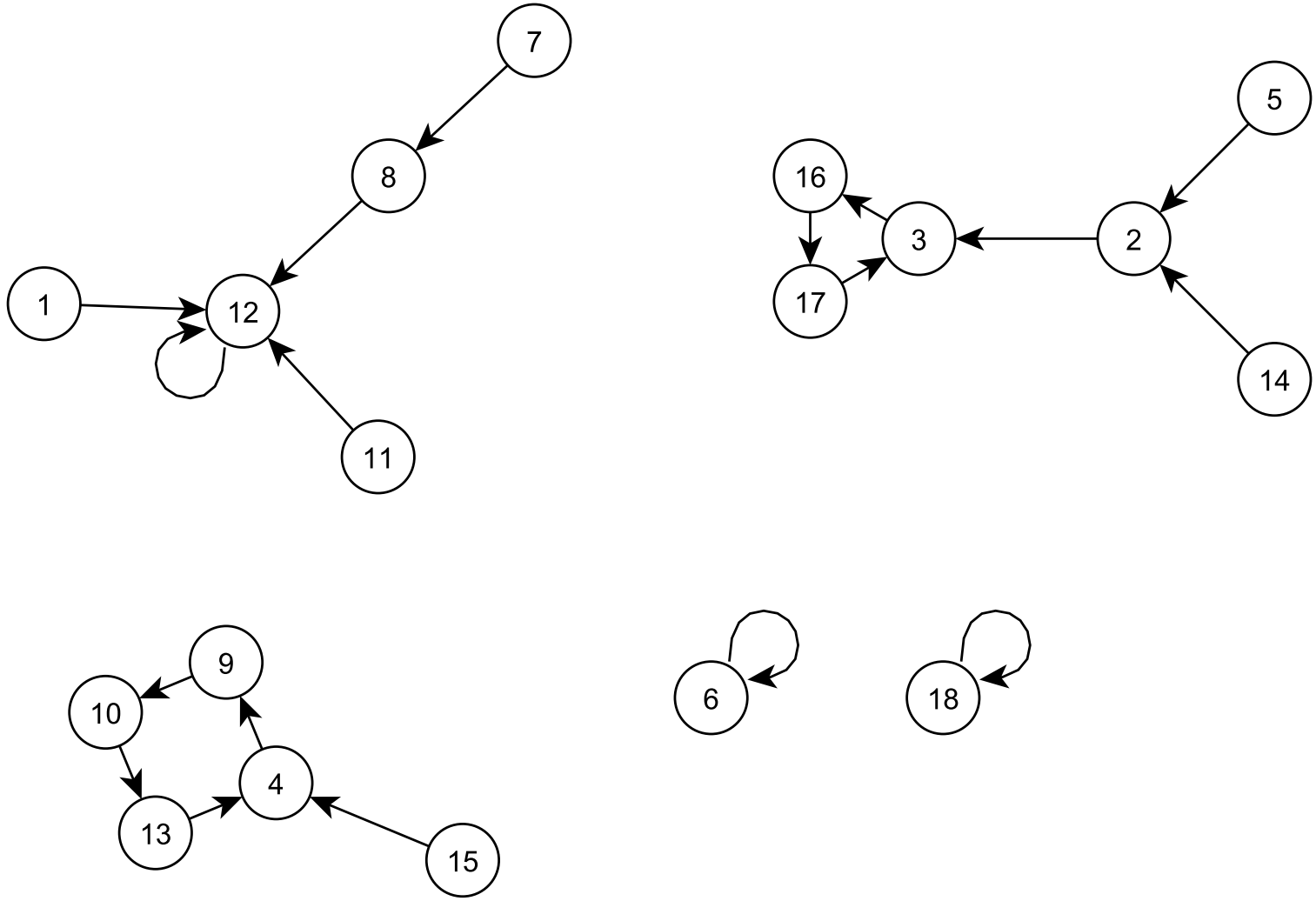
We start by examining the behavior of these functional graphs, and then use that information to improve our expected values.

What is a functional graph?

Definition A *functional graph* is a directed graph where each vertex has precisely one directed edge coming out from it.

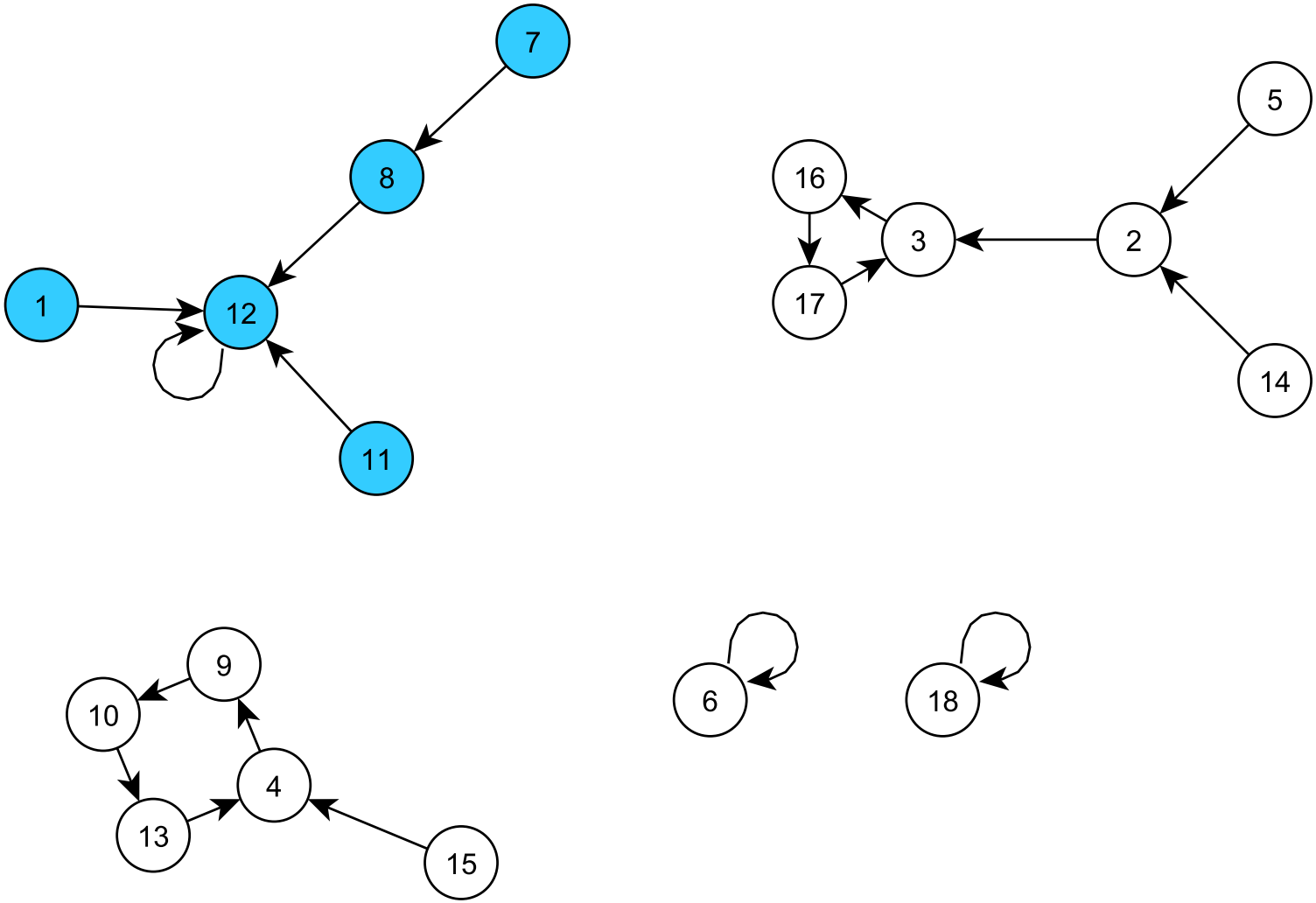
In the functional graph of $x \mapsto xg^x \pmod{p}$, each vertex, or *node*, is an element in $(\mathbb{Z}/p\mathbb{Z})^* = \{1, ..., p-1\}$, where p is prime.

For example...



