Periods of Iterations of Mappings over Finite Fields with Indegrees Restricted to $\{0, k\}$

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Banff – October 27, 2016
Joint work with Rodrigo Martins, Claudio Qureshi and Eric Schmutz

Iterations of functions over finite fields

In general, let $\mathcal{F}_n$ be the set of functions ("mappings") from the set $[1..n]$ to itself. With any $\varphi \in \mathcal{F}_n$ there is associated a functional graph on n nodes, with a directed edge from vertex u to vertex v if $\varphi(u) = v$. We are interested here in functions over finite fields.

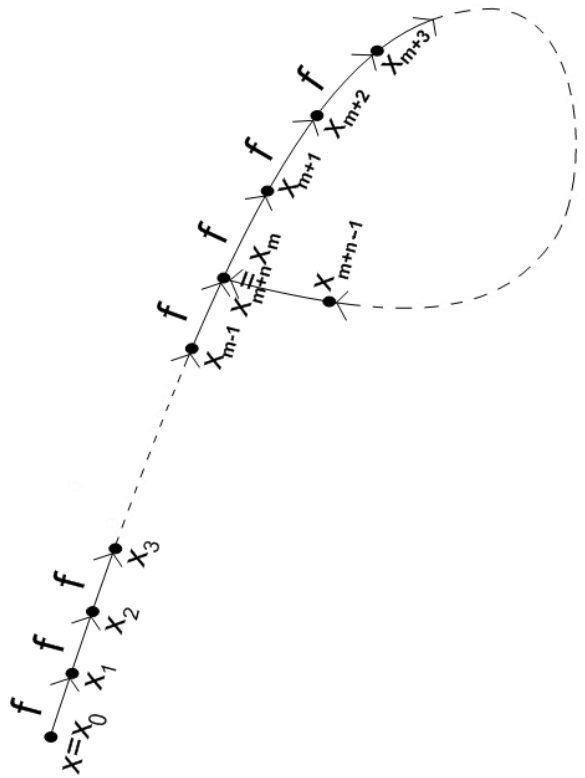
Functional graphs of mappings are sets of connected components; the components are directed cycles of nodes; and each of those nodes is the root of a tree.

The dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years, in part due to their applications in cryptography and integer factorization methods like Pollard rho algorithm.

Finite dynamics

Let X be a finite set and $f : X \to X$.

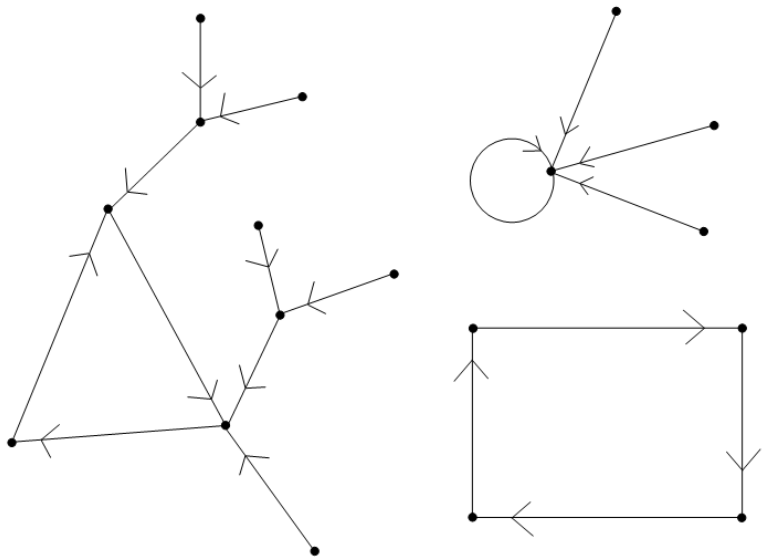
- For $x \in X$, let $n \geq 1, m \geq 0$ be the smallest integers such that $f^{n+m}(x) = f^m(x)$. Then, $\mathrm{per}(x) = n, \mathrm{pper}(x) = m$.



Finite dynamics

Let X be a finite set and $f : X \to X$.

- For $x \in X$, let $n \geq 1, m \geq 0$ be the smallest integers such that $f^{n+m}(x) = f^m(x)$. Then, $\mathrm{per}(x) = n, \mathrm{pper}(x) = m$.
- Functional graph: directed graph $\mathcal{G}_f$ with vertex set X and edges $(x, f(x))$ for $x \in X$ ($\mathrm{indeg}(x) = \#f^{-1}(x)$ and $\mathrm{outdeg}(x) = 1$).



Results on univariate dynamics

- (T.Rogers) Dynamics of $x \mapsto x^2$.

  T.Rogers. "The graph of the square mapping on the prime fields". Disc.Math 148, 317-324, 1996.

- (A.Peinado et al.) Dynamics of $x \mapsto x^2 + c$.

  A.Peinado, F.Montoya, J.Muñoz, A.Yuste. "Maximal periods of $x^2 + c$ in $\mathbb{F}_q$". LNCS 2227, 219-228, 2001.

- (T.Vasiga, J.Shallit) Dynamics of $x \mapsto x^2 - 2$.

  T.Vasiga, J.Shallit. "On the iteration of certain quadratic maps over GF(p)". Disc.Math 227, 219-240, 2004.

- (W.-S.Chou, I.E.Shparlinski) Dynamics of $x \mapsto x^e$.

  W.-S.Chou, I.E.Shparlinski. "On the cycle structure of repeated exponentiation modulo a prime". Journal of Number Theory 107, 345-356, 2004.

Results on univariate dynamics (cont)

- (S.Ugolini) Dynamics of $x \mapsto x + x^{-1}$ and $x \mapsto x^d + x^{-d}$.

  S.Ugolini. "Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three and five". Journal of Number Theory 133, 1207-1228, 2013.

- (T.Gassert) Dynamics of Chebyshev polynomials.

  T.Gassert. "Chebyshev action on finite fields". Disc.Math 315-316, 83-94, 2014.

- (C.Qureshi, D.Panario) Dynamics of Rédei functions.

  C.Qureshi, D.Panario. "Rédei actions on finite fields and multiplication map in cyclic groups". SIAM Journal on Discrete Mathematics 29, 1486-1503, 2015.

- (R.Martins, D.Panario) Heuristics and randomness.

  R.Martins, D.Panario. "On the heuristic of approximating polynomials over finite fields by random mappings". International Journal of Number Theory 12, 1987–2016, 2016.

Topics of interest in finite dynamics

Iterations of functions over finite fields have centered on:

- period and preperiod;
- (average) rho length;
- number of connected components;
- length of cycles (largest, smallest, average);
- number of fix points and conditions to be a permutation;
- isomorphic graphs (mathematically, algorithmically);
- average behavior varying p, $2 \leq p \leq N, N \to \infty$;
- and so on.

