AN UNDERDETERMINED MATRIX MOMENT PROBLEM AND ITS APPLICATION TO COMPUTING ZEROS OF $L$-FUNCTIONS

PETER SARNAK

(JOINT WORK WITH M. RUBINSTEIN)
The impact of Ilya's work shows no signs of slowing down and will no doubt continue for years to come.

For the topic of this lecture I mention:

- His major role in the formulation of the modern theory of automorphic forms using representation theory (W. Gelfand, Graev).

- Starting in the early 70's with his discovery of a Hecke theory for GL3 automorphic forms and related Euler products continuing to a complete converse theorem, theory of Rankin-Selberg L-functions, doubling method for more general L-functions (W. Jacquet-Shalika, Rallis,Cogdell, Shahidi, ...).

- His results and techniques are the standard ones that are used as far as the analytic properties of L-functions.

In this lecture we exploit them for computational complexity.
Complexity of Computing Zeros

\( \pi \) an automorphic cusp form on \( \text{GL}_m / \mathbb{Q} \) \((m = 2)\).

\( L(s, \pi) \) its standard \( L \)-function

\[ L(s, \pi_p) = \text{local factor at } p \]

\[ L(s, \pi) = \prod_p L(s, \pi_p) \quad p < \infty \]

\[ \Delta(s, \pi) = L(s, \pi_\infty)L(s, \pi) \]

Analytic continuation and functional eqn:

\[ \Delta(1-s, \pi) = W(\pi) N_{\pi}^{s-\frac{1}{2}} \Delta(s, \pi) \]

\( \pi = \overline{\pi} \) (assumption) self-dual

\( W(\pi) = \pm 1 \) : root number

\( N_{\pi} \) is the conductor, it is a product over primes at which \( \pi \) is ramified.

\( N_{\pi} \) measures the complexity of \( \pi \); want to compute zeros of \( L(s, \pi) \) near \( \frac{1}{2} \).
EXPlicate with elliptic curves
Weierstrass form:
$$E: y^2 + axy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$a_j \in \mathbb{Z}.$$
Corresponding invariants are
$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2^2a_4$$
$$c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$
Discriminant
$$\Delta = -b_2^2b_8 - 8b_2^3b_4 - 27b_6^2 + 9b_2b_4b_6$$

We assume that $$(c_4,c_6)=1$$ and $$(c_4,6)=1$$ so that $$E$$ has only multiplicative bad reduction.

$$\Rightarrow$$ $N_E$ the conductor of $$E$$ is square free part of $$|\Delta|$$, assume latter is sq. free.

$$N_E = |\Delta|$$
$$W(E) = -\left(\frac{c_6}{N_E}\right) \mu(N_E);$$

$$\mu$$ the Mobius function the parity of the number of prime factors.

The order of vanishing of $$L(5,E)$$ at $$s = 5$$ is the rank of $$E/\text{R} (\text{BSD}).$$
One can compute $L(s, \varepsilon P)$ the local factor at $p$ in poly log($p$) steps (Schoof).

\[ L(s, E) = \sum_{n=1}^{\infty} \lambda_E(n) n^{-s} \]

Then for any $x$ we can compute the $\lambda_E(n)$'s in $x^{1+o(1)}$ steps.

Riemann's Gold Standard:

Given $w(E)$, using the "approximate functional equation" (Riemann-Siegel formula) one can compute $L(s, E)$ for $s$ near $\frac{1}{2}$ in $N_E^{\frac{1}{2} + o(1)}$ steps.

$w(E)$ is a product over $p$'s dividing $N_E$ of $w_p(E)$, so $w(E)$ can be computed in $N_E^{\frac{1}{2}}$ steps trivially.
ONE CAN COMPUTE THE COUNTING FN.

\[ S(E,t) = \# \{ \rho = \frac{1}{2} + i \sigma : 0 < \sigma \leq t, L(\rho, E) = 0 \} \]

AND IN PARTICULAR THE RANK IN 

\[ N^{\frac{1}{2} + o(1)} \] STEPS.