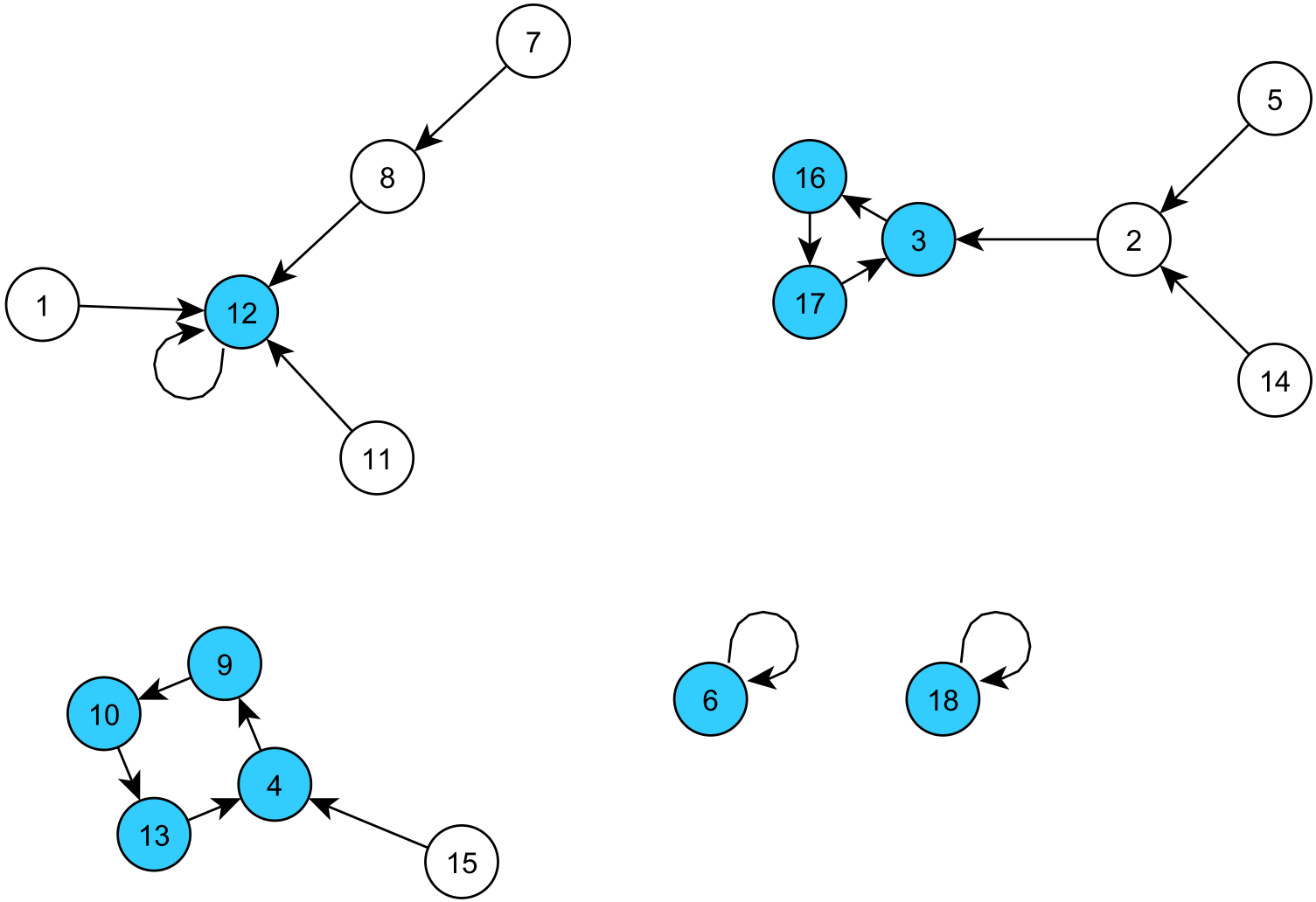
$$x \mapsto x12^x \pmod{19}$$

Some objects of interest in functional graphs are



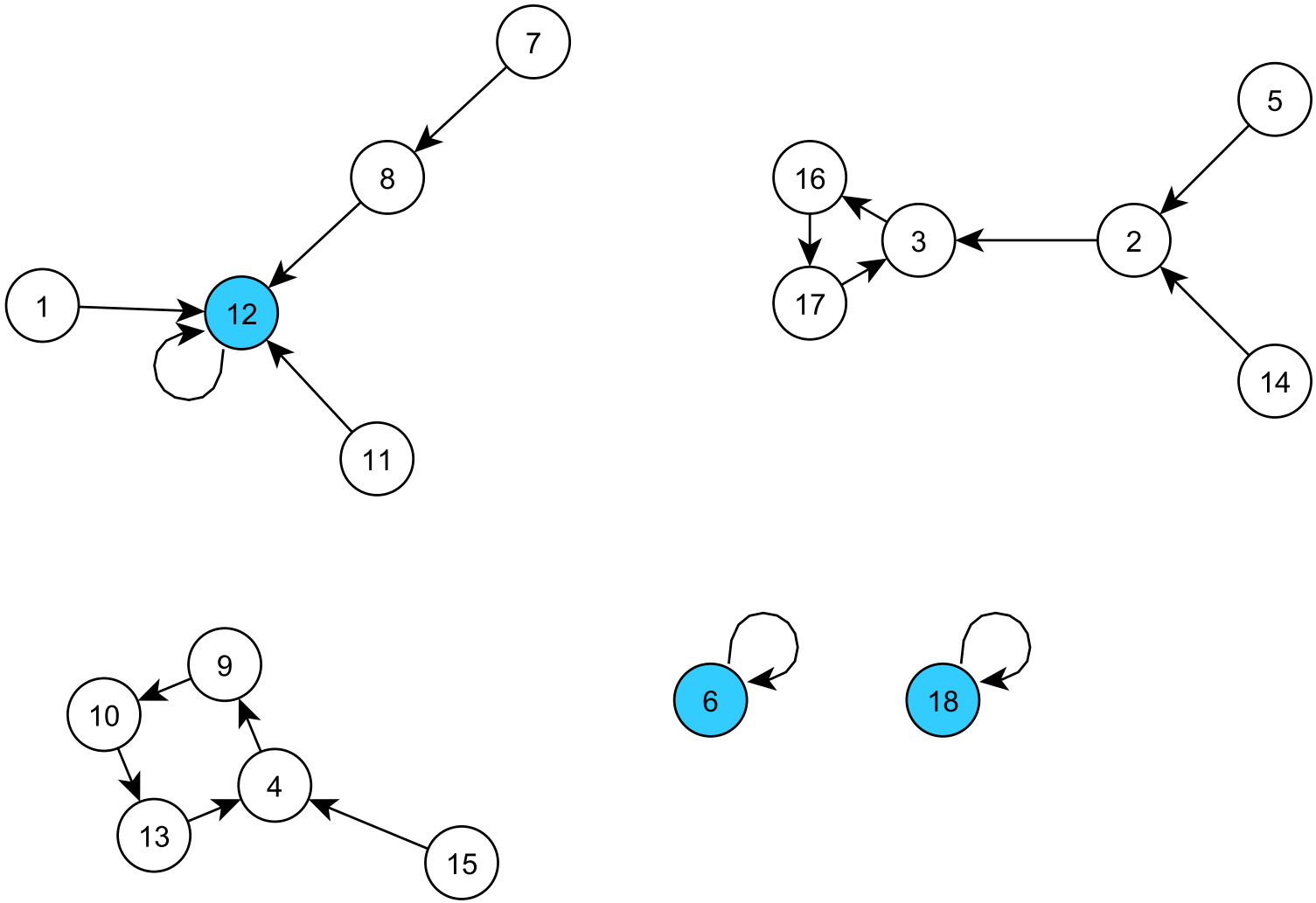
Connected components

Some objects of interest in functional graphs are



Cycles

Some objects of interest in functional graphs are



Fixed points

Some objects of interest in functional graphs are

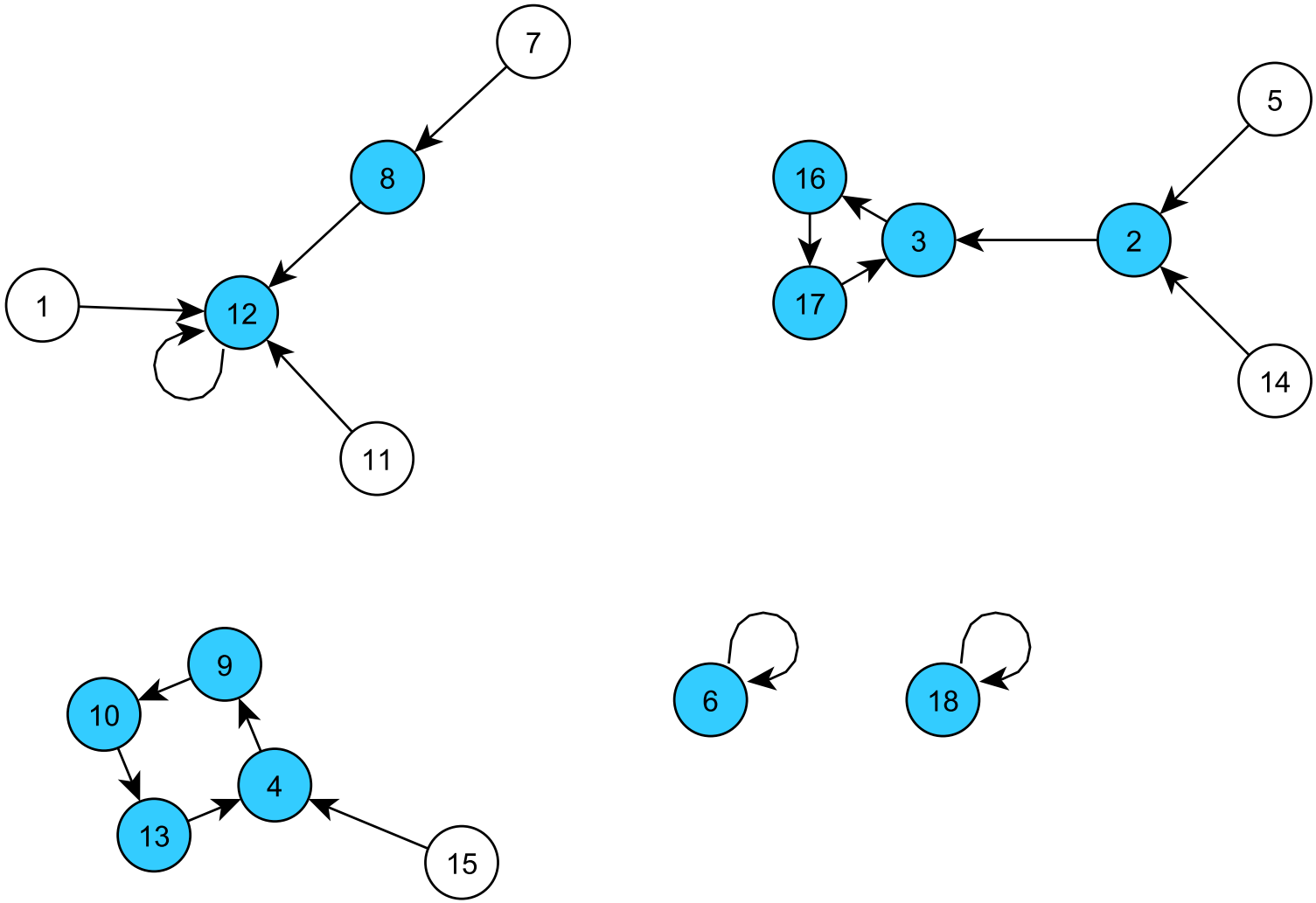


Image nodes

Definition Let $g \in \{1, ..., p-1\}$. The *order* of g is the smallest positive integer n such that $g^n \equiv 1 \pmod{p}$.

Definition Let $g \in \{1, ..., p-1\}$. The *order* of g is the smallest positive integer n such that $g^n \equiv 1 \pmod{p}$.

- The order of g divides $p-1$.

Definition Let $g \in \{1, ..., p-1\}$. The *order* of g is the smallest positive integer n such that $g^n \equiv 1 \pmod{p}$.

- The order of g divides $p-1$.

Example Let $g = 7$, $p = 19$. $7^1 \equiv 7, 7^2 \equiv 11, 7^3 \equiv 1 \pmod{19}$, so the order of 7 is 3.

Definition A *primitive root* of a prime p is an integer $g \in \{1, ..., p-1\}$ such that g has order $p-1$.

Definition A *primitive root* of a prime p is an integer $g \in \{1, ..., p-1\}$ such that g has order $p-1$.

- A *primitive root* g is a *generator* of $(\mathbb{Z}/p\mathbb{Z})^*$, i.e. $\{g, g^2, ..., g^{p-1}\} = \{1, 2, ..., p-1\}$.

Definition A *primitive root* of a prime p is an integer $g \in \{1, ..., p-1\}$ such that g has order $p-1$.

- A *primitive root* g is a *generator* of $(\mathbb{Z}/p\mathbb{Z})^*$, i.e. $\{g, g^2, ..., g^{p-1}\} = \{1, 2, ..., p-1\}$.

Example Let $p = 19$. The primitive roots are $2, 3, 10, 13, 14, 15$. They all have order $p-1$.

Definition Let n be a positive integer. Then $g \in \{1, ..., p-1\}$ is an n^{th} *power residue* if $x^n \equiv g \pmod{p}$ has a solution.

Definition Let n be a positive integer. Then $g \in \{1, ..., p-1\}$ is an n^{th} *power residue* if $x^n \equiv g \pmod{p}$ has a solution.

- When $n = 2$, we call g a *quadratic residue*

Definition Let n be a positive integer. Then $g \in \{1, ..., p-1\}$ is an n^{th} *power residue* if $x^n \equiv g \pmod{p}$ has a solution.

- When $n = 2$, we call g a *quadratic residue*

Example Let $p = 19$. We see that $5 \equiv 9^2 \pmod{19}$, so 5 is a quadratic residue mod 19.

Basic Behavior

If $g = 1$, every $x \in (\mathbb{Z}/p\mathbb{Z})^*$ is a fixed point.

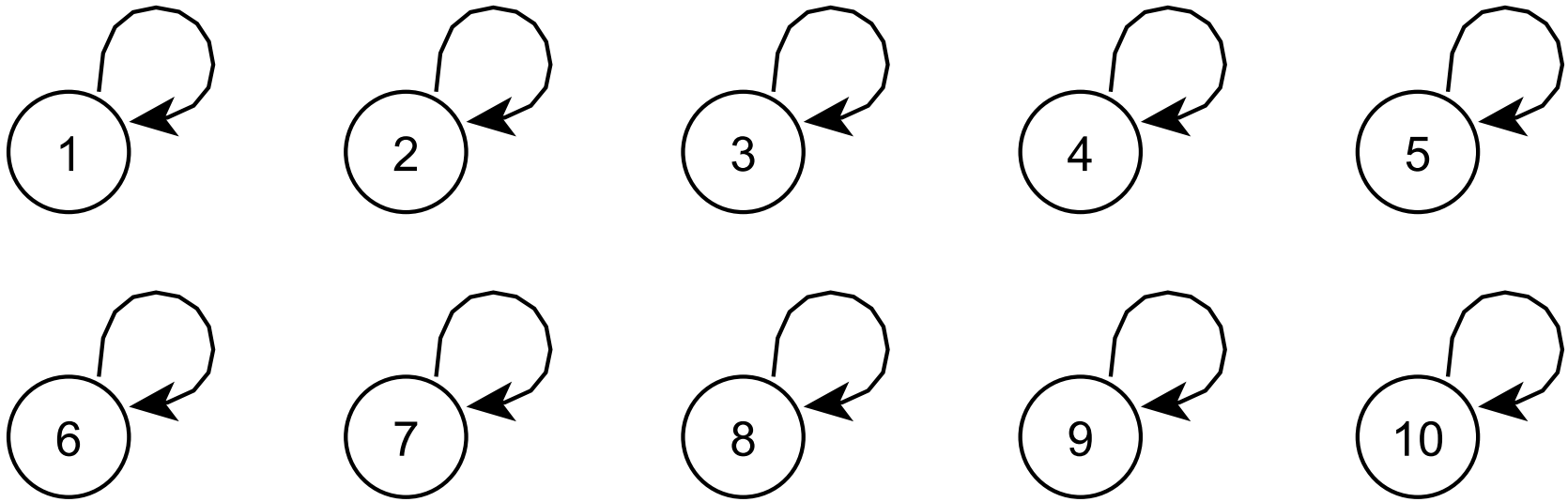


Figure: $g = 1$, $p = 11$

In every graph, $1 \mapsto g$ and $(p-1) \mapsto (p-1)$.

