# Some topics in finite dynamical systems and error correcting codes in several metrics

Claudio Qureshi
Universidad de la República
cqureshi@fing.edu.uy

Seminario CyTeD
12 de octubre, 2022

# Contents

# Brief Self-introduction

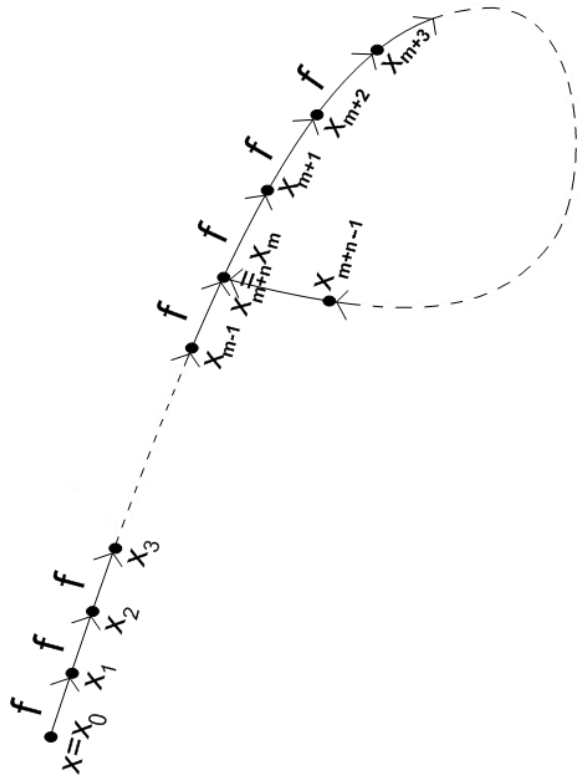
- Bachelor degree in mathematics UdelaR (2007). Final project: "Introduction to Elliptic Curves" (spanish). Sup: Gonzalo Tornaría.
- Master degree in mathematics UdelaR (2012). Master thesis: "Elliptic Curve Cryptography and Discrete Logarithm: implementation of random self-reducibility" (spanish). Sup: Gonzalo Tornaría.
- PhD degree in applied mathematics Unicamp-Carleton University (2015). PhD. thesis: "Perfect codes in the Lee and Chebyshev metrics and iterating Rédei functions.". Sup: Sueli Costa and Daniel Panario.
- Postdoc researcher:
  - CNPq postdoc at Unicamp (2016)
  - Fields Institute postdoc at Carleton University (2017)
  - Fapesp postdoc at Unicamp (2018)
  - Pedeciba postdoc at UdelaR (2019)

# Contents

# Finite dynamics

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

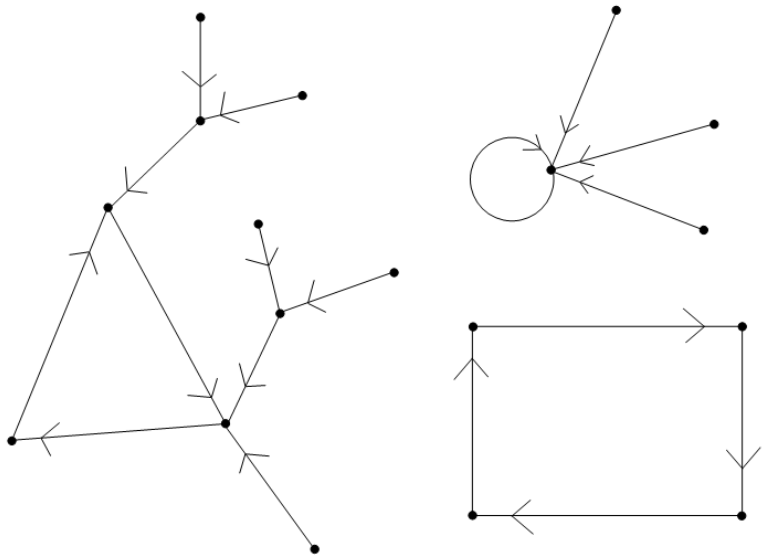
- For $x \in X$, let $n \geq 1, m \geq 0$ be the smallest integers such that $f^{n+m}(x) = f^m(x)$. Then, $\mathrm{per}(x) = n, \mathrm{pper}(x) = m$.



# 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 $\mathcal{G}(f/X)$ with vertex set $X$ and edges $(x, f(x))$ for $x \in X$ ($\mathrm{indeg}(x) = \#f^{-1}(x)$ and $\mathrm{outdeg}(x) = 1$).



# 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.

Two types of results:

- Explicit description (only possible for well structured maps).
- Asymptotic results for family of maps.

# Some special cases of dynamical systems over finite fields

- Quadratic maps (Rogers'96, Peinado et.al '01, Vasiga-Shallit '04).
- Power maps on finite fields (Chou-Shparlinski'04)
- Maps of the form $x \to k \cdot (x^d + x^{-d})$ (Ugolini'14).
- Redei functions (Panario-Q.'15 and Martins-Panario-Q.'16)
- Chebyshev polynomials (Gassert'14, Panario-Q.'19)
- Maps induced by endomorphism of elliptic curves (Ugolini'18)
- Linearized polynomials (Panario-Reis'19)
- Power maps on residually finite Dedekind domains (Q.-Reis'19)
- Maps of the form $x \to x^n h(x^{\frac{q-1}{m}})$ (Alves-Brochero'22)
- Power map in flower groups (Q.-Reis'22)

R. Martins, D. Panario, C. Qureshi. A Survey on Iterations of Mappings over Finite Fields. In: *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*. De Gruyter, Berlin. 2019

# Applications

## Some applications of FDS in cryptography

- Integer factorization
- Discrete logarithm problem
- Pseudorandom number generators

## The beginning: Pollard's rho method

Pollard, J. M. (1975). "A Monte Carlo method for factorization".

# Pollard's method

Brief history:

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

Used in (brief list):

- D. Johnson, A. Menezes, S. Vanstone, ECDSA, 2001.
- Wiener M., Zuccherato R., Faster attacks on elliptic curve cryptosystems, 1998.
- R. Gallant, R. Lambert, S. Vanstone, Improving the parallelized Pollard lambda search on anomalous binary curves, 2000.

# Pollard's rho method

- Iteration function: $f(x) = x^2 + a$.
- Rho path of a random element $x_0$:

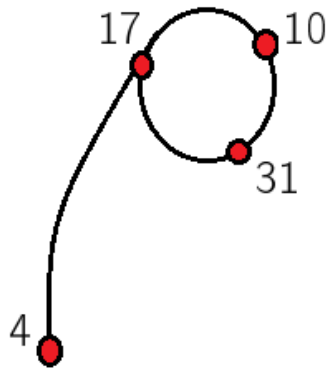



Figure: Rho path of $x_0 = 4$ under $f(x) = x^2 + 1 \in \mathbb{Z}_{35}[x]$.

$$\begin{array}{ccccccccc} 4 & \to & 17 & \to & 10 & \to & 31 & \to & 17 \quad \text{modulo } 35 \\ 4 & \to & 3 & \to & 3 & \to & 3 & \to & 3 \quad \text{modulo } 5 \end{array}$$

- $gcd(17 - 10, 35) = 5 \Rightarrow$ non trivial factor!

