

Möbius Randomness and Dynamics

Peter Sarnak
Mahler Lectures 2011

$$n \geq 1,$$

$$\mu(n) = \begin{cases} (-1)^t & \text{if } n = p_1 p_2 \cdots p_t \text{ distinct,} \\ 0 & \text{if } n \text{ has a square factor.} \end{cases}$$

$$1, -1, -1, 0, -1, 1, -1, 1, -1, 0, 0, 1, \dots$$

Is this a “random” sequence?

$$\frac{1}{\zeta(s)} = \prod_p (1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

so the zeros of $\zeta(s)$ are closely connected to

$$\sum_{n \leq N} \mu(n).$$

Prime Number Theorem

elementarily
 \Longleftrightarrow

$$\sum_{n \leq N} \mu(n) = \sum_{n \leq N} \mu(n) \cdot 1 = o(N).$$

Riemann Hypothesis \Longleftrightarrow For $\varepsilon > 0$,

$$\sum_{n \leq N} \mu(n) = O_{\varepsilon}(N^{1/2+\varepsilon}).$$

- Usual randomness of $\mu(n)$, square-root cancellation.
(Old Heuristic) “Möbius Randomness Law” (EG, I–K)

$$\sum_{n \leq N} \mu(n) \xi(n) = o(N)$$

for any “reasonable” independently defined bounded $\xi(n)$.

This is often used to guess the behaviour for sums on primes using

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^e, \\ 0 & \text{otherwise,} \end{cases}$$
$$\Lambda(n) = - \sum_{d|n} \mu(d) \log d.$$

What is “reasonable”?

Computational Complexity (?): $\xi \in P$ if $\xi(n)$ can be computed in $\text{polylog}(n)$ steps.

Perhaps $\xi \in P \implies \mu$ is orthogonal to ξ ?

I don't believe so since I believe factoring and μ itself is in P .

Problem: Construct $\xi \in P$ bounded such that

$$\frac{1}{N} \sum_{n \leq N} \mu(n) \xi(n) \rightarrow \alpha \neq 0.$$

Dynamical view of complexity of a sequence (Furstenberg disjointness paper 1967)

Flow: $F = (X, T)$, X a compact metric space, $T : X \rightarrow X$ continuous. If $x \in X$ and $f \in C(X)$, the sequence (“return times”)

$$\xi(n) = f(T^n x)$$

is realized in F .

Idea is to measure the complexity of $\xi(n)$ by realizing $\xi(n)$ in a flow F of low complexity.

Every bounded sequence can be realized; say $\xi(n) \in \{0, 1\}$,
 $\Omega = \{0, 1\}^{\mathbb{N}}$, $T : \Omega \rightarrow \Omega$,

$$T((x_1, x_2, \dots)) = (x_2, x_3, \dots)$$

i.e. shift.

If $\xi = (\xi(1), \xi(2), \dots) \in \Omega$ and $f(x) = x_1$, $x = \xi$ realizes $\xi(n)$.

In fact, $\xi(n)$ is already realized in the potentially much simpler flow
 $F_\xi = (X_\xi, T)$, $X_\xi = \overline{\{T^j \xi\}_{j=1}^\infty} \subset \Omega$.

The crudest measure of the complexity of a flow is its Topological Entropy $h(F)$. This measures the exponential growth rate of distinct orbits of length m , $m \rightarrow \infty$.

Definition

F is deterministic if $h(F) = 0$. $\xi(n)$ is deterministic if it can be realized in a deterministic flow.

A Process: is a flow together with an invariant probability measure

$$F_\nu = (X, T, \nu),$$
$$\nu(T^{-1}A) = \nu(A) \quad \text{for all (Borel) sets } A \subset X.$$

$h(F_\nu) =$ Kolmogorov–Sinai entropy.

$h(F_\nu) = 0$, F_ν is deterministic, and it means that with ν -probability one, $\xi(1)$ is determined from $\xi(2), \xi(3), \dots$

Theorem

$\mu(n)$ is not deterministic.

A much stronger form of this should be that $\mu(n)$ cannot be approximated by a deterministic sequence.

Definition

$\mu(n)$ is disjoint (or orthogonal) from F if

$$\sum_{n \leq N} \mu(n) \xi(n) = o(N)$$

for every ξ belonging to F .