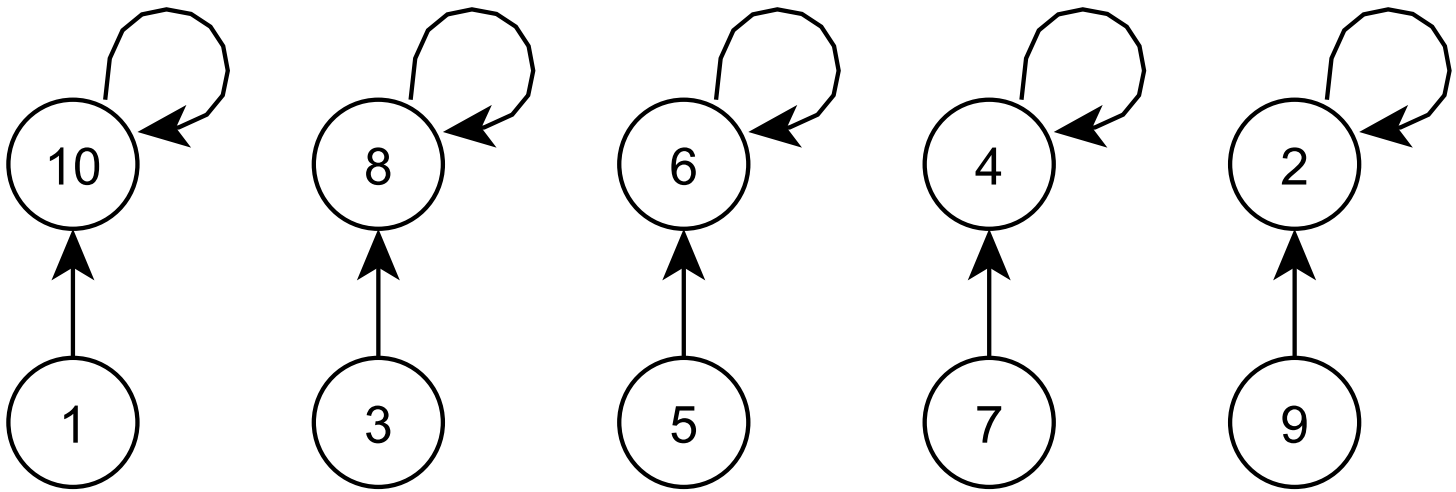


Figure: $g = 10$, $p = 11$

Fixed Points

The fixed points of the DLM functional graphs are precisely the multiples of the order of g.

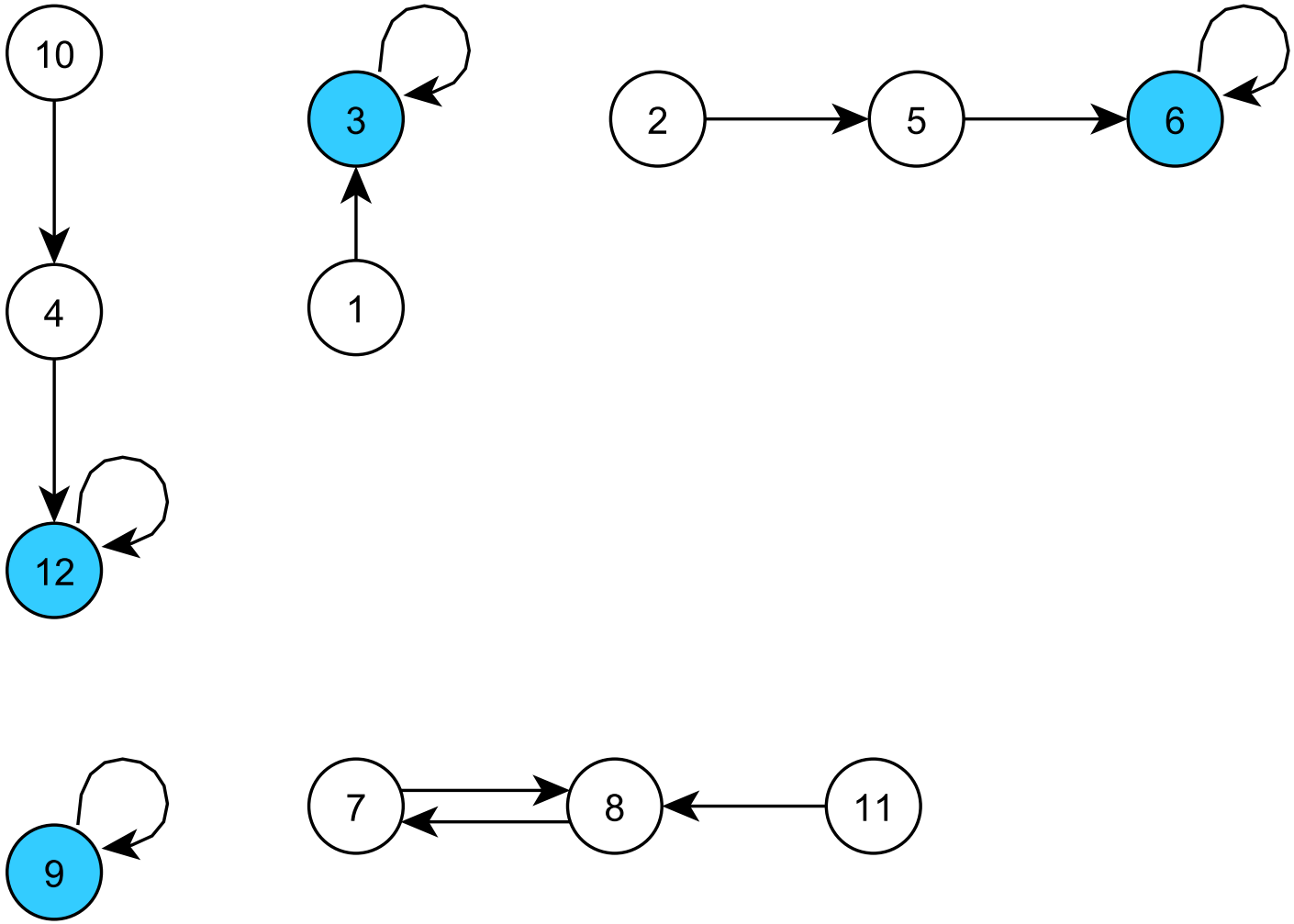


Figure: $g = 3$, $p = 13$

The number of fixed points is $\frac{p-1}{n}$, where $n = \mathrm{ord}_p(g)$.

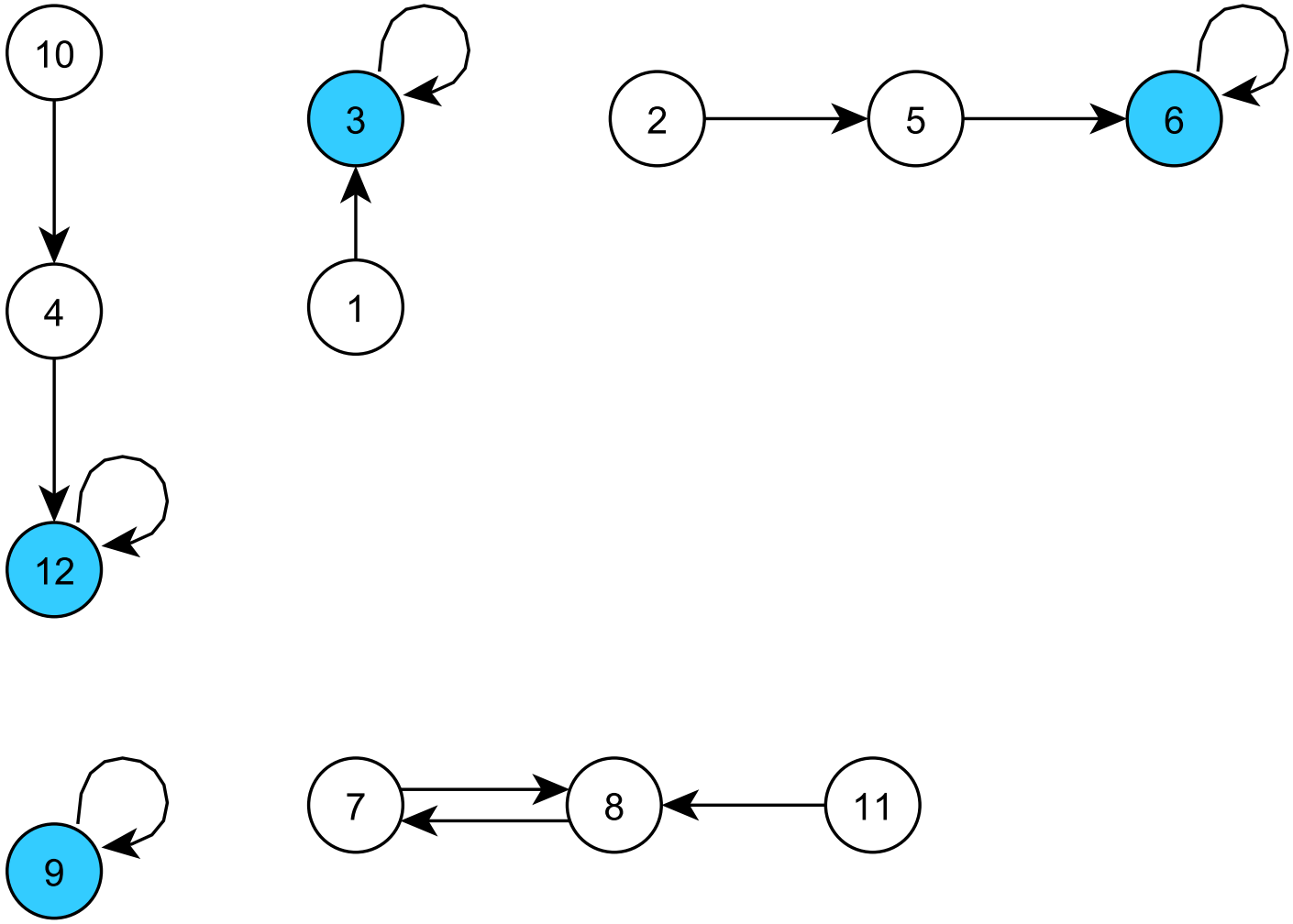


Figure: $g = 3$, $p = 13$

Cycles

If the graph contains an m-cycle, then the sum of the m nodes in the cycle is divisible by the order of g.

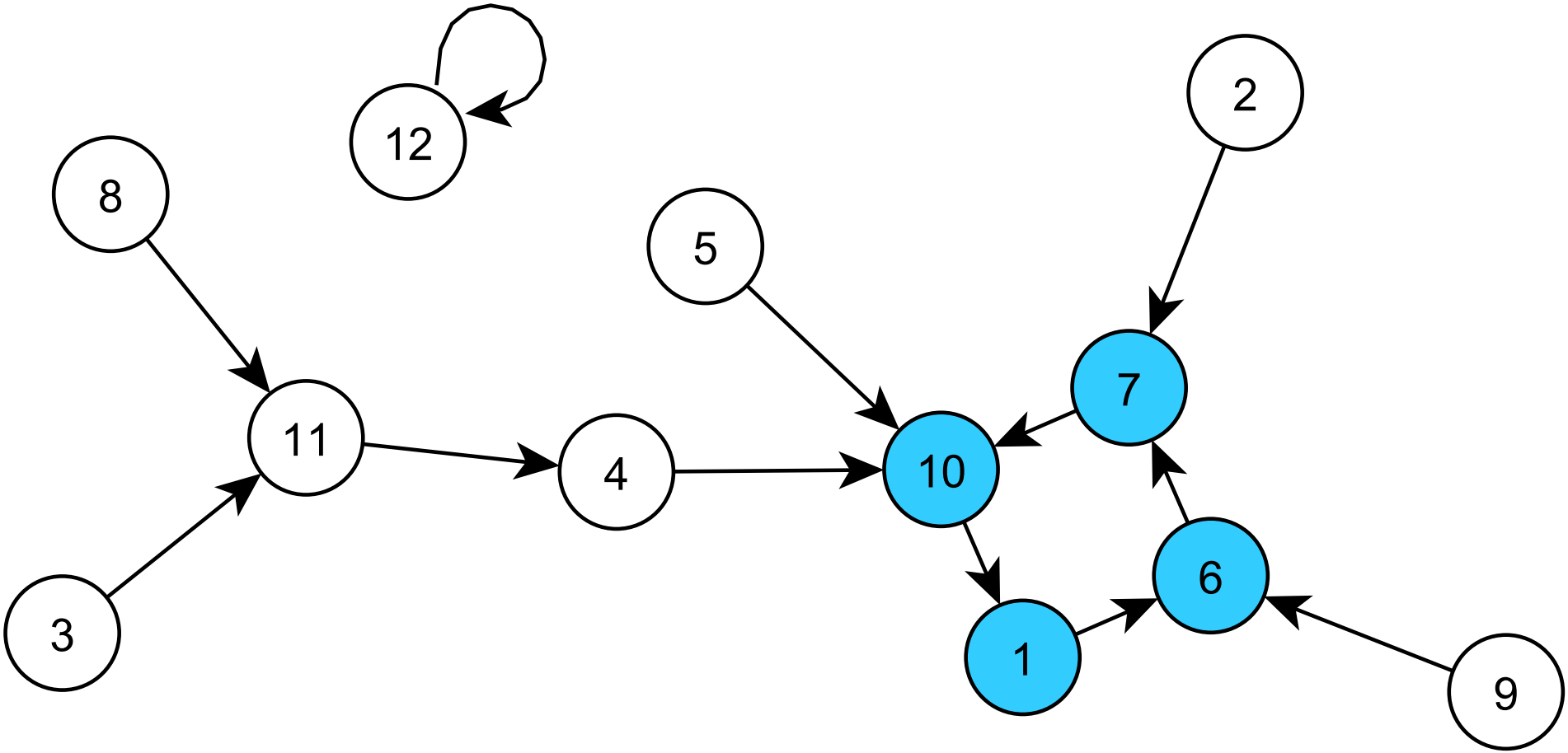


Figure: $g = 6$, $p = 13$

Power Residues

Some results about power residues

$$x \mapsto xg^x \pmod{p}$$

Theorem If g has order n, then g is an $\frac{p-1}{n}^{\text{th}}$ power residue.

