On the cycle structure of iterating Rédei functions

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

XXI CLA – July 29, 2016
Joint work with Claudio Qureshi and Rodrigo Martins

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

Finite dynamical systems have applications in several areas including physics, biology, and cryptography:

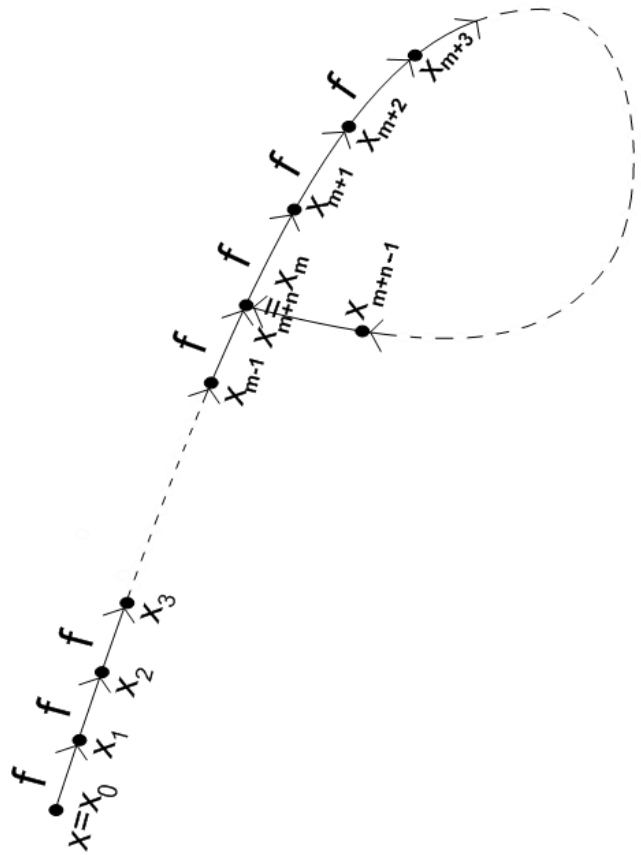
- Pollard's rho algorithm for integer factorization and improvements.
- Algorithms based in the Pollard's rho method for the discrete logarithm problem:
  - over the multiplicative subgroup of $\mathbb{F}_q$;
  - over the additive group of an elliptic curve defined over a finite field.

Let us introduce some definitions...

Finite dynamics

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

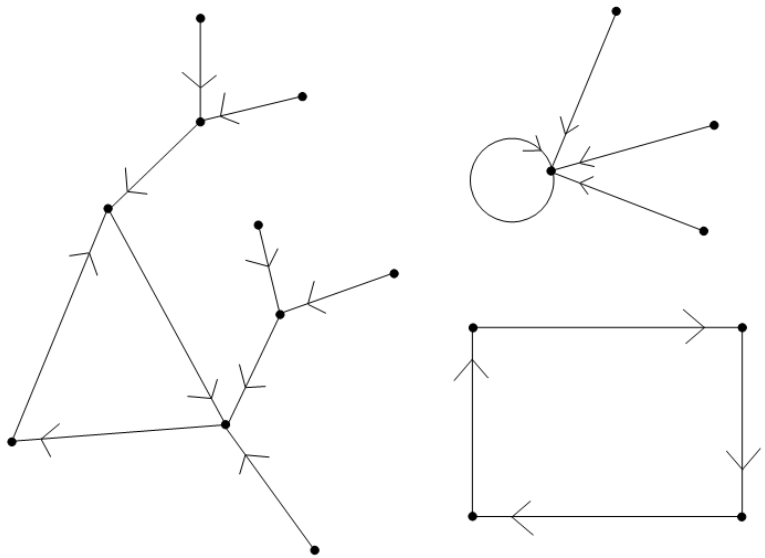
- For $x \in X$, let $n \geq 1, m \geq 0$ be the smallest integers such that $f^{n+m}(x) = f^m(x)$. Then, $per(x) = n, pper(x) = m$.



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, $per(x) = n, pper(x) = m$.
- Functional graph: directed graph $\mathcal{G}(f/X)$ with vertex set X and edges $(x, f(x))$ for $x \in X$ ($indeg(x) = \#f^{-1}(x)$ and $outdeg(x) = 1$).



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);
- and so on.

Iterations of some functions have strong symmetries that can be mathematically explained. We show as an example the action of Rédei functions over non-binary finite fields whose functional graphs present these type of symmetries.

Finite dynamics

Study of certain special cases

- (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 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.

- (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.

Finite dynamics

Study of certain special cases

- (T.Rogers) Dynamics of $x \mapsto x^2$.
- (A.Peinado et.al) Dynamics of $x \mapsto x^2 + c$.
- (T.Vasiga, J.Shallit) Dynamics of $x \mapsto x^2 - 2$.
- (S.Ugolini) Dynamics of $x \mapsto x + x^{-1}$ and $x \mapsto x^d + x^{-d}$.
- (T.Gassert) Dynamics of Chebyshev polynomials.

