SOME CHALLENGES FOR COMPUTING AUTOMORPHIC FORMS AND THEIR L-FUNCTIONS

PETER SARNAK

ICERM NOV 2015

AUTOMORPHIC FORMS ON GL_n:

ALL KNOWN L-FUNCTIONS ARE (OR ARE EXPECTED TO BE) L-FUNCTIONS OF AUTOMORPHIC CUSP FORMS ON

$$G = GL_n.$$

$$H := L^2_{cusp}(G(\mathbb{Q})\backslash G(\mathbb{A}), \chi)$$

χ A DIRICHLET CENTRAL CHARACTER.

- DECOMPOSE THE REGULAR REPRESENTATION OF $G(\mathbb{A})$ ON H INTO (COUNTABLY MANY) IRREDUCIBLES OF $G(\mathbb{A})$; H_π.
- EACH π IS A CUSPIDAL AUTOMORPHIC FORM (REPRESENTATION).

$$\pi \cong \bigotimes_{v} \pi_v \quad , v = \infty \text{ OR } v = p$$

$$\pi_v \in \widehat{G(\mathbb{Q}_v)}_{unit}$$ AND UNRAMIFIED FOR v LARGE

LET $AUT(G)$ DENOTE THE SET OF SUCH π'S.

<u>RAMANUJAN</u> <u>CONJECTURE</u>:

$$\pi_v \in \widehat{G(\mathbb{Q}_v)}_{temp} \quad \text{FOR ALL } v.$$

$\widehat{G(\mathbb{Q}_v)}_{temp}$ COMES WITH ITS FELL TOPOLOGY AND THE UNRAMIFIED REPRESENTATIONS; $T(\mathbb{Q}_v)$, ARE AN OPEN/COMACT SUBSET $(v \neq \infty)$.

• LET $$T = \prod_{v} \widehat{G(\mathbb{Q}_v)}_{temp}$$

BE THE RESTRICTED PRODUCT W.R.T THE $T(\mathbb{Q}_v)$'S.

• EACH $\pi \in AUT(G)$ DETERMINES A POINT t_π IN T AND

$$\pi \longmapsto t_\pi$$ IS INJECTIVE AND DISCRETE.

(multiplicity one, J-S-PS, MORENO, BRUMLEY)

<u>NOTE:</u> IF WE PUT THE PRODUCT TOPOLOGY ON T THEN ONE CAN SHOW THAT $\pi \to t_\pi$ IS DENSE.

<u>LANDSCAPE</u> <u>TO BE COMPUTED:</u>

(1) TO FIND SEPARATING OPEN SETS U IN T CONTAINING EXACTLY ONE t_π AND THEN FOR EACH SUCH A DECREASING SEQUENCE OF NBH'S OF t_π S.T. $U \supset U_1 \supset U_2 \dots \; ; \; \bigcap U_j = t_\pi$

(2) IF π IS ALGEBRAIC (SAY IN THE SENSE OF CLOZEL) TO DETERMINE π_v EXACTLY FOR v UP TO SOME SIZE.

STANDARD L-FUNCTIONS, CONDUCTOR AND ROOT NUMBER

W.R.T. THE STANDARD REPR. OF G IN $GL_n(\mathbb{C})$

$L(s,\pi_v)^{-1}$ IS A POLYNOMIAL OF DEGREE n (AT MOST) IN v^{-s},
($v=\infty$ IT IS A PRODUCT OF n-GAMMA FUNCTIONS).

$$\Lambda(s,\pi) := \prod_v L(s,\pi_v)$$

$$\Lambda(1-s,\tilde{\pi}) = \varepsilon(\pi)\, N_\pi^{s-1/2}\, \Lambda(s,\pi)$$

$\tilde{\pi}$ IS THE CONTRAGREDIENT TO π,
$N_\pi \in \mathbb{N}$ IS THE CONDUCTOR OF π
$\varepsilon(\pi)$ THE ROOT NUMBER $(|\varepsilon(\pi)|=1)$.