Some results about power residues

$$x \mapsto xg^x \pmod{p}$$

Theorem If g has order n, then g is an $\frac{p-1}{n}^{\text{th}}$ power residue.

Proposition Given that g is an $\frac{p-1}{n}^{\text{th}}$ power residue, x is an $\frac{p-1}{n}^{\text{th}}$ power residue $\iff$ xg^x is an $\frac{p-1}{n}^{\text{th}}$ power residue.

Some results about power residues

$$x \mapsto xg^x \pmod{p}$$

Theorem If g has order n, then g is an $\frac{p-1}{n}^{\text{th}}$ power residue.

Proposition Given that g is an $\frac{p-1}{n}^{\text{th}}$ power residue, x is an $\frac{p-1}{n}^{\text{th}}$ power residue $\iff$ xg^x is an $\frac{p-1}{n}^{\text{th}}$ power residue.

- In other words, all the $\frac{p-1}{n}^{\text{th}}$ power residues map to each other.

Here, $g = 12$ has order 6 and is a 3^{rd} power residue.

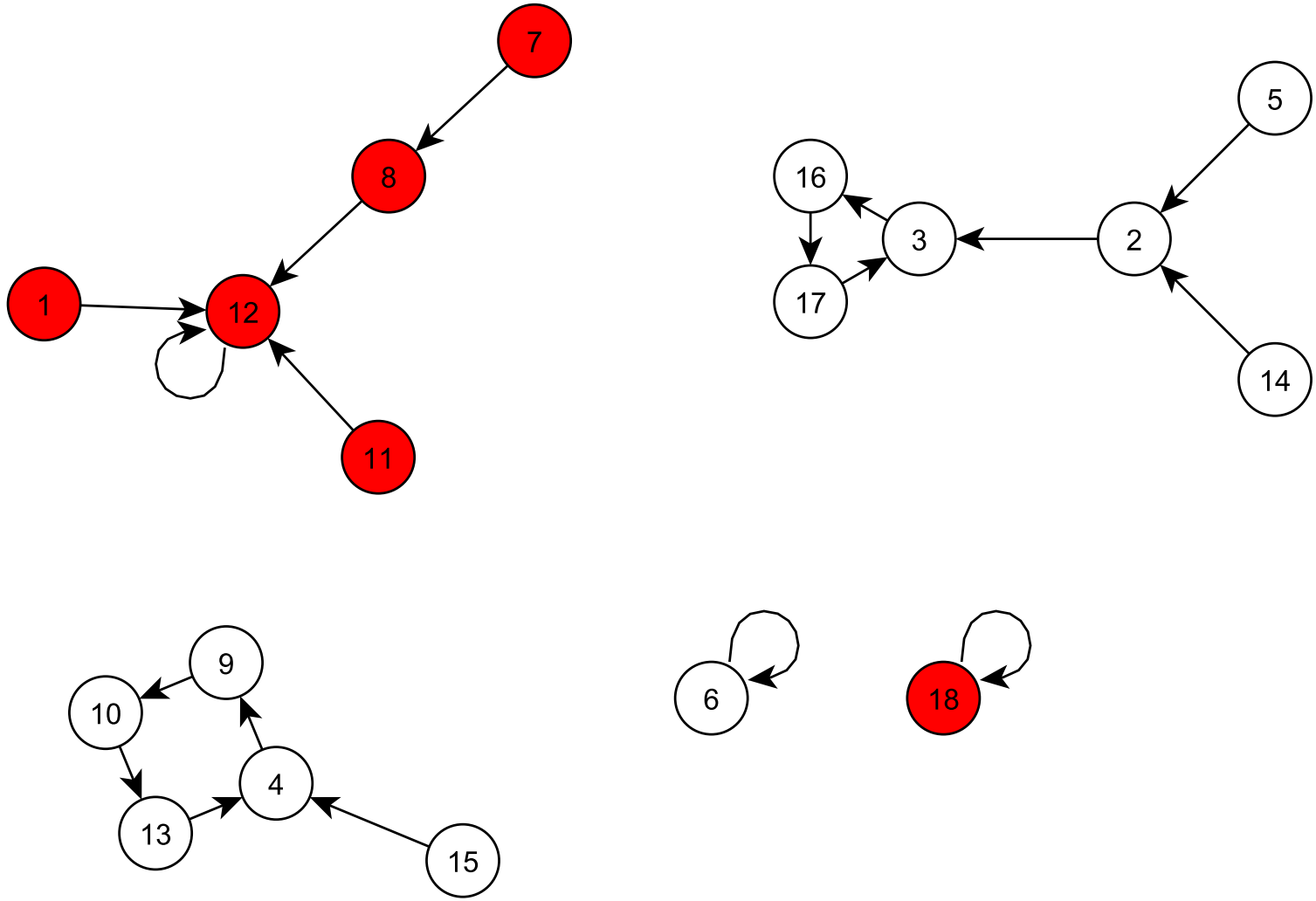


Figure: $x \mapsto x12^x \pmod{19}$

Connected Components

The order of g is an upper bound on the number of nodes in a connected component that contains a $\frac{p-1}{n}^{\text{th}}$ power residue.

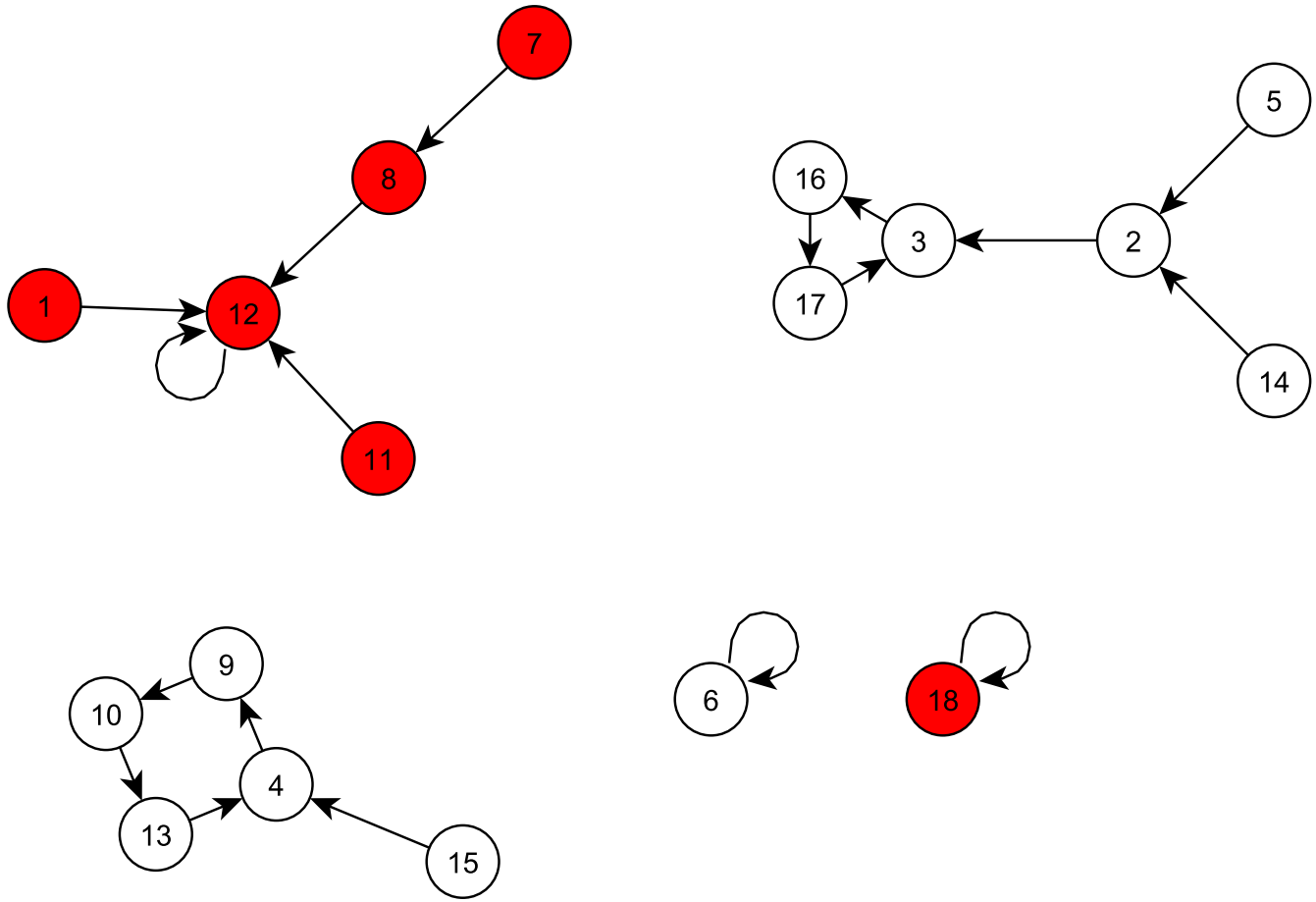


Figure: $x \mapsto x12^x \pmod{19}$

Further results

- Suppose g has order n. Then the group generated by g, $\{g, g^2, ..., g^n\}$, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, we'll call it H.

Further results

- Suppose g has order n. Then the group generated by g, $\{g, g^2, ..., g^n\}$, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, we'll call it H.
- The elements of H are precisely the $\frac{p-1}{n}^{\text{th}}$ power residues mod p.

Further results

- Suppose g has order n. Then the group generated by g, $\{g, g^2, ..., g^n\}$, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, we'll call it H.
- The elements of H are precisely the $\frac{p-1}{n}^{\text{th}}$ power residues mod p.
- What about cosets of H?

Further results

- Suppose g has order n. Then the group generated by g, $\{g, g^2, ..., g^n\}$, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, we'll call it H.
- The elements of H are precisely the $\frac{p-1}{n}^{\text{th}}$ power residues mod p.
- What about cosets of H?

  Example Let $g = 12$, $p = 19$.

Further results

- Suppose g has order n. Then the group generated by g, $\{g, g^2, ..., g^n\}$, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, we'll call it H.
- The elements of H are precisely the $\frac{p-1}{n}^{\text{th}}$ power residues mod p.
- What about cosets of H?

Example Let $g = 12$, $p = 19$.

H	1	7	8	11	12	18
2H	2	14	16	3	5	17
4H	4	9	13	6	10	15

All elements of H are $\frac{p-1}{n} = \frac{19-1}{6} = 3^{\text{rd}}$ power residues.

The elements of distinct left cosets of H all map to each other.