# Pollard's rho method

## Main idea

- Choose $a \notin \{0, -2\}$ and $x_0 \in \mathbb{Z}_n$ at random and consider the sequence of iterated $x_0, x_1 = f(x_0), x_2 = f(x_2), \ldots$ until find two element such that $\gcd(x_i - x_j, n) \neq 1$).
- If for some prime divisor $p$ of $n$ we have $\rho(x_0, p) < \rho(x_0, n)$ this method returns a non-trival factor of $n$. Otherwise choose a new pair $(x_0, a) \in \mathbb{Z}_n^2$.

## Heuristic assumption:

- behaviour similar to a random mapping.
- It is not clear how "close" particular polynomials and rational functions are to random mappings.

# Estimation for $T$ and $B$ regarding $\{0, k\}$-mappings

## Results for permutations and unrestricted maps

- Erdös and Turan (1967): Lognormality result for $T : S_n \to \mathbb{R}$.
- Harris (1973): Lognormality result for $T : \Omega_n \to \mathbb{R}$.
- Schmutz (2011): Estimates for $\log E_n(T)$ and $\log E_n(B)$.

## The class of $\{0, k\}$-mappings

Pollard (1981) uses $\{0, k\}$-mappings as heuristic model for polynomials of the form $x^k + a$ with $k \equiv 1 \pmod{p}$ and obtain an speed up of his factorization algorithm. He was able to use this improvement to factor the eight Fermat number.

# Estimation for $T$ and $B$ regarding $\{0,k\}$-mappings

## Theorem [MPQS20]

- Estimates for $T, B : \Omega_n^{\{0,k\}} \to \mathbb{R}$:
  - $\log E_n^{\{0,k\}}(T) = k_0 \frac{(n/\lambda)^{\frac{1}{3}}}{\log^{\frac{2}{3}}(n/\lambda)}(1+o(1))$, with $\lambda = k-1$ and $k_0 \simeq 3.36$.
  - $\log E_n^{\{0,k\}}(B) = \frac{3}{2}(n/\lambda)^{\frac{1}{3}}(1+o(1))$.
  - Lognormality result for $T : \Omega_n^{\{0,k\}} \to \mathbb{R}$.

# Description of the functional graph

Finite dynamical systems (FDS): $(X, f)$, where $X$ is a finite abstract set and $f : X \to X$ is a function.

Functional graph: is a directed graph $G(f/X)$ with vertex set $X$ and the directed edge $a \to b$ is in $G(f/X)$ if and only if $f(a) = b$.

The functional graph describes the dynamics of $f$ over $X$. For instance, the orbit $\{a, f(a), f(f(a)), \ldots\}$ of an element $a \in X$ is described by a *path* in the functional graph $G(f/X)$.

Each connected component of $G(f/X)$ contains a directed cycle and every node in this cycle is the root of a directed tree (direction of edges is from leaves to the root).

# Description of the functional graph

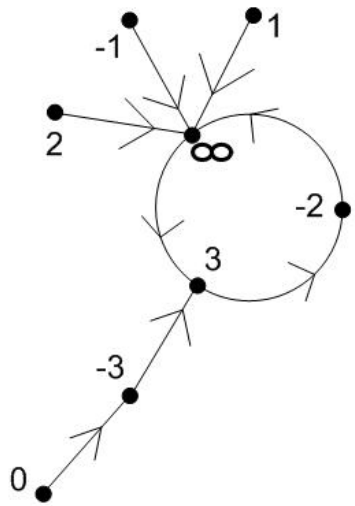



Figure: Example of a connected component of a functional graph

## Definition

We say that a connected component is *homogeneous* if the rooted trees attached to the cyclic nodes are isomorphic.

# Description of the functional graph

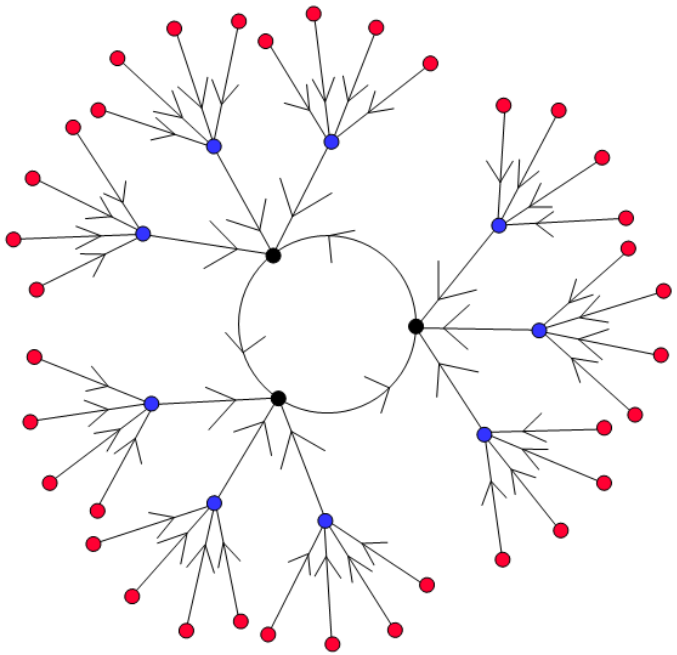


Figure: Example of an homogeneous connected component of a functional graph

# Description of the functional graph

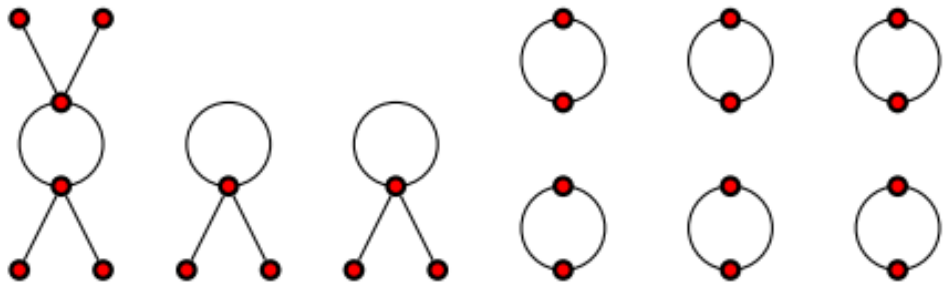
## Remark

When the connected components of a functional graph $G(f/X)$ are homogeneous we can express $G(f/X) = \bigoplus_{i \in I} n_i \times \mathrm{Cyc}(f_i, T_i)$.

# Description of the functional graph

## Remark

When the connected components of a functional graph $G(f/X)$ are homogeneous we can express $G(f/X) = \bigoplus_{i \in I} n_i \times \mathrm{Cyc}(f_i, T_i)$.



