The graph structure of Chebyshev polynomials over finite fields

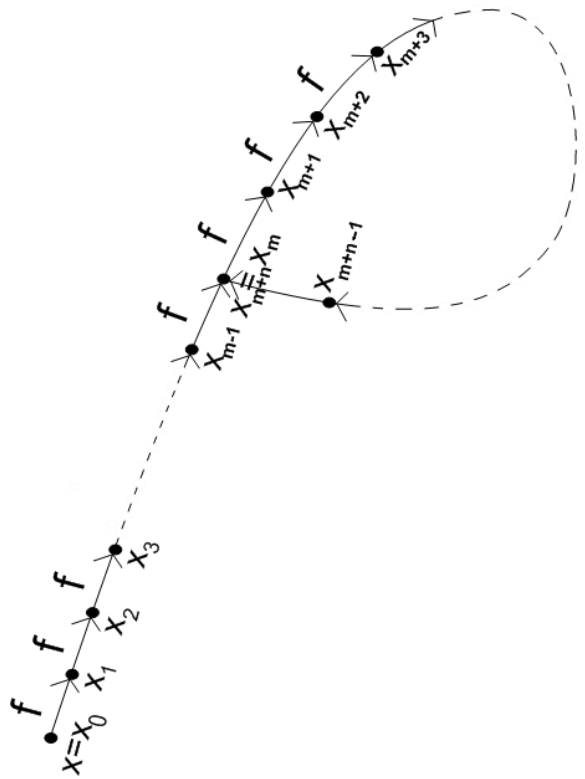
Claudio Qureshi
School of Mathematics and Statistics
Carleton University
cqureshi@gmail.com

Carleton Finite Fields Day
September 29, 2017
Joint work with Daniel Panario

Finite dynamics

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

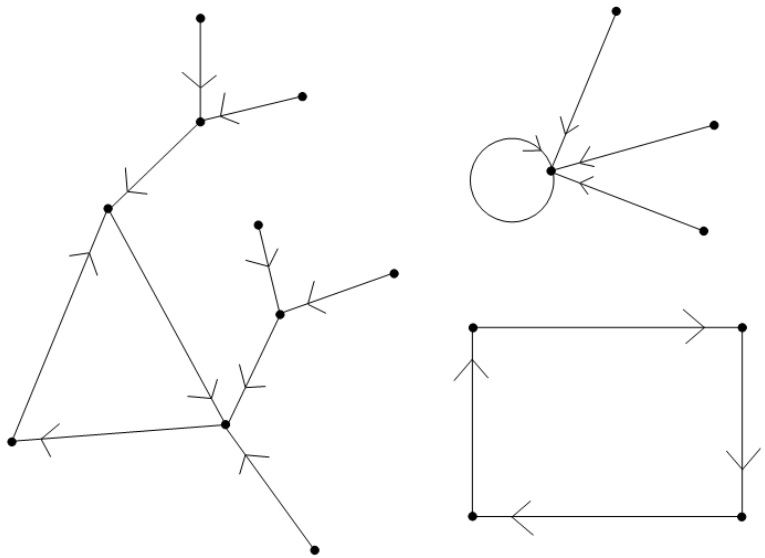
- For $x \in X$, let $n \geq 1, m \geq 0$ be the smallest integers such that $f^{(n+m)}(x) = f^{(m)}(x)$. Then, $per(x) = n, pper(x) = m$.



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 $outdeg(x) = 1$).



Chebyshev polynomials

The Chebyshev polynomial T_n of degree n is the only degree-n polynomial with integer coefficients verifying [1]

$$T_n(x + x^{-1}) = x^n + x^{-n}, \text{ for all non-zero } x \in \mathbb{Z}.$$

This is a family of multiplicative polynomials: $T_n \circ T_m = T_{nm}$ for all $m, n \in \mathbb{Z}^+$. In particular, $T_n^{(k)} = T_{n^k}$, where $f^{(k)}$ denotes the composition of f with itself k times.

Examples:

$$T_0(x) = 1, T_1(x) = x, T_2(x) = x^2 - 2,$$
$$T_3(x) = x^3 - 3x, T_4(x) = x^4 - 4x^2 + 2, \ldots.$$

[1] Another way: $T_n((x + x^{-1})/2) = (x^n + x^{-n})/2$, for all non-zero $x \in \mathbb{Z}$.

Chebyshev and Dickson polynomials

Chebyshev polynomials are closely related to Dickson polynomials. Let n be a positive integer. For $a \in \mathbb{Z}$, we define the n-th Dickson polynomial of the first kind $D_n(x, a)$ by

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

Dickson polynomials are related to the Chebyshev polynomials through the connection [2]

$$D_n(x, 1) = T_n(x).$$

[2] With the other definition this becomes $D_n(2x, 1) = 2T_n(x)$.

The functional graph of Chebyshev polynomials

Describing the dynamics of the Chebyshev polynomial T_n acting on the finite field $\mathbb{F}_q$ is equivalent to describing the Chebyshev's graph $\mathcal{G}(T_n/\mathbb{F}_q)$.

Iterations of Chebyshev polynomials over finite fields have been treated in Gassert (2014). He gives the graph and periodicity properties for Chebyshev polynomials over finite fields when the degree of the polynomial is a prime number.

We study the action of Chebyshev functions of any degree over non-binary finite fields. We give a structural theorem for the functional graph from which it is easy to derive many periodicity properties of these iterations.

Example: the functional graph of T_{30} on $\mathbb{F}_{13}$ [3]