CAN ONE DO BETTER; BREAK THE 

\( \frac{1}{2} \) BARRIER, OR EVEN \( N^{o(1)} \) STEPS 

I. E. SUBEXPONENTIAL.

THE ELUSIVE PARITY:
THE PARITY OF THE NUMBER OF PRIME FACTORS OF A NUMBER IS ONE OF ITS 
BEST KEPT SECRETS. THEORETICALLY IN 
SIEVE THEORY THERE IS THE WELL KNOWN 
SIEVE LIMIT ON RECOGNISING PARITY. 
COMPUTATIONALLY AS FAR AS WE KNOW 
THE FASTEST WAY TO COMPUTE \( \mu(N) \) 
IS TO FACTOR \( N \) — AND THESE ARE PROBABLY 
OF THE SAME COMPLEXITY. THE BEST 
FACTORIZING ALGORITHMS ARE SUBEXPONENTIAL 
IN \( N \), AND GIVE BENCH MARKS FOR OUR PROBLEM.
THEOREM (RUBINSTEIN / SAR)

One can compute $W(E)$ (without factoring $N_E$) and $S(E, t)$ for many $t$'s in subexponential (in $\log N_E$) time.

REMARKS:

(a) We are assuming GRH throughout.

(b) The theory of the Rankin-Selberg $L$-function shows that $\lambda$ is determined by its first $(\log N_E)^{2+\varepsilon} \lambda_{\pi(p)}$'s !

(c) The algorithm when it terminates gives correct answers. The fact that it does terminate quickly depends on conjectures (Katz / SAR) relating the distribution of the zeros to random matrix theory.
The basis of the computation is the explicit formula of Riemann, Guinand, Weil:

\[ \phi \in \mathcal{F}(\mathbb{R}), \hat{\phi} \text{ F.T} \hat{\phi} \text{ compact support} \]

\[ \phi \text{ even} \]

\[ \sum \phi(t) = \frac{\hat{\phi}(0)}{\pi} \log N + \]

\[ \frac{1}{\pi} \int_{-\infty}^{\infty} \phi(t) \Re \left( \frac{L'(\frac{1}{2} + it, \Pi)}{L(\frac{1}{2} + it, \Pi)} \right) \, dt \]

\[ - \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{C(n)}{\sqrt{n}} \hat{\phi} \left( \frac{\log n}{2\pi} \right) \]

where \[ L'/L(\frac{1}{2}, \Pi) = - \sum_{n=1}^{\infty} \frac{C(n)}{n^{\frac{1}{2}}} \]

If we compute \( C(n) \) for \( n \leq x \), by limiting support \( \phi \), the above is a system of equations for the \( \gamma \)'s.
This system reduces to the following basic problem with
\[ \log N_n \approx n \]

**Undetermined Moment Problem**

\[ O(2n+1) \text{ orthogonal group size } 2n+1 \]

For \( A \in O(2n+1) \)

\[ P_A(\lambda) = \det(\lambda I - A) = \lambda^{2n+1} + \lambda^{2n} + \ldots + \lambda^{2} + \lambda + 1 \]

\[ q_{2n+1} = -\det A, \quad q_j = -(\det A) q_{2n+1} - j \]

Since \( \lambda^{2n+1} P_A(\lambda^{-1}) = (\det A) P_A(\lambda) \) self reciprocal

We are given the first \( R \)-moments

\[ s_j(A) = \text{trace}(A^j), \quad 0 \leq j \leq k \]

\[ = (\det A)^j + \sum_{y=1}^{n} 2 \cos(j \theta_y) \]

Here the \( 2m+1 \) eigenvalues of \( A \) are \( \det A, e^{i \theta_1}, e^{-i \theta_1}, \ldots, e^{i \theta_n}, e^{-i \theta_n} \).
IF \( r = n \) AND \( \det A = \pm 1 \) IS KNOWN THEN (4) AND (5) AND NEWTON GIVE THE \( \Theta_j \)'s FOR ALL \( j \) AND HENCE \( \Theta_j \)'s.

OUR L-FUNCTION PROBLEM ONCE WE HAVE COMPUTED THE \( C(n) \)'s FOR \( m \leq n \), REDUCES TO (5) WITH

\[
\frac{r}{\pi} = 2 \times
\]

SO \( \alpha = \frac{1}{2} \) (RIEMANN'S GOLD STANDARD) CORRESPONDS EXACTLY TO \( r = n \) WHEN EVERYTHING CAN BE COMPUTED.

COMPLEXITY \( \alpha < \frac{1}{2} \) YIELDS THE CORRESPONDING UNDERDETERMINED PROBLEM:

GIVEN \( y \in \mathbb{R}^k \), \( y = (s_1, s_2, \ldots, s_k) \) OUR GIVEN MOMENTS WHAT CAN WE SAY ABOUT \( \det A \) AND THE \( \Theta_j \)'s?
FORBIDDEN SET $F(y)$:

Let $F(y) \subset [0, \pi]$ be the set of $t$'s which are not the eigenvalues of any $A$ whose first $k$-moments are $y$.