Iterations of some functions have strong symmetries that can be mathematically explained.

Example: dynamics of Rédei functions

- Rédei function: $(x+\sqrt{y})^n = N(x,y) + D(x,y)\sqrt{y}$.
  For $a \in \mathbb{F}_q^* \to R_n(x,a) = \frac{N(x,a)}{D(x,a)}$ defined over $\mathbb{P}^1(\mathbb{F}_q)$.
- We denote by $\mathcal{G}(n,a,q)$ its functional graph.

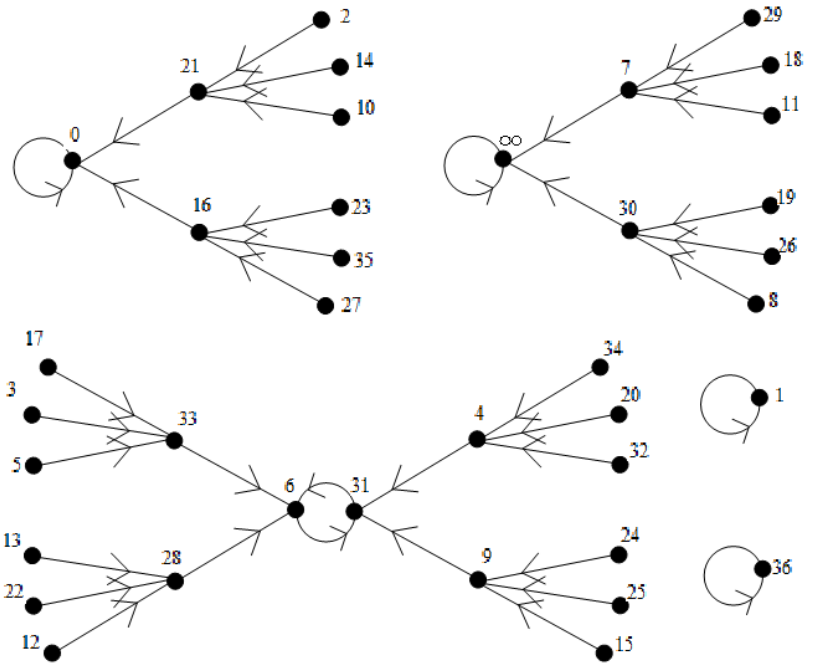


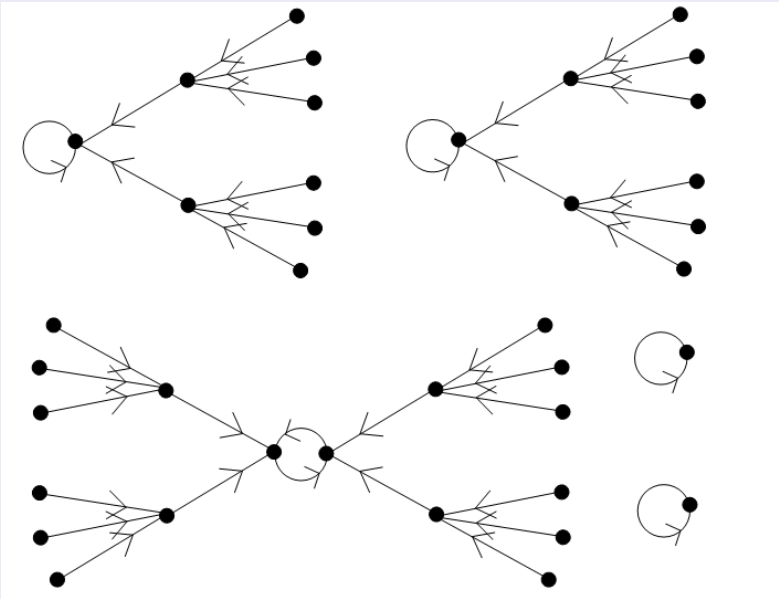
Figure: The functional graph $\mathcal{G}(3,1,37)$ associated to the Rédei function $R_3(x,1) = \frac{x^3+3x}{3x^2+1}$ defined over the projective line $\mathbb{P}^1(\mathbb{F}_{37})$.

Rédei functional graph

Example: the functional graph of $R_3(x,1) = \frac{x^3+3x}{3x^2+1}$ over $P^1(\mathbb{F}_{37})$

- $q - \left(\frac{a}{q}\right) = 36 = 2^2 \cdot 3^2 \Rightarrow \omega = 4, \nu = 9, n = 3$ and $9(3) = (3,3)$

$$\begin{aligned} \mathcal{G}(3,1,37) &\simeq \bigoplus_{d|4} \left\{ \frac{\varphi(d)}{o_d(3)} \times Cyc(o_d(3), T_{(3,3)}) \right\} \oplus \{\bullet, \bullet\} \\ &\simeq 2 \times Cyc(1, T_{(3,3)}) \oplus Cyc(2, T_{(3,3)}) \oplus \{\bullet, \bullet\} \end{aligned}$$



Algebraic dynamical system (ADS)

Definition 1

Let $F_1, \ldots, F_m \in \mathbb{F}_q(X_1, \ldots, X_m)$ be m rational functions in m variables over the finite field $\mathbb{F}_q$ of q elements. The algebraic dynamical system (ADS) generated by $\mathcal{F} = \{F_1, \ldots, F_m\}$ is the dynamical system formed by $F_i^{(0)} = X_i$ and the iterations

$$F_i^{(k)} = F_i(F_1^{(k-1)}, \ldots, F_m^{(k-1)}), \quad k = 1, 2, \ldots, \quad i = 1, \ldots, m.$$

ADSs are challenging mathematical objects with interesting algebraic and number theoretic properties. They have found applications in pseudorandom number generators (PRNGs), biology and physics; see Shparlinski's survey in Section 10.5 of G.Mullen, D.Panario "Handbook of Finite Fields". CRC Press, 2013.

Part II
Heuristic - Polynomials and Random Mappings

Dynamics of Polynomials over FF - Pollard's Method

- Proposed originally for the factorization of integers in 1975.
- Used for the factorization of the 8th Fermat number in 1981.
- Variant for the discrete logarithm problem (DLP) in 1978.
- Considered by many the most efficient method against the ECDLP.

D. Johnson, A. Menezes, S. Vanstone, *Elliptic Curve Digital Signature Algorithm*, Int. J. of Information Security, 2001.

Wiener M., Zuccherato R., *Faster attacks on elliptic curve cryptosystems*, Proceedings of Selected Areas in Cryptography: 5th Annual International Workshop, 1998.

R. Gallant, R. Lambert, S. Vanstone, *Improving the parallelized Pollard lambda search on anomalous binary curves*, Mathematics of Computation, 2000.

... and many more.

Random Mappings

Definition

(i) *A mapping is a function of the form* $\varphi : [n] \longrightarrow [n]$.