$\vdots$

- $\rightarrow$ We focus on Rédei functions

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 $\mathbb{P}^1(\mathbb{F}_q)$.

$$
\begin{aligned}
R_1(x) &= x \\
R_2(x) &= \frac{x^2+a}{2x} \\
R_3(x) &= \frac{x^3+3ax}{3x^2+a} \\
R_4(x) &= \frac{x^4+6ax^2+a^2}{4x^3+4ax} \\
R_5(x) &= \frac{x^5+10ax^3+5a^2x}{5x^4+10ax^2+a^2} \\
R_6(x) &= \frac{x^6+15ax^4+15a^2x^2+a^3}{6x^5+20ax^3+6a^2x} \\
R_7(x) &= \frac{x^7+21ax^5+35a^2x^3+7a^3x}{7x^6+35ax^4+21a^2x^2+a^3} \\
&\vdots
\end{aligned}
$$

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.

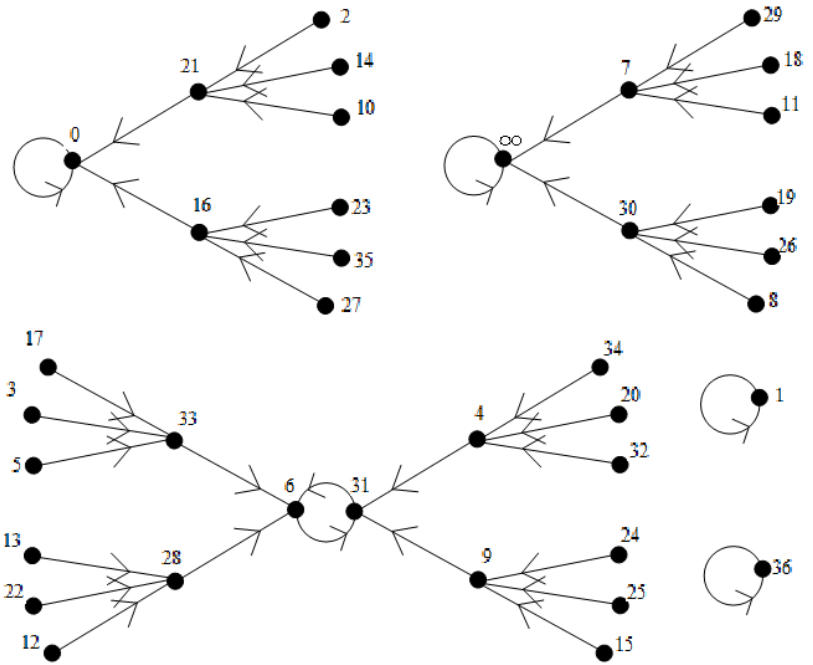


Figure: The functional graph $\mathcal{G}(3,1,37)$ associated to the Rédei function $R_3(x,1) = \frac{x^3+3x}{3x^2+1}$ defined over the projective line $\mathbb{P}^1(\mathbb{F}_{37})$.

Rédei functions

Some applications of Rédei functions

- Pseudorandom number generators based on Rédei functions.

  J. Gutierrez, A. Winterhof. "Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions". Finite Fields and Their Appl.14, 410-416, 2008.

- Method to solve Pell equation via Rédei functions.

  S. Barbero, U. Cerruti, N. Murru. "Solving the Pell equation via Rédei rational functions". The Fibonacci Quarterly 48, 348-357, 2010.

- Cryptosystem based on Rédei functions.

  R. Nobauer. "Cryptanalysis of the Rédei scheme". Contributions to General Algebra 3, 255-264, 1984.

- Application to permutation polynomials.

  M. Zieve. "Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$". To appear in Monatsh. Math.

Description of the Rédei functional graph

Isomorphism theorem for Rédei functional graph
[Cor.3.8 and Th.3.16 of Qureshi and Panario (2015)]

Let $n \in \mathbb{Z}^+$, $a \in \mathbb{F}_q^*$ and $\chi : \mathbb{F}_q \to \{\pm 1\}$ the quadratic character in $\mathbb{F}_q$. We express $q - \chi(a) = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n, \omega) = 1$. Then:

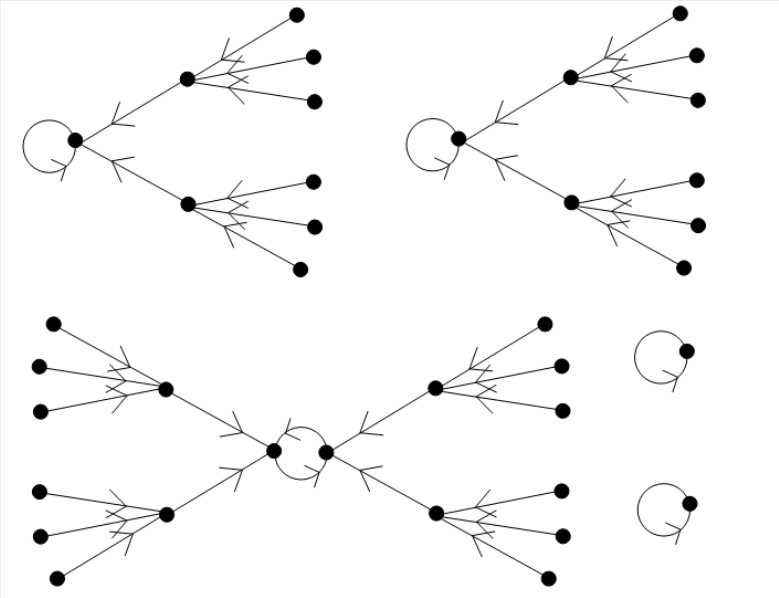
$$\mathcal{G}(n, a, q) \simeq \bigoplus_{d \mid \omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T_{\nu(n)}) \right\} \oplus (1 + \chi(a)) \times \{\bullet\}.$$