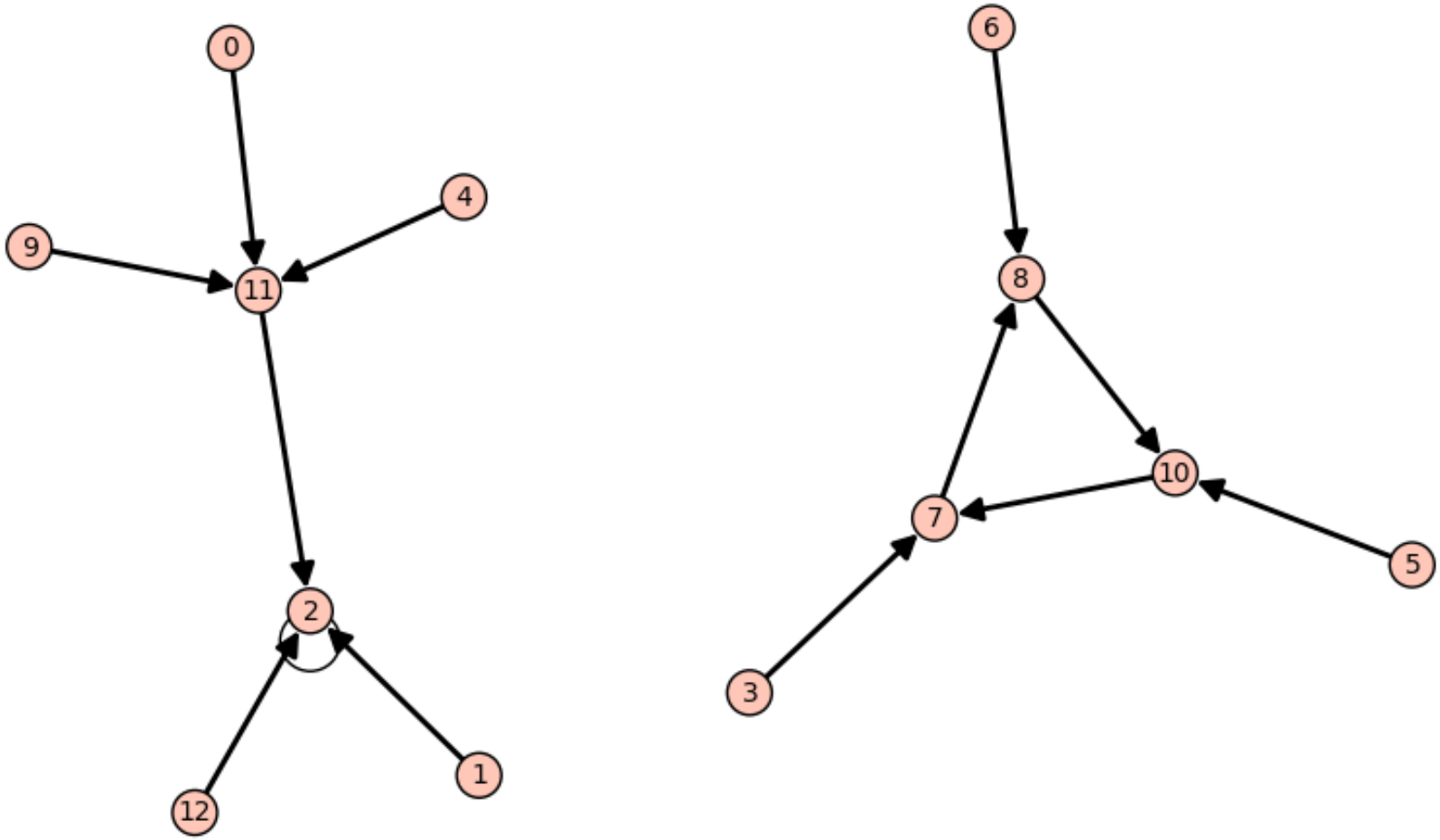


Figure: The graph $\mathcal{G}(30, 13) = \mathrm{Cyc}(1, T) \oplus \mathrm{Cyc}(3, T')$.

[3] $T_{30}(x) = x^{30} - 30x^{28} + 405x^{26} - 3250x^{24} + 17250x^{22} - 63756x^{20} + 168245x^{18} - 319770x^{16} + 436050x^{14} - 419900x^{12} + 277134x^{10} - 119340x^{8} + 30940x^{6} - 4200x^{4} + 225x^{2} - 2$

Example: the functional graph of T_{30} on $\mathbb{F}_{19}$

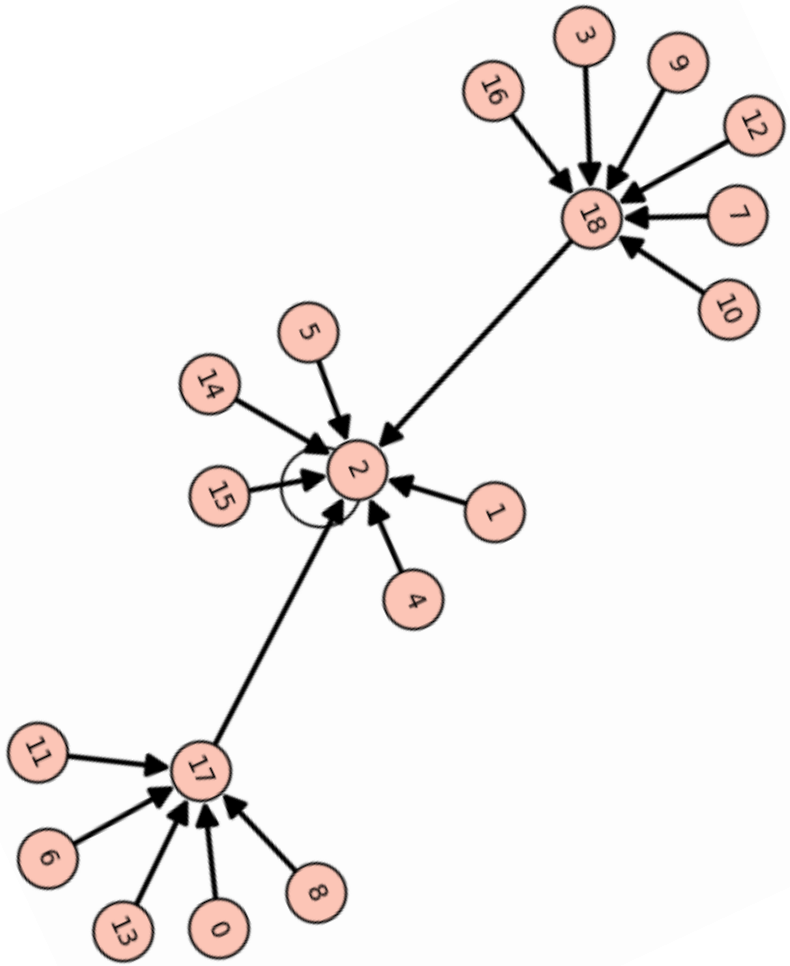


Figure: The graph $\mathcal{G}(30, 19) = \mathrm{Cyc}(1, T)$.

