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

Dedicated to Igor Shparlinski

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

CIRM – March 29, 2016

Joint work with Rodrigo Martins, Claudio Qureshi and Eric Schmutz

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.

Average rho length of polynomials: approximated by mappings.

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.*

- Functional graph of a mapping: edge from i to j if $\varphi(i) = j$.
- Interesting parameters: rho length of a random node, number of components, number of cyclic nodes, etc.

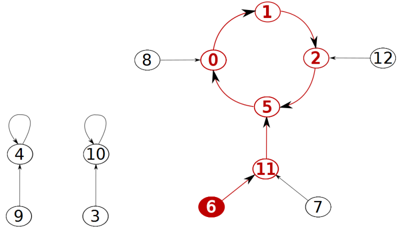


Figure : Average rho length.

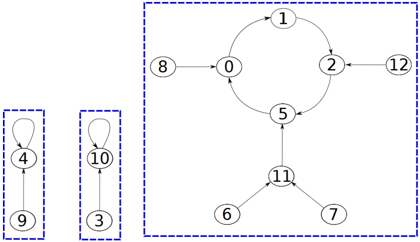


Figure : # components.

Heuristic - Polynomials and Mappings

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

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

Theorem

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

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

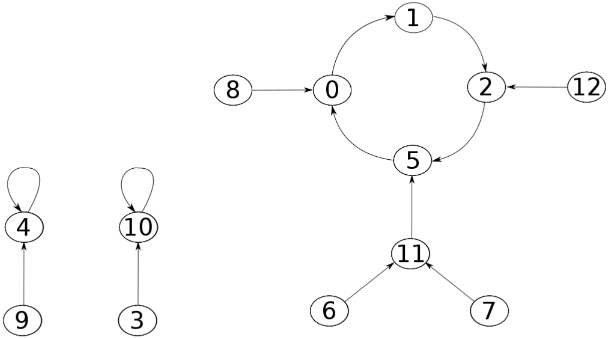


Figure : Functional graph of $f(x) = x^2 + 1 \pmod{13}$.

Heuristic - Polynomials and Mappings

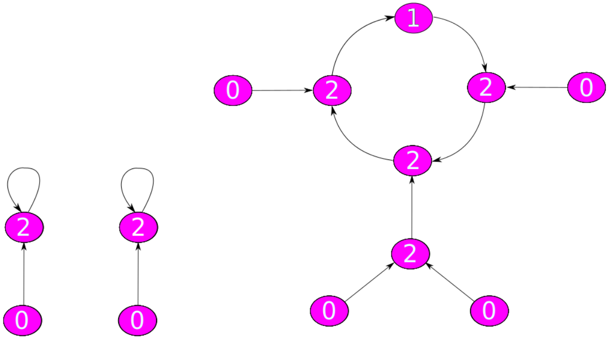


Figure : Distribution of indegrees of $f(x) = x^2 + 1 \pmod{13}$.

- $x^2 + a \pmod{p}$: 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,

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

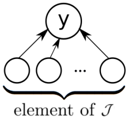
Example 1

Let $f(x) = x^2$ over $\mathbb{F}_p$, $p > 2$. 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 $j > 1$.



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,

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

Theorem (Arney & Bender, 1982)

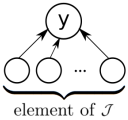
If λ is the asymptotic average coalescence of $\mathcal{J}$-mappings, then

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

for unrestricted mappings: $\lambda = 1$

Heuristic - Polynomials and Mappings

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



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,

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

Theorem (Arney & Bender, 1982)

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

(i) $\mathbb{E}_n^{\mathcal{J}}[\textbf{rho length}] \sim \sqrt{\pi n / 2\lambda}$, *as* $n \to \infty$.

similar results 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: $f(x) = x^m + 1$, $m = 2^k$.

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

Our results - Introducing $\{0, k\}$-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

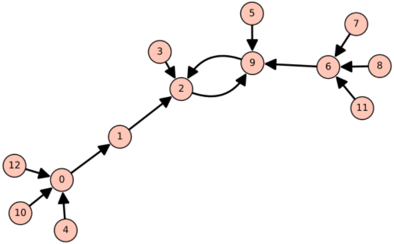
(i) *there is exactly one node with indegree* 1*;*

(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.
  3. R. Martins, D. Panario, On the Heuristic of Approximating Polynomials over Finite Fields by Random Mappings, to appear in IJNT, 2016.