Main Conjecture (Möbius Randomness Law)

μ is disjoint from any deterministic F . In particular, μ is orthogonal to any deterministic sequence.

NB We don't ask for rates in $o(N)$.

Why believe this conjecture?

There is an old conjecture.

Conjecture (Chowla: self correlations)

$$0 \leq a_1 < a_2 < \dots < a_t,$$

$$\sum_{n \leq N} \mu(n + a_1) \mu(n + a_2) \cdots \mu(n + a_t) = o(N).$$

The trouble with this is no techniques are known to attack it and nothing is known towards it.

Proposition

Chowla \implies Main Conjecture.

The proof is purely combinatorial and applies to any uncorrelated sequence.

The point is that progress on the main conjecture can be made, and these hard-earned results have far-reaching applications. The key tool is the bilinear method of Vinogradov — we explain it in dynamical terms at the end.

Cases of Main Conjecture Known:

- (i) F is a point \iff Prime Number Theorem.
- (ii) F finite \iff Dirichlet's theorem on primes in progressions.
- (iii) $F = (\mathbb{R}/\mathbb{Z}, T_\alpha)$, $T_\alpha(x) = x + \alpha$, rotation of circle;
Vinogradov/Davenport 1937.

- (iv) Extends to any Kronecker flow [i.e. $F = (G, T_\alpha)$, G compact abelian, $T_\alpha(g) = \alpha + g$] and also to any deterministic affine automorphism of such (Liu–S.). (If T has positive entropy, then Main Conjecture fails).
- (v) $F = (\Gamma \setminus N, T_\alpha)$, where N is a nilpotent Lie group and Γ a lattice in N , $T_\alpha(\Gamma x) = \Gamma x \alpha$, $\alpha \in N$ (Green–Tao 2009).
- (vi) If (X, T) is the dynamical flow corresponding to the Morse sequence (connected to the parity of the sums of the dyadic digits of n); Mauduit and Rivat (2005).

- The last is closely connected to a proof that $\mu(n)$ is orthogonal to any bounded depth polynomial size circuit function — see Gil Kalai’s blog 2011.
 - In all of the above, the dynamics is very rigid. For example, it is not weak mixing.
- (vii) A source of much more complex dynamics but still deterministic in the homogeneous setting is to replace the abelian and nilpotent groups by G semisimple. So $F = (\Gamma \backslash G, T_\alpha)$ with α ad-unipotent (to ensure zero entropy) and Γ a lattice in G .
- In this case, F is mixing of all orders (Moses).
 - The orbit closures are algebraic, “Ratner Rigidity”.

Main Conjecture is true for $X = \Gamma \backslash \mathrm{SL}_2(\mathbb{R})$, $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, i.e. horocycle flows; Bourgain–S. 2011.

Dynamical System associated with μ

Simplest realization of μ :

$$\{-1, 0, 1\}^{\mathbb{N}} = X, \quad T \text{ shift}$$

$$\omega = (\mu(1), \mu(2), \dots) \in X$$

$$X_M = \overline{\{T^j \omega\}_{j=1}^{\infty}} \subset X$$

$M = (X_M, T_M)$ is the Möbius flow.

Look for factors and extensions:

$$\eta = (\mu^2(1), \mu^2(2), \dots) \in Y = \{0, 1\}^{\mathbb{N}}$$

$$Y_S = \text{closure in } Y \text{ of } T^j \eta$$

$S := (Y_S, T_S)$ is the square-free flow.

$$\begin{array}{ccc}
 \pi : X_M & \rightarrow & Y_M \\
 (x_1, x_2, \dots) & \mapsto & (x_1^2, x_2^2, \dots) \\
 X_M & \xrightarrow{T_M} & X_M \\
 \pi \downarrow & & \downarrow \pi \\
 Y_S & \xrightarrow{T_S} & Y_S
 \end{array}$$

S is a factor of M .

Using an elementary square-free sieve, one can study S !

Definition

$A \subset \mathbb{N}$ is admissible if the reduction \bar{A} of $A \pmod{p^2}$ is not all of the residue classes $\pmod{p^2}$ for every prime p .