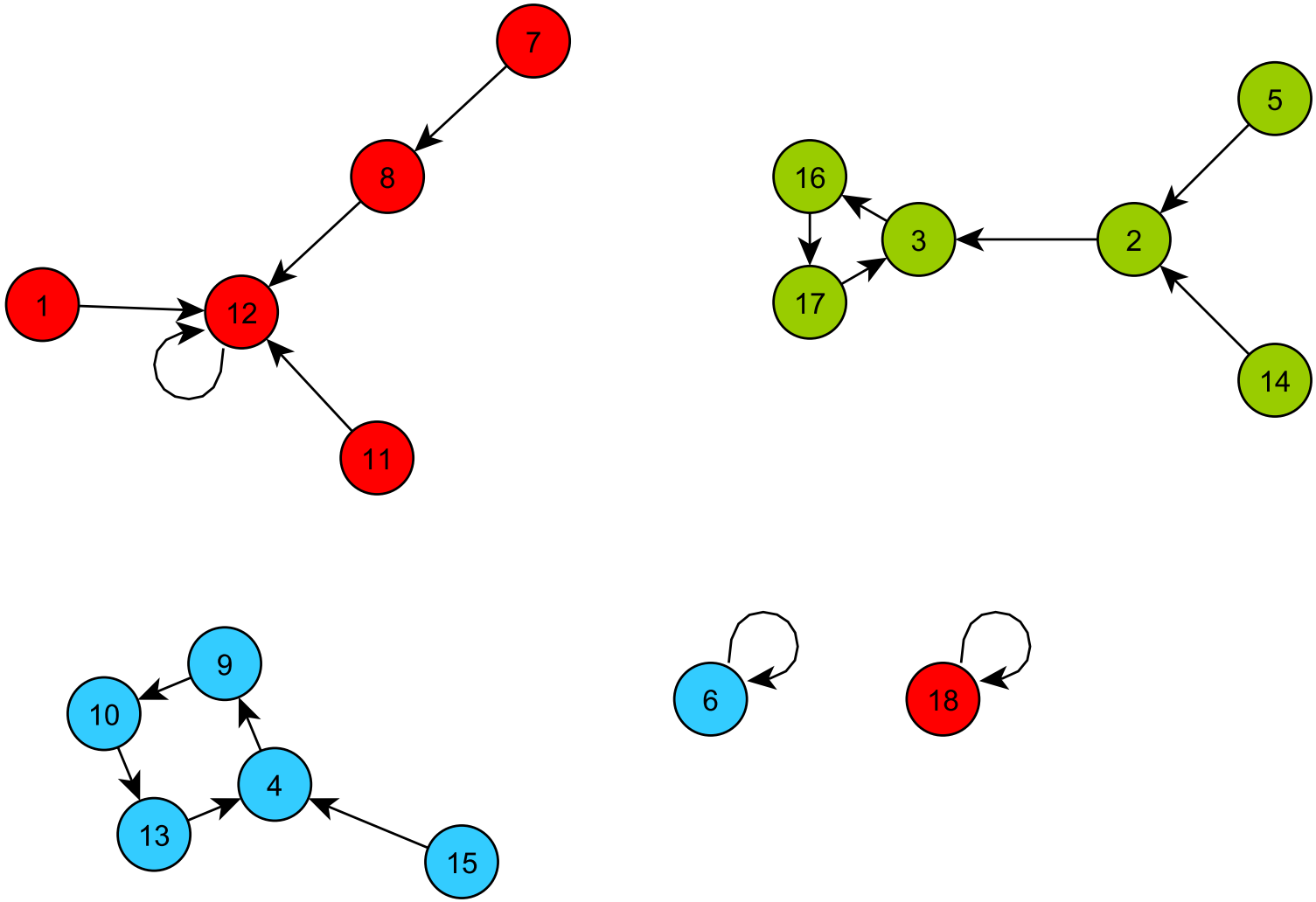


Figure: $x \mapsto x12^x \pmod{19}$

The order of g is an upper bound on the number of nodes in any given connected component.

- A connected component of the functional graph consists entirely of elements of a left coset xH, for some $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

The order of g is an upper bound on the number of nodes in any given connected component.

- A connected component of the functional graph consists entirely of elements of a left coset xH, for some $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

Corollary If g has order n, then $\frac{p-1}{n}$ is a lower bound on the number of connected components of the functional graph.

The order of g is an upper bound on the number of nodes in any given connected component.

- A connected component of the functional graph consists entirely of elements of a left coset xH, for some $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

Corollary If g has order n, then $\frac{p-1}{n}$ is a lower bound on the number of connected components of the functional graph.

These graphs act more like $\frac{p-1}{n}$ graphs of n nodes each!

Statistical Analysis

How much do DLM-induced graphs look like random graphs?

- We want to gather data about the graphs our mapping creates.

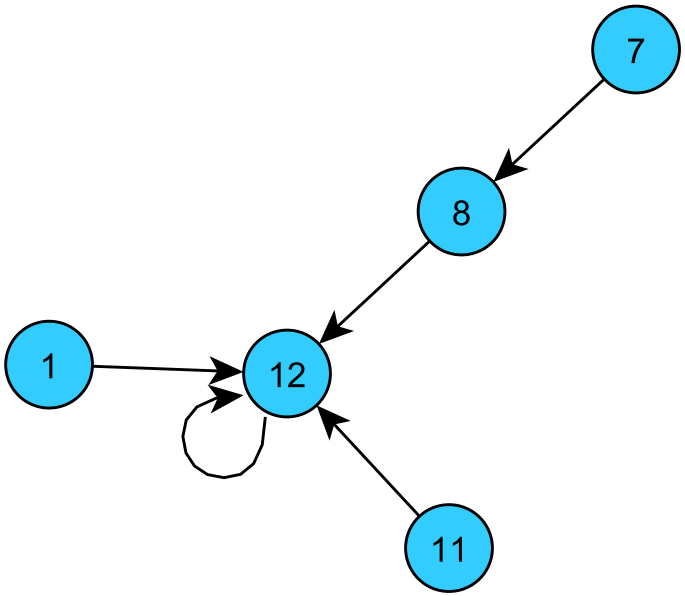
How much do DLM-induced graphs look like random graphs?

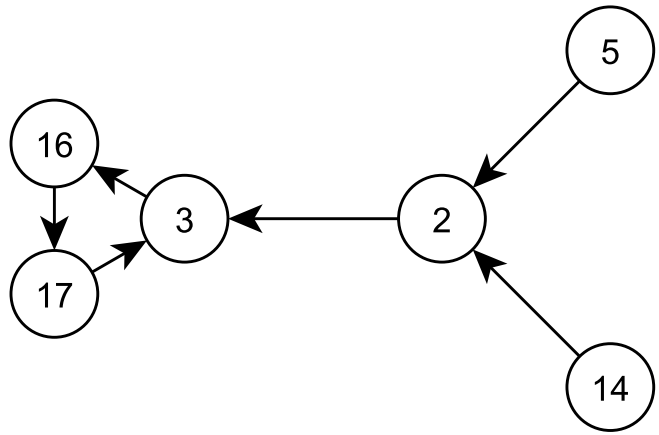
- We want to gather data about the graphs our mapping creates.
- We want to compare that data to expected values.

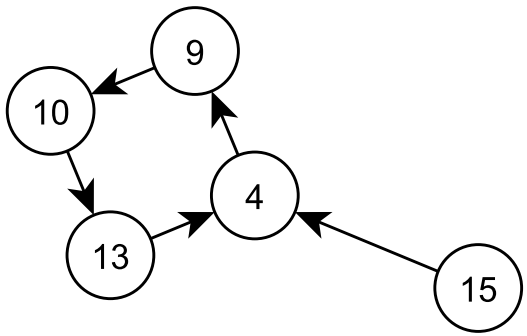
How much do DLM-induced graphs look like random graphs?

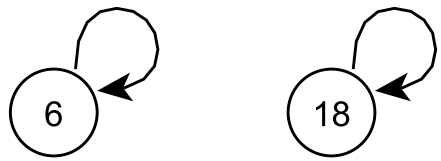
- We want to gather data about the graphs our mapping creates.
- We want to compare that data to expected values.
- We want to use statistical software to see if there is a significant difference between our observations and our predictions.

We determined that the following graph characteristics would be most important to study.