(ii) *A random mapping is a mapping chosen uniformly at random.*

- Interesting parameters: rho length of a random node, number of components, number of cyclic nodes, etc.
- Average rho length of polynomials: approximated by mappings.

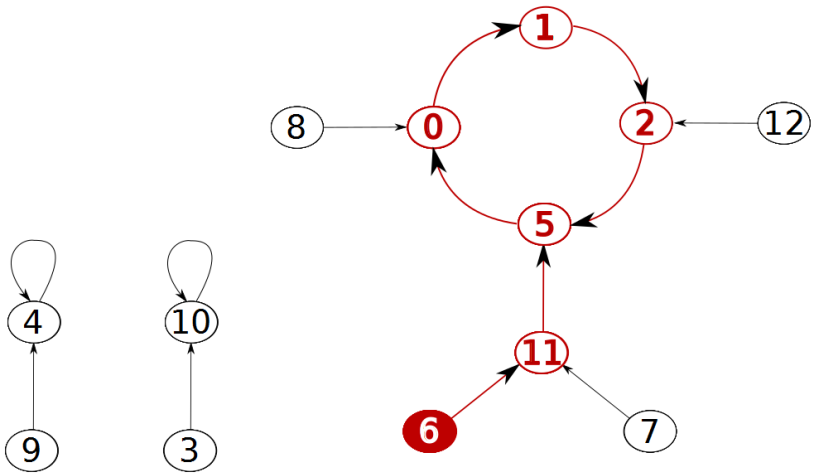


Figure : Average rho length.

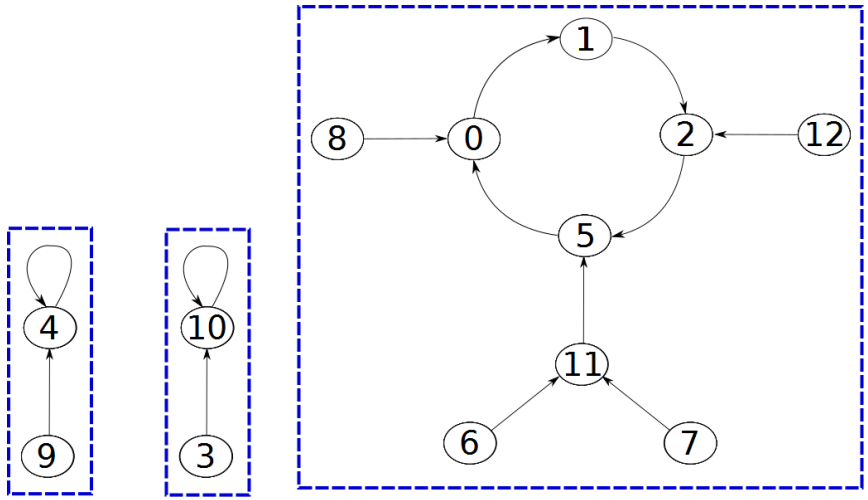


Figure : # components.

Heuristic - Polynomials and Mappings

- Heuristic proposed by Pollard in the analysis of his algorithm.

Average rho length of quadratic polynomials	Heuristic $\approx$	Average rho length of mappings

Theorem

$$\mathbb{E}_n[\rho] \sim \sqrt{\frac{\pi n}{2}}, \quad as \quad n \to \infty.$$

For example: J. Arney , E. Bender, *Random mappings with constraints on coalescence and number of origins*, Pacific J. Math, 1982.

- Refinement of the heuristic?

Arithmetic properties of quadratic polynomials X Parameters that affect the structure of a class of mappings

Heuristic - Polynomials and Mappings

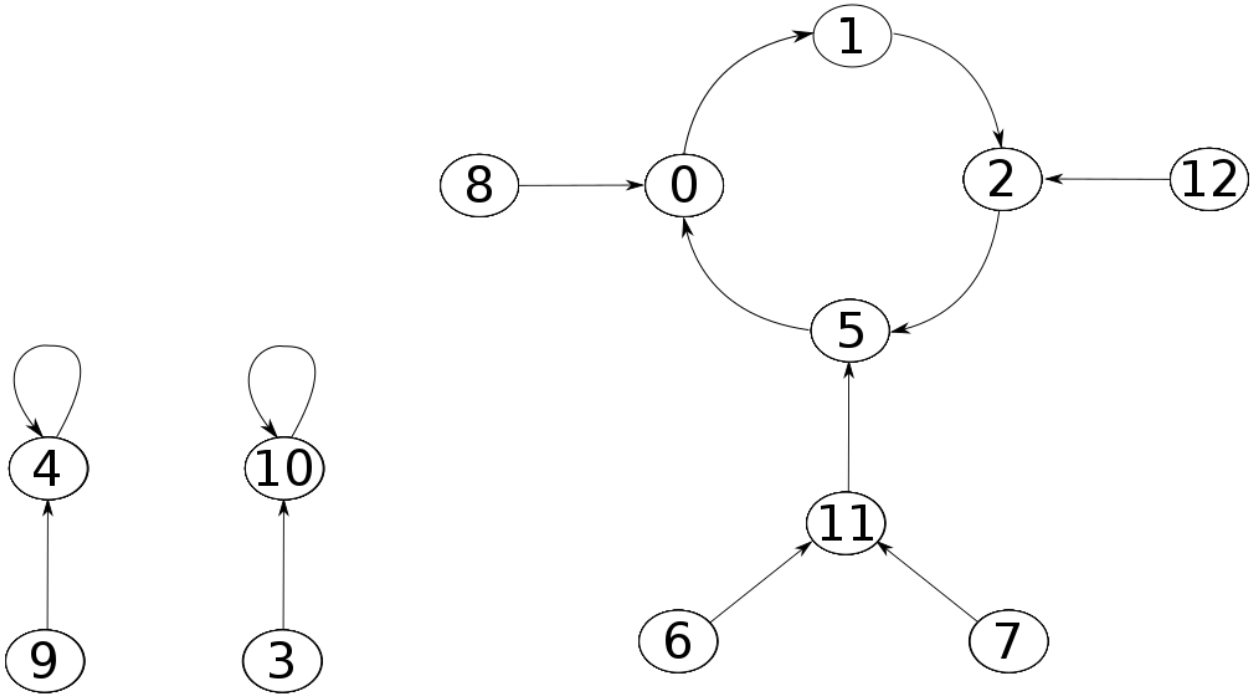


Figure : Functional graph of $f(x) = x^2 + 1 \pmod{13}$.