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 $9(3) = (3,3)$

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



Description of the tree $T_{\nu(n)}$

The ν-serie generated by n

For ν and n positive integers with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$, we define the sequence:

$$\begin{cases} \nu_1 = \gcd(\nu, n), \\ \nu_{i+1} = \gcd\left(\frac{\nu}{\nu_1\nu_2\ldots\nu_i}, n\right) & \text{for } i \geq 1. \end{cases}$$

If $D = \max\{i \geq 1 : \nu_i > 1\}$, we define $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$.
By convention, for $\nu = 1$ we define $\nu(n) = (1)$ for all n.

Tree associated with ν-series

Definition of T_V for V a ν-series

If $V = (\nu_1, \nu_2, \ldots, \nu_D)$ is a ν-series, we define recursively the tree T_V associated with V as follows:

$$\begin{cases} T_V^0 = \bullet, \\ T_V^k = \langle \nu_k \times T_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle \text{ for } 1 \leq k \leq D, \end{cases}$$

and

$$T_V = \langle (\nu_D - 1) \times T_V^{D-1} \oplus \bigoplus_{i=1}^{D-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle.$$

For $V = (1)$ we define $T_V = \bullet$.

Tree associated with ν-series

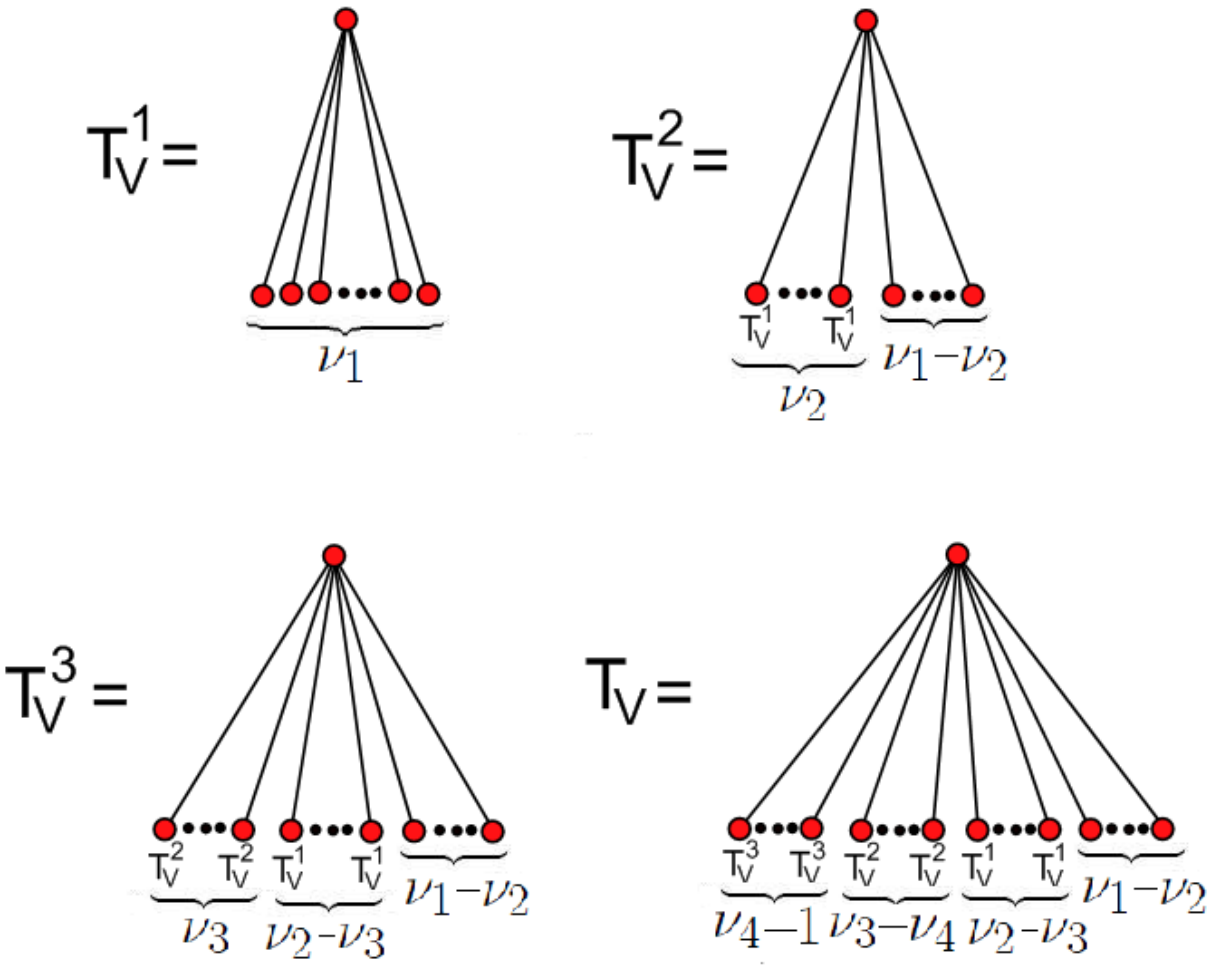


Figure: Inductive definition of T_V for $V = (\nu_1, \nu_2, \nu_3, \nu_4)$.