The graph $\mathrm{Cyc}(2, \mathcal{T}_{(3)}) \oplus (2 \times \mathrm{Cyc}(1, \mathcal{T}_{(3)})) \oplus (6 \times \mathrm{Cyc}(2))$

Figure: Example of functional graph whose connected components are homogeneus

# Description of the functional graph

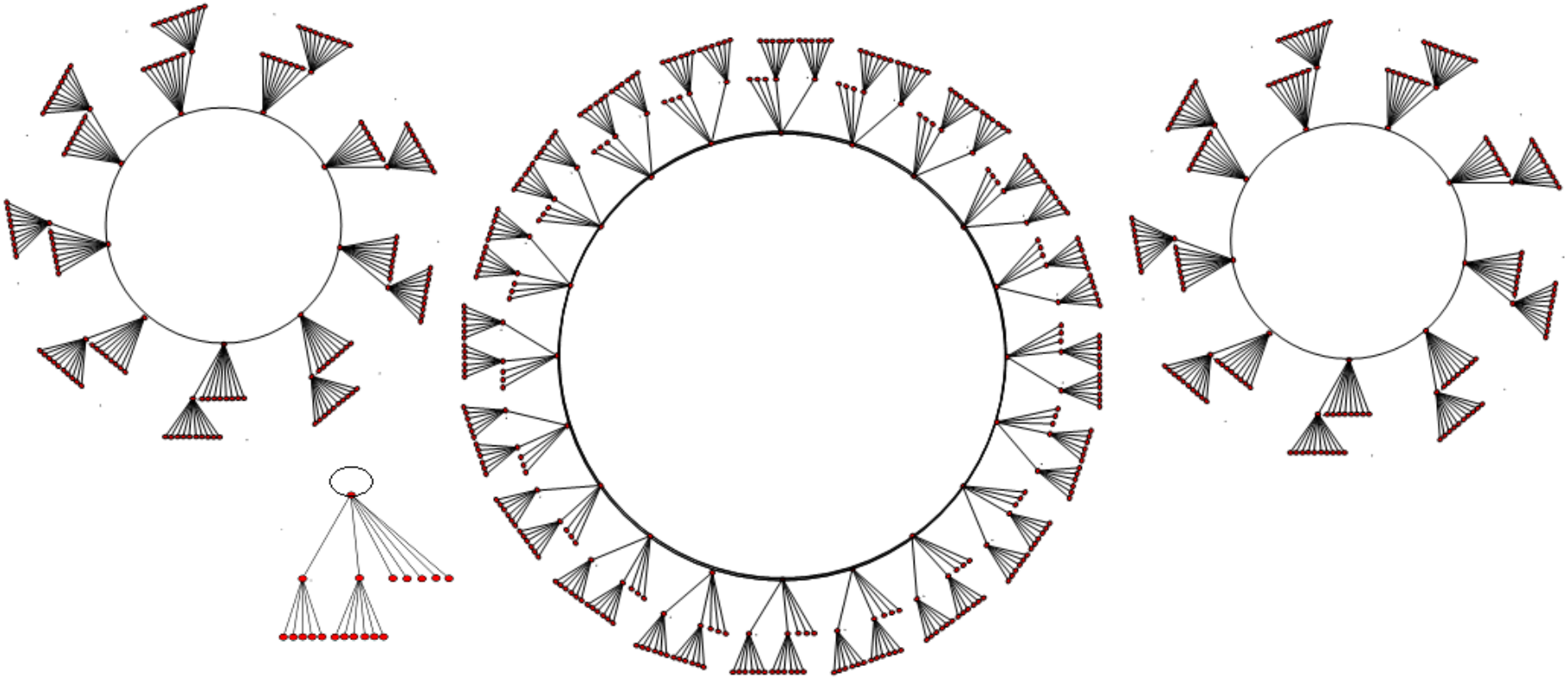


Figure: Another bigger example (Chebyshev polynomial!)

# Elementary rooted trees

Elementary rooted trees were introduced in [QP15] and [QR19].
We can associate with each decreasing sequence of positive integers $V = (\nu_1, \nu_2, \ldots, \nu_D)$ a rooted tree $T_V$, defined recursively as:

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

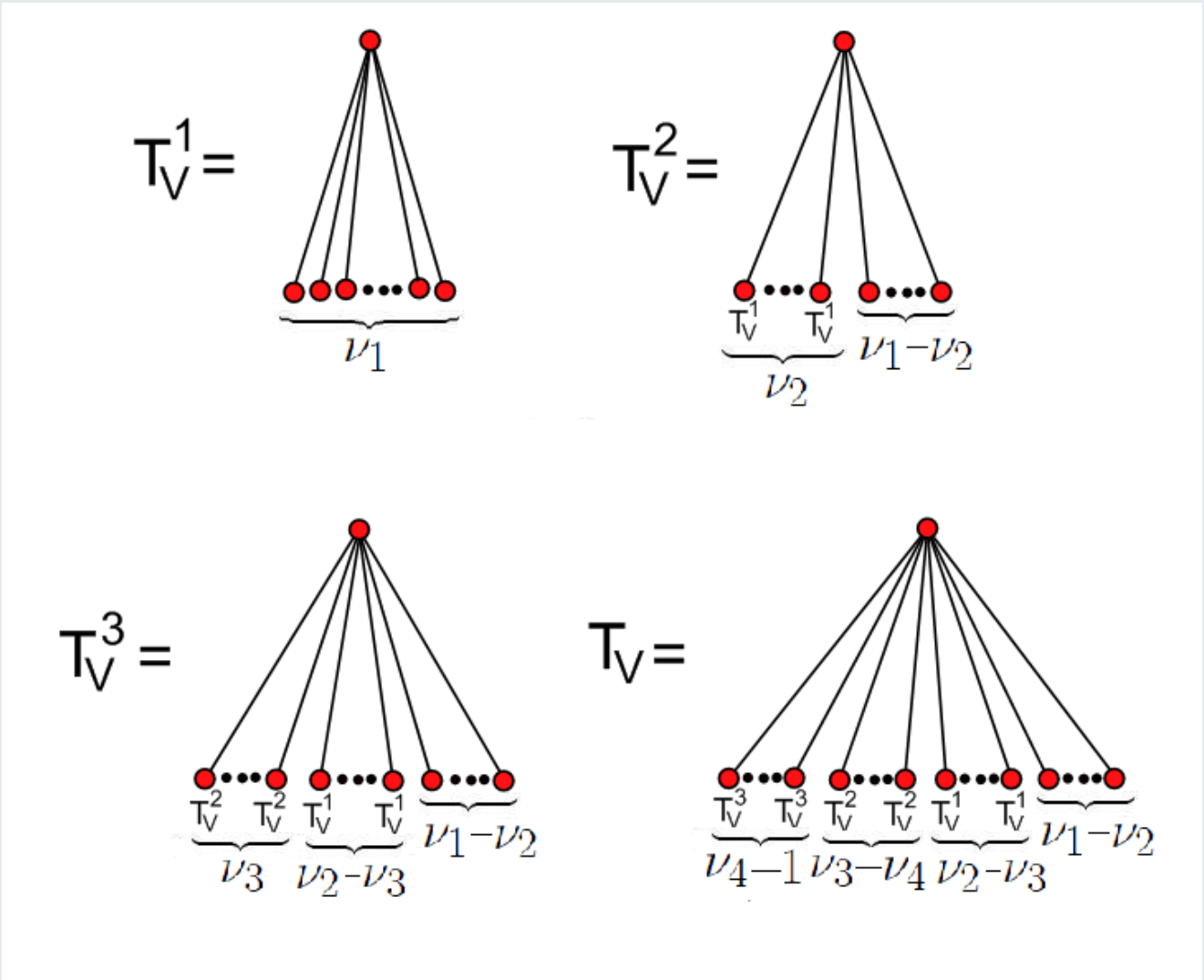
and

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

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

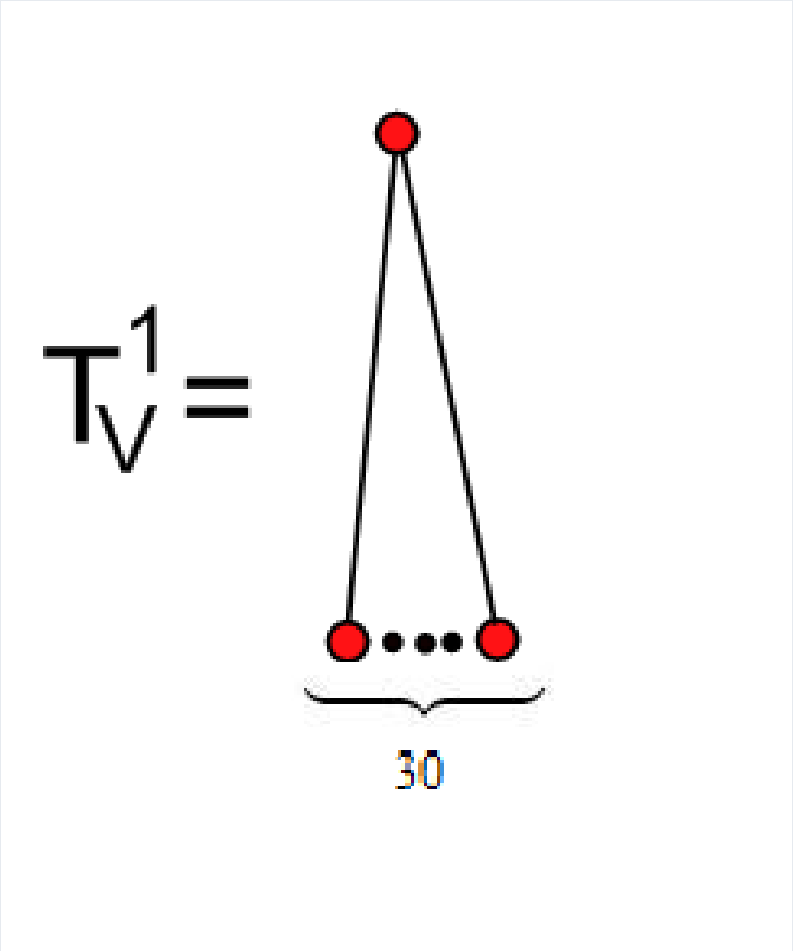
# Example

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



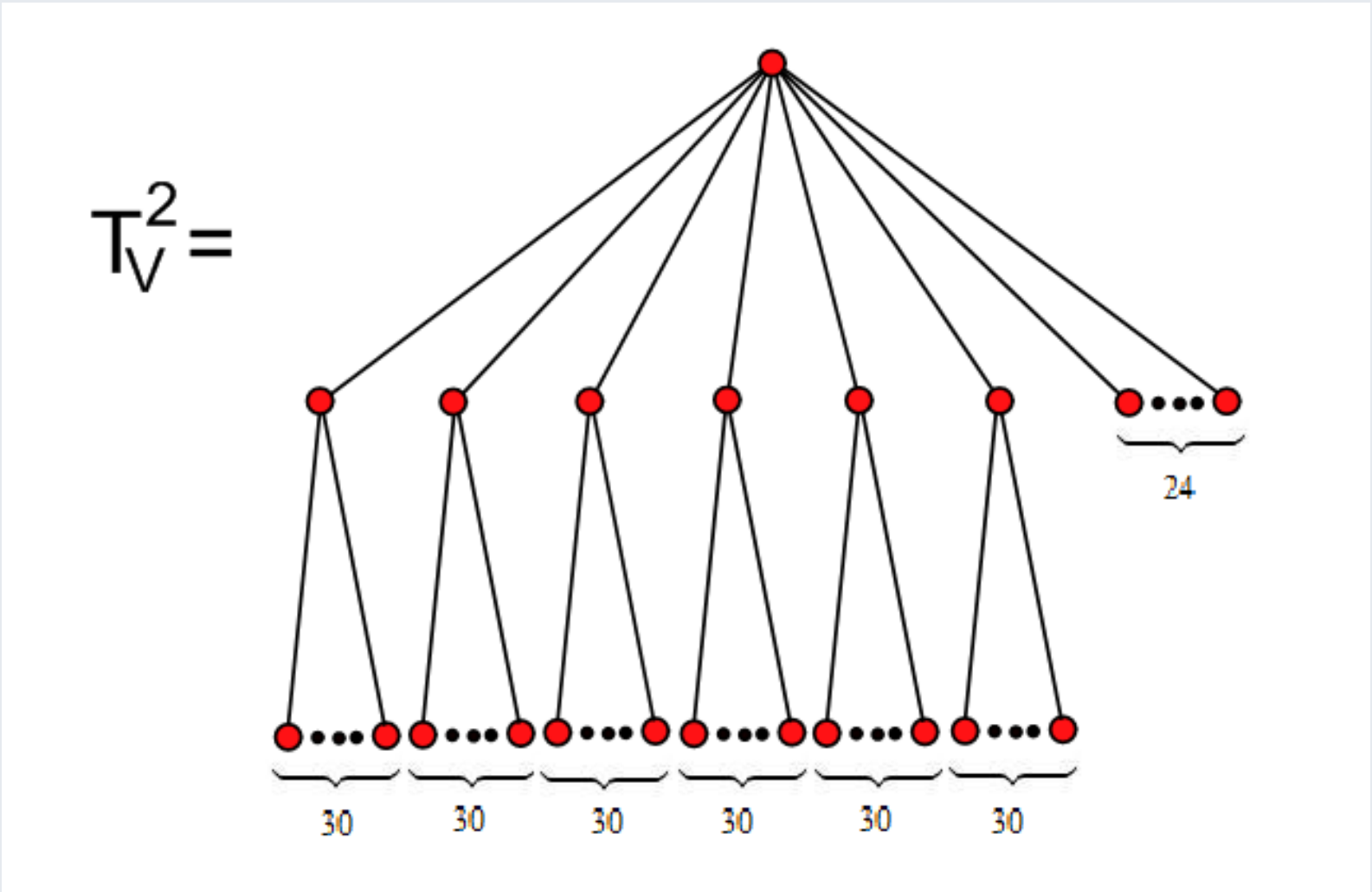
# An explicit example

Figure: Inductive definition of $T_V$ for $V = (30, 6, 2)$.