Heuristic - Polynomials and Mappings

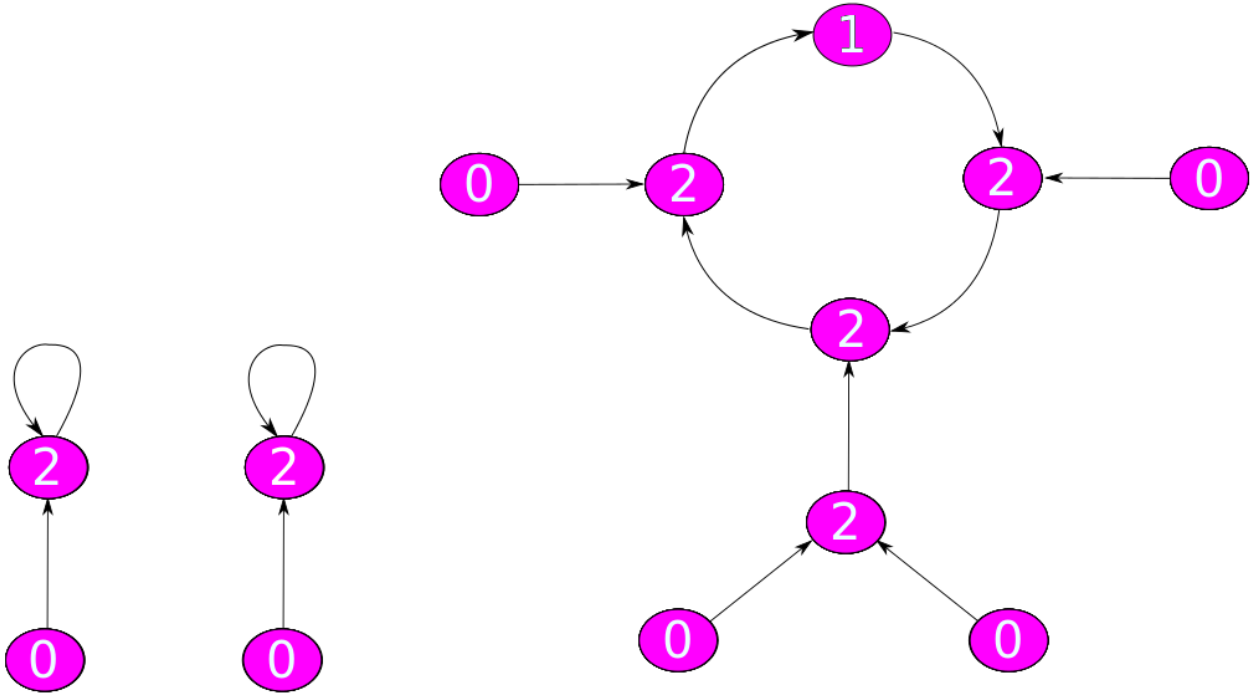


Figure : Distribution of indegrees of $f(x) = x^2 + 1 \pmod{13}$.

- $x^2 + a \pmod{p}$: all but one nodes have indegree either 0 or 2.
- Mappings considered in the heuristic: no restriction on indegrees.
- Distribution of indegrees: relevant?

Heuristic - Polynomials and Mappings

Definition (Coalescence of a mapping)

$V(\varphi)$: the variance of the distribution of indegrees of a mapping φ.

- If $X = X_\varphi$ is the indegree of a random node,

$$\mathbb{E}[X] = \sum_{y \in [n]} \frac{1}{n} |\varphi^{-1}(y)| = 1 \quad \text{and} \quad \mathbb{V}[X] = -1 + \sum_{y \in [n]} \frac{1}{n} |f^{-1}(y)|^2.$$

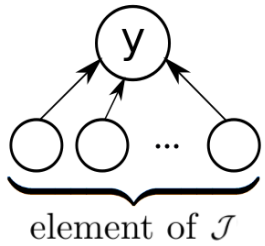
Example 2

Let f over $\mathbb{F}_p$, $p > 2$, of degree 2. Since the expected preimage size of a random uniform element of $\mathbb{F}_p$ is 1, it follows that

$$V(f) = \sum_{x \in \mathbb{F}_p} \frac{1}{p} |f^{-1}(x)|^2 - 1 = \frac{1}{p} + \frac{p-1}{2} \cdot \frac{1}{p} \cdot 4 - 1 = 1 - \frac{1}{p}.$$

Heuristic - Polynomials and Mappings

- $\mathcal{J}$-mappings: mappings with indegrees in a fixed set $\mathcal{J} \subseteq \mathbb{N}$ containing zero and some $j > 1$.



Theorem (Arney & Bender, 1982)

If λ is the asymptotic average coalescence of $\mathcal{J}$-mappings, then

$$\mathbb{E}_n^{\mathcal{J}}[\textit{rho length}] \sim \sqrt{\pi n/2\lambda}, \quad \textit{as} \quad n \to \infty.$$

In the unrestricted case $\lambda = 1$.

Similar results hold for other parameters.

Heuristic - Polynomials and Mappings

(variance of the)

Distribution of indegrees:
Affects the structure of a class of mappings.

- Let f be a polynomial modulo p and let $V(f)$ be its coalescence. The Brent-Pollard heuristic predicts that the average rho length of f is:

$$\sqrt{\frac{\pi n}{2V(f)}}.$$

- Factorization of the eighth Fermat number: $f(x) = x^{2^m} + 1$.

Brent R., Pollard J., *Factorization of the eighth Fermat number*, Math. Comp., 1981.

Our results: $\{0, k\}$-Polynomials - $\{0, k\}$-Mappings

- We consider $\{0, k\}$-mappings with the following motivation.

Theorem

Let $f(x) = x^k + a$ be a polynomial modulo p. If $p \equiv 1 \pmod{k}$, then

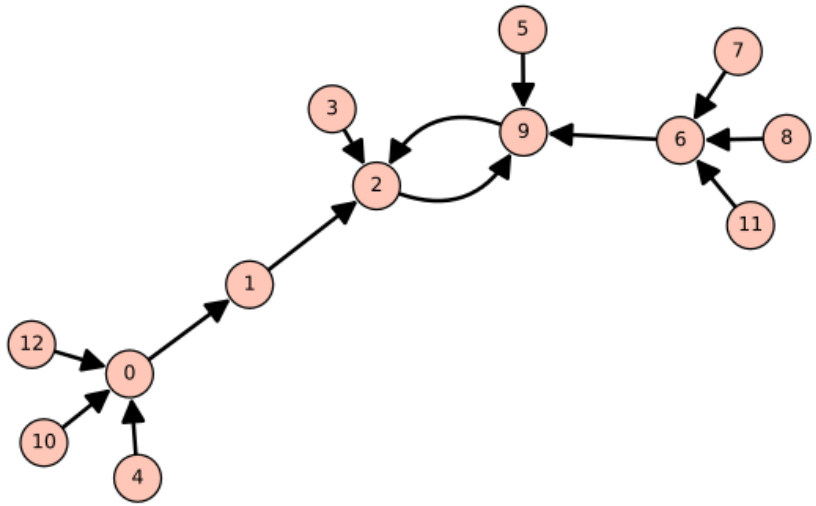
(i) *there is exactly one node with indegree 1;*

(ii) *there are exactly $(p-1)/k$ nodes with indegree k;*

(iii) *all the other nodes have indegree 0.*

We refer to these polynomials as $\{0, k\}$-polynomials.