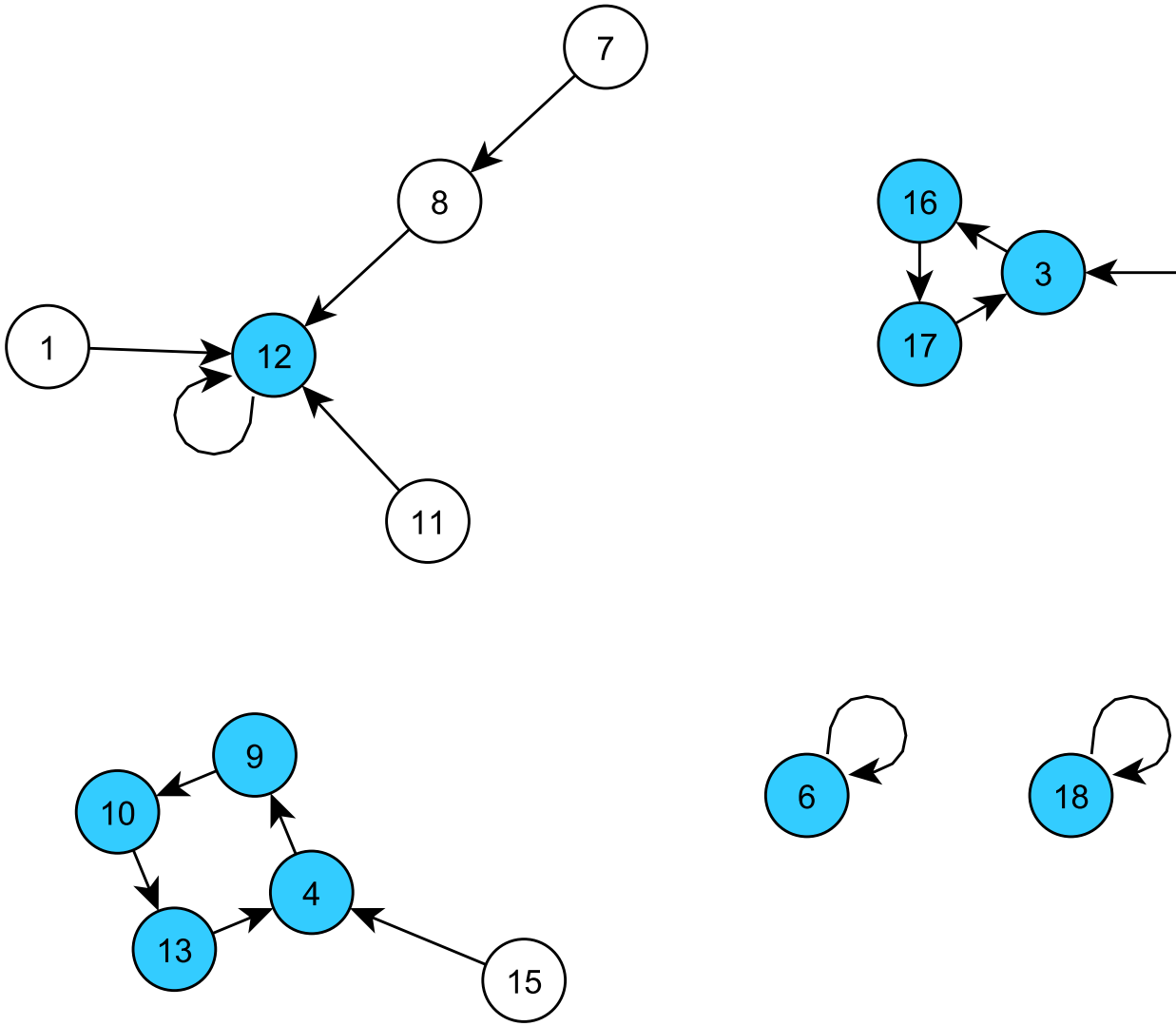






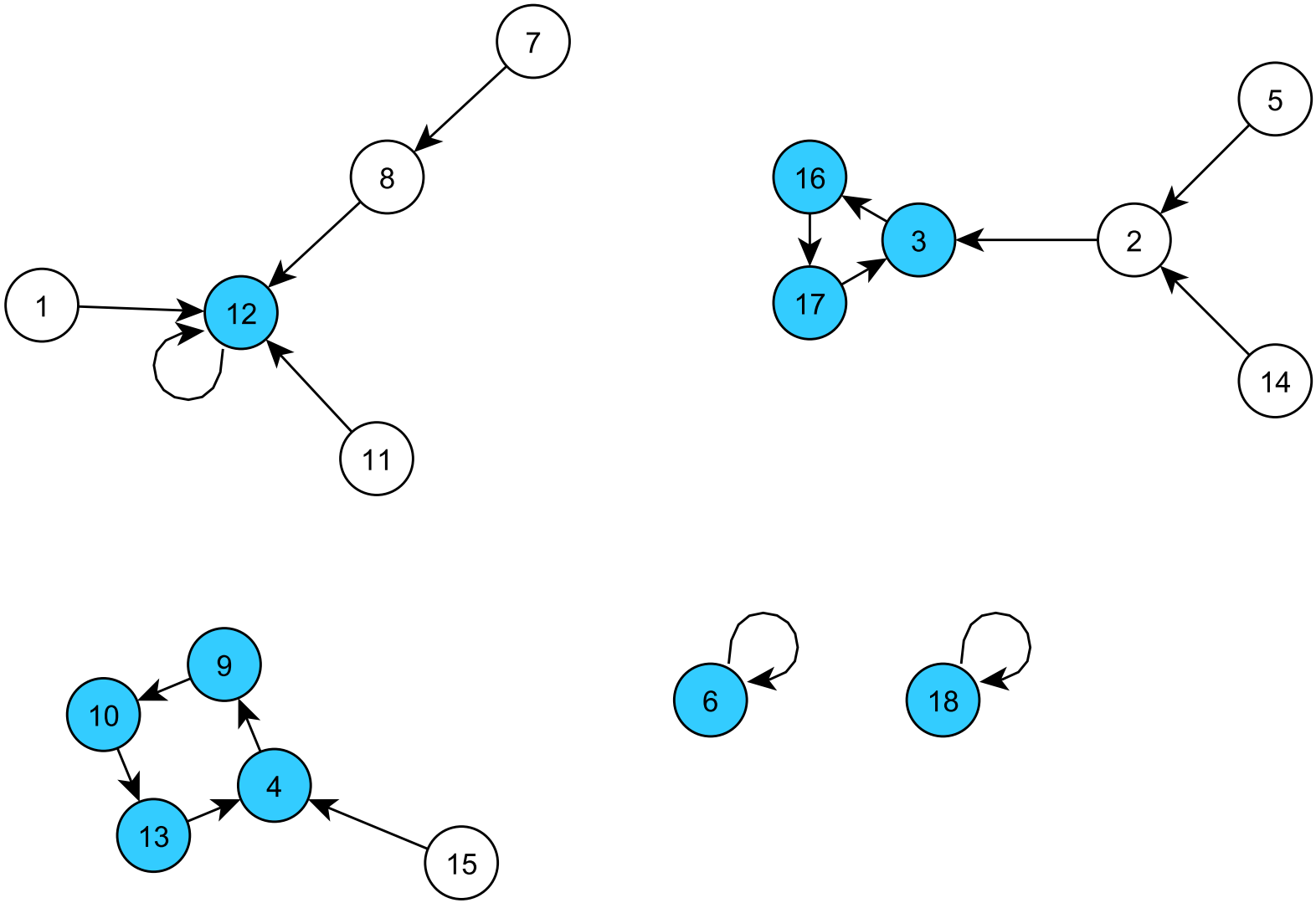
Number of components

We determined that the following graph characteristics would be most important to study.



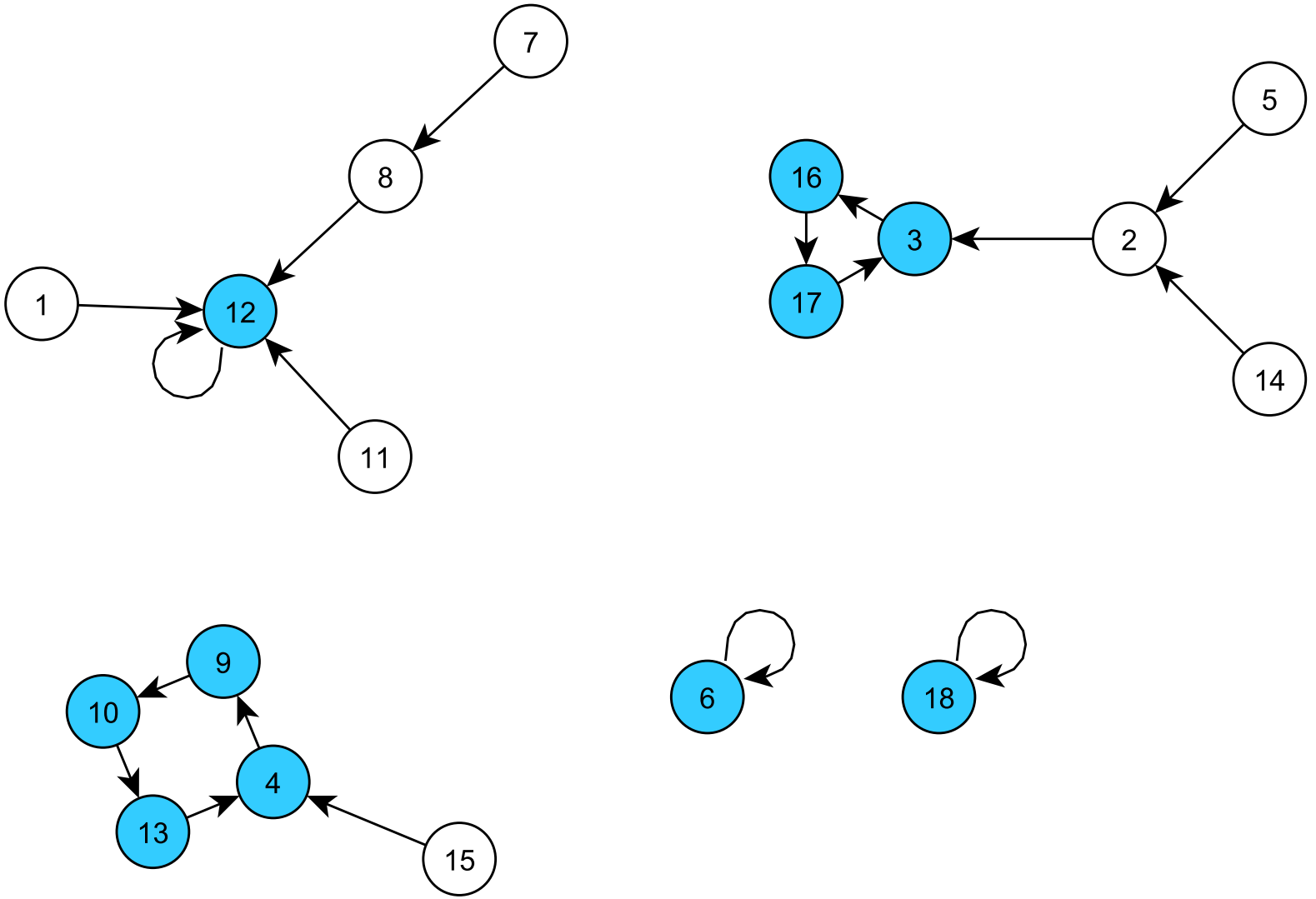
Number of cyclic nodes

We determined that the following graph characteristics would be most important to study.



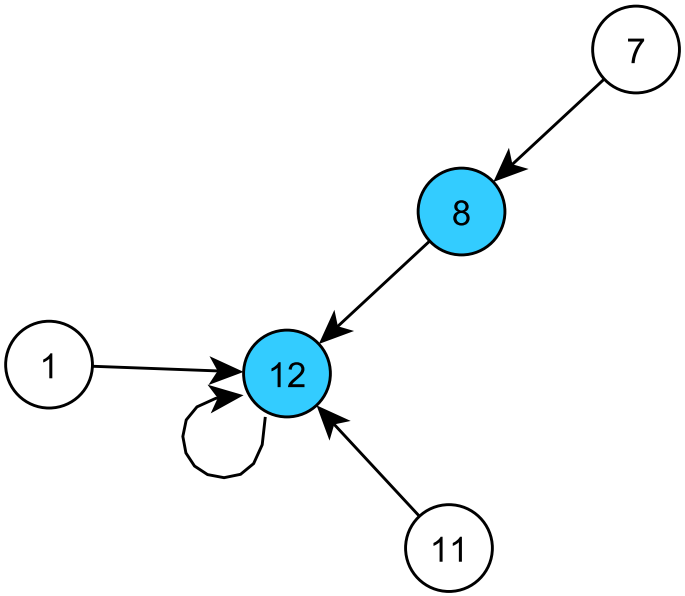
Total cycle length

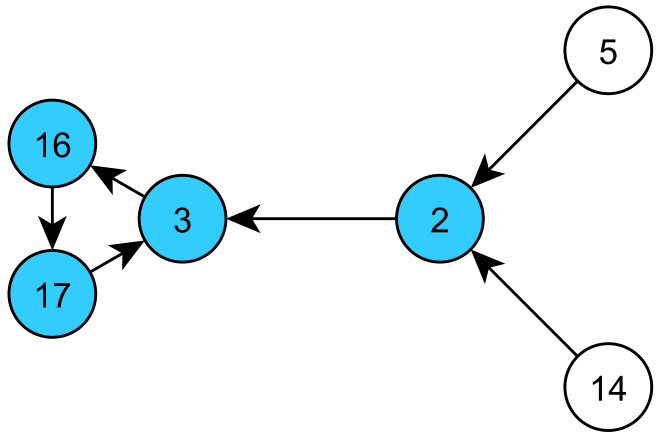
We determined that the following graph characteristics would be most important to study.

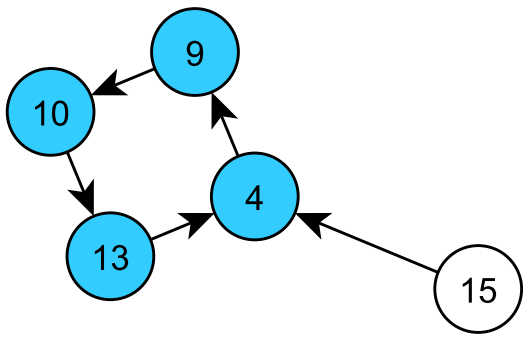


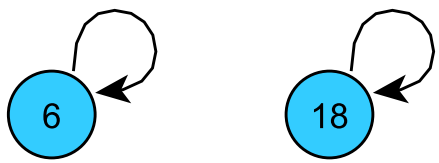
Total distance to cycle

We determined that the following graph characteristics would be most important to study.