ANALYTIC CONDUCTOR $C(\pi)$

$$\log c(\pi) := \log N_\pi + \sum_{j=1}^{n} \operatorname{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{1}{4}+\frac{\lambda_j(\pi_\infty)}{2}\right)\right)$$

WHERE $$L(s,\pi_\infty) = \prod_{j=1}^{n} \Gamma_{\mathbb{R}}\left(\frac{s+\lambda_j(\pi_\infty)}{2}\right)$$

(IWANIEC-S, RUBINSTEIN).

• $C(\pi)$ IS A NATURAL HEIGHT FUNCTION ON AUT(G).

$$M_n(X) = |\{\pi \in \mathrm{AUT}(G) : C(\pi) \leq X\}|$$

IS FINITE, AND IS AT MOST $\mathrm{Poly}_n(X)$ (BRUMLEY).

PROBLEM 1: PROVE AN ANALOGUE OF SCHANUEL

$$M_n(X) \sim A_n X^{B_n} \quad \text{as } X \to \infty.$$

(known for $n=1$, $n=2$ BRUMLEY-MILICEVIC).

• ASSUMING GRH THE POINTS $t_\pi \in T$ ARE VERY WELL SPACED, KNOWING THE FIRST $(\log C(\pi))^2$ π_v's APPROXIMATELY DETERMINES π.

COMPUTATIONAL LANDSCAPE

$n=1$: PRIMITIVE DIRICHLET CHARACTERS – WELL UNDERSTOOD.

$n=2$: FOR ALGEBRAIC FORMS WELL STUDIED (CREMONA, H. COHEN, W. STEIN ....)

AND THESE ARE WELL UNDERSTOOD EXCEPT FOR FINITE EVEN GALOIS REPRESENTATIONS.

- FOR TRANSCENDENTAL π'S

SOLVE THE EIGENVALUE PROBLEM WITH FOURIER EXPANSION (COLLOCATION)

HEJHAL, ...

USING THE TRACE FORMULA

GOLOVSHANSKI - SMORTOV, BOOKER - STROMBERGSSON ....

$n \geq 3$:

ALGEBRAIC π'S:

(•) $n = 3$ AND π'S CORRESPONDING TO THE COHOMOLOGY OF THE MANIFOLDS

$$X_N = \Gamma_N \backslash G(\mathbb{R}) / K \quad ,$$

Γ_N A CONGRUENCE SUBGROUP; A. ASH, ...

(•) FOR $n=4$ AND π'S WHICH COME FROM GSp_4 THERE IS A LOT OF WORK BRUMER, ... PARAMODULAR CONJECTURE.

· IN GENERAL IF π COMES FROM GEOMETRY AND IS NOT KNOWN TO CORRESPOND TO AN AUTOMORPHIC FORM, ONE CAN (AT LEAST IN PRINCIPLE) PROCEED BY USING KNOWN CASES OF FUNCTORIALITY (ARTHUR, ...) TO TRANSFER π TO A SHIMURA VARIETY WHERE ONE CAN ATTACH TO IT A GALOIS REPRESENTATION. COUPLED WITH THE ORIGINAL π ONE HAS TWO GALOIS REPRENTATIONS, WHICH IF THEY AGREE AT ENOUGH PLACES (IN TERMS OF THEIR CONDUCTORS) AGREE AT ALL PLACES (FALTINGS).

GENERAL π', NECESSARY CONDITIONS:

THE APPROXIMATE FUNCTIONAL EQN FOR $L(s, \pi)$ AT DIFFERENT S's, LEADS TO EQUATIONS FOR THE t_π's WHICH WHEN GIVEN A BOUND FOR $C(\pi)$ YIELDS REGIONS IN T WHICH PROVABLY FREE OF t_π's, AS WELL AS NBH's IN T WHICH ARE LIKELY TO CONTAIN A POINT t_π.