Tree associated with ν-series

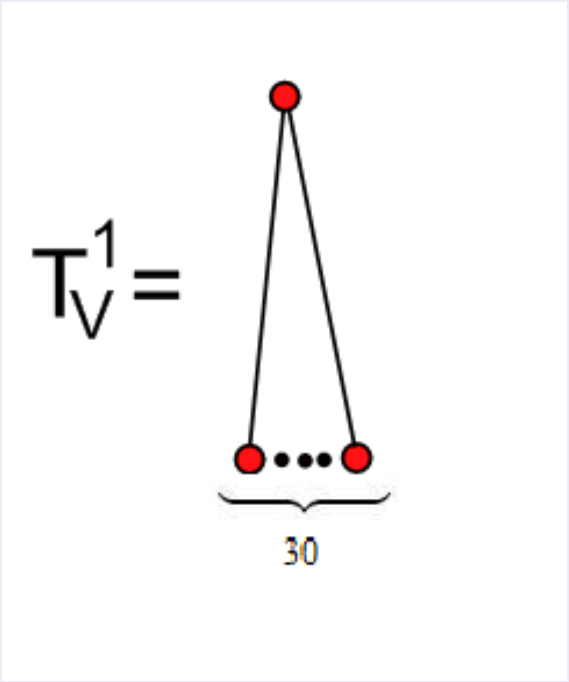
Example 1

We consider $V = 360(30) = (30, 6, 2) \Rightarrow T_V = ?$

$T_V^1 = \langle 30 \times \bullet \rangle$

$T_V^2 = \langle 6 \times T_V^1 \oplus 24 \times \bullet \rangle$

$T_V = \langle T_V^2 \oplus 4 \times T_V^1 \oplus 24 \times \bullet \rangle$



Tree associated with ν-series

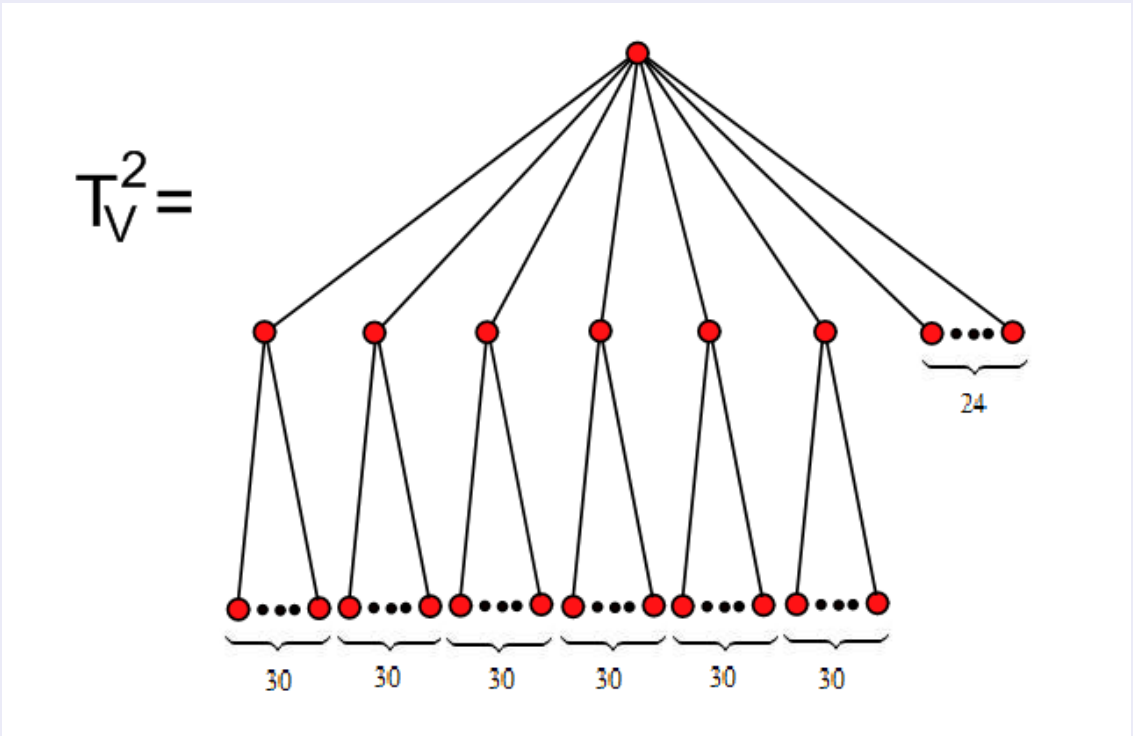
Example 1

We consider $V = 360(30) = (30, 6, 2) \Rightarrow T_V = ?$

$T_V^1 = \langle 30 \times \bullet \rangle$

$T_V^2 = \langle 6 \times T_V^1 \oplus 24 \times \bullet \rangle$

$T_V = \langle T_V^2 \oplus 4 \times T_V^1 \oplus 24 \times \bullet \rangle$



Tree associated with ν-series

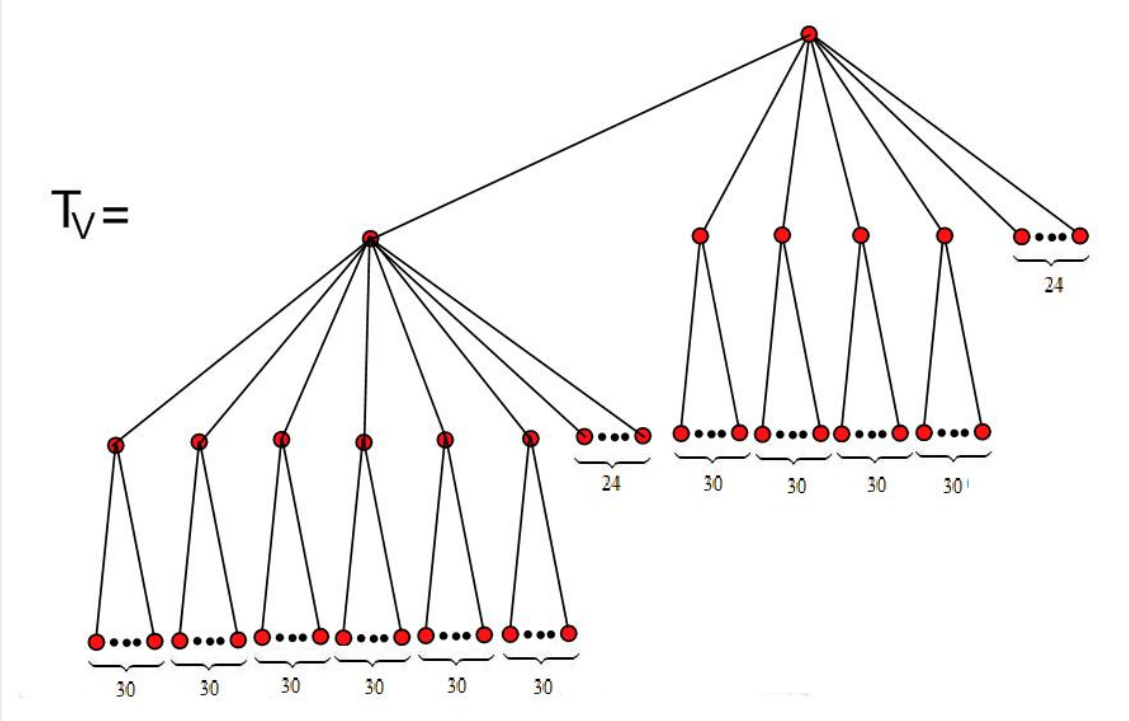
Example 1

We consider $V = 360(30) = (30, 6, 2) \Rightarrow T_V = ?$

$T_V^1 = \langle 30 \times \bullet \rangle$

$T_V^2 = \langle 6 \times T_V^1 \oplus 24 \times \bullet \rangle$

$T_V = \langle T_V^2 \oplus 4 \times T_V^1 \oplus 24 \times \bullet \rangle$



Tree associated with ν-series

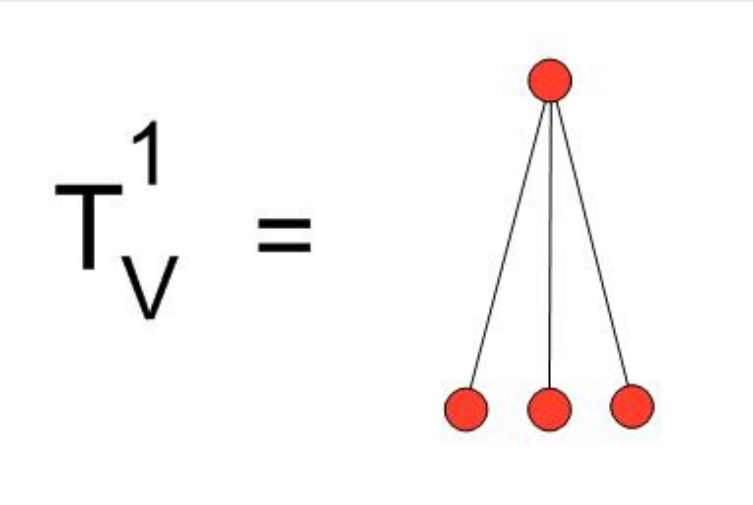
Example 2

We consider $V = 27(3) = (3, 3, 3) \Rightarrow T_V = ?$

$T_V^1 = \langle 3 \times \bullet \rangle$

$T_V^2 = \langle 3 \times T_V^1 \rangle$

$T_V = \langle 2 \times T_V^2 \rangle$



Tree associated with ν-series