Example: the functional graph of T_{30} on $\mathbb{F}_{23}$

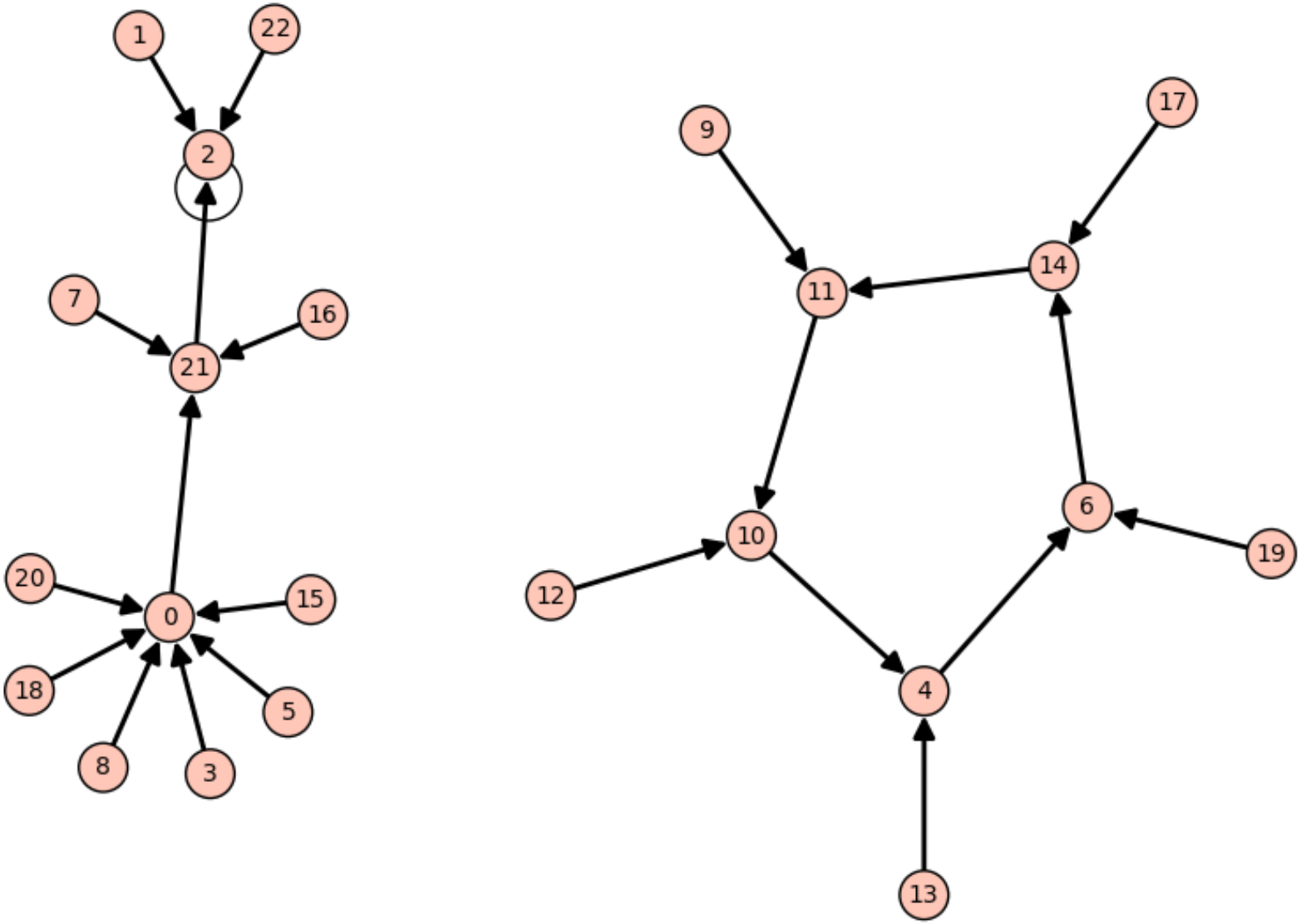


Figure: The graph $\mathcal{G}(30, 23) = \mathrm{Cyc}(1, T) \oplus \mathrm{Cyc}(5, T')$.

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$

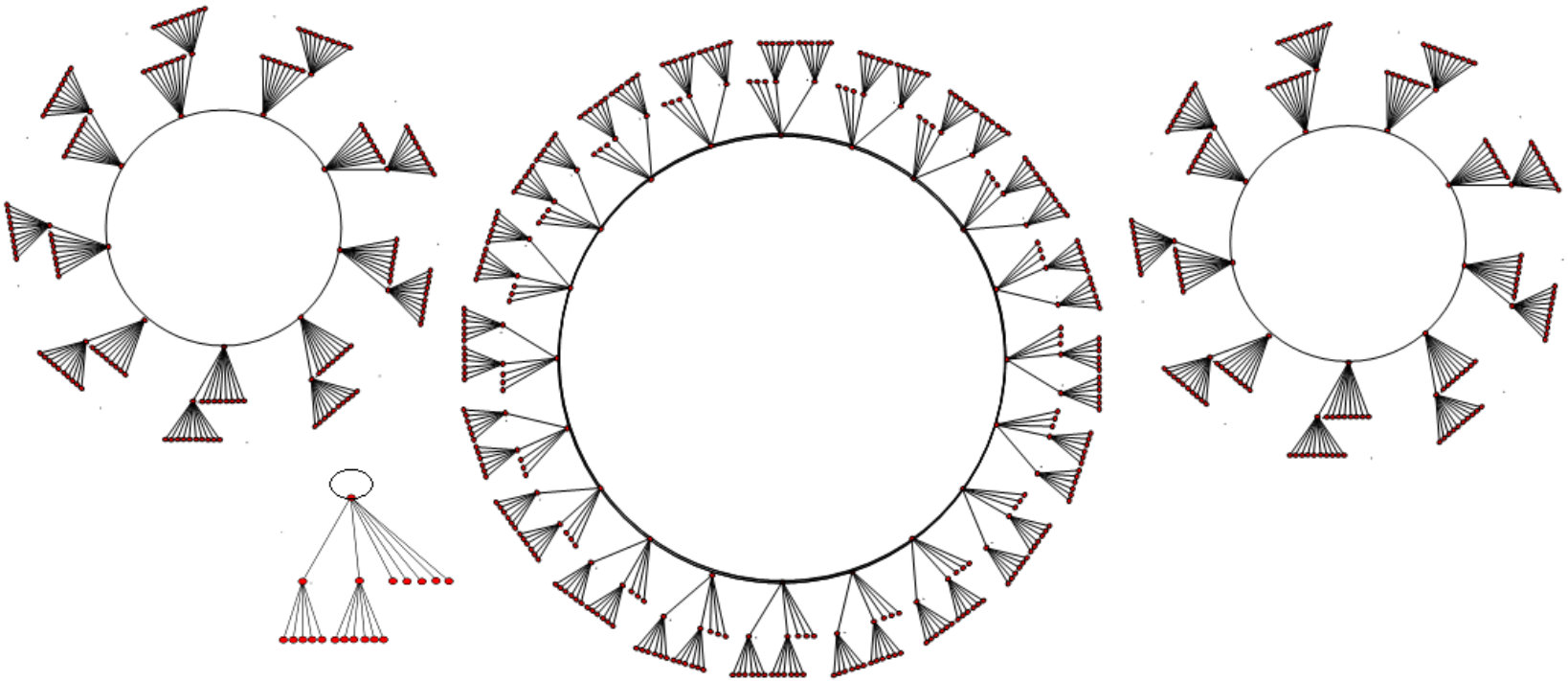


Figure: The Chebyshev functional graph $\mathcal{G}(T_{30}/\mathbb{F}_{739})$.

Description of the Chebyshev polynomial graph

Notation.

For $n, d \in \mathbb{Z}^+$ with $\gcd(n, d) = 1$ we denote the order and the semiorder of n modulo d by

- $o_d(n)$ the least positive integer satisfying $n^{o_d(n)} \equiv 1 \pmod{d}$.
- $\tilde{o}_d(n)$ the least positive integer satisfying $n^{\tilde{o}_d(n)} \equiv \pm 1 \pmod{d}$

For $n, m \in \mathbb{Z}^+$ we denote by

- $\mathrm{rad}(m)$ the radical of m (product of the distinct primes divisors of m). (Example. $m = 2^4 \cdot 5^2 \cdot 11 \cdot 17^5 \Rightarrow \mathrm{rad}(m) = 2 \cdot 5 \cdot 11 \cdot 17$)
- The n-decomposition of m is $m = \nu\omega$, where $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(\omega, n) = 1$.