(BOOKER, BIAN, S.D. MILLER, FARMER-KOUTSOLATIS-LEUMURELL, ...)

· THIS IS AN EFFICIENT MEANS OF GETTING A FIRST APPROXMATION TO THE LANDSCAPE.

THE USE OF THE APPROXIMATE FUNCTIONAL EQUATION DOES NOT BY ITSELF PROVE THE EXISTENCE OF ANY π, OR L-FUNCTION FOR THAT MATTER.

TO DO SO ONE HAS TO GO TO THE SOURCE, NAMELY TO THE SPECTRAL THEORY OF $G(\mathbb{Q})\backslash G(\mathbb{A})$. THAT ONE CAN DO SO IN PRINCIPLE AT LEAST FOR π'S THAT ARE EVERYWHERE UNRAMIFIED WAS SHOWN BY MIN LEE (2015) "APPROXIMATE CONVERSE THEOREM".

ANOTHER WAY WHICH I THINK IS COMPUTATIONALLY MORE EFFICIENT IS TO USE THE TRACE FORMULA.

LAPID AND OTHERS HAVE SHOWN HOW TO USE ARTHUR'S TRACE FORMULA ANALYTICALLY AND IT IS TIME TO DO SO COMPUTATIONALLY.

- BASIC STEP IN PRINCIPLE IS TO FIND h_1, h_2 ON T, $h_1 \le \chi_U(t) \le h_2$.

$$\sum_{\pi \in AUT} \left(h_2(t_\pi) - h_1(t_\pi) \right) < 1 \quad (*)$$

SO THAT $\#\{\pi \in AUT(G) : t_\pi \in U\}$ (DETERMINED)

(*) IS COMPUTED BY THE TRACE FORMULA VIA OPTIMIZATIONS (SEE BELOW)

PROBLEM 2: GIVE A COMPUTATIONALLY EFFICIENT PROCEDURE TO COMPUTE THE LANDSCAPE. PERHAPS ORDERING THE π'S BY THEIR ANALYTIC CONDUCTOR.

COMPLEXITY OF COMPUTING ZEROS:

(REST IS JOINT WITH M. RUBINSTEIN)

GIVEN π AND ASSUMING THAT WE CAN COMPUTE π_v EFFICIENTLY (SAY IN POLY(LOG v) STEPS) WHAT IS THE COMPLEXITY FOR COMPUTING THE ZEROS OF $L(s,\pi)$ NEAR $s=\frac{1}{2}$?

TO BE CONCRETE LET

$$E: \; y^2 = x^3 + ax + b$$

BE AN ELLIPTIC CURVE / $\mathbb{Q}$, $a, b \in \mathbb{Z}$

THE DISCRIMINAT $D = D(E)$ IS SAY SQUARE-FREE.

WHAT IS THE COMPLEXITY FOR COMPUTING

(1) $\varepsilon(E)$ THE ROOT NUMBER

(2) THE RANK OF E (ASSUME BSD).

(3) THE ZEROS OF $L(s, E)$ NEAR $s = \frac{1}{2}$.

• NOTE THAT ONE CAN COMPUTE THE $a_E(p)$'s IN POLY(LOG p) STEPS (SCHOOF).

<u>RIEMANN'S GOLD STANDARD:</u>

USING THE APPROXIMATE FUNCTIONAL EQUATION (OR RIEMANN-SIEGEL) FOR ANY π FOR WHICH ONE COMPUTE π_v EFFICIENTLY, ONE CAN COMPUTE $L(s, \pi)$ FOR s NEAR $1/2$, IN $O_\varepsilon(C(\pi)^{1/2+\varepsilon})$ STEPS, AND AS ACCURATELY AS DESIRED.

$\Rightarrow$ The root number, rank and zeros near ½ can be computed in $N_E^{1/2+\epsilon}$ steps.

PROBLEM 3: TO BREAK THE SQUARE-ROOT BARRIER, IS THERE AN ALGORITHM TO COMPUTE THESE QUANTITIES IN N_E^{α} STEPS WITH $\alpha < 1/2$?