Theorem

- (i) Y_S consists of all points $y \in Y$ whose support is admissible.
- (ii) The flow S is not deterministic; in fact,

$$h(S) = \frac{6}{\pi^2} \log 2.$$

- (iii) S is proximal;

$$\inf_{n \geq 1} d(T^n x, T^n y) = 0 \quad \text{for all } x, y.$$

- (iv) S has a nontrivial joining with the Kronecker flow
 $K = (G, T)$, $G = \prod_p (\mathbb{Z}/p^2\mathbb{Z})$, $Tx = x + (1, 1, \dots)$.
- (v) S is not weak mixing.

At the ergodic level, there is an important invariant measure for S .
On cylinder sets C_A , $A \subset \mathbb{N}$ finite,

$$C_A = \{y \in Y : y_a = 1 \text{ for } a \in A\}$$

$$\nu(C_A) = \prod_p \left(1 - \frac{t(\bar{A}, p^2)}{p^2}\right)$$

where $t(\bar{A}, p^2)$ is the number of reduced residue classes of $A \pmod{p^2}$. ν extends to a T -invariant probability measure on Y whose support is Y_S .

Theorem

$S_\nu = (Y_S, T_S, \nu)$ satisfies

- (i) η is generic for ν ; that is, the sequence $T^n \eta \in Y$ is ν -equidistributed.
- (ii) S_ν is ergodic.
- (iii) S_ν is deterministic as a ν -process.
- (iv) S_ν has $K_\mu = (K, T, dg)$ as a Kronecker factor.

- Since S is a factor of M , $h(M) \geq h(S) > 0 \implies \mu(n)$ is not deterministic!
- One can form a process N_ν which is a completely positive extension of S and which conjecturally describes M and hence the precise randomness of $\mu(n)$. In this way, the Main Conjecture can be seen as a consequence of a disjointness statement in Furstenberg's general theory.
- We don't know how to establish any more randomness in M than the factor S provides.
- The best we know are the cases of disjointness proved.

Vinogradov (Vaughan) "Sieve" expresses $\sum_{n \leq N} \mu(n)F(n)$ in terms of Type I and Type II sums:

In dynamical terms:

$$I) \quad \sum_{n \leq N} f(T^{nd_1}x).$$

Individual Birkhoff sums associated with (X, T^{d_1}) , i.e. sums of f on arithmetic progressions.

$$II) \quad \sum_{n \leq N} f(T^{d_1 n}x)f(T^{d_2 n}x) \quad (\text{Bilinear sums}).$$

Individual Birkhoff sums associated with the joinings (X, T^{d_1}) with (X, T^{d_2}) .










In Bourgain–S., we give a finite version of this process. Allows for having no rates (only main terms) in the type // sums.



With this and $X = (\Gamma \backslash \mathrm{SL}_2(\mathbb{R}), T_\alpha)$, $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ unipotent, one can appeal to Ratner's joining of horocycles theory (1983) to compute and handle the type // sum.

\implies prove of the disjointness of $\mu(n)$ with such horocycle flows.

The method should apply to the general ad-unipotent system $\Gamma \backslash G$ by appealing to Ratner's general rigidity theorem.

Some references:

-  J. Bourgain and P. Sarnak, “Disjointness of Möbius from horocycle flows”, preprint, 2011.
-  S. Chowla, *The Riemann Hypothesis and Hilbert’s Tenth Problem*, Gordon and Breach, New York, 1965.
-  H. Davenport, *Quat. J. Math.* **8** (1937), 313–320.
-  H. Furstenberg, *Math. Syst. Th.* **1** (1961), 1–49.
-  B. Green and T. Tao, “The Möbius function is orthogonal to nilsequences”, to appear in *Ann. Math.*
-  H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS, 2004.
-  Gil Kalai, Blog, gilkalai.wordpress.com/2011/02/21.
-  M. Ratner, *Ann. Math.* **118** (1983), 277–313.
-  M. Ratner, *Ann. Math.* **134** (1991), 545–607.

-  P. Sarnak, “Three lectures on the Möbius function randomness and dynamics”, publications.ias.edu/sarnak.
-  I. M. Vinogradov, *Recueiv Math.* **8** (1937), 313–320.