Description of the Chebyshev polynomial graph

Isomorphism theorem for Chebyshev polynomial graph

Let $q-1=\nu_0\omega_0$ and $q+1=\nu_1\omega_1$ be the n-decomposition of $q-1$ and $q+1$, respectively. Let $B=\{a\in\mathbb{F}_q : T_n^{(k)}=\pm 2 \text{ for some } k\geq 0\}$ and $A=\mathbb{F}_q\setminus B$. Then $\mathcal{G}(T_n/\mathbb{F}_q)=\mathcal{G}(T_n/A)\oplus\mathcal{G}(T_n/B)$. For the non-binary component A we have the following isomorphism formula:

$$\mathcal{G}(T_n/A)=\bigoplus_{\substack{d|\omega_0\\ d>2}}\frac{\varphi(d)}{2\tilde{o}_d(n)}\times\mathrm{Cyc}\left(\tilde{o}_d(n),T_{\nu_0(n)}\right)\bigoplus_{\substack{d|\omega_1\\ d>2}}\frac{\varphi(d)}{2\tilde{o}_d(n)}\times\mathrm{Cyc}\left(\tilde{o}_d(n),T_{\nu_1(n)}\right)$$

For the binary component B we have the isomorphism

$$\mathcal{G}(T_n/B)=\begin{cases}2\times\mathrm{Cyc}\left(1,\frac{1}{2}T_{\nu_0(n)}+\frac{1}{2}T_{\nu_1(n)}\right) & \text{if } n \text{ is odd.}\\ \mathrm{Cyc}\left(1,\frac{1}{2}T_{\nu_0(n)}+\frac{1}{2}T_{\nu_1(n)}-\langle\bullet\rangle\right) & \text{if } n \text{ is even.}\end{cases}$$

Estimates on N, T_0, C and T of Chebyshev iterations

We apply our structural theorem to deduce explicit formulas for the parameters N, T_0, C and T for Chebyshev polynomials, where

- N is the number of cycles (that is, the number of connected components),
- T_0 is the number of cyclic (periodic) points,
- C is the expected value of the period,
- T is the expected value of the preperiod, and
- R is the expected rho length.

The average rho length can be obtained from $R = C + T$.

Parameters of Chebyshev iterations

Estimates on N, T_0, C and T of Chebyshev iterations

Let n be a positive integer. Let $q-1=\nu_0\omega_0$ and $q+1=\nu_1\omega_1$ be the n-decomposition of $q-1$ and $q+1$, respectively. Let $\tilde{o}_d(n)$ be the least positive integer satisfying $n^{\tilde{o}_d(n)} \equiv \pm 1 \pmod{d}$, $\nu_0(n)=(a_1,\ldots,a_D)$ and $\nu_1(n)=(b_0,\ldots,b_{D'})$. Then, the following holds:

- the number of cycles in $\mathcal{G}(T_n/\mathbb{F}_q)$ is $N(n,q)=\frac{1}{2}(\sum_{d|\omega_0}\frac{\varphi(d)}{\tilde{o}_d(n)}+\sum_{d|\omega_1}\frac{\varphi(d)}{\tilde{o}_d(n)})$;
- the number of periodic points is given by $T_0(n,q)=\frac{\omega_0+\omega_1}{2}$;
- the expected value of per(a) where a runs over the elements of $\mathbb{F}_q$ is $C(n,q)=\frac{q-1}{2q}(\frac{1}{\omega_0}\sum_{d|\omega_0}\varphi(d)\tilde{o}_d(n))+\frac{q+1}{2q}(\frac{1}{\omega_1}\sum_{d|\omega_1}\varphi(d)\tilde{o}_d(n))$;
- the expected value of pper(a) where a runs over the elements of $\mathbb{F}_q$ is $T(n,q)=\frac{q-1}{2q}(\frac{1}{\nu_0}\sum_{i=1}^{D-1}a_1\ldots a_i)+\frac{q+1}{2q}(\frac{1}{\nu_1}\sum_{i=1}^{D'-1}b_1\ldots b_i)$.

Sketch of isomorphism theorem proof

Ingredient 1: Splitting the graph in two components: the non-binary and the binary component

Consider $B = \{a \in \mathbb{F}_q : T_n^{(k)} = \pm 2 \text{ for some } k \geq 0\}$ and $A = \mathbb{F}_q \setminus B$.

- If n is even $T_n(-2) = T_n(2) = 2$ and B is the (backward) orbit of the fixed point 2. If n is odd $T_n(-2) = -2$ and $T_n(2) = 2$. In this case B is the union of the (backward) orbit of the fixed points 2 and -2. Thus, B is T_n-invariant.
- A is the complement of a T_n-invariant set, thus A is T_n-invariant.
- Then

$$\mathcal{G}(T_n/\mathbb{F}_q) = \mathcal{G}(T_n/A) \oplus \mathcal{G}(T_n/B).$$

Sketch of proof (for the non-binary component)

Ingredient 2: Splitting of the non-binary component $\mathcal{G}(T_n/A)$

Let H be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ with order $q+1$ and $\eta : H \cup \mathbb{F}_q^* \to \mathbb{F}_q$ be the map given by $\eta(\alpha) = \alpha + \alpha^{-1}$.

- For $a \in \mathbb{F}_q \setminus \{\pm 2\}$, $\eta^{-1}(a) = \{\alpha, \alpha^{-1}\}$, the roots of $x^2 - ax + 1 = 0$;
  - $a^2 - 4$ is a square $\Rightarrow \eta^{-1}(a) = \{\alpha, \alpha^{-1}\} \subseteq \mathbb{F}_q^* \setminus \{\pm 1\}$; $\longleftarrow \mathbb{F}_q^+$
  - $a^2 - 4$ is a non-square $\Rightarrow \eta^{-1}(a) = \{\alpha, \alpha^{-1}\} \subseteq H \setminus \{\pm 1\} \longleftarrow \mathbb{F}_q^-$.

  $\eta^{-1}(2) = \{1\}$, $\eta^{-1}(-2) = \{-1\}$.
- From above we decompose $\mathbb{F}_q = \mathbb{F}_q^+ \cup \mathbb{F}_q^- \cup \{\pm 2\}$.
- We also prove that $A \cap \mathbb{F}_q^+$ and $A \cap \mathbb{F}_q^-$ are T_n-invariant which gives us the following decomposition:

$$\mathcal{G}(T_n/A) = \mathcal{G}(T_n/A \cap \mathbb{F}_q^+) \oplus \mathcal{G}(T_n/A \cap \mathbb{F}_q^-).$$

Sketch of proof (for the non-binary component)

Ingredient 3: Restricting to the periodic points

Consider again the map $\eta : H \cup \mathbb{F}_q^* \to \mathbb{F}_q$, $\eta(\alpha) = \alpha + \alpha^{-1}$.
Let P be the set of T_n-periodic points, $\alpha \in H \cup \mathbb{F}_q^*$ and $a = \eta(\alpha) \in \mathbb{F}_q$.