- If $F(y)$ is large we learn something about the eigenvalues — they are restricted to lie in the union of intervals which form the admissible set

$$G(y) = [0, \pi] \setminus F(y)$$

- If $k < n$, $F(y)$ may be empty for example if the $\theta$'s lie on an arithmetic progression, but for typical $y$ and $k$ not too small this won't happen.

EXACT COUNT SET $E_y(t)$:

$E(y)$ consists of all $t$'s in $[0, \pi]$ for which the number $S_y(t)$ of eigenvalues $\theta_j, \theta_k, \ldots$ etc, lie in $[0, t]$ is determined independent of $A$. 
How to compute these efficiently and what do they look like as a function of $\alpha = k/n$?

**Moment Curve:**

Closely related to the above is the moment curve; $t = \cos \Theta$

$-1 \leq t \leq 1$

$M: [-1, 1] \to \mathbb{R}^k$; $M(t) = (t, t^2, \ldots, t^k)$

$C := M([-1, 1]) \subset \mathbb{R}^k$

For $M \geq 1$ (our interest is $n > k$)

$A(k, n) := C + C + C \ldots + C$; $n$-times

$C \subset \mathbb{R}^k$
Basic Complexity Problem: 

For $z \in \mathbb{R}^k$ is $z \in A(k,n)$?

Does this have an efficient solution (i.e., polynomial time)?

Note that for $A(k,k)$ it does since in this case we get the full characteristic polynomial and hence recover the roots efficiently.

But how about $n = 2k$?

Relevance: To compute $F(y)$ we consider for each $t \in [-1,1]$ whether 

$y - M(t) \in A(k,n-1)$

This is so iff $t \in F(y)$. 

Figure 4. Heat maps depicting the distribution of points in the sets $A(2, 4), A(2, 5)$.

Then, for $u = c(t_1) + c(t_2) + \ldots + c(t_k) \in A(k, n)$,

$$v(u) = \sum_{j=1}^{n} f(t_j).$$

Hence $v(u) \leq 0$ for all $u \in A(k, n)$ iff $f(t) \leq 0$ for all $t$.
Figure 1. Plots depicting the admissible sets (i.e. complement of $F(y)$), for 2 Haar sampled matrices in $SO(2n)$, with $n = 5, 10, 20, 30$, and $k = n - j$, with $j = 0, 1, 2$. The horizontal depicts the points $t \in [0, 1/2]$ in the admissible set, while the vertical axis is $j$. ($j = 2$ needs to be redrawn to higher resolution. will include $n = 5, 30$ later today)
OUR (EFFICIENT) ALGORITHM INVOLVES AN ITERATIVE CONVEXIFICATION OF THE BASIC PROBLEM COUPLED WITH A SECOND LINEAR PROGRAM.

IT YIELDS (GOOD IN TYPICAL SITUATIONS) LOWER BOUNDS FOR F(y) AND E(y).

MORE GENERALLY, FOR G(y) ∈ [-1,1] LET

\[ C_G = M(G) \subset R^k \]

AND

\[ A_G(k, n) = C_G + C_G + \ldots + C_G \]

OUR INTEREST IS G A UNION OF INTERVALS (FINITELY MANY).

THE QUESTION OF WHETHER \( z \in \mathbb{R}^k \)
IS IN \( A_G(k, n) \) IS ALREADY HARD

SINCE FOR \( k=1 \) AND G SAY n POINTS, IT CONTAINS THE SUBSUM PROBLEM WHICH IS NP COMPLETE (KARP)
We relax the problem to determine if \( z \) is in the convex hull of \( A \):

\[ z \in \text{CH}(\text{AG}(k, n)) \text{ iff there is a separating hyperplane} \]

\[
\min \left\{ b_0 + b_1 x_1 + \ldots + b_k x_k \right\} < 0 \quad \text{LP1}
\]

Subject to \( b_0 + b_1 x_1 + \ldots + b_k x_k = 0 \) for \( \text{TEG} \)

For exact counting, \( JC([-1, 1]) \) interval estimate:

\[
S_y(J) = \sum \left\{ \theta_i \text{'s, det A in } J : M(A)=y \right\}
\]

\[
\sum_{i=0}^{k} \left( \sum_{j=0}^{k} b_j t^j \right) x_i(t) \leq \sum_{j=0}^{k} c_j t^j \text{, } t \in \text{JNG}
\]

Linear program:

\[
\Delta_y(J) = \min_{b,c} \left[ U(y) - L(y) \right] \quad \text{LP2}
\]
IF \( \Delta_y(j) < 1 \) then \( S_y(j) \)

which is an integer is determined!