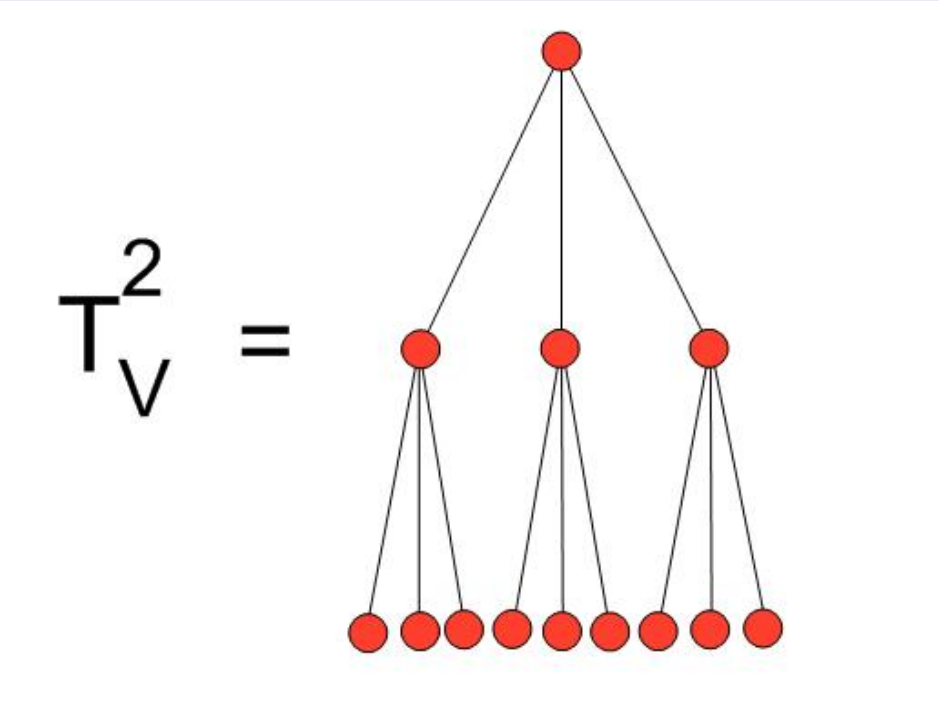
Example 2

We consider $V = 27(3) = (3, 3, 3) \Rightarrow T_V = ?$

$T_V^1 = \langle 3 \times \bullet \rangle$

$T_V^2 = \langle 3 \times T_V^1 \rangle$

$T_V = \langle 2 \times T_V^2 \rangle$



Tree associated with ν-series

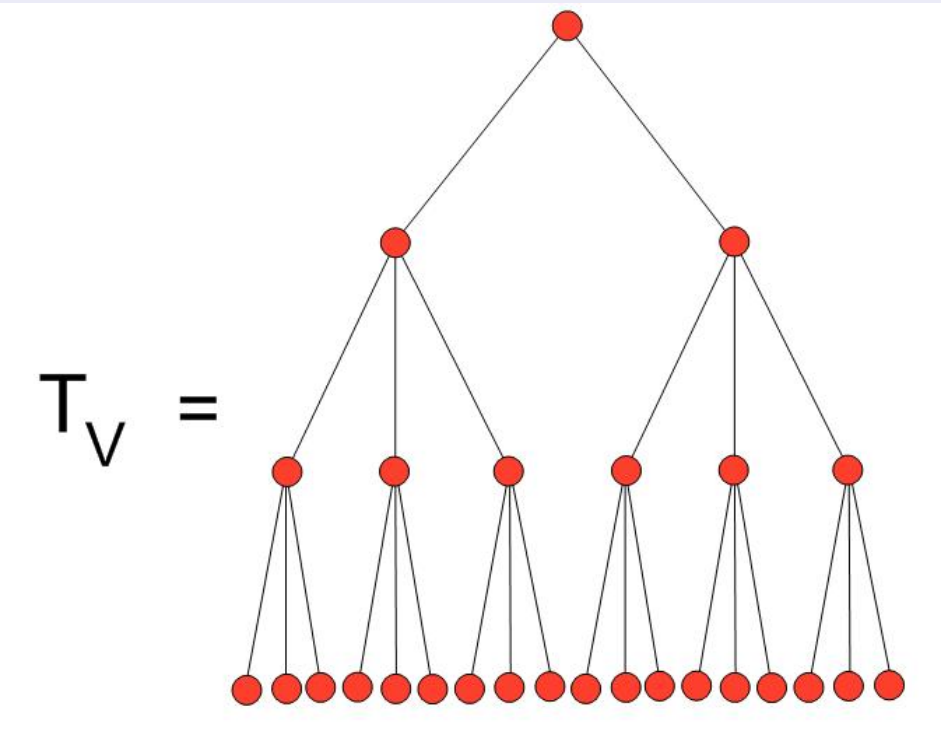
Example 2

We consider $V = 27(3) = (3, 3, 3) \Rightarrow T_V = ?$

$T_V^1 = \langle 3 \times \bullet \rangle$

$T_V^2 = \langle 3 \times T_V^1 \rangle$

$T_V = \langle 2 \times T_V^2 \rangle$



New results coming...

Some estimates on the cycle structure of Rédei functions

We fix $n \in \mathbb{Z}^+, \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$. Let $\mathbb{D}_q^a = \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\}$.
We consider the Rédei function $R_n(x, a)$ as a map in $\mathbb{D}_q^a$ and denote by $\mathcal{G}(n, a, q)$ its functional graph.

We are interested on the following parameters:

- $N(n, a, q) =$ number of connected components in $\mathcal{G}(n, a, q)$,
- $T_0(n, a, q) =$ number of periodic points in $\mathcal{G}(n, a, q)$,
- $C(n, a, q) = \frac{1}{q-\chi(a)} \sum_{u \in \mathbb{D}_q^a} per(u)$,
- $T(n, a, q) = \frac{1}{q-\chi(a)} \sum_{u \in \mathbb{D}_q^a} pper(u)$;

and also in an asymptotic estimated for