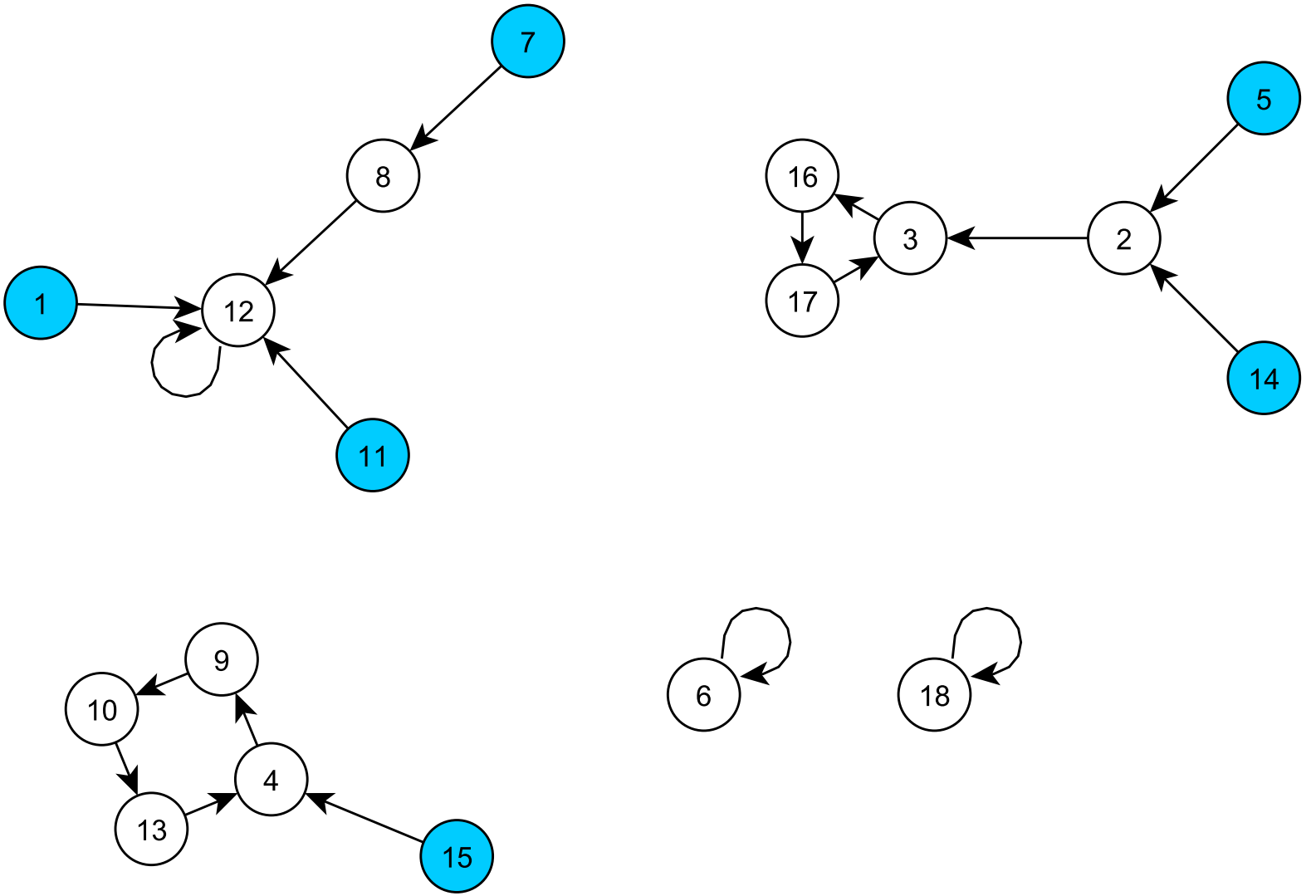






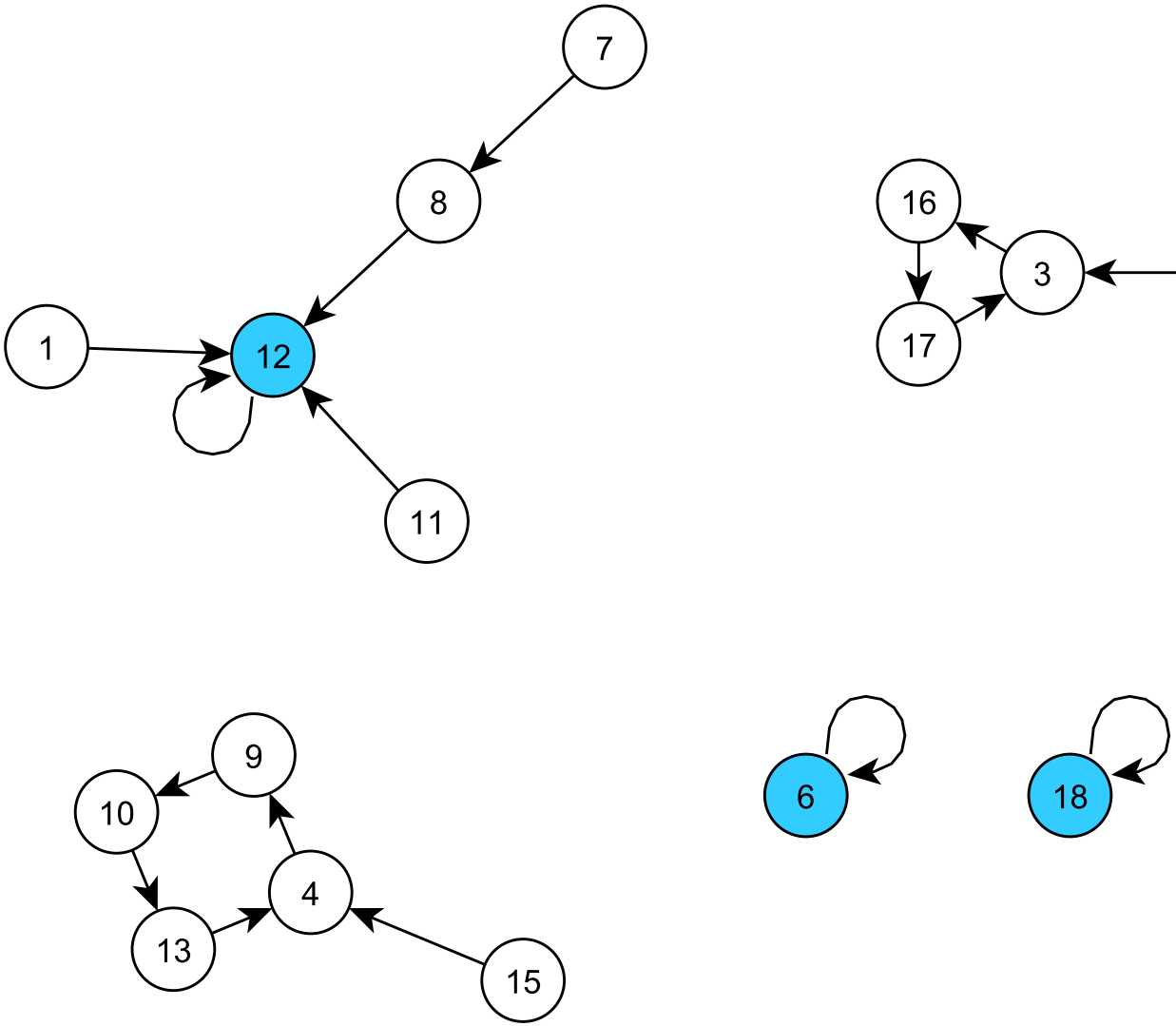
Number of image nodes

We determined that the following graph characteristics would be most important to study.



Number of terminal nodes

We determined that the following graph characteristics would be most important to study.



Number of fixed points

In addition to total sum statistics, we are also looking at maxima and averages.

- Maximum cycle length
- Maximum tail length
- Average cycle length
- Average tail length

After determining the relevant graph characteristics, we found results from literature that give asymptotic forms for the expected values of specific random graph characteristics.

- Number of components $\sim \frac{1}{2} \ln n$
- Number of cyclic nodes $\sim \sqrt{\frac{\pi n}{2}}$
- Number of terminal nodes $\sim e^{-1} n$
- Tail length, cycle length $\sim \sqrt{\frac{\pi n}{8}}$
- Maximum tail length $\sim \sqrt{2\pi n} \ln 2$
- Maximum cycle length $\sim 0.78248\sqrt{n}$

For our analysis, we used the first twenty safe primes greater than 40,000. For each prime, we gathered data for the graphs from $g = 2$ to $g = p - 2$.

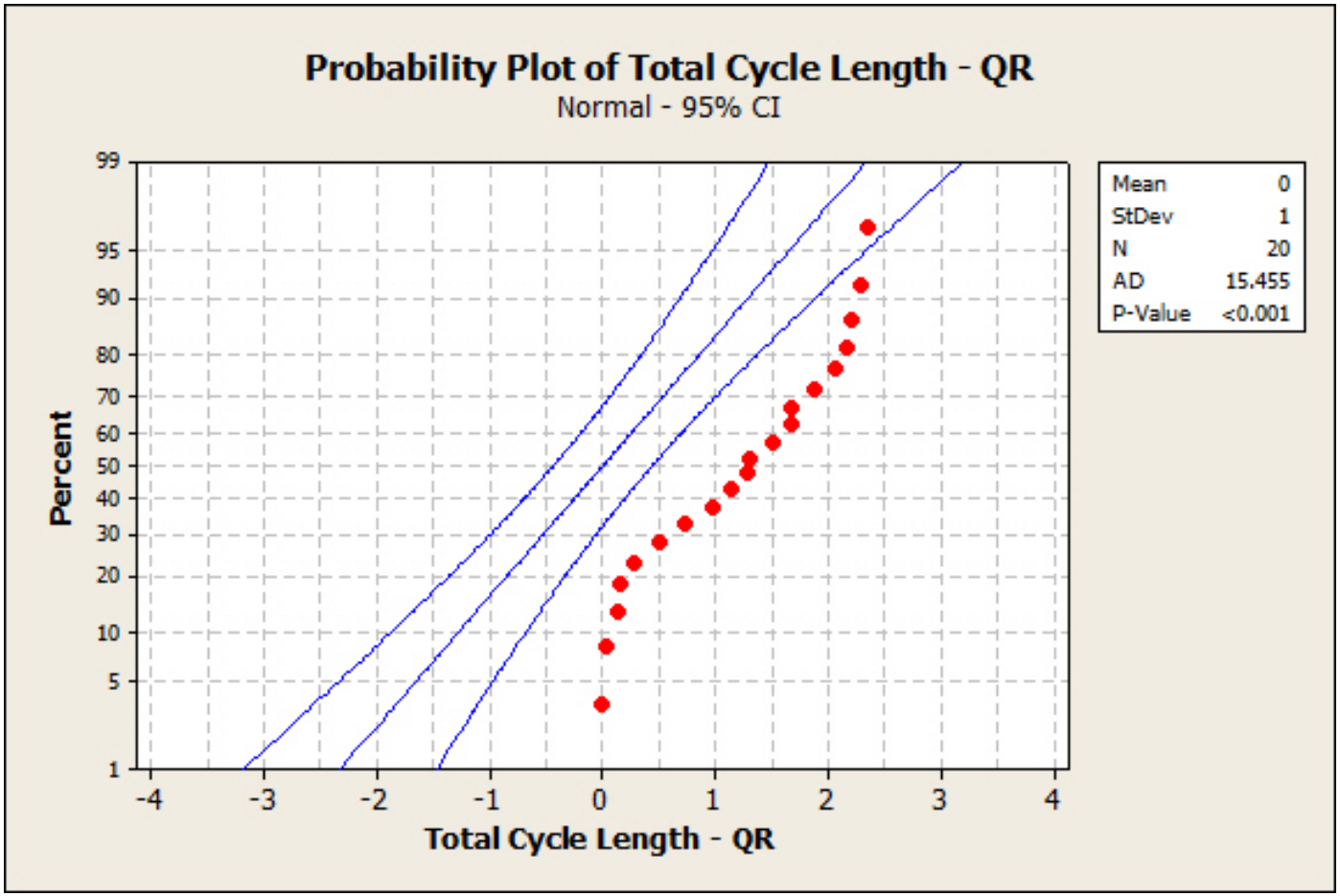
- We excluded $g = 1$ and $g = p - 1$ from our analysis since we already know the precise structure of those graphs.
- We chose safe primes since we are interested in analyzing our results based on the order of g: order $p - 1$ for primitive roots, and order $\frac{p-1}{2}$ for quadratic residues.
- After calculating the averages of the graphs we generated, we calculated the expected means for each order and for each graph characteristic.

After we collected the data, we used Minitab to analyze our results.

Some statistical methods we used include:

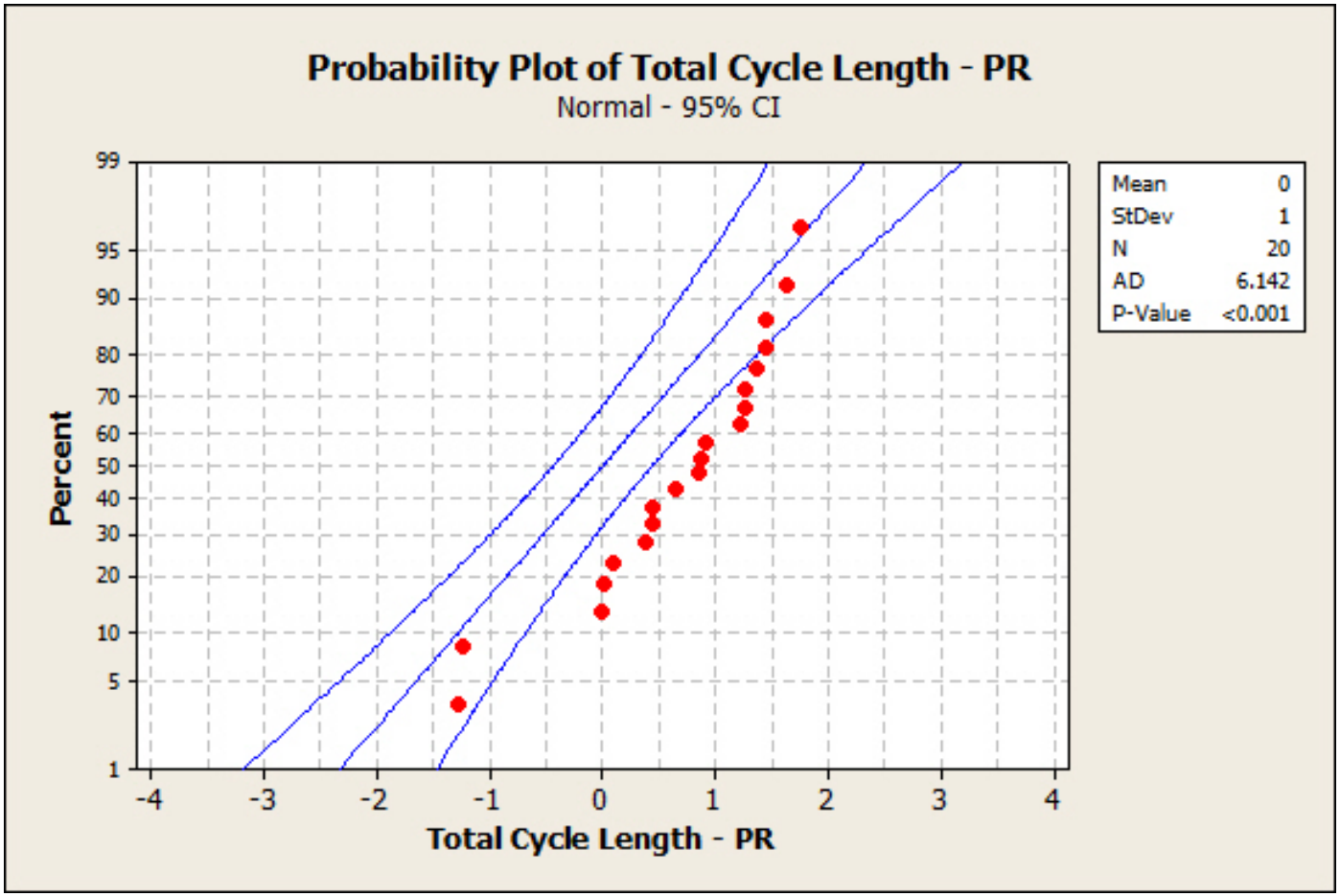
- *t*-tests - How similar is our observed mean to our hypothesized mean?
- Probability plots - Do our *t* values have the expected mean and standard deviation? Is our data normally distributed?

