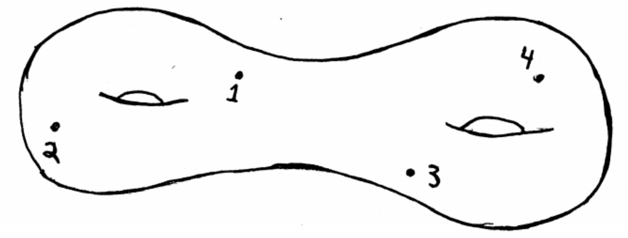
Polynomial Statistics, Necklace Polynomials, and the Arithmetic Dynamical Mordell-Lang Conjecture

Trevor Hyde
University of Michigan

Part I

Factorization Statistics and Point Configurations in $\mathbb{R}^3$



Factorization Statistics

▷ $\mathrm{Poly}_d(\mathbb{F}_q) =$ the set of monic degree d polynomials in $\mathbb{F}_q[x]$.

▷ The **factorization type** of $f(x) \in \mathrm{Poly}_d(\mathbb{F}_q)$ is the partition of d given by the degrees of the irreducible factors of $f(x)$.

Ex.

$$x^2(x+1)(x^2+1)^3 \in \mathrm{Poly}_9(\mathbb{F}_3)$$

has factorization type $\lambda = (1^3\, 2^3)$.

▷ A **factorization statistic** is a function $P : \mathrm{Poly}_d(\mathbb{F}_q) \to \mathbb{Q}$ such that $P(f)$ depends only on the factorization type of $f(x)$.

Ex. $R =$ total number of $\mathbb{F}_q$-roots with multiplicity.

Ex. $F =$ total number of irreducible factors.

Expected Values

If P is a factorization statistic, let $E_d(P)$ denote the expected value of P on $\mathrm{Poly}_d(\mathbb{F}_q)$

$$E_d(P) = \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} P(f).$$

Ex. (Quadratic excess)
$Q(f) = $ # red. quad. factors $-$ # irred. quad. factors

d	$E_d(Q)$
3	$\frac{2}{q} + \frac{1}{q^2}$
4	$\frac{2}{q} + \frac{2}{q^2} + \frac{2}{q^3}$
5	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{2}{q^4}$
6	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{3}{q^5}$
10	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{6}{q^5} + \frac{6}{q^6} + \frac{8}{q^7} + \frac{8}{q^8} + \frac{5}{q^9}$

Expected Values

$Q(f) =$ # red. quad. factors $-$ # irred. quad. factors

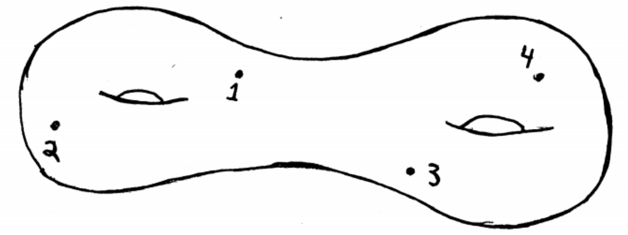
d	$E_d(Q)$	$E_d(Q)_{q=1}$
3	$\frac{2}{q} + \frac{1}{q^2}$	3
4	$\frac{2}{q} + \frac{2}{q^2} + \frac{2}{q^3}$	6
5	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{2}{q^4}$	10
6	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{3}{q^5}$	15
10	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{6}{q^5} + \frac{6}{q^6} + \frac{8}{q^7} + \frac{8}{q^8} + \frac{5}{q^9}$	45

- Degree $d - 1$
- Positive integer coefficients
- Coefficients sum to $\binom{d}{2}$
- Coefficientwise convergence as $d \to \infty$

Configuration Space

Let X be a topological space.

- $\mathrm{PConf}_d(X) = \{(x_1, x_2, \ldots, x_d) \in X^d : x_i \neq x_j\}$.
- Symmetric group S_d acts on $\mathrm{PConf}_d(X)$ by permuting coordinates.
- $H^k(\mathrm{PConf}_d(X), \mathbb{Q})$ is an S_d-representation for each k.