- We prove that $a \in P$ if and only if $\mathrm{ord}(\alpha)$ is coprime with n. In this case:
  - If $\alpha \in \mathbb{F}_q^*$, then $\mathrm{ord}(\alpha) \mid q-1 = \nu_0\omega_0 \Rightarrow \mathrm{ord}(\alpha) \mid \omega_0$.
  - If $\alpha \in H$, then $\mathrm{ord}(\alpha) \mid q+1 = \nu_1\omega_1 \Rightarrow \mathrm{ord}(\alpha) \mid \omega_1$.
- For $d \mid \omega_0, d \mid \omega_1$ we define $P_d = \{a \in H \cup \mathbb{F}_q^* : \mathrm{ord}(\alpha) = d\}$.
- We prove the following decomposition in T_n-invariant sets:
  - $A \cap \mathbb{F}_q^+ \cap P = \biguplus_{\substack{d \mid \omega_0 \\ d>2}} P_d$ and $A \cap \mathbb{F}_q^- \cap P = \biguplus_{\substack{d \mid \omega_1 \\ d>2}} P_d$.

Let $\mathcal{G}^{\mathrm{per}}$ be the restriction graph to the periodic points.

Sketch of proof (for the non-binary component)

continuation...

- From which we obtain:
  - $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^+) = \bigoplus_{\substack{d \mid \omega_0 \\ d>2}} \mathcal{G}(T_n/P_d)$ and
  - $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^-) = \bigoplus_{\substack{d \mid \omega_1 \\ d>2}} \mathcal{G}(T_n/P_d)$.
- We use a counting argument to prove that $\#P_d = \varphi(d)/2$ for $d > 2$ and that the period of the points in P_d is exactly $\tilde{o}_d(n)$. Therefore,
  - $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^+) = \bigoplus_{\substack{d \mid \omega_0 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\,(\tilde{o}_d(n), \bullet)$ and
  - $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^-) = \bigoplus_{\substack{d \mid \omega_1 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\,(\tilde{o}_d(n), \bullet)$.

Sketch of proof (for the non-binary component)

Ingredient 4: Description of the trees

Let $r_n(x) = x^n$ and $\tilde{A} = \eta^{-1}(A)$. The following diagrams commute:

$$\begin{array}{ccc} H \cap \tilde{A} & \xrightarrow{\eta} & \mathbb{F}_q^- \cap A \\ {\scriptstyle r_n}\uparrow & & \uparrow{\scriptstyle T_n} \\ H \cap \tilde{A} & \xrightarrow{\eta} & \mathbb{F}_q^- \cap A \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{F}_q^* \cap \tilde{A} & \xrightarrow{\eta} & \mathbb{F}_q^+ \cap A \\ {\scriptstyle r_n}\uparrow & & \uparrow{\scriptstyle T_n} \\ \mathbb{F}_q^* \cap \tilde{A} & \xrightarrow{\eta} & \mathbb{F}_q^+ \cap A \end{array}$$

where in both cases η establishes a 2-1 correspondence. We prove:

- α is r_n-periodic if and only if $a = \eta(\alpha)$ is T_n-periodic;

and the following results relating to the trees:

- $\mathcal{T}_a(T_n/\mathbb{F}_q^- \cap A) = \mathcal{T}_\alpha(r_n/H \cap \tilde{A}) = \mathcal{T}_\alpha(r_n/H) = \mathcal{T}_0(m_n/\mathbb{Z}_{q+1})$ and
- $\mathcal{T}_a(T_n/\mathbb{F}_q^+ \cap A) = \mathcal{T}_\alpha(r_n/\mathbb{F}_q^* \cap \tilde{A}) = \mathcal{T}_\alpha(r_n/\mathbb{F}_q^*) = \mathcal{T}_0(m_n/\mathbb{Z}_{q-1})$,

where $m_n(x) = nx$ is the multiplication-by-n map.

Sketch of proof (for the non-binary component)

Ingredient 5: Trees associated with ν-series

In the paper "Rédei actions on finite fields and multiplication map in cyclic groups", SIAM Journal on Discrete Mathematics 29 (2015), 1486-1503; we prove the following result about the functional graph of the multiplication-by-n map on the cyclic group $\mathbb{Z}_{\nu\omega}$ (with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(\omega, n) = 1$):

$$\mathcal{G}(m_n/\mathbb{Z}_{\nu\omega}) = \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T_{\nu(n)}) \right\}.$$

If $q-1 = \nu_0\omega_0$ and $q+1 = \nu_1\omega_1$ are the n-decomposition of $q-1$ and $q+1$, we conclude that all the trees attached to cyclic points in $\mathcal{G}(T_n/A \cap \mathbb{F}_q^+)$ are isomorphic to $T_{\nu_0(n)}$ and all the trees attached to cyclic points in $\mathcal{G}(T_n/A \cap \mathbb{F}_q^-)$ are isomorphic to $T_{\nu_1(n)}$.

Sketch of proof (for the non-binary component)

Ingredient 5: Trees associated with ν-series (continuation)

If $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$, we define the following sequence: $\nu_1 = \gcd(\nu, n)$

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

Let $D = \max\{i \geq 1 : \nu_i > 1\}$, then $\nu(n) := (\nu_1, \nu_2, \dots, \nu_D)$ is the ν-series relative to n. By convention, for $\nu = 1$ we define $\nu(n) = (1)$ for all n.
The tree $T_{(\nu_1,\nu_2,\dots,\nu_D)}$ associated with the ν-series is defined as:

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

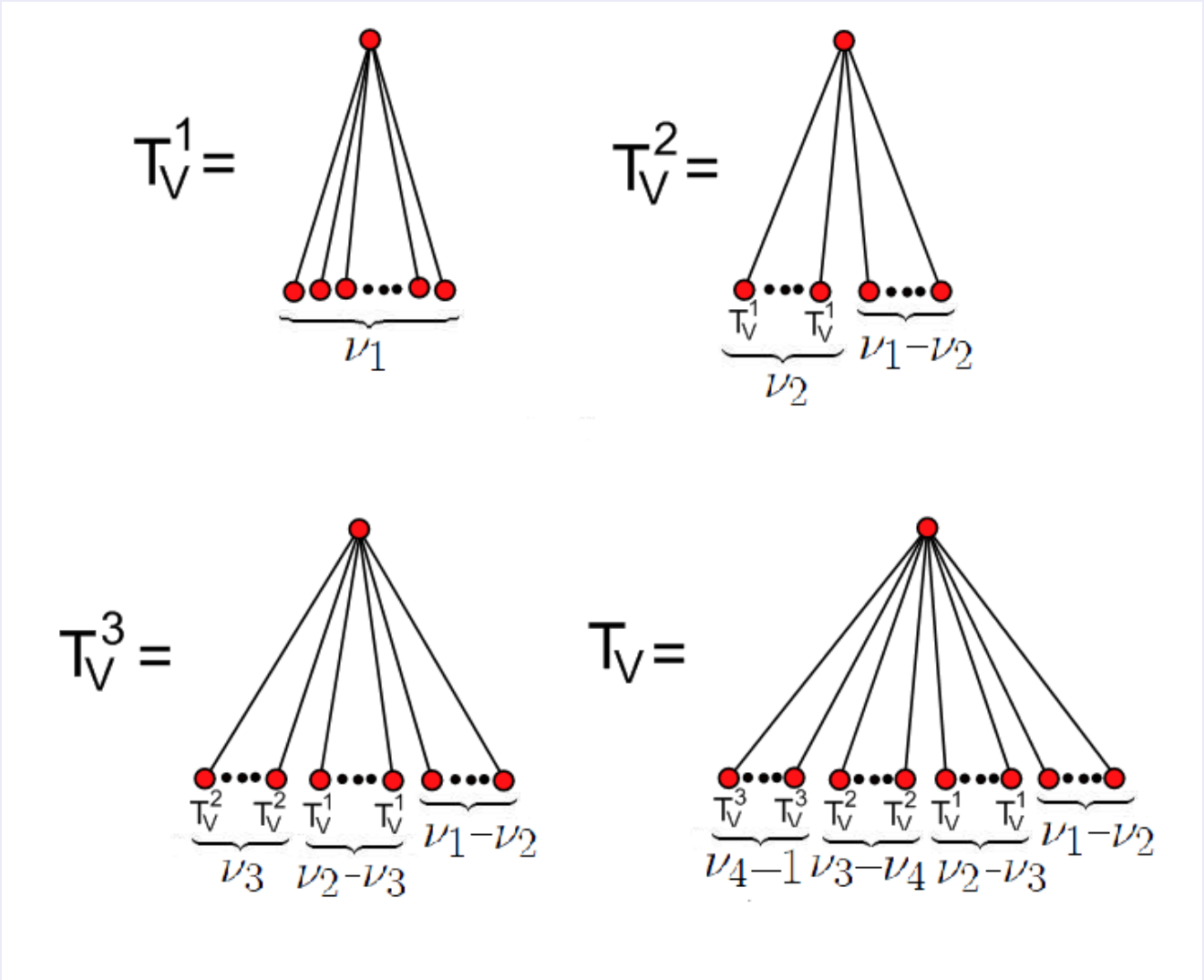
and

$$T_{(\nu_1,\nu_2,\dots,\nu_D)} = \langle (\nu_D - 1) \times T^{D-1} \oplus \bigoplus_{i=1}^{D-1} (\nu_i - \nu_{i+1}) \times T^{i-1} \rangle.$$

By convention $T_{(1)} = \bullet$.

Sketch of proof (for the non-binary component)

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



Sketch of proof (for the non-binary component)

Ingredient 5: Trees associated with ν-series (continuation)

Given that

- $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^+) = \bigoplus_{\substack{d|\omega_0 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\left(\tilde{o}_d(n), \bullet\right)$ and
- $\mathcal{G}^{\mathrm{per}}(T_n/A \cap \mathbb{F}_q^-) = \bigoplus_{\substack{d|\omega_1 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\left(\tilde{o}_d(n), \bullet\right)$,

we obtain

- $\mathcal{G}(T_n/A \cap \mathbb{F}_q^+) = \bigoplus_{\substack{d|\omega_0 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\left(\tilde{o}_d(n), T_{\nu_0(n)}\right)$ and
- $\mathcal{G}(T_n/A \cap \mathbb{F}_q^-) = \bigoplus_{\substack{d|\omega_1 \\ d>2}} \frac{\varphi(d)}{2\tilde{o}_d(n)} \times \mathrm{Cyc}\left(\tilde{o}_d(n), T_{\nu_1(n)}\right)$,

and using that

$$\mathcal{G}(T_n/A) = \mathcal{G}(T_n/A \cap \mathbb{F}_q^+) \oplus \mathcal{G}(T_n/A \cap \mathbb{F}_q^-),$$

we conclude the proof.

Chebyshev polynomial graph

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$.

- 30-decomposition of 738 and 740: $739-1=738=\nu_0\omega_0$ with $\nu_0=18,\omega_0=41$, and $739+1=740=\nu_1\omega_1$ with $\nu_1=20,\omega_1=37$. Since $\varphi(41)=40$, $\tilde{o}_{41}(30)=20$ ($30^i\not\equiv\pm1 \pmod{41}$ for $1\leq i<20$ and $30^{20}\equiv-1 \pmod{41}$), $\varphi(37)=36$, $\tilde{o}_{37}(30)=9$ ($30^i\not\equiv\pm1 \pmod{37}$ for $1\leq i<9$ and $30^9\equiv-1 \pmod{37}$), the non-binary component of $\mathcal{G}(T_{30}/\mathbb{F}_{739})$ is given by:
$\mathcal{G}^{\text{non-bin}}(T_{30}/\mathbb{F}_{739})=\mathrm{Cyc}(20,T_{18(30)})\oplus 2\times\mathrm{Cyc}(9,T_{20(30)})$.
We have $18(30)=(6,3)$ and $20(30)=(10,2)$. Therefore

$$\mathcal{G}^{\text{non-bin}}(T_{30}/\mathbb{F}_{739})=\mathrm{Cyc}(20,T_{(6,3)})\oplus 2\times\mathrm{Cyc}(9,T_{(10,2)}).$$

The binary component is given by

$$\mathcal{G}^{\text{bin}}(30,739)=\mathrm{Cyc}\left(1,\frac{1}{2}T_{(6,3)}+\frac{1}{2}T_{(10,2)}-\langle\bullet\rangle\right).$$