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

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

Parameter **T**: Definition

Definition (Parameter **T**)

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

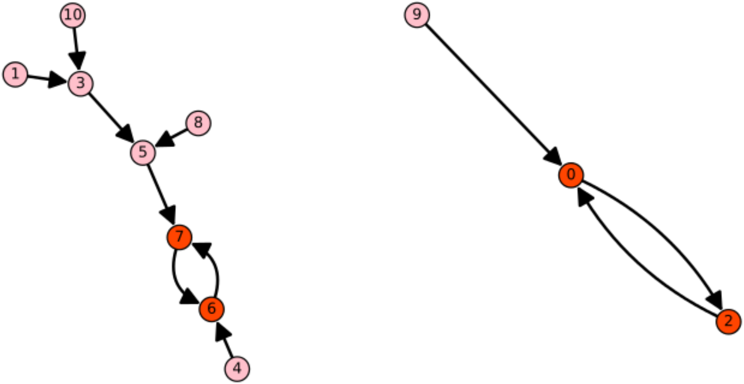


Figure : The mapping $\varphi(x) = x^6 + 2 \pmod{11}$ satisfies $\mathbf{T}(\varphi) = 2$.

Parameter **T**: Definition

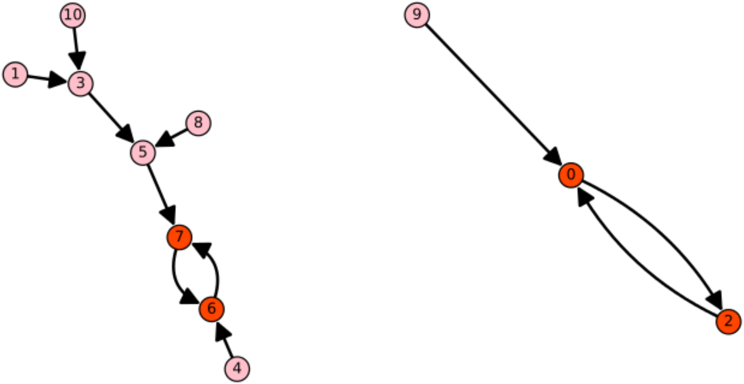


Figure : LCM of the length of the cycles: $\mathbf{T}(\varphi) = 2$.

- Equivalent definitions for **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 $m \geq n$.
  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 $x \in \mathbb{R}$:
$$\lim_{n\to\infty} \mathbb{P}_n \left[\frac{\log \mathbf{T} - h_n}{b_n} \le x \right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt,$$
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.

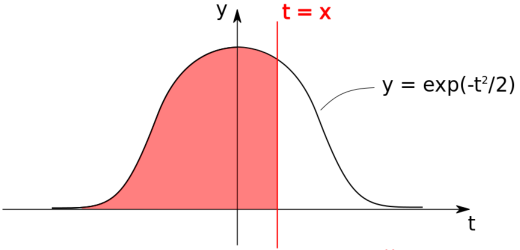


Figure : Region with area $A = \int_{-\infty}^{x} e^{-t^2/2} dt$.

Parameter $\mathbf{T}$: Expected Value

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

For any fixed $x \in \mathbb{R}$:

$$\lim_{n\to\infty} \mathbb{P}_n\left[\frac{\log \mathbf{T} - h_n}{b_n} \le x\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt,$$

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

Definition (Parameter B)

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

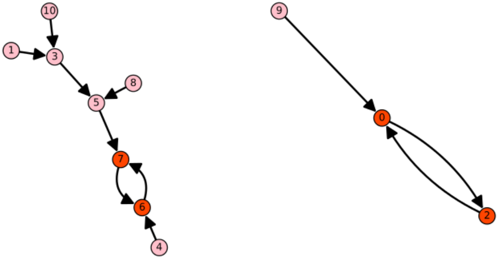


Figure : Product of the length of the cycles: $\mathbf{B}(\varphi) = 4$.

Parameter **B** - Expected Value

Theorem (Expected value of B)

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

E. Schmutz, Period lengths for iterated functions. C. P. C., 2011.

- **B** may be a good approximation for **T**: for any $\delta, \varepsilon > 0$,

$$\mathbb{P}_n\left[\frac{\log \mathbf{B} - \log \mathbf{T}}{\log^{1+\delta} n} \geq \varepsilon\right] \leq \frac{c(\log\log n)^2}{\varepsilon \log^{\delta} n} \to 0, \quad \text{as } n \to \infty.$$

E. Schmutz, Period lengths for iterated functions. C. P. C., 2011.

Our results

- $\{0,k\}$-polynomials: best modelled by $\{0,k\}$-mappings.

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

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

Our results

- $\{0, k\}$-polynomials: best modelled by $\{0, k\}$-mappings.

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

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

Our results

- $\{0, k\}$-polynomials: best modelled by $\{0, k\}$-mappings.