- $S_0(n, a, N) = \frac{1}{\pi(N)} \sum_{p \leq N} T_0(n, a, p)$,
- $S(n, a, N) = \frac{1}{\pi(N)} \sum_{p \leq N} T(n, a, p)$.

Previous estimates on the cycle structure of functions

Estimates for N, T_0, C, T, S and S_0 respect to other maps

- For the map $x \mapsto x^2$ in $\mathbb{F}_p$.
  Vasiga and Shallit, On the iteration of certain quadratic maps over GF(p), Discrete Math., vol. 277, pp. 219-240, 2004.

- For the map $x \mapsto x^e$ in $\mathbb{F}_p$.
  Chou and Shparlinski, On the cycle structure of repeated exponentiation modulo a prime, Journal of Number Theory, vol. 107, pp. 345-356, 2004.

If a is a square element in $\mathbb{F}_p$, then the dynamics of $R_n(x, a)$ over $\mathbb{D}_p^a$ coincides with the one of $x \mapsto x^e$ over $\mathbb{F}_p^*$. Since our results hold for all $a \in \mathbb{F}_q^*$, our work on Rédei functions can be seen as a generalization of Chou and Shparlinski. Moreover, the dynamics of $R_n(x, a)$ over $\mathbb{D}_p^a$ is similar to the one of the n-map $x \longmapsto nx$ over the integers modulo $p \pm 1$, depending on the quadratic character of a in $\mathbb{F}_p$; see also Sha (2012).

Estimates on N, T_0, C and T of Rédei functions

Theorem (Estimates for N, T_0, C and T respect to Rédei functions)