Expected Values

- Let ψ_d^k be the S_d-character of $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$.
- Let $\langle P_1, P_2 \rangle = \frac{1}{d!} \sum_{\sigma \in S_d} P_1(\sigma) P_2(\sigma)$.

Theorem (H. 2017)

Let P be a factorization statistic, then

$$E_d(P) := \frac{1}{q^d} \sum_{f \in \mathrm{Poly}_d(\mathbb{F}_q)} P(f) = \sum_{k=0}^{d-1} \frac{\langle P, \psi_d^k \rangle}{q^k}.$$

$E_d(Q)$ has $\mathbb{N}$ coefficients

- $Q(f) = \#$ red. quad. factors $-$ $\#$ irred. quad. factors
- If $\sigma \in S_d$, then $Q(\sigma) =$ trace of σ acting on $\bigwedge^2 \mathbb{Q}[d]$.
- Q is an S_d-character $\Longrightarrow \langle Q, \psi_d^k \rangle \in \mathbb{N}$.

$$E_d(Q) = \sum_{k=0}^{d-1} \frac{\langle Q, \psi_d^k \rangle}{q^k}.$$

d	$E_d(Q)$
3	$\frac{2}{q} + \frac{1}{q^2}$
4	$\frac{2}{q} + \frac{2}{q^2} + \frac{2}{q^3}$
5	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{2}{q^4}$
6	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{3}{q^5}$

Coefficientwise Convergence

Let x_j for $j \geq 1$ be the class function

$$\begin{aligned} x_j(\sigma) &= \#\, j\text{-cycles of } \sigma, \\ x_j(f) &= \#\text{ deg. } j \text{ irreducible factors of } f. \end{aligned}$$

$P \in \mathbb{Q}[x_1, x_2, \ldots]$ are called **character polynomials**.

Theorem (H. 2017)

If P is a character polynomial, then

$$\lim_{d \to \infty} E_d(P) = \sum_{k=0}^{\infty} \frac{\langle P, \psi^k \rangle}{q^k},$$

where $\langle P, \psi^k \rangle := \lim_{d \to \infty} \langle P, \psi_d^k \rangle$.

▷ Equiv. to **rep. stability** of $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q})$ for each $k \geq 0$.

Quadratic Excess is a Character Polynomial

$$Q = \binom{x_1}{2} - \binom{x_2}{1} \implies Q \text{ is a char. poly.}$$

Therefore $E_d(Q)$ converge coefficientwise as $d \to \infty$

d	$E_d(Q)$
3	$\frac{2}{q} + \frac{1}{q^2}$
4	$\frac{2}{q} + \frac{2}{q^2} + \frac{2}{q^3}$
5	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{2}{q^4}$
6	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{3}{q^5}$
10	$\frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{6}{q^5} + \frac{6}{q^6} + \frac{8}{q^7} + \frac{8}{q^8} + \frac{5}{q^9}$

$$\lim_{d \to \infty} E_d(Q) = \frac{2}{q} + \frac{2}{q^2} + \frac{4}{q^3} + \frac{4}{q^4} + \frac{6}{q^5} + \frac{6}{q^6} + \frac{8}{q^7} + \frac{8}{q^8} + \dots$$

Splitting Measures

Let $\lambda = (1^{m_1}2^{m_2}\cdots)$ be a partition of d.

▷ The **splitting measure** $\nu(\lambda) =$ prob. of $f \in \mathrm{Poly}_d(\mathbb{F}_q)$ having factorization type λ.

▷ Let $M_d(q) := \frac{1}{d}\sum_{e|d}\mu(e)q^{d/e}$ be the d**th necklace polynomial**.

Theorem (H. 2017)

$$\nu(\lambda) = \frac{1}{z_\lambda}\sum_{k=0}^{d-1}\frac{\psi_d^k(\lambda)}{q^k} = \frac{1}{q^d}\prod_{j\geq 1}\left(\!\!\binom{M_j(q)}{m_j}\!\!\right),$$

where ψ_d^k *is the* S_d*-character of* $H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3),\mathbb{Q})$.