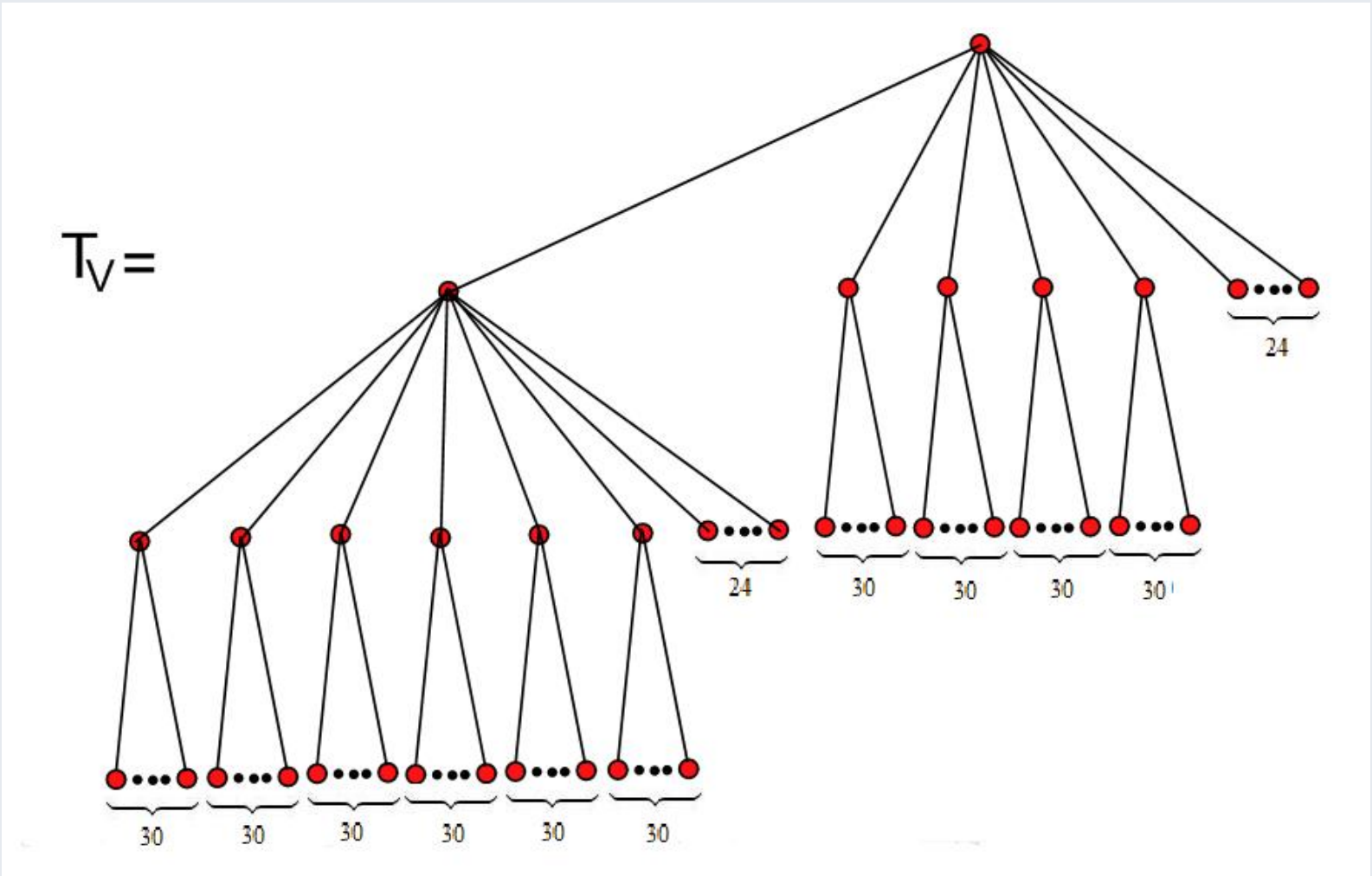
# An explicit example

Figure: Inductive definition of $T_V$ for $V = (30, 6, 2)$.



# An explicit example

Figure: Inductive definition of $T_V$ for $V = (30, 6, 2)$.



# Elementary trees

## Special case

$V$ multiplicative chain $\leftrightarrow$ $T_V$ is the tree of a power map on a cyclic group.

## The iterated gcd of $n$ relative to $t$

$\gcd_t(n) = (1)$ if $\gcd(t, n) = 1$, otherwise $\gcd_t(n) = (\nu_1, \ldots, \nu_D)$ where

$$\nu_1 = \gcd(t, n), \quad \nu_{i+1} = \gcd\left(t, \frac{n}{\nu_1 \cdots \nu_i}\right), \text{ for } i \geq 1,$$

and $D$ is the least positive integer such that $\nu_{D+1} = 1$.

## Some properties.

- $\nu_i$ is multiple of $\nu_{i+1}$ for $i = 1, 2, \ldots, D-1$;
- If $\nu := \prod_{i=1}^{D} \nu_i$ then $n = \nu\omega$ where $\omega$ is the greatest divisor of $n$ which is coprime with $t$ (we refer to it as the $t$-decomposition of $n$)

# Iterated greatest commom divisor in $\mathbb{Z}$

## Example

For $n = 360$ and $t = 30$ we have $\gcd_{30}(360) = (30, 6, 2)$. Indeed,

$$\begin{aligned} \nu_1 &= \gcd(30, 360) = 30; & \frac{360}{30} &= 12 \\ \nu_2 &= \gcd(30, 12) = 6; & \frac{12}{6} &= 2 \\ \nu_3 &= \gcd(30, 2) = 2; & \frac{2}{2} &= 1 \\ \nu_4 &= \gcd(30, 1) = 1; & \Rightarrow D &= 3. \end{aligned}$$

# Dynamic of power maps over cyclic groups

**Theorem [QP15]: Consider $\varphi_t : \mathcal{C}_n \to \mathcal{C}_n$ s.t. $\varphi_t(x) = x^t$.**

Let $n = \nu\omega$, where $\omega$ is the greatest divisor of $n$ that is relatively prime with $t$. Then $\mathcal{C}_n$ has exactly $\omega$ elements that are $\varphi_t$-periodic and the following isomorphism formula holds:

$$\mathcal{G}(\varphi_t/\mathcal{C}_n) = \bigoplus_{d|\omega} \left( \frac{\varphi(d)}{o_d(t)} \times \mathrm{Cyc}\left(o_d(t), T_{\mathrm{gcd}_t(\nu)}\right) \right).$$

Moreover, the tree $T_{\mathrm{gcd}_t(\nu)}$ has $\nu$ vertices and depth $D$.

# Dynamic of Chebyshev polynomials over finite fields

## Theorem [QP17]: Consider the chebyshev polinomial $T_n : \mathbb{F}_q \to \mathbb{F}_q$

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. There is a partition of $\mathbb{F}_q = R \cup Q \cup S$ in $T_n$-invariant sets (i.e $\mathcal{G}(T_n/\mathbb{F}_q) = \mathcal{G}(T_n/R) \oplus \mathcal{G}(T_n/Q) \oplus \mathcal{G}(T_n/S)$) such that:

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

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

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

# Dynamic of power maps over quotients of RFDD

In [QR19] we extended the result of [QR15] to the map $\Gamma_{a,\mathfrak{n}}$ given by

$$\begin{array}{rccc} \Gamma_{a,\mathfrak{n}}: & \mathfrak{D}/\mathfrak{n} & \longrightarrow & \mathfrak{D}/\mathfrak{n} \\ & x & \longmapsto & \Psi_{\mathfrak{n}}(a)\cdot x. \end{array}$$

where $\Psi_{\mathfrak{n}}(a)$ is the projection to the quotient and $\mathfrak{D}, a$ and $\mathfrak{n}$ are as below.