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

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

Our results

- $\{0, k\}$-polynomials: best modelled by $\{0, k\}$-mappings.

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

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

Sketch of 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 $k_0 = (3l)^{2/3}3/2 = 3.36\ldots$.

Numerical Results - Motivation for the Experiments

- Motivation for our theoretical results: heuristic approximations!
  1. $\{0, 2\}$-mappings: polynomials $x^2 + a \pmod{p}$.
  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.
  3. R. Martins, D. Panario, On the Heuristic of Approximating Polynomials over Finite Fields by Random Mappings, to appear in IJNT, 2016.
- Experiments above concern the rho length of nodes.
- We run experiments for the parameters **T** and **B**.

Numerical Results

- First 50 primes greater than 10^3.
- p random mappings chosen at random for each p.
- All p quadratic polynomials of the form $x^2 + a \pmod{p}$.
- Computation of $\mathbf{T}$, $\mathbf{B}$ and the respective average values $\overline{\mathbf{T}}$, $\overline{\mathbf{B}}$.
- Computation of the ratios

$$R_{\mathbf{T}} = \frac{\log \overline{\mathbf{T}}}{3.36 \cdot \sqrt[3]{n/\log^2 n}} \quad \text{and} \quad R_{\mathbf{B}} = \frac{\log \overline{\mathbf{B}}}{1.5 \cdot \sqrt[3]{n}}$$

.

Class of functions	$R_{\mathbf{T}}$
unrestricted maps on p nodes	0.7921
$x^2 + a \pmod{p}$	0.7965

Table : Experimental average value of $\mathbf{T}$.

Ratio between the results on random mappings and quadratic polynomials:

0.9945

Numerical Results

- First 2×50 primes greater than 10^3.
- p random $\{0,3\}$-mappings chosen at random for each $p \equiv 1 \pmod 3$.
- All p cubic polynomials of the form $x^3 + a \pmod p$, $p \equiv 1 \pmod 3$.
- Computation of $\mathbf{T}$, $\mathbf{B}$ and the respective average values $\overline{\mathbf{T}}$, $\overline{\mathbf{B}}$.
- Computation of the ratios

$$R_{\mathbf{T}} = \frac{\log \overline{\mathbf{T}}}{3.36 \cdot \sqrt[3]{n/2 \cdot \log^2 n}} \quad \text{and} \quad R_{\mathbf{B}} = \frac{\log \overline{\mathbf{B}}}{1.5 \cdot \sqrt[3]{n/2}}$$

.

Class of functions	$R_{\mathbf{T}}$
random $\{0,3\}$-maps on p nodes	0.8106
$x^3 + a \pmod p$	0.8176

Table : Experimental average value of $\mathbf{T}$.

Ratio between the results on $\{0,3\}$-mappings and $\{0,3\}$-polynomials:

0.9914

Numerical Results

- First 2×50 primes greater than 10^3.
- p random $\{0, 4\}$-mappings chosen at random for each $p \equiv 1 \pmod 4$.
- All p quartic polynomials of the form $x^4 + a \pmod p$, $p \equiv 1 \pmod 4$.
- Computation of $\mathbf{T}$, $\mathbf{B}$ and the respective average values $\overline{\mathbf{T}}$, $\overline{\mathbf{B}}$.
- Computation of the ratios

$$R_{\mathbf{T}} = \frac{\log \overline{\mathbf{T}}}{3.36 \cdot \sqrt[3]{n/3 \cdot \log^2 n}} \quad \text{and} \quad R_{\mathbf{B}} = \frac{\log \overline{\mathbf{B}}}{1.5 \cdot \sqrt[3]{n/3}}$$

.

Class of functions	$R_{\mathbf{T}}$
random $\{0, 4\}$-maps on p nodes	0.8121
$x^4 + a \pmod p$	0.8026

Table : Experimental average value of $\mathbf{T}$.

Ratio between the results on $\{0, 4\}$-mappings and $\{0, 4\}$-polynomials:

1.0118

Conclusions and Future Work

We give the expected value of the parameter **T**, the lcm of the length of the cycles in $\{0, k\}$-mappings, and also of the parameter **B**, the product of the length of the cycles. In addition, we also have results for:

- Case $k = k(n) = o(n)$.
- Experiments on the parameter **B**.
- Convergence in distribution of $\log \mathbf{T}$ for $\{0, k\}$-mappings.

Future work include:

- Distribution of $\log \mathbf{B} - \log \mathbf{T}$ for $\{0, k\}$-mappings.
- Extend results to $\mathcal{J}$-mappings.
- Estimates on the distribution of **T** and **B** over (general) polynomials.