▷ Equivalent to result on expected values of factorization stats.

$\mathbb{C} \approx \mathbb{F}_1$ Heuristic

Idea: Compactly supported Euler characteristic $\chi_c(X)$ of a space generalizes cardinality $|X|$ of a finite set.

▷ $\chi_c(\mathbb{C}) = 1 \Longrightarrow \mathbb{C} \approx \mathbb{F}_1$.

$$\nu(\lambda)_{q=1} = \frac{1}{z_\lambda} \sum_{k=0}^{d-1} \psi_d^k(\lambda) = \begin{cases} 1 & \lambda = (1^d) \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

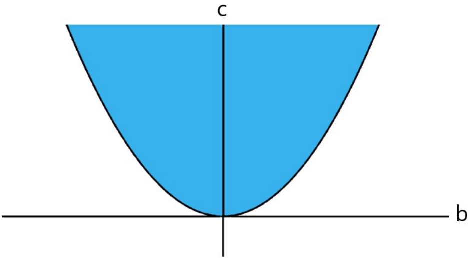
$$\bigoplus_{k=0}^{d-1} H^{2k}(\mathrm{PConf}_d(\mathbb{R}^3), \mathbb{Q}) \cong \mathbb{Q}[S_d].$$

▷ *If P is a factorization statistic, then $E_d(P)_{q=1} = P(1^d)$.*

▷ **Ex.** Let Q be the quadratic excess, $E_d(Q)_{q=1} = \binom{d}{2}$.

Part II

Higher Necklace Polynomials and Liminal Reciprocity



Multivariate Irreducibles

- $\mathrm{Irr}_{d,n}(\mathbb{F}_q) :=$ set of monic degree d irreducible polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

- $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ is a finite set.

Proposition (H. 2017)

For $d, n \geq 1$ there exists a polynomial $M_{d,n}(x) \in \mathbb{Q}[x]$ such that

$$|\mathrm{Irr}_{d,n}(\mathbb{F}_q)| = M_{d,n}(q).$$

We call $M_{d,n}(x)$ the ***higher necklace polynomials****.*

▷ When $n = 1$ (univariate polys.) Gauss found a formula,

$$M_{d,1}(x) = M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}.$$

Higher Necklace Polynomials

▷ No known explicit formula for $M_{d,n}(x)$ with $n > 1$.

n	$M_{3,n}(x)$
1	$-\frac{1}{3}x + \frac{1}{3}x^3$
2	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{1}{3}x^3 - \frac{3}{3}x^5 - \frac{2}{3}x^6 + \ldots$
3	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{3}{3}x^4 + \frac{3}{3}x^5 + \frac{1}{3}x^6 - \frac{3}{3}x^7 + \ldots$
4	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{2}{3}x^4 + \frac{6}{3}x^5 + \frac{7}{3}x^6 + \frac{6}{3}x^7 + \ldots$
5	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{2}{3}x^4 + \frac{5}{3}x^5 + \frac{10}{3}x^6 + \frac{12}{3}x^7 + \ldots$
6	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{2}{3}x^4 + \frac{5}{3}x^5 + \frac{9}{3}x^6 + \frac{15}{3}x^7 + \ldots$
7	$-\frac{1}{3}x - \frac{1}{3}x^2 + \frac{2}{3}x^4 + \frac{5}{3}x^5 + \frac{9}{3}x^6 + \frac{14}{3}x^7 + \ldots$

▷ The **d**egree is fixed, the **n**umber of variables is increasing.

Liminal Reciprocity

Recall that

$$M_{d,1}(x) = \frac{1}{d}\sum_{e|d}\mu(e)x^{d/e}.$$

Theorem (H. 2017)

Let $d \geq 1$ be fixed, then the sequence of polynomials $M_{d,n}(x)$ converges coefficientwise to a rational function $M_{d,\infty}(x)$ given explicitly by

$$M_{d,\infty}(x) = -M_{d,1}\left(\frac{1}{1-\frac{1}{x}}\right).$$

Note: "Reciprocity" comes from the equivalent identity

$$M_{d,1}(x) = -M_{d,\infty}\left(\frac{1}{1-\frac{1}{x}}\right).$$

Liminal Reciprocity

Theorem (H. 2017)

Let $d \geq 1$ be fixed, then the sequence of polynomials $M_{d,n}(x)$ converges coefficientwise to a rational function $M_{d,\infty}(x)$ given explicitly by

$$M_{d,\infty}(x) = -M_{d,1}\left(\frac{1}{1-\frac{1}{x}}\right).$$

- Chen showed "homological stability in co-degrees" for $\mathrm{Irr}_{d,n}(\mathbb{C})$.
- Geometric interpretation of reciprocity?