## Theorem [QR19]

Let $\mathfrak{D}$ be a residually finite Dedekind Domain and $\mathfrak{n}$ a nonzero ideal of $\mathfrak{D}$. For $a \in \mathfrak{D}$, write $\mathfrak{n} = \mathfrak{m}_0 \cdot \mathfrak{n}_0$, where $\mathfrak{m}_0 + \langle a \rangle = \mathfrak{D}$ and $\langle a \rangle \subseteq \mathrm{rad}(\mathfrak{n}_0)$ Then the following holds:

$$\mathcal{G}(\Gamma_{a,\mathfrak{n}}) = \bigoplus_{\mathfrak{m}|\mathfrak{m}_0} \frac{\varphi_{\mathfrak{D}}(\mathfrak{m})}{o_{\mathfrak{m}}(a)} \times \mathrm{Cyc}(o_{\mathfrak{m}}(a), T_{\gcd_a(n_0)}).$$

# Special cases

- Dynamic of the $a$-map over cyclic groups;
- Dynamic of Redei functions over finite fields;
- Dynamic of Chebyshev polynomials over finite fields;
- Dynamic of maps induced by endomorphisms of ordinary elliptic curves over finite fields;
- Dynamic of linearized polynomials over finite fields.

# Power maps over abelian groups

## Theorem [QR22]

Let $G$ be an abelian group and write $G = \mathcal{C}_{r_1} \times \cdots \times \mathcal{C}_{r_k}$, where $\mathcal{C}_r$ denotes a cyclic group of order $r$. Let $r_i = \nu_i \omega_i$ where $\omega_i$ is the greatest divisor of $r_i$ that is relatively prime with $t$, $\boldsymbol{\nu} := (\nu_1, \ldots, \nu_k)$, $\boldsymbol{\omega} := (\omega_1, \ldots, \omega_k)$ and $\gcd_t(\nu) := \prod_{i=1}^k \gcd_t(\nu_i)$. For $\boldsymbol{d} = (d_1, \ldots, d_k)$ define $\varphi(\boldsymbol{d}) := \prod_{i=1}^k \varphi(d_i)$ and $o_{\boldsymbol{d}}(t) = \operatorname{lcm}\{o_{d_i}(t) : 1 \leq i \leq k\}$. Then G has exactly $\prod_{i=1}^k \omega_i$ elements that are $\varphi_t$-periodic and the following isomorphism formula holds:

$$\mathcal{G}(\varphi_t/G) = \bigoplus_{\boldsymbol{d}|\boldsymbol{\omega}} \frac{\varphi(\boldsymbol{d})}{o_{\boldsymbol{d}}(t)} \times \operatorname{Cyc}\left(o_{\boldsymbol{d}}(t), T_{\gcd_t(\boldsymbol{\nu})}\right)$$

# Power maps over flower groups

## Theorem [QR22]

Let $t$ be a positive integer and $G$ be a flower group of type $(c_0; c_1, \ldots, c_k)$. Let $c_i = \nu_i \cdot \omega_i$ be the $t$-decomposition of $c_i$, $1 \leq i \leq k$. Then there exists a rooted tree $\mathcal{T}_t(G)$ such that the functional graph $\mathcal{G}(\varphi_t/G)$ of the map $\varphi_t : G \to G$ with $g \mapsto g^t$ is isomorphic to

$$\left( \bigoplus_{i=1}^{k} \bigoplus_{\substack{d_i \mid \omega_i \\ d_i \nmid \omega_0}} \frac{\varphi(d_i)}{o_{d_i}(t)} \times \mathrm{Cyc}\left(o_{d_i}(t), \mathcal{T}_{\gcd_t(\nu_i)}\right) \right) \oplus \left( \bigoplus_{d_0 \mid \omega_0} \frac{\varphi(d_0)}{o_{d_0}(t)} \times \mathrm{Cyc}\left(o_{d_0}(t), \mathcal{T}_t(G)\right) \right),$$

where $\mathcal{T}_t(G) = \mathcal{T}_t(c_0; c_1, \ldots, c_k)$ equals the tree attached to $1 \in G$ in $\mathcal{G}(\varphi_t/G)$ (the central tree).

# Power maps over Flower groups

## Theorem [QR22]

Let $c_0, c_1, \ldots, c_k$ be positive integers with $k \geq 2$ and $c_0 \mid c_i$ for $1 \leq i \leq k$. Then, the following holds:

i) $\mathcal{T}_t(c_0; c_1, \ldots, c_k) = \mathcal{T}_t(c_0; c_{\theta(1)}, \ldots, c_{\theta(k)})$, for every $\theta \in S_k$.

ii) If $\gcd(c_0, t) = 1$, then $\mathcal{T}_t(c_0; c_1, \ldots, c_k) = \sum_{i=1}^{k} \mathcal{T}_{\gcd_t(\nu_i)}$.

iii) If $\gcd(t, \frac{c_k}{c_0}) = 1$ then $\mathcal{T}_t(c_0; c_1, \ldots, c_{k-1}, c_k) = \mathcal{T}_t(c_0; c_1, \ldots, c_{k-1})$.

iv) If $c_k \mid t$ then
$\mathcal{T}_t(c_0; c_1, \ldots, c_{k-1}, c_k) = \mathcal{T}_t(c_0; c_1, \ldots, c_{k-1}) + \langle (c_k - c_0) \times \bullet \rangle$.

v) $\mathcal{T}_t(c_0; c_1) = \mathcal{T}_{\gcd_t(c_1)}$.

# Special cases

- The projective general linear group $\mathrm{PGL}(2, q)$.
- Generalized quaternions
- Semidirect products of cyclic groups

# Open problems

## Some open problems

- Extend the description of the functional graph associated to the power map to more general class of non-abelian groups.
- Does the dynamics of the power maps over a group $G$ determine the isomorphism class of $G$?
- How many (non-isomorphic) trees can appear in a functional graph $\mathcal{G}(\varphi_t/G)$ and how this number grows with $|G|$?
- Extend some of the result obtained for $\{0, k\}$-mappings to $J$-mappings.

## Returning to the origins

- Could we use our knowledge about the dynamics of certain class of mapping to design interesting new algorithms with application in cryptography? (for example factorization algorithms).

# Contents

# Discrete memoryless channels

## Definition

A (discrete memoryless) channel $W$ with input and output alphabet $\mathcal{X} = \{x_1, \ldots, x_N\}$ is determined by its transition matrix $[W] = (\Pr(x_i|x_j))_{1 \leq i,j \leq N}$ where $\Pr(x_i|x_j)$ is the probability of receiving $x_i$ given that $x_j$ was sent.

## Example

Let $W : \mathcal{X} \to \mathcal{X}$ be the ternary channel with $\mathcal{X} = \{0, 1, 2\}$ and transition matrix

$$[W] = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/4 & 5/12 & 1/3 \\ 1/4 & 1/6 & 7/12 \end{pmatrix}$$

We have $\Pr(0|0) = 1/2$, $\Pr(1|0) = \Pr(2|0) = 1/4$, $\Pr(0|1) = 1/4$, $\Pr(1|1) = 5/12$, $\Pr(2|1) = 1/3$, $\Pr(0|2) = 1/4$, $\Pr(1|2) = 1/6$ and $\Pr(2|2) = 7/12$.

# The $n$-fold channel

## Definition

The $n$-fold channel associated with $W$ is the channel $W^n : \mathcal{X}^n \to \mathcal{X}^n$ given by the following probability distribution: the probability of receiving $x = (x_1, \ldots, x_n) \in \mathcal{X}^n$ if $y = (y_1, \ldots, y_n) \in \mathcal{X}^n$ was sent is given by:

$$\text{Prob}_{W^n}(x|y) = \prod_{i=1}^{n} \text{Prob}_W(x_i|y_i)$$

## Example

Let $W : \mathcal{X} \to \mathcal{X}$ be the ternary channel of the previous example. The probability distribution of $W^2 : \mathcal{X}^2 \to \mathcal{X}^2$ is
$\text{Prob}_{W^2}(x_1x_2|y_1y_2) = \text{Prob}(x_1|y_1) \cdot \text{Prob}(x_2|y_2)$.
For instance, $\text{Prob}_{W^2}(12|20) = \frac{1}{6} \cdot \frac{1}{4} = \frac{1}{24}$.