REMARK: IN THE t-ASPECT, EG FOR $\zeta(\frac{1}{2}+it)$ ONE CAN BREAK THE $C(t)^{1/2}$ BARRIER (SCHÖNAGE, HEATH-BROWN, ODLYZKO, HIARY : $\alpha = 4/13$, VISHE $\alpha = 7/16$ FOR $L(\frac{1}{2}+it,\pi)$, π ON GL_2 — t aspect).

• IN WHAT FOLLOWS WE ASSUME GRH.

WHAT CAN BE COMPUTED IN SUBEXPONENTIAL (IN $\log N_E$) TIME?

- FOR $0 \leq T$, LET $M_E(T)$ BE THE NUMBER OF ZEROS OF $L(s,E)$ IN THE SEGMENT $\left[\frac{1}{2}-iT, \frac{1}{2}+iT\right]$ COUNTED WITH MULTIPLICITIES.

"theorem" (not implemented yet):

There is a Las-Vegas algorithm which for $\alpha > 0$ computes

(i) $M_E(T_1) < M_E(T_2) \cdots < M_E(T_k)$ WHERE $0 \leq T_1 < T_2 \cdots < T_k$; $k \gg \exp\left(\frac{-1}{\alpha^2}\right) \frac{\log N_E}{2\pi}$

(ii) $\varepsilon(E)$ $\quad$ (= parity of $M_E(T_j)$)

IN N_E^{α} steps.

LAS-VEGAS MEANS THAT THE ALGORITHM IF IT WORKS GIVES A VERIFIABLY CORRECT ANSWER. KATZ-S CONJECTURES FOR THE DISTR^N OF LOW LYING ZEROS FOR THIS FAMILY IMPLY THAT THE ALGORITHM WILL WORK FOR MOST E'S AND WE BELIEVE ALL E'S ONCE NE IS LARGE.

THE METHOD USES THE EXPLICIT FORMULA FOR $L(s,E)$.

WITH "COMPLEXITY α" THIS ALLOWS US TO COMPUTE

$$\sum_j h(\gamma_j(E)) \; ; \quad \text{WHERE } \tfrac{1}{2} + i\gamma_j(E) \text{ ARE THE ZEROS OF } \Lambda(s,E)$$

FOR $h \in \mathcal{S}(\mathbb{R})$ WITH $\text{Support } \hat{h} \subset \left(-\frac{\alpha \log N_E}{2\pi}, \frac{\alpha \log N_E}{2\pi}\right)$

- NOTE THAT THE DENSITY OF ZEROS $\gamma_j(E)$ NEAR 0 IS $(\log N_E)/2\pi$.

- ONE LOCALIZES AND PERIODIZES THIS BAND LIMITED INVERSION PROBLEM LEADING TO:

M ODD INTEGER $\quad \left(M \approx \frac{\log N_E}{2\pi}\right)$

$M = 2k+1$, $A \in O(M)$ WITH EIGENVALUES

$$e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_k}, e^{-i\theta_1}, \ldots, e^{-i\theta_k}, \det A .$$

$= \{z_1, \ldots, z_M\}$, $|z_j| = 1$, $0 \le \theta_1 \le \ldots \le \theta_k \le \pi$.

WE ARE GIVEN THE (ELEMENTARY SYMMETRIC) POWER SUMS IN THE ROOTS

$$S_m = \sum_{j=1}^{M} z_j^m \quad \in \mathbb{R} \qquad \text{— (**)}$$

for $0 \leq m \leq \alpha M$.

PROBLEM 4: WHAT CAN ONE SAY ABOUT THE z_j's, $\det A$, ALLOWING Poly(M) COMPUTATIONS ~~AND~~ WITH THE INFORMATION (**), IE COMPLEXITY α?

IF $\quad P_A(x) = \det(xI - A) = x^M + a_1 x^{M-1} + \dots + a_M$

THE $\quad a_M = \det A, \; a_{M-\ell} = (\det A) a_\ell$.