Figure: Functional graph of $x^3 + 1 \pmod{13}$.



Our Results - Motivations

- Examples:
  1. $\{0, 2\}$-mappings: polynomials $x^2 + a \pmod{p}$, p odd.
  2. $\{0, k\}$-mappings: polynomials $x^k + a \pmod{p}$, $p \equiv 1 \pmod{k}$.
- Heuristic approximation of polynomials by mappings:
  1. J. M. Pollard, A monte carlo method for factorization, BIT, 1975.
  2. R. Brent and J. Pollard, Factorization of the eighth Fermat number, Math. Comp. 1981.

We focus here on cycles and periods of iterations of mappings over finite fields with indegrees restricted to $\{0, k\}$.

Our Results

Let $\mathbf{T}(f)$ and $\mathbf{B}(f)$ denote, respectively, the least common multiple and the product of the length of the cycles of f. Harris (1973) proved that $\log \mathbf{T}$ converges in distribution to a standard normal distribution. Schmutz (2011) gives asymptotic estimates for the expected value of $\mathbf{T}$ and $\mathbf{B}$ over all mappings on n nodes.

We obtain the following results:

- we give asymptotic estimates for the expected value of $\mathbf{T}$ and $\mathbf{B}$ over $\{0, k\}$-mappings;
- we prove that $\log \mathbf{T}$ and $\log \mathbf{B}$ converge in distribution to a standard normal distribution, when properly centered and normalized;
- we show that $\log \mathbf{B} - \log \mathbf{T}$ converges in probability to zero, when properly normalized;
- we present theoretical and numerical results concerning the use of $\{0, k\}$-mappings as heuristic models for $\{0, k\}$-polynomials.

Part III
Cycles of $\{0, k\}$-Mappings

Parameter $\mathbf{T}$: Definition

Definition (Parameter $\mathbf{T}$)

If φ is a mapping, then $\mathbf{T}(\varphi)$ is the least common multiple of the length of the cycles of φ.

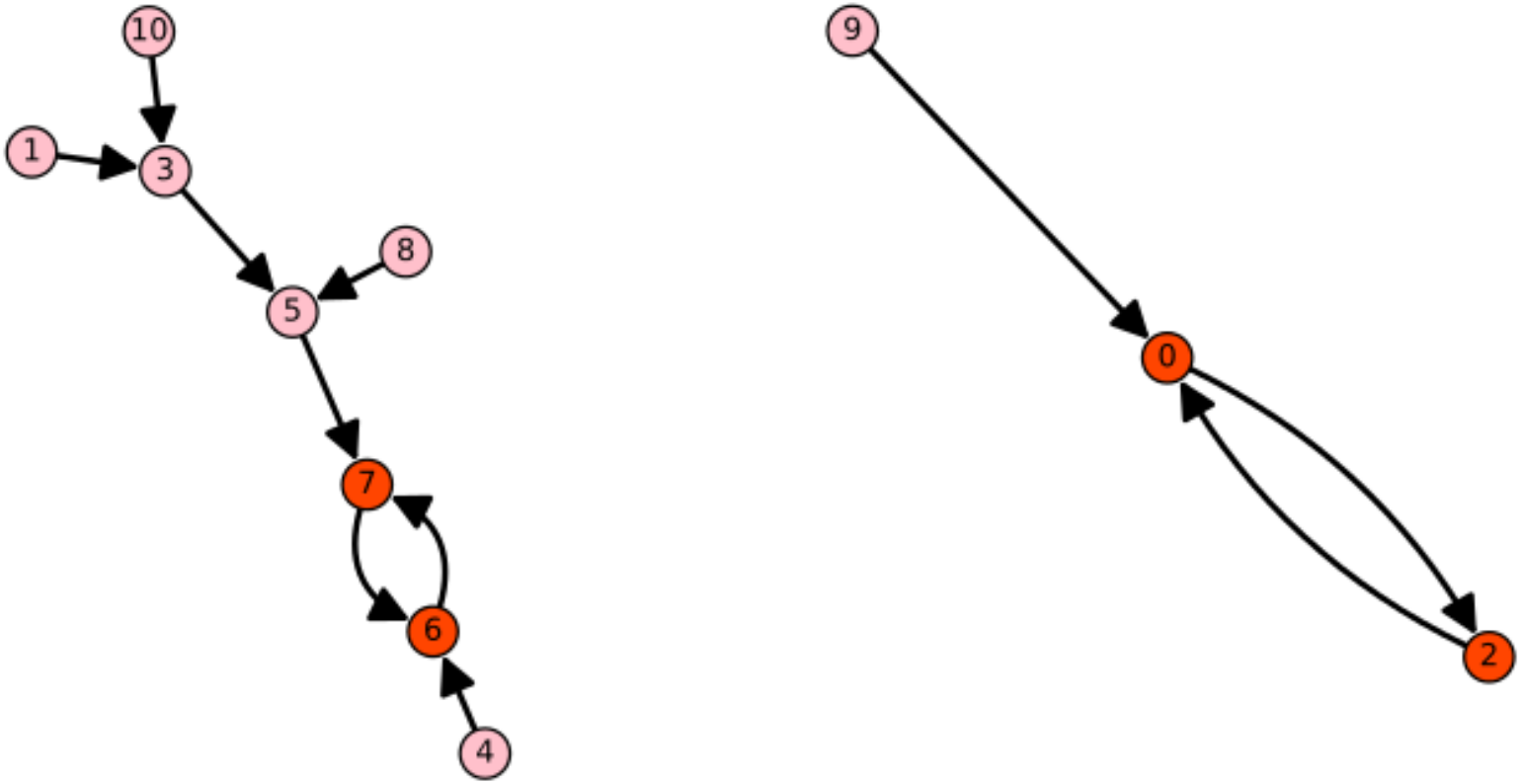


Figure : The mapping $\varphi(x) = x^6 + 2 \pmod{11}$ satisfies $\mathbf{T}(\varphi) = 2$.