# Metrizable channels

## Definition

A metric $d : \mathcal{X} \times \mathcal{X} \to [0, \infty)$ is compatible with the channel $W$ iff for every code $C \subseteq \mathcal{X}$ and every $x \in \mathcal{X}$, we have
$\arg\max_{y \in C} \Pr(x \text{ received} | y \text{ sent}) = \arg\min_{y \in C} d(x, y)$.

## Proposition

A metric $d$ is compatible with $W$ iff
$\Pr(x|y) \geq \Pr(x|z) \Leftrightarrow d(x, y) \leq d(x, z)$ for all $x, y, z \in \mathcal{X}$.

## Definition

A (discrete memoryless) channel $W : \mathcal{X} \to \mathcal{X}$ is metrizable if for every positive integer $n$, there is a metric $d_n$ such that $d_n$ is compatible with $W^n$.

# Binary channels

## Definition

Binary channels are given by two parameters $(p, q)$ with $0 \leq p, q < 1$ and $p + q < 1/2$. The probability distribution is given by $\text{Prob}(0|0) = 1 - p$, $\text{Prob}(1|0) = p$, $\text{Prob}(0|1) = q$ and $\text{Prob}(1|1) = 1 - q$. We denote $W = BAC(p, q)$.

## Equivalence of channels

Two channels $W, W' : \mathcal{X} \to \mathcal{X}$ are equivalent if decoding by maximum likelihood gives the same result.

# Some results

## Theorem [QCRF18]

There are a finite number of equivalence classes of $n$-fold BAC channels and we also give an explicit description of these classes.

## Corollary

For fixed $n \geq 1$, in order to determine if an $n$-fold binary channel is metrizable we have to check only finite possibilities.

# Some results

## Theorem [Q18]

The memoryless binary channel is metrizable.

## Remark

The case $n \leq 3$ and $p = 0$ was proved by Firer and Walker in a previous paper "Matched metrics and channels" (2015)

## Open problems

- What ternary memoryless channels are metrizable?
- Describe the equivalence classes of $n$-fold ternary memoryless channels.
- Possible relation with cryptography?

# Perfect codes and correspondence between lattices and codes

## Perfect codes

Consider a metric space $(\mathbb{Z}_q^n, d)$ where $d$ is an invariant by translation.

- An $n$-dimensional $q$-ary code is a subset $C \subseteq \mathbb{Z}_q^n$.
- Important parameters: minimum distance, packing radius and covering radius.
- $C$ is perfect when the packing radius equals the covering radius.

## Correspondence between (linear) codes and lattice

- $\{\Lambda : q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n\} \longleftrightarrow \{C \leq Z_q^n\}$
- Metric $\ell^1 \longleftrightarrow$ Lee metric;
- Metric $\ell^\infty \longleftrightarrow$ Chebyshev or maximum metric;
- Fact: The correspondence preserve perfect codes if $q \geq 2e + 1$.

# Perfect codes in the Lee metric

SIAM J. APPL. MATH.
Vol. 18, No. 2, January 1970

**PERFECT CODES IN THE LEE METRIC AND THE PACKING OF POLYOMINOES***

SOLOMON W. GOLOMB AND LLOYD R. WELCH†

**1. The geometry of Shannon's five-phase code.** In [4] Shannon considered the problem of coding to completely eliminate errors in a channel using a 5-symbol alphabet, with the error pattern as shown in Fig. 1. The alphabet may be regarded as the integers modulo 5. When the integer $r$ is sent, either $r$ or $r+1$ is received, with respective probabilities $p$ and $q$. If one forms a "code" consisting of sending each symbol $m$ times to represent the fact that it occurred once in the message, then there is still a probability of $q^m$ that an error will occur. However, there exists a code using only two code symbols per message symbol which eliminates errors entirely (see Fig. 2). In this code, if $(a, b)$ is a codeword, then it may be received as either $(a, b)$ or $(a+1, b)$ or $(a, b+1)$ or $(a+1, b+1)$. However, we can associate all four of these received messages *uniquely* with $(a, b)$ when we use the code of Fig. 2. This is most readily seen via the geometric presentation in Fig. 3. The 25 possible codewords $(a, b)$ are represented by the 25 cells, with coordinates $(a, b)$. The codewords of Fig. 2 correspond to the cells with dots in them. Each dot is

## Perfect Lee codes exist for the following parameters:

- For every $e \geq 1$ there is an $e$-perfect Lee code $C \subseteq \mathbb{Z}^1$.
- For every $e \geq 1$ there is an $e$-perfect Lee code $C \subseteq \mathbb{Z}^2$.
- For every $n \geq 1$ there is a 1-perfect Lee code $C \subseteq \mathbb{Z}^n$.

Conjecture: For $n \geq 3$ and $e \geq 2$, there are no $e$-perfect Lee codes in $\mathbb{Z}^n$.

# Perfect codes in the Lee metric

**Survey of papers on the Golomb-Welch conjecture:**

P. Horak, D. Kim, 50 years of the Golomb-Welch conjecture, IEEE Trans. Inf. Theory 64(4), 3048-3061, 2018.

# Perfect codes in the Lee metric

## Some results towards the Golomb-Welch conjecture (Fixed dimension):

- (Golomb-Welch 1970): For $n \geq 3$ fixed. There is an integer $e_n \geq 2$ ($e_n$ unspecified) such that there are no $e$-perfect Lee codes in $\mathbb{Z}^n$ for $e \geq e_n$.
- (Golomb-Welch 1970) $e_n = 2$ holds for $n = 3$.
- (Post 1975 and Horak-Kim 2018): $e_n = \frac{\sqrt{2}}{2}n - \frac{3\sqrt{2}-2}{4}$ holds for $n \geq 6$ and $e_n = n - 1$ holds for $3 \leq n \leq 5$.
- (Lepistö 1981 and Horak-Kim 2018): $e_n = \max\{\sqrt{2.1n} - 2,285\}$.
- (Spacapan 2007) $e_n = 2$ holds for $n = 4$.
- (Horak 2009) $e_n = 2$ holds for $n = 5$.

# Perfect codes in the Lee metric

## Some results towards the Golomb-Welch conjecture (Fixed radius):

- (Horak-Grossek 2010) There are no **linear** 2-perfect Lee codes in $\mathbb{Z}^n$ for $n \leq 12$.
- (Kim 2017) There are no 2-perfect Lee codes in $\mathbb{Z}^n$ if $\#B^n(2) = 2n^2 + 2n + 1$ is a prime number satisfying certain conditions.
- (Campello-Costa-Q. 2018) There are no **linear** 2-perfect Lee codes in $\mathbb{Z}^n$ for infinitely many values of $n$.
- (Zhang-Ge 2017) For $e = 3$ and $e = 4$ there are no **linear** $e$-perfect Lee codes in $\mathbb{Z}^n$ for infinitely many values of $n$.
- (Q.2020) If $e$ contains a digit 1 in its base-3 representation not in the unit place, there are no **linear** $e$-perfect Lee codes in $\mathbb{Z}^n$ for infinitely many values of $n$
- (Leung-Zhou 2020) There are no **linear** 2-perfect Lee codes in $\mathbb{Z}^n$ for $n \geq 3$.