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$

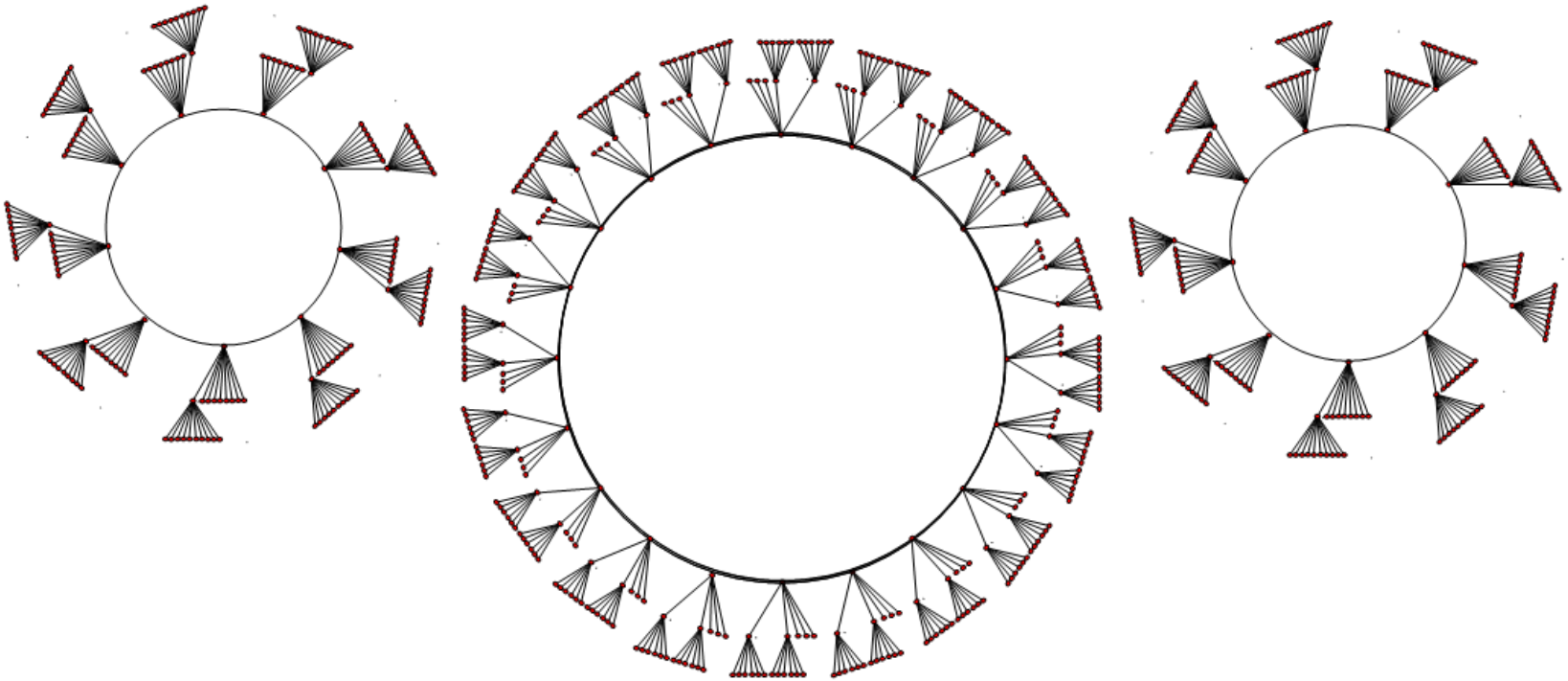


Figure: The non-binary component
$\mathcal{G}^{\text{non-bin}}(T_{30}/\mathbb{F}_{739}) = \text{Cyc}(20, T_{(6,3)}) \oplus 2 \times \text{Cyc}(9, T_{(10,2)})$.

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$

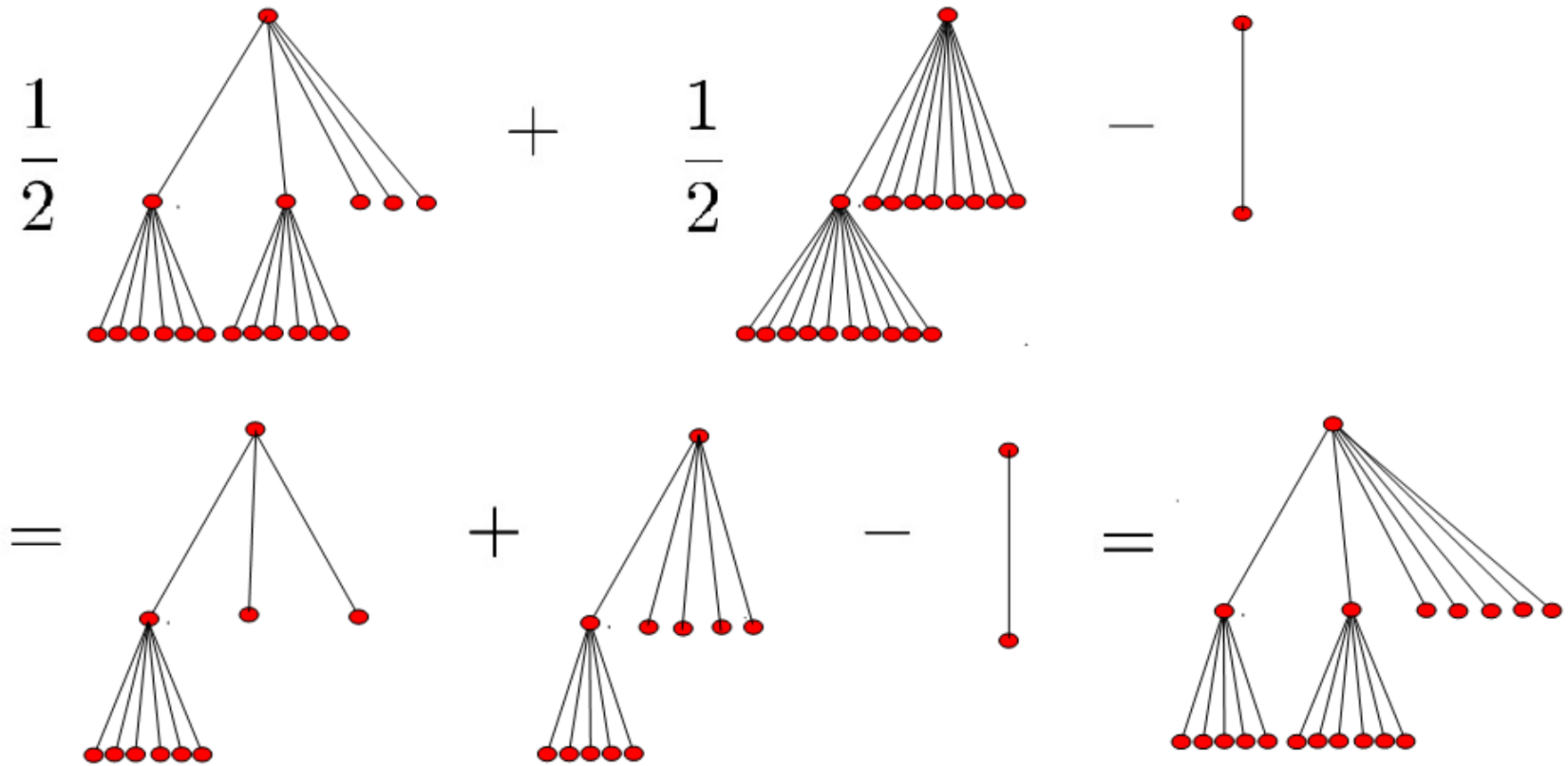


Figure: The binary component graph
$\mathcal{G}^{\mathsf{bin}}(30, 739) = \mathsf{Cyc}\left(1, \frac{1}{2}T_{(6,3)} + \frac{1}{2}T_{(10,2)} - \langle\bullet\rangle\right)$.