Parameter $\mathbf{T}$: Definition

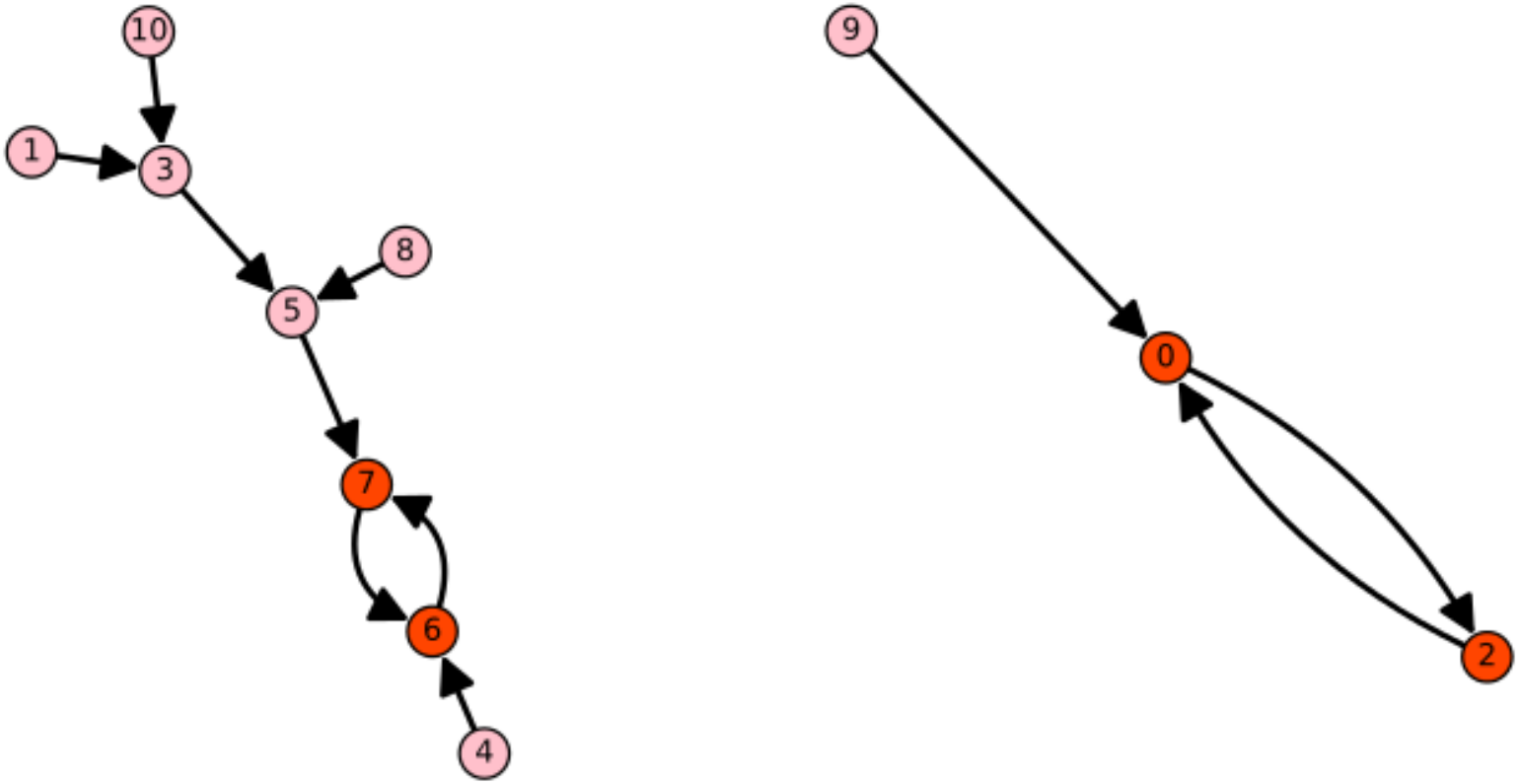


Figure : LCM of the length of the cycles: $\mathbf{T}(\varphi) = 2$.

- Equivalent definitions for $\mathbf{T}$:
  1. Period of the sequence $\varphi^{(m)} = \varphi \circ \varphi^{(m-1)}$, $m \geq 1$.
  2. The least integer $T \geq 1$ s.t. $\varphi^{(m+T)} = \varphi^{(m)}$ for all $m \geq m_0$.
  3. Order of the permutation given by the cyclic nodes.

Parameter **T**: Convergence to Gaussian Distribution

Theorem (Convergence in distribution of $\log \mathbf{T}$)

For any fixed $x \in \mathbb{R}$:
$$\lim_{n\to\infty} \mathbb{P}_n \left[\frac{\log \mathbf{T} - h_n}{b_n} \leq x \right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt,$$
where $h_n = (\log^2 n)/8$ *and* $b_n = (\log^{3/2} n)/\sqrt{24}$.

B. Harris, The asymptotic distribution of the order of elements in symmetric semigroups, Journal of Combinatorial Theory Series A, 1973.

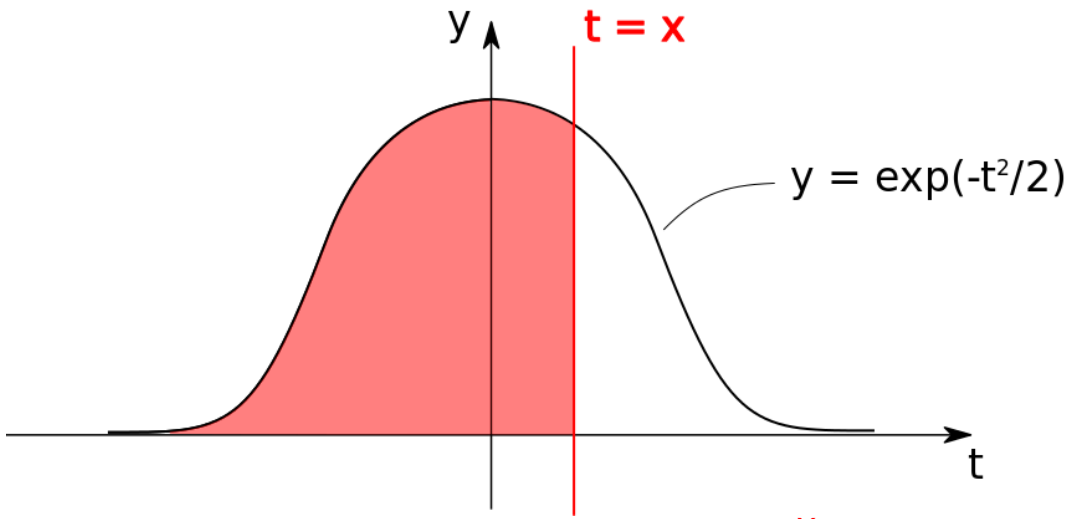


Figure : Region with area $A = \int_{-\infty}^{x} e^{-t^2/2} dt$.

Parameter $\mathbf{T}$: Expected Value

Theorem (Convergence in distribution of $\log \mathbf{T}$)

For any fixed $x \in \mathbb{R}$:
$$\lim_{n\to\infty} \mathbb{P}_n \left[\frac{\log \mathbf{T} - h_n}{b_n} \leq x \right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt,$$
where $h_n = (\log^2 n)/8$ *and* $b_n = (\log^{3/2} n)/\sqrt{24}$.