Euler Characteristics

Let χ_c denote the **compactly supported Euler characteristic,**

$$\chi_c(X \sqcup Y) = \chi_c(X) + \chi_c(Y) \qquad \chi_c(X \times Y) = \chi_c(X) \cdot \chi_c(Y).$$

▷ $\chi_c(\mathbb{C}) = 1$ and $\chi_c(\mathbb{R}) = -1$ $\quad (\mathbb{C} \approx \mathbb{F}_1$ and $\mathbb{R} \approx \mathbb{F}_{-1}.)$

Theorem (H. 2018)

Let $d, n \geq 1$, then

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1)$$

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1)$$

Euler Characteristics

The **balanced binary expansion** of n is the unique expression of n as an alternating sum of an even number of powers of 2.

Theorem (H. 2018)

Let $d, n \geq 1$ and let $n = \sum_{k \geq 0} b_k 2^k$ be the balanced binary expansion of n, then

$$\begin{aligned}
\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) &= M_{d,n}(1) &&= \begin{cases} n & d = 1 \\ 0 & \textit{otherwise.} \end{cases} \\
\chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) &= M_{d,n}(-1) &&= \begin{cases} b_k & d = 2^k \\ 0 & \textit{otherwise.} \end{cases}
\end{aligned}$$

Ex. $n = 13 = 2^4 - 2^2 + 2 - 1$

$$\chi_c(\mathrm{Irr}_{d,13}(\mathbb{R})) = \begin{cases} -1 & d = 1,\ 2^2 \\ 1 & d = 2,\ 2^4 \\ 0 & \text{otherwise.} \end{cases}$$

Euler Characteristics for $n = 1$

When $n = 1$ we can compute $M_{d,1}(\pm 1)$ geometrically.

▷ Since $\mathbb{C}$ is alg. closed, only have irred. polynomials in degree 1.

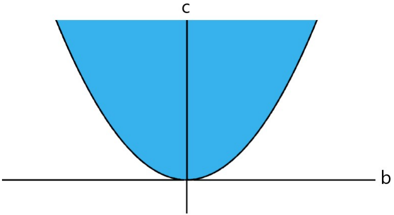
$$\mathrm{Irr}_{d,1}(\mathbb{C}) = \begin{cases} \mathbb{C} & d = 1 \\ \emptyset & d > 1 \end{cases} \implies M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases}$$

Euler Characteristics for $n = 1$

▷ All irred. polys. over $\mathbb{R}$ have degree at most 2.

$$\mathrm{Irr}_{d,1}(\mathbb{R}) = \begin{cases} \mathbb{R} & d = 1 \\ \mathcal{U} & d = 2 \\ \emptyset & d > 2 \end{cases} \Longrightarrow M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

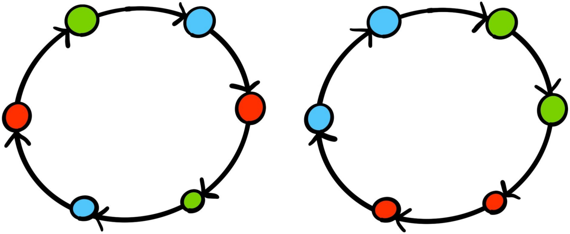
▷ $\mathcal{U} = \{x^2 + bx + c : b^2 - 4c < 0\}$



▷ **Note:** $n = 1 = 2 - 1$ is the balanced binary expansion of 1.