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$

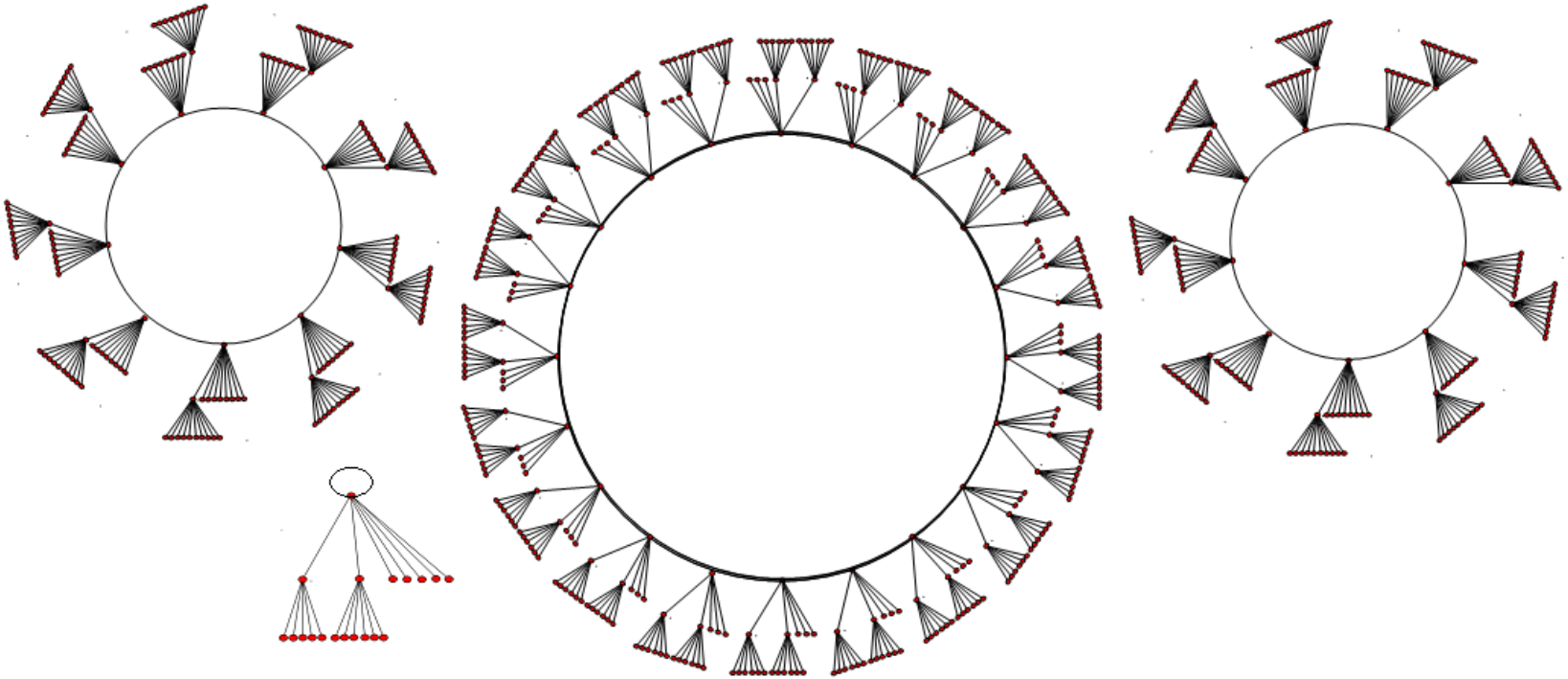


Figure: The Chebyshev functional graph $\mathcal{G}(T_{30}/\mathbb{F}_{739})$.

Example: the functional graph of T_{30} on $\mathbb{F}_{739}$

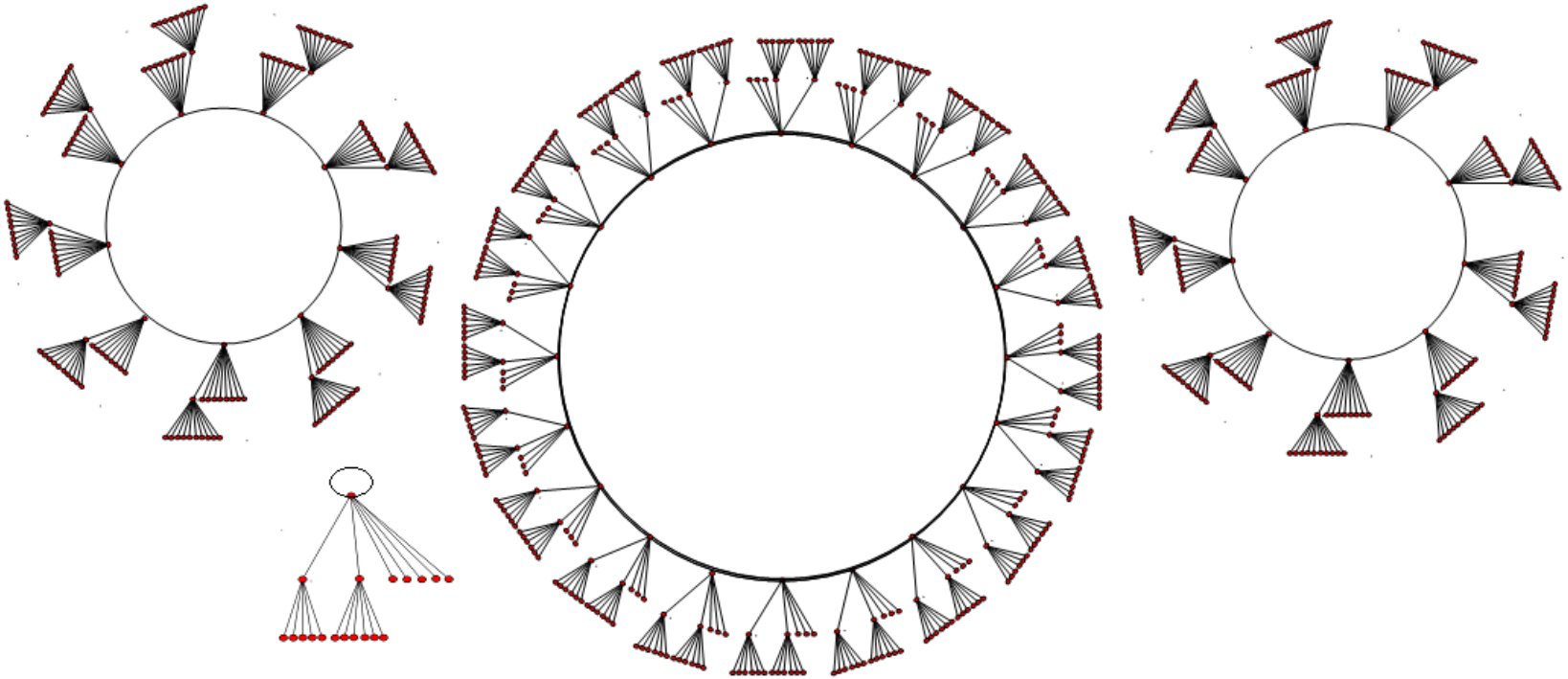


Figure: The Chebyshev functional graph $\mathcal{G}(T_{30}/\mathbb{F}_{739})$.

Thanks for your attention!