B. Harris, The asymptotic distribution of the order of elements in symmetric semigroups, Journal of Combinatorial Theory Series A, 1973.

Theorem (Expected value of $\mathbf{T}$)

$$\mathbb{E}_n[\mathbf{T}] = \exp\left(k_0 \sqrt[3]{\frac{n}{\log^2 n}} (1 + o(1)) \right), \quad \text{as } n \to \infty.$$

where $k_0 \approx 3.36$.

Schmutz, E. Period lengths for iterated functions. Combinatorics, Probability and Computing, 2011.

Parameter **B**

Definition (Parameter **B**)

If f is a mapping, then $\mathbf{B}(\varphi)$ is product of the length of the cycles of φ.

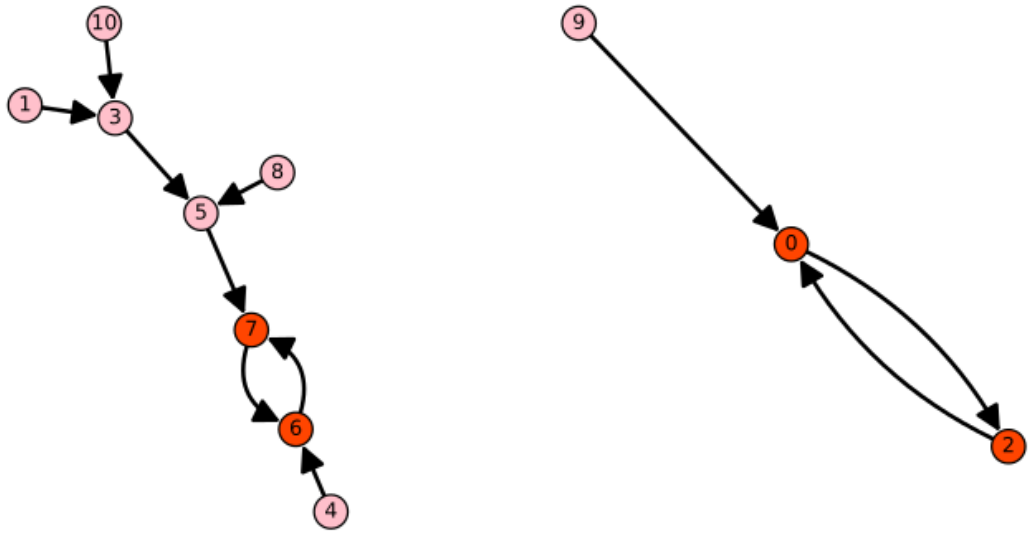


Figure : Product of the length of the cycles: $\mathbf{B}(\varphi) = 4$.

Theorem (Expected value of **B**)

$$\mathbb{E}_n[\mathbf{B}] = \exp\left(\frac{3}{2}\sqrt[3]{n}\big(1 + o(1)\big)\right), \quad \text{as } n \to \infty.$$

Our results: $\{0, k\}$-mappings modelling $\{0, k\}$-polynomials

Theorem (Schmutz 2011)

$$\log \mathbb{E}_n^{\mathbb{N}}[\mathbf{B}] \sim \frac{3}{2} \cdot \sqrt[3]{n} \quad \textit{and} \quad \log \mathbb{E}_n^{\mathbb{N}}[\mathbf{T}] \sim k_0 \cdot \sqrt[3]{n} \cdot \frac{1}{\log^{2/3} n}$$

Theorem (Martins, Panario, Qureshi, Schmutz 2016)

$$\log \mathbb{E}_n^{\{0,k\}}[\mathbf{B}] \sim \frac{3}{2} \cdot \sqrt[3]{\frac{n}{\lambda}} \quad \textit{and} \quad \log \mathbb{E}_n^{\{0,k\}}[\mathbf{T}] \sim k_0 \cdot \sqrt[3]{\frac{n}{\lambda}} \cdot \frac{1}{\log^{2/3} n}$$

- Arney & Bender results:

Average rho length of unrestricted mappings

$$\mathbb{E}_n^{\mathbb{N}}[\rho] \overset{n\to\infty}{\sim} \sqrt{\frac{\pi n}{2}}.$$

Average rho length of $\mathcal{J}$-mappings

$$\mathbb{E}_n^{\mathcal{J}}[\rho] \overset{n\to\infty}{\sim} \sqrt{\frac{\pi n}{2\lambda}}.$$

Our results: $\{0, k\}$-mappings modelling $\{0, k\}$-polynomials

- Expected value of $\mathbf{T}$ for $\{0, k\}$-mappings:

  Let $\mathbb{E}_n^{\{0,k\}}(\mathbf{T})$ be the expected value of $\mathbf{T}$ over the class of mappings on n nodes with indegrees restricted to the set $\{0, k\}$, $n = kr$. Then,

$$\log \mathbb{E}_n^{\{0,k\}}(\mathbf{T}) = k_0 \frac{(n/\lambda)^{1/3}}{\log^{2/3}(n/\lambda)}(1 + o(1)),$$

  as r approaches infinity, where $\lambda = k - 1$, $k_0 = \frac{3}{2}(3I)^{2/3}$ and

$$I = \int_0^\infty \log\log\left(\frac{e}{1 - e^{-t}}\right) dt.$$

- Expected value of $\mathbf{B}$ for $\{0, k\}$-mappings:

  Let $\mathbb{E}_n^{\{0,k\}}(\mathbf{B})$ be the expected value of $\mathbf{B}$ over the class of mappings on n nodes with indegrees restricted to the set $\{0, k\}$, $n = kr$. Then, as r approaches infinity and for $\lambda = k - 1$,

$$\log \mathbb{E}_n^{\{0,k\}}(\mathbf{B}) = \frac{3}{2}\left(\frac{n}{\lambda}\right)^{1/3}(1 + o(1)).$$

Our results: $\{0, k\}$-mappings modelling $\{0, k\}$-polynomials

- Convergence in distribution of $\log \mathbf{T}$ for $\{0, k\}$-mappings:

  Let $k = k(r)$ and $n = n(r)$ be sequences such that $n = kr$ and, for some $0 < \alpha < 1$, $k = o(n^{1-\alpha})$ as r approaches infinity. Let $\mu_n = \frac{1}{2}\log^2(\sqrt{n/\lambda})$ and $\sigma_n^2 = \frac{1}{3}\log^3(\sqrt{n/\lambda})$. Let $\mathbf{T}(f)$ denote the least common multiple of the length of the cycles of a mapping f and, for $r \geq 1$, let X_n be the random variable defined over the space of $\{0, k\}$-mappings on n nodes as $X_n = (\log \mathbf{T} - \mu_n)/\sigma_n$. Then, the sequence defined by X_n converges in distribution to a standard normal distribution.