Part III

Cyclotomic Factors of Necklace Polynomials



Factoring Necklace Polynomials

$$M_d(x) = M_{d,1}(x) = \frac{1}{d}\sum_{e|d} \mu(e)x^{d/e}.$$

- ▷ Euler char. computation shows $M_d(\pm 1) = 0$ for $d > 2$.
- ▷ Equivalently: $x^2 - 1$ divides $M_d(x)$ for $d > 2$.
- ▷ How does $M_d(x)$ factor?

Ex. $d = 10$

$$M_{10}(x) = \tfrac{1}{10}(x^{10} - x^5 - x^2 + x)$$

$$= \tfrac{1}{10}(x^3 + x^2 - 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)x$$

How Does $M_d(x)$ Factor?

$$M_{10}(x) = \frac{1}{10}(x^{10} - x^5 - x^2 + x)$$

$$= \frac{1}{10}(x^3 + x^2 - 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)x$$

$$= \frac{1}{10}(x^3 + x^2 - 1) \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

▷ $\Phi_m(x)$ is the *m*th **cyclotomic polynomial**, the minimal polynomial over $\mathbb{Q}$ of ζ_m a primitive *m*th root of unity.

More Examples

$$M_{105}(x) = \frac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^{7} + x^{5} + x^{3} - x)$$
$$= f_1 \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

$$M_{253}(x) = \frac{1}{253}(x^{253} - x^{23} - x^{11} + x)$$
$$= f_2 \cdot \Phi_{24} \cdot \Phi_{22} \cdot \Phi_{11} \cdot \Phi_{10} \cdot \Phi_8 \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

$$M_{741}(x) = \frac{1}{741}(x^{741} - x^{247} - x^{57} - x^{39} + x^{19} + x^{13} + x^{3} - x)$$
$$= f_3 \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x,$$

f_1, f_2, f_3 are non-cyclotomic irred. polynomials of degrees 92, 210, and 708 respectively.

Cyclotomic Factor Phenomenon

Conjecture (H. 2018)

If $\Phi_m(x)$ divides $M_d(x)$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.

Theorem (H. 2018)

Let $m, d \geq 1$.

- *Ubiquity*
  - *If $p \mid d$ is a prime and $p \equiv 1 \bmod m$, then $x^m - 1 \mid M_d(x)$.*
    ▷ *In particular, $x^{p-1} - 1 \mid M_d(x)$ for each $p \mid d$.*
- *Multiplicative Inheritance*
  - *If $x^m - 1 \mid M_d(x)$, then $x^m - 1 \mid M_{de}(x)$.*
  - *If $x^m + 1 \mid M_d(x)$ and e is odd, then $x^m + 1 \mid M_{de}(x)$.*
    ▷ *$M_d(x)$ generally does not divide $M_{de}(x)$.*
- *Necessary Condition*
  - *If $x^m - 1 \mid M_d(x)$, then $m \mid \varphi(d)$.*
    ▷ *$\varphi(d) := |(\mathbb{Z}/(d))^\times|$ is the **Euler totient function**.*

Cyclotomic Factor Phenomenon

Theorem (H. 2018)

Let $f(x) \in \mathbb{Q}[x]$ and $d \geq 1$.

1. *If $x^m - 1$ divides $M_d(x)$, then*

$$x^m - 1 \ \text{ divides } \ \frac{1}{d}\sum_{e|d} \mu(e) f(x^{d/e}).$$

2. *If $x^m + 1$ divides $M_d(x)$ and $f(x)$ is an odd polynomial, then*

$$x^m + 1 \ \text{ divides } \ \frac{1}{d}\sum_{e|d} \mu(e) f(x^{d/e}).$$

Cyclotomic Factor Phenomenon (CFP)

- Cyclotomic factors of $M_d(x)$ detect multiplicative relations in **cyclotomic units**.
- CFP partially extends to higher necklace polynomials $M_{d,n}(x)$
- There is a G**-necklace polynomial** $M_G(x)$ for every finite group G.
  - If $G = C_d$, then $M_{C_d}(x) = M_d(x)$.
  - If G is solvable, then CFP holds for $M_G(x)$.

Thank you!