- FROM NEWTON'S IDENTITIES WE CAN RECOVER a_m, $m \leq \alpha M$ FROM (**).
- IF $\alpha = 1/2$ THEN THIS ALLOWS US BY THE THE SELF-RECIPROCALITY TO RECOVER P_A AND ALL THE ROOTS, THAT IS RIEMANN'S GOLD STANDARD.
- IF $\alpha < 1/2$ THE SYSTEM IS UNDERDETERMINED.

- IN FACT IF THE θ_j's ARE EQUALLY SPACED (PICKET FENCE) AND $\alpha < 1/2$ THEN ONE CANNOT RECOVER INFORMATION ABOUT ANY INDIVIDUAL θ_j INCLUDING $\det A$.

- WHAT WE EXPLOIT ARE THE FLUCTUATIONS IN THE DISTRIBUTION OF THE ZEROS FROM BEING A PICKET FENCE, ALBEIT THAT THESE ARE SMALL DUE TO THE RIGIDITY OF THE ZEROS ACCORDING TO THE SYMMETRY TYPE $O(\infty)$, FOR TYPICAL $A \in O(M)$.

- OUR PROBLEM 4, IS REALLY ONE IN REAL (RANDOM) ALGEBRAIC GEOMETRY. OVER THE COMPLEX NUMBERS KNOWING αM OF THE COEFFICIENTS OF $P_A(x)$ TELLS US LITTLE ABOUT THE ZEROS (EXCEPT IF THERE ARE LARGE ONES). THE CONDITION $|z_j|=1$ IS A STRONG CONSTRAINT ON THE OTHER COEFF GIVEN THE FIRST αM OF THEM.

ONE IS REALLY STUDYING THE HAAR-INDUCED MEASURES ON THE LEVEL SETS

$$a_m(\theta) = b_m \quad , \quad m \leq \alpha M$$

IN THE M-TORUS.

· LIMITS: USING THIS ONE CAN SHOW THAT FOR A TYPICAL θ, ONE CANNOT WITH $\alpha < 1/2$ RESOLVE ALL THE ZEROS OF P_A TO ANY ACCURACY BETTER THAN $M^{-4/3}$ (RECALL $M \approx (\log N_E)/2\pi$). THIS USES J. VINSON'S THESIS WHICH GIVES THE MINIMAL SPACING FOR THE ZEROS OF A TYPICAL SUCH A.

THE ALGORITHM FOR $\mathcal{E}(E)$ IS SUBEXPONENTIAL IN N_E. IF N_E IS SQUARE-FREE THEN

$$\mathcal{E}(E) = \mu(N_E);$$ THE MOBIUS FUNCTION.

THAT IS WE HAVE A SUBEXPONENTIAL ALGORITH TO COMPUTE $\mu(N_E)$. THIS IS DONE WITHOUT FACTORING N_E !

(COMPUTING $\mu(N)$ IS BELIEVED TO BE AS HARD AS FACTORING N).

OUR ALGORITHM EXPLOITS COMPUTING $a_p(E)$ FOR SMALL p's (MUCH SMALLER THAN N_E) TO GAIN INFORMATION ABOUT THE PARITY OF THE NUMBER OF PLACES WHERE E HAS BAD REDUCTION.

• ONE CAN LET α GO TO 0 WITH N_E AND COMPARE WITH THE SPEED OF THE BEST FACTORING ALGORITHMS (THIS IS SIMILAR TO BOOKER-HIARY-KEATING'S ANALYTIC METHOD FOR DETERMINING IF N IS SQUARE-FREE).

• WE HAVE NOT AS YET OPTIMIZED OUR METHOD WITH $\alpha \downarrow 0$. OUR ENEMY IS THE STRONG SZEGO LIMIT THEOREM (JOHANSSEN-DEIFT) WHICH SHOWS THAT A POLY($\log N_E$) IS OUT OF REACH.