**ITERATION:**

**INITIALIZE** \( G = [-1,1] \)

FOR EACH \( t \in [-1,1] \) RUN LP1

TO CHECK IF \( y - M(t) \in CH(A(R, n-1)) \)

IF NOT \( t \in F_1(y) \).

FOR EACH \( t \in F_1(y) \) RUN LP2

TO OBTAIN \( E_1(y) \) WHEN \( S_y([-1,1]) \) IS DETERMINED.

**ITERATE:** \( G_2(y) = [-1,1] \setminus F_1(y) \),

\( F_2(y), G_2(y), E_2(y), \ldots \)

\( F_1(y) \subset F_2(y) \subset \ldots \subset F_0(y) \subset F(y) \)

\( E_1(y) \subset E_2(y) \subset \ldots \subset E_0(y) \subset E(y) \)

\( S_y(t) \) \( t \in E_0(y) \).
NB: AT THE FIRST STEP \( G = [-1, 1] \)

LP1 AND LP2 HAVE EXPLICIT SOLUTIONS

BY HAMBURGER, CHEBYSHEV AND MARKOV. WE USE THESE AT THIS STEP AND IT

ALSO IS IMPORTANT FOR ANALYSIS.

**Theorem:** \( z \in \mathbb{R}^k \) is in \( \text{CH}(C) \)

IFF THE HANKEL MATRICES

\[
\begin{pmatrix}
3i+j \\
\end{pmatrix}_{i=0,1,\ldots,v}
\]

\[
\begin{pmatrix}
3i+j \\
\end{pmatrix}_{i=0,1,\ldots,v, j=0,1,\ldots,v-1}
\]

AND

\[
\begin{pmatrix}
3i+j+1 - 3i+j - 3i+j+2 \\
\end{pmatrix}_{i=0,1,\ldots,v-1}
\]

\[
\begin{pmatrix}
3i+j+1 - 3i+j - 3i+j+2 \\
\end{pmatrix}_{i=0,1,\ldots,v-1, j=0,1,\ldots,v-1}
\]

ARE NONNEGATIVE.

THE SOLUTION OF LP2 FOR \( G = [-1, 1] \)

BY CHEBYSHEV AND MARKOV USES THEIR

THEORY OF NODES AND WEIGHTS

(VIA PADE APPROXIMATIONS)
Figure 6. The same as the previous figure, but for 30 pairs of zeros, symmetric about 0, chosen uniformly and independently at random, for $k = 15$ (top) and $k = 30$ (bottom). We notice that there are larger gaps (as well as many smaller gaps) in comparison to the SO(60) example, and that more of the gaps are detected sooner.
\( F_1(y) \) may be empty in which case we learn nothing.

The key point that we establish is that if \( 2\chi = k/m \) goes to 0 slowly then both \( F_1(y) \) and \( E_1(y) \) are non-empty (in fact quite large) if \( y = M(A) \) is drawn at random w.r.t. Haar measure on \( O(2n+1) \).

Note that once \( E_\infty(y) \neq \emptyset \) and \(-1 < t < 1\) is in \( E_\infty(y) \) then the parity of \( S_y(t) \) is even iff \( \det A = 1 \), that is we determine \( \text{w}(A) \) \( \Rightarrow \) subexponential comp. of \( \text{w}(E) \).
What is the limit of \( \frac{\log n}{n} \) for \( W(A) \) to be computed?

A limit is set by the very strong Szegö limit type theorem of Johansson / Lambert (2019):

Let \( Y_+(k,n), Y_-(k,n) \) be the push forward moment measures (on \( \mathbb{R}^k \)) of Haar measure on \( O^+(2n+1) \) and \( O^-(2n+1) \). Then for \( k = n^\alpha, 0 < \alpha < \frac{1}{3} \)

\[
\text{Total Variation} \left[ Y_+(k,n), Y_-(k,n) \right] \leq C e^{-(1-\alpha) n^{1-\alpha}}
\]

so certainly there is no polynomial time computation of \( W(\mathbb{N}_n) \) by this method.
To end we put these questions in the broader context of ramification.

The global Hasse/Weil zeta function of a smooth projective variety over $\mathbb{Q}$ carries conjecturally some striking information:

- That its reduction at primes $p$ which are at most polynomial in the logarithm of the conductor $N_v$ of $V$, already determines the full zeta function of $V$.

So the basic complexity question is which global quantities associated with $V$ can be computed efficiently?