Let $n \in \mathbb{Z}^+$, $a \in \mathbb{F}_q^*$ and $q - \chi(a) = \nu\omega$ with $\text{rad}(\nu) \mid \text{rad}(n)$ and $\gcd(n, \omega) = 1$. Let $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$ be the ν-series associated to n. For the Rédei function $R_n(x, a)$ on $\mathbb{D}_q^a$ we have the following quantities:

$$N(n, a, q) = \sum_{d \mid \omega} \frac{\varphi(d)}{o_d(n)}, \qquad T_0(n, a, q) = \omega,$$

$$C(n, a, q) = \frac{1}{\omega} \sum_{d \mid \omega} \varphi(d) o_d(n), \qquad T(n, a, q) = \frac{1}{\nu} \sum_{j=1}^{D-1} \nu_1 \ldots \nu_j.$$

Estimates on N, T_0, C and T of Rédei functions

Sketch of proof

When $\chi(a) = 1$ we have that $\{\pm\sqrt{a}\}$ are isolated fixed points of $R_n(x, a)$ and the isomorphism formula over $\mathbb{D}_q^a$ gives

$$\mathcal{G}(n, a, q) = \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T_{\nu(n)}) \right\}$$

We obtain

- $N(n, a, q) = \sum_{d|\omega} \frac{\varphi(d)}{o_d(n)}$.
- $T_0(n, a, q) = \sum_{d|\omega} \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) = \sum_{d|\omega} \varphi(d) = \omega$.
- $C(n, a, q) = \frac{1}{\nu\omega} \sum_{u \in D_q} per(u)$
  $= \frac{1}{\nu\omega} \sum_{d|\omega} \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) \cdot \#T_{\nu(n)} \cdot o_d(n) = \frac{1}{\omega} \sum_{d|\omega} \varphi(d) o_d(n)$.