# Codes in the $\ell^p$ metric

## The $\ell_p$ metrics in $\mathbb{Z}_q^n$ (S. Golomb, 1969)

$$d_p(x,y) = \begin{cases} \left(\sum_{i=1}^n d_L(x_i,y_i)^p\right)^{\frac{1}{p}} & \text{for } 1 \leq p < \infty \\ \max\{d_L(x_i,y_i) : 1 \leq i \leq n\} & \text{for } p = \infty \end{cases}$$

- $p = 1 \Rightarrow$ Lee metric,
- $p = 2 \Rightarrow$ Euclidean metric,
- $p = \infty \Rightarrow$ Chebyshev metric.

## Conjecture about perfect codes in the $\ell_p$ metric

If $C \subseteq \mathbb{Z}_q^n$ is perfect in the $\ell_p$ metric, $1 < p < \infty$ then $C$ is perfect either in the Lee metric ($p = 1$) or in the Chebyshev metric ($p = \infty$).

A. Campello, G. C. Jorge, J. E. Strapasson, S. I. Costa, *Perfect codes in the $\ell_p$ metric*, European Journal of Combinatorics, 53, 72-85, 2016.

# Perfect codes in the Chebyshev metric - applications and connections

## Rank modulation codes

- T. Klove, T. Lin, D. Tsai, W. Tzeng, Permutation arrays under the Chebyshev distance, IEEE Transaction on Information Theory 56(6): 2611-2617, 2010.
- M. Shieh, S. Tsai, Decoding frequency permutation arrays under Chebyshev distance, IEEE Transaction on Information Theory 56(11): 5730-5737, 2010.
- I. Tamo, M. Schwartz, Correcting limited-magnitude errors in the rank-modulation scheme, IEEE Transaction on Information Theory 56: 2551-2560, 2010.

## Connection with cube tilings of $\mathbb{R}^n$

- A. P. Kisielewicz, K. Przeslawski, *The coin exchange problem and the structure of cube tilings*, Electron. J. Combin. 19: #R26, 2012.
- A. Kisielewicz, K. Przeslawski, *The structure of cube tilings under symmetry conditions*, Discrete Comput. Geom. 48: 777-782, 2012.
- A. P. Kisielewicz, *On the structure of cube tilings of R3 and R4*, Journal of Combinatorial Theory, series A 120: 1-10, 2013.

# Perfect codes in the Chebyshev metric

## Connection with other areas

- Combinatorics and graph theory.

  K. Corrádi, S. Szabó, *A combinatorial approach for Keller's conjecture*, Period. Math. Hungar. 21, pp.95-100, 1990.

- Coding theory.

  J. C. Lagarias, P. W. Shor, *Cube tilings and nonlinear codes*, Discrete Comput. Geom. 11: 359-391, 1994.

- Algebra.

  S. Szabó, *Topics in factorization of abelian groups*, Hindustan Book Ag., New Delhi, 2004.

- Harmonic analysis.

  M. N. Kolountzakis, *Lattice tilings by cubes: whole, notched and extended*, Electron. J. Combin. 5: #R14, 1998.

- Music theory.

  M. Andreatta, *On group-theoretical methods applied to music: some compositional and implementational aspects*, Persp. of Mathematical and Computer-Aided Music Theory, University of Osnabrück (in press).

# Perfect codes in the Chebyshev metric

**Theorem (S. Costa - Q.)**

Let $q = (2e+1)t$. The isomorphism classes of $e$-perfect $q$-ary codes in the Chebyshev metric form a lattice of the poset of isomorphism classes of abelian groups of order $t^n$.

# Perfect codes in the Lee and Chebyshev metric

## Question

Being perfect or quasi perfect is a desirable characteristic of a code in order to be used in cryptographic applications (for example in McEliece cryptosystem). Does the security depends on the metric to be used?

[Gassert14] T. A. Gassert.
Chebyshev action on finite fields.
*Discr. Math.* 315: 83–94 (2014).

[MPQS20] R. Martins, D. Panario and C. Qureshi, E. Schmutz
Periods of iterations of functions with restricted preimage sizes
*AMC Trans. on Algorithms.* 16(3), 1–28 (2020).

[MPQ19] R. Martins, D. Panario and C. Qureshi
A Survey on Iterations of Mappings over Finite Fields.
In: *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications.* Edited by Kai-Uwe Schmidt and Arne Winterhof. Radon Series on Computational and Applied Mathematics, De Gruyter, Berlin. 2019

[PR18] D. Panario and L. Reis.
The functional graph of linear maps over finite fields and applications.
*Des. Codes Cryptogr.* 87(2), 437–453 (2019).

[PMMY01] A. Peinado, F. Montoya, J. Munoz and A. J. Yuste
Maximal periods of $x^2 + c$ in $\mathbb{F}_q$.
*In: International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer* pp. 219–228 (2001).

[Q18] C. Qureshi
Matched metrics to the binary asymmetric channels
*IEEE Trans. on Information Theory*, 65(2), 1106–1112 (2018).

[QCRF18] C. Qureshi, S. Costa, C. Rodrigues and M. Firer.
On equivalence of binary asymmetric channels regarding the maximum likelihood decoding.
*IEEE Trans. on Information Theory*, 64(5), 3528–3537 (2018).

[QP15] C. Qureshi and D. Panario.
Rédei actions on finite fields and multiplication map in cyclic groups.
*SIAM J. on Discr. Math.* 29: 1486–1503 (2015).

[QP18] C. Qureshi and D. Panario.
The graph structure of Chebyshev polynomials over finite fields and applications.
*Des. Codes Cryptogr.* 87(2), 393–416 (2019).

[QPM17] C. Qureshi, D. Panario and R. Martins.
Cycle structure of iterating Rédei functions.
*Adv. Math. Comm.* 11(2): 397–407 (2017).

[QR19] C. Qureshi, L. Reis.

Dynamics of the a-map over residually finite Dedekind Domains and applications
*Journal of Number Theory, 204, 134-154 (2019).*


[QR21] C. Qureshi, L. Reis.
On the functional graph of the power map over finite groups
*https://arxiv.org/abs/2107.00584* (2020)


[Rogers96] T. Rogers.
The graph of the square mapping on the prime fields.
*Discr. Math.* 144: 317–324 (1996).


[Toledo05] R. A. H. Toledo,
Linear Finite Dynamical Systems.
*Commun. Algebra.* 33 (9): 2977-2989 (2005).


[Ugolini13] S. Ugolini
Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three and five.
*J. Num. Theory* 133: 1207–1228 (2013).


[Ugolini14] S. Ugolini
On the iterations of certain maps $x \mapsto k \cdot (x + x^{-1})$ over finite fields of odd characteristic.

*J. Num. Theory* 142: 274–297 (2014).

[Ugolini18] S. Ugolini.
Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields.
*Periodica Math. Hungarica* 77.2: 237–260 (2018).

[VS04] T. Vasiga and J. Shallit.
On the iteration of certain quadratic maps over $GF(p)$.
*Discr. Math.* 277: 219–240 (2004).

Thank you for your attention!