  In other words, for any real number x,

$$\mathbb{P}_n^{\{0,k\}}(\log \mathbf{T} \leq \mu_n + x\sigma_n) = \phi(x) + o_x(1),$$

  as r approaches infinity, where the notation $o_x(\cdot)$ indicates that the error term depends on x. Moreover, if c is a positive constant, then the convergence is uniform for $|x| \leq c\sqrt{\log n}$.

Our results: $\{0, k\}$-mappings modelling $\{0, k\}$-polynomials

- Convergence in distribution of $\log \mathbf{B}$ for $\{0, k\}$-mappings: similar results as for $\mathbf{T}$ above (statement skipped here).
- $\mathbf{B}$ may be a good approximation for $\mathbf{T}$:
  Let $k = k(r)$ and $n = n(r)$ be sequences such that $n = kr$ and, for some $0 < \alpha < 1$, $k = o(n^{1-\alpha})$ as r approaches infinity. For $r \geq 1$, let χ_n be the random variable defined over $\{0, k\}$-mappings on n nodes as $\chi_n = (\log \mathbf{B} - \log \mathbf{T})/\sigma_n$, where $\sigma_n = \frac{1}{\sqrt{3}} \log^{3/2}(\sqrt{n/\lambda})$. Then, the sequence defined by χ_n converges in probability to zero. In other words, for all $\varepsilon > 0$ we have, as r approaches infinity,

$$\mathbb{P}_n^{\{0,k\}}(\chi_n > \varepsilon) = o(1).$$

- We also consider $k = k(n) = o(n)$.
- We have experiments on the parameters $\mathbf{T}$ and $\mathbf{B}$.

Sketch of a Proof

Let $\Omega_n^{\{0,k\}}$ be the set of $\{0,k\}$-mappings, $\mathcal{Z} = \mathcal{Z}(f)$ be the set of cyclic nodes of a mapping $f \in \Omega_n^{\{0,k\}}$ and denote by $\mathbf{Z} = |\mathcal{Z}|$.

We index probabilities and expected values by the set of allowed indegrees of the class of mappings in question: $\mathbb{N}$ in the general random case and $\{0,k\}$ in our case. We can write the expected value of $\mathbf{T}$ over $\Omega_n^{\{0,k\}}$ as

$$\begin{aligned}\mathbb{E}_n^{\{0,k\}}[\mathbf{T}] &= \sum_{m=1}^{n} \mathbb{P}_n^{\{0,k\}}[\mathbf{Z}=m]\mathbb{E}_n^{\{0,k\}}[\mathbf{T}|\mathbf{Z}=m] \\ &= \sum_{m=1}^{n} \mathbb{P}_n^{\{0,k\}}[\mathbf{Z}=m]M_m\end{aligned}$$

where M_m is the expected order of a random permutation of S_m.

Sketch of Proof (cont)

Lemma

If f is a $\{0, k\}$-mapping on n nodes, then $n = kh$ for some $h \leq 1$ and the coalescence of a f is $\lambda = \lambda(f) = k - 1$.

Indeed, since there are exactly $h = n/k$ nodes with indegree k, the coalescence of a $\{0, k\}$-mapping satisfies

$$\lambda = \frac{n}{k} \cdot \frac{1}{n} \cdot k^2 - 1 = k - 1.$$

For $\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = m]$ we use the following result:

Lemma (Rubin and Sitgreaves, 1953)

If $\lambda = k - 1$, then

$$\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = m] = \lambda k^{m-1} \binom{h-1}{m-1} \binom{n-1}{m}^{-1}.$$

Sketch of Proof (cont)

For M_m, the expected order of a random uniform permutation, we use classical results due to Erdös-Turan and others; we use a version with improved error terms given in the next lemma.

Lemma (Stong 1998)

Let M_m be the expected order of a random permutation of S_m and let $\beta_0 = \sqrt{8I}$ where

$$I = \int_0^\infty \log\log\left(\frac{e}{1-e^t}\right) dt.$$

Then,

$$\log M_m = \beta_0 \sqrt{\frac{m}{\log m}} + O\left(\frac{\sqrt{m}\log\log m}{\log m}\right).$$

Sketch of Proof (cont)

Let $\widehat{m}$ be the integer that maximizes $\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = m]M_m$. We estimate the expected value of $\mathbf{T}$ by noting that, for all $m_0 \in [1, n]$,

$$\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = m_0]M_{m_0} \leq \mathbb{E}_n^{\{0,k\}}[\mathbf{T}] \leq n\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = \widehat{m}]M_m.$$

To study $\mathbb{P}_n^{\{0,k\}}[\mathbf{Z} = m]M_m$, we extend the binomials in Rubin and Sitgreaves's result using the Gamma function, and use Stong's result to finally consider the function

$$\phi_{n,\varepsilon}(x) = \lambda x k^{x-1} \frac{\Gamma(h)}{\Gamma(h-x+1)} \frac{\Gamma(n-x)}{\Gamma(n)} \exp\left(\beta_\varepsilon \sqrt{\frac{x}{\log x}}\right),$$

for $n \geq 1$, $-1 < \varepsilon < 1$, $\phi_{n,\varepsilon} \colon (1, n) \to \mathbb{R}$ and $\beta_\varepsilon = \beta_0 + \varepsilon$.

Sketch of Proof (cont)

We show that $\log \phi_{n,\varepsilon}(x)$ has a unique maximum in $(1, n)$ at

$$\beta_\varepsilon^{2/3} \sqrt{\frac{3}{8}} \left(\frac{n}{\lambda}\right)^{2/3} \frac{1}{\log^{1/3} n}.$$

At that value, for $k_\varepsilon = \beta_\varepsilon^{4/3} \frac{3^{5/3}}{2^3}$, $\log \phi_{n,\varepsilon}(x)$ takes the value

$$k_\varepsilon \left(\frac{n}{\lambda}\right)^{1/3} \frac{1}{\log^{2/3} n}(1 + o(1)).$$

With that we prove the main result:

$$\mathbb{E}_n^{\{0,k\}}[\mathbf{T}] = \exp\left(k_0 \left(\frac{n}{\lambda}\right)^{1/3} \frac{1}{\log^{2/3} n}(1 + o(1))\right),$$

where $\lambda = k - 1$ and $k_0 = (3I)^{2/3}3/2 = 3.36\ldots$.

Conclusions and Future Work

We give, for $\{0, k\}$-mappings, the expected value of the parameter **T**, the lcm of the length of the cycles in $\{0, k\}$-mappings, and the parameter **B**, the product of the length of the cycles. We give lognormality results for these parameters, and study the difference $\log \mathbf{B} - \log \mathbf{T}$.

In addition, we also have results for $k = k(n) = o(n)$; an algorithm for generating uniform $\{0, k\}$-mappings; and some theoretical and experimental results on the parameters for certan families of $\{0, k\}$-polynomials.

Future work include extending these results to other type of $\mathcal{J}$-mappings.