Estimates on N, T_0, C and T of Rédei functions

Sketch of proof

If $h(j)$ denotes the number of vertices at depth j in $T_{\nu(n)}$, again, from the isomorphism formula we have $T(n,a,q) = \frac{1}{\nu}\sum_{j=1}^{D} jh(j)$. Let $h_i(j)$ be the number of vertices at depth j in T^i. Using the recurrence formula for $T_{\nu(n)}$:

$$\begin{cases} T^0 = \bullet, \\ T^k = \langle \nu_k \times T_V^{k-1} \oplus \bigoplus_{i=1}^{k-1}(\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle \text{ for } 1 \leq k \leq D, \\ T_{\nu(n)} = \langle (\nu_D - 1) \times T_V^{D-1} \oplus \bigoplus_{i=1}^{D-1}(\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle, \end{cases}$$

we obtain $h_k(j) = \nu_k h_{k-1}(j-1) + \sum_{i=1}^{k-1}(\nu_i - \nu_{i+1})h_{i-1}(j-1)$ with $h_0(0) = 1, h_0(j) = 0$ for $j > 0$ implying $h_i(j) = \nu_1 \cdots \nu_j$ for $0 \leq j \leq i$ and $h(j) = h_D(j) - h_{D-1}(j-1) = \nu_1 \cdots \nu_j - \nu_1 \cdots \nu_{j-1}$. Using partial sums on $\sum_{j=1}^{D} jh(j)$ we obtain the desired formula for $T(n,a,q)$. □

Estimates on S_0 for Rédei functions

The S_0 case

Remember that

$$S_0(n,a,N) = \frac{1}{\pi(N)} \sum_{p \leq N} T_0(n,a,p)$$

where $T_0(n,a,p) = \omega$ is the number of periodic points in the Rédei graph. We have that ω is the maximum coprime-with-n divisor of $p - \chi_p(a)$ (that is, $p - \chi_p(a) = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(\omega, n) = 1$).

Estimates on S_0 for Rédei functions

The S_0 case

We denote by n a positive integer and $Q = p_1 \cdots p_s$ the square-free part of n, $\mathcal{L} = \langle p_1, \ldots, p_s \rangle$ the multiplicative semigroup generated by the prime divisors of n. For $m \in \mathbb{Z}^+$ we denote by $[m] = \{1, \ldots, m\}$ and $\mathrm{Cop}(m) = \{i \in [m] : \gcd(i, m) = 1\}$.

Theorem (Estimates for S_0 for the Rédei functions)

Let n and a be positive integers, and $p_1, \ldots, p_s$ be the distinct prime divisors of n. Then

$$S_0(n, a, N) \sim \frac{N}{2} \cdot \prod_{i=1}^{s} \left(\frac{p_i^2 - p_i - 1}{p_i^2 - 1} \right).$$

Proof ideas

The key idea used by Chou and Shparlinski and that we follow here is to express $S_0(n, a, N)$ as a sum in $\nu \in \mathcal{L}$ where every term is a finite sum of primes in arithmetic progression. To obtain a similar expression in our case, we need some results that are consequences of the quadratic reciprocity law. Then, we use asymptotic results of analytic number theory to estimate the sums.

The results in Chou and Shparlinski for S_0 in the exponential case use similar sums on primes but their final result is $S_0 \sim \theta_0 N$, where θ_0 is expressed as an infinite sum over the $\nu \in \mathcal{L}$. Here we compute the constant of the main term involving a nice product of primes.

Estimates on S for Rédei functions

The S case

Remember that

$$S(n,a,N) = \frac{1}{\pi(N)} \sum_{p \leq N} T(n,a,p)$$

where $T(n,a,p) = \frac{1}{\nu} \sum_{j=1}^{D-1} \nu_1 \dots \nu_j$ is the average value of the tail length.

Theorem (Estimates for S for the Rédei functions)

Let n and a be positive integers, $p_1, \dots, p_s$ be the distinct prime divisors of n with $Q = p_1 \cdots p_s$, and $\mathcal{L} = \langle p_1, \dots, p_s \rangle$. For $\nu \in \mathcal{L}$ we denote by $\lambda(\nu) = \frac{1}{\nu} \sum_{i=1}^{D-1} \nu_1 \cdots \nu_i$ where $(\nu_1, \dots, \nu_D)$ is the ν-series generated by n. Then,

$$\lim_{N \to \infty} S(n,a,N) = \frac{1}{\varphi(Q)} \sum_{\nu \in \mathcal{L}} \frac{\lambda(\nu) \# \mathcal{U}_\nu}{\nu},$$

where $\mathcal{U}_\nu = \{u \in \{1, \dots, Q\} : \gcd(u, Q) = \gcd(\nu u + 1, Q) = 1\}$.

Thanks for your attention!