Initially, our data did not seem to match the expected values very well.



$$\mu = 1.215, \sigma = 0.8225$$

Initially, our data did not seem to match the expected values very well.

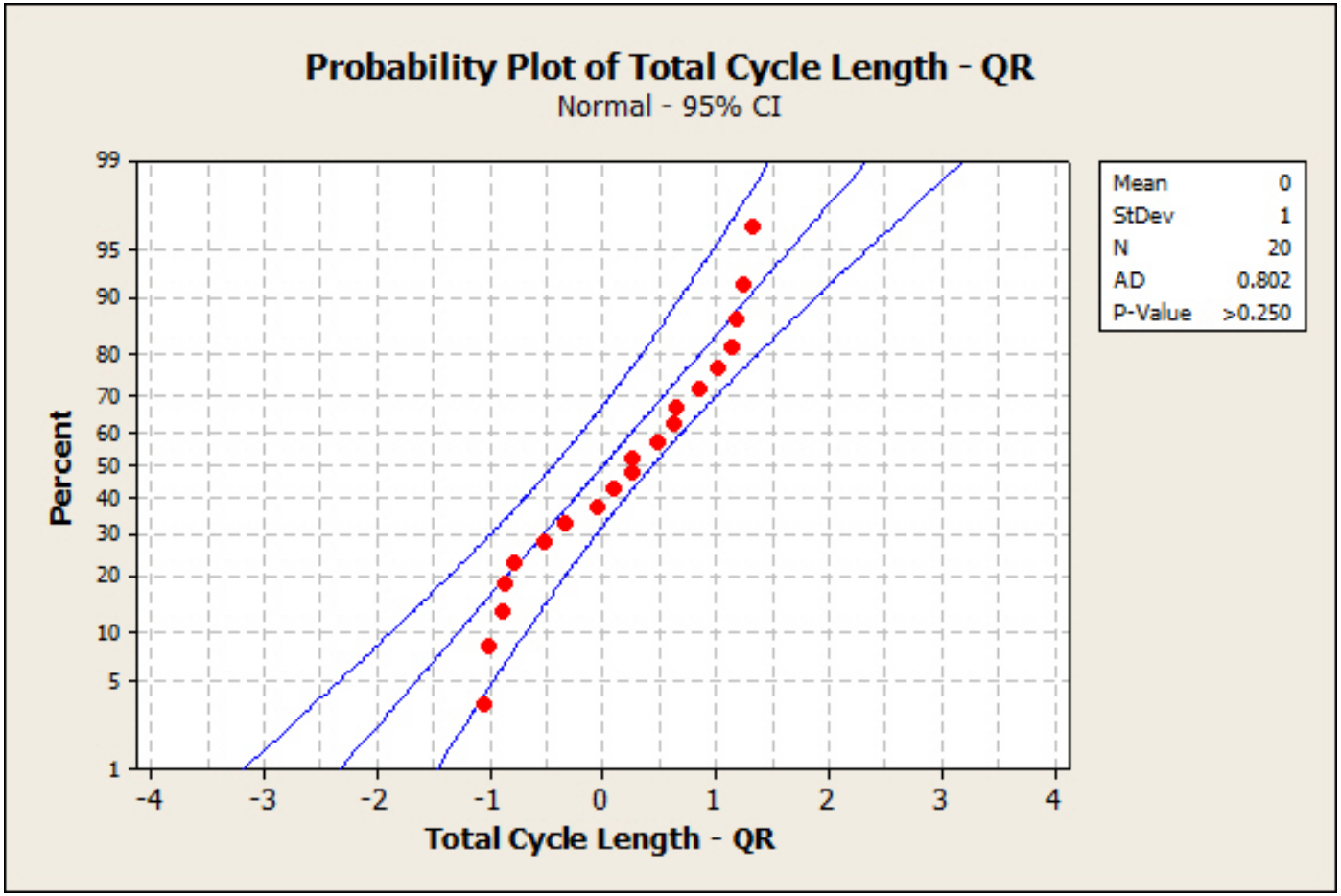


$$\mu = 0.6735, \sigma = 0.8516$$

We attributed this discrepancy to bad expected values.

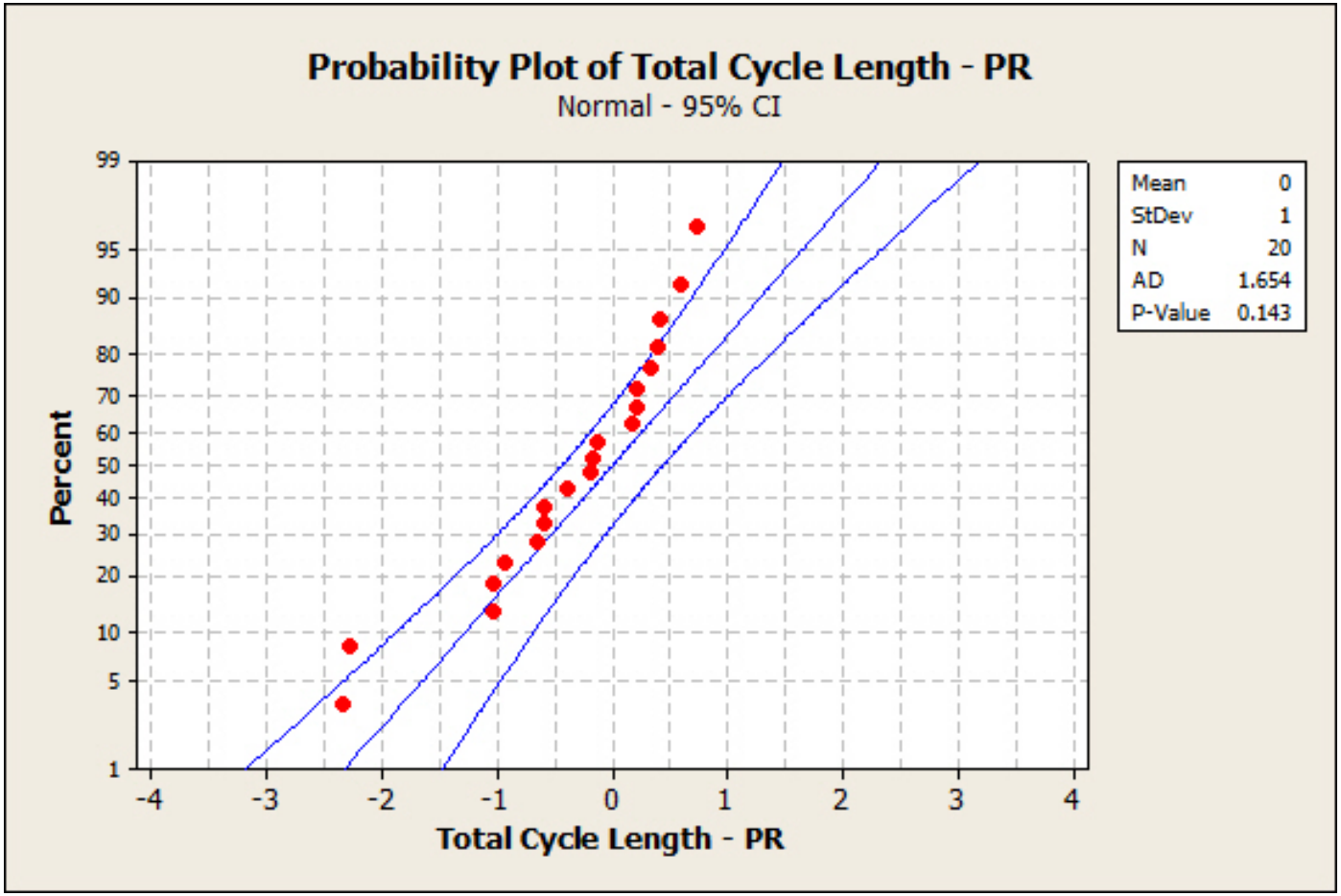
- We used Maple to calculate a second term for the asymptotic approximation for each of our graph characteristics.
- After adding this term to the approximation, we immediately saw changes to our statistical analysis.
- Some characteristics, like the average number of terminal and image nodes, were not greatly affected by this addition of the second term.

After the addition of the second term, our data looked much better.



$$\mu = 0.178,\ \sigma = 0.8255$$

After the addition of the second term, our data looked much better.



$$\mu = -0.363,\ \sigma = 0.8560$$

Conclusions

- Some characteristics of the DLM-induced graphs do seem to exhibit some slight nonrandomness.

- It's unlikely that this nonrandomness is anything that could be exploited quickly or efficiently.

Future Work

We will...

- manipulate the generating function for the number of image nodes to take advantage of the known fixed point.
- use methods from literature to construct expected variances for different characteristics of random functional graphs.

Thank you!

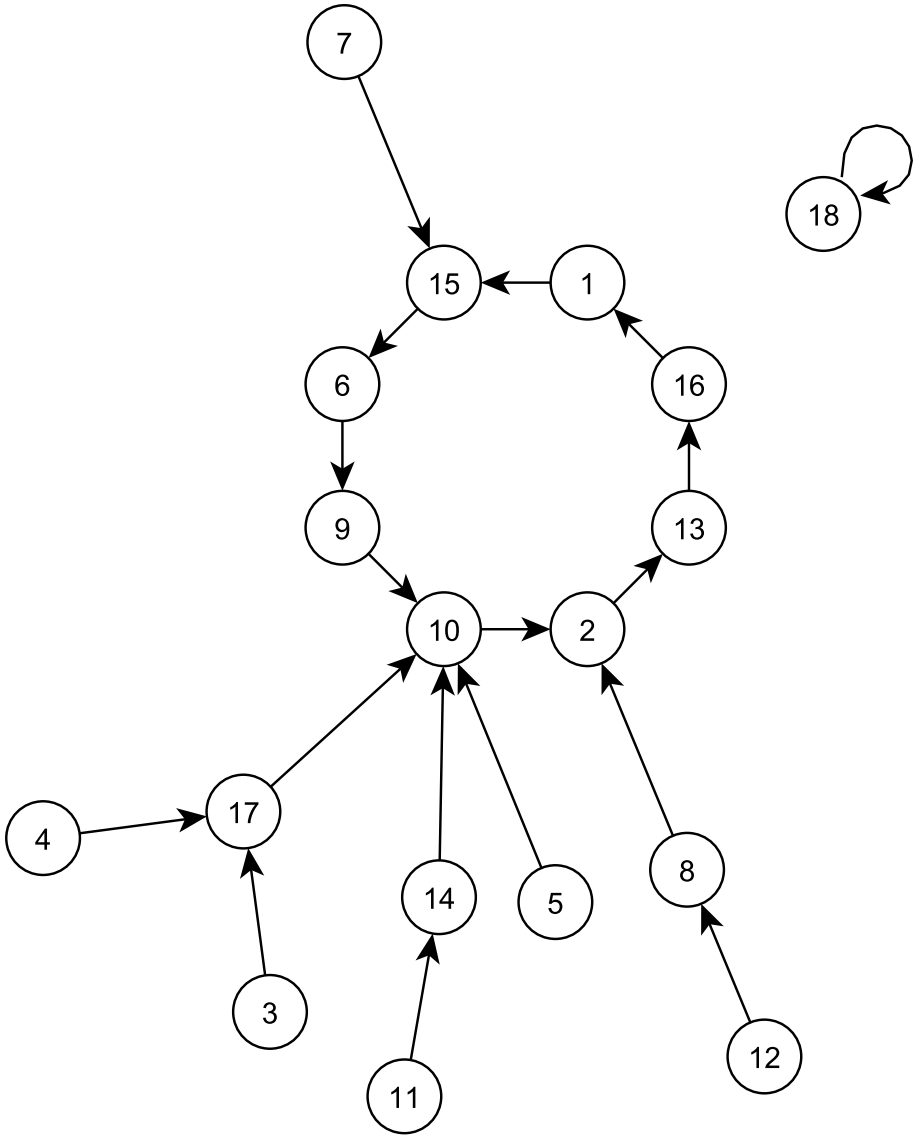


Figure: $g = 15$, $p = 19$