AN UNDERDETERMINED MOMENT PROBLEM FOR EIGENVALUES OF MATRICES IN CLASSICAL GROUPS AND ITS APPLICATION TO COMPUTING ROOT NUMBERS AND ZEROS OF L-FUNCTIONS.

PETER SARNAK

AROUND FROBENIUS DISTRIBUTIONS AND RELATED TOPICS III

OCT 2022

JOINT WITH MICHAEL RUBINSTEIN

AN UNDERDETERMINED MOMENT PROBLEM

$G = G_n = O(2n+1)$ COMPACT

μ_n THE HAAR PROB. MEASURE ON G_n.

$A \in G_n$ ITS EIGENVALUES ARE

$$\pm 1, e^{i\theta_1}, e^{-i\theta_1}, \ldots, e^{i\theta_n}, e^{-i\theta_n}$$

WHICH WE COLLECT AS

$$(\varepsilon, \theta_1, \ldots, \theta_n) \; ; \; 0 \le \theta_j \le \pi \; , \; \varepsilon = \pm 1 = \det A.$$

$j \ge 0$; $\quad S_j(A) := \text{TRACE}(A^j) = \varepsilon^j + 2 \sum_{\nu=1}^{n} \cos(j\theta_\nu)$.

- FOR $k \ge 1$ $\quad M_{k,n} : G_n \longrightarrow \mathbb{R}^k$

  THE MOMENT MAP; $M(A) = (S_1, \ldots, S_k) = y \in \mathbb{R}^k$.

- OUR INTEREST IS WHAT CAN WE SAY ABOUT $(\varepsilon, \theta_1, \ldots, \theta_n)$ GIVEN $y \in M_k(G_n)$.

FOR $k < n$ THE LEVEL SETS IN $(\varepsilon, \theta_1, \ldots, \theta_n)$ ARE POSITIVE DIMENSIONAL AND ARE SEMI-ALGEBRAIC SETS IN $\mathbb{R}^k$. THEIR SHAPE ALLOWS US TO RECOVER SOME QUANTITIES ASSOCIATED WITH $(\varepsilon, \theta_1, \ldots, \theta_n)$.

- THE $\mathcal{E}$-RECOVERABLE SET $R(\mathcal{E})$ IS THE SUBSET OF y's IN $M_k(G_n)$ FOR WHICH y DETERMINES $\mathcal{E}$.

FOR $y \in M_k(G_n)$ THE SUBSET $F(y)$ OF $[0,\pi]$ FOR WHICH NO $\mathcal{E}$ OR θ OF ANY A WITH $M_k(A) = y$. IS IN $F(y)$ IS CALLED THE y-FORBIDDEN SET. IT CONSISTS OF FINITELY MANY OPEN CONNECTED INTERVALS.

- THE F-RECOVERABLE SET $R(F)$ IS THE SET OF y's FOR WHICH $F(y)$ IS NOT EMPTY.

THE SUBSET OF t's IN $[0,\pi]$ FOR WHICH THE EXACT COUNT OF THE NUMBER OF $\mathcal{E}, \theta_j$'s IN $[0,t]$ IS DETERMINED BY y, IS CALLED THE EXACT COUNT SET DENOTED $N(y)$.

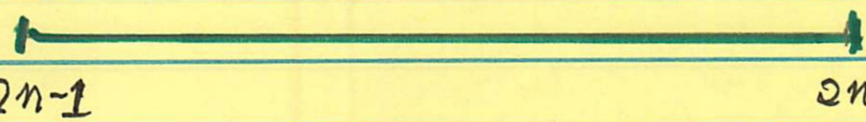
IT CONSISTS OF FINITELY MANY OF THE SUBINTERVALS OF $F(y)$.

- THE N-RECOVERABLE SET IS THE SET OF y's FOR WHICH $N(y) \neq \emptyset$ AND IS DENOTED $R(N)$.

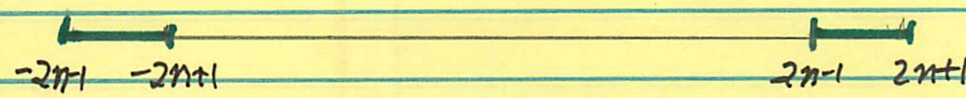
THE PUSH FORWARD OF μ_n ON G_n TO $M_k(G_n)$ GIVES A PROBABILITY MEASURE ON THE LATTER RELATIVE TO WHICH PROBABILITIES ARE MEASURED.

- FOR $k=1$, S_1 IS LINEAR IN $\cos\theta_j$ AND THE VARIOUS SETS ARE EASILY DETERMINED:

$M_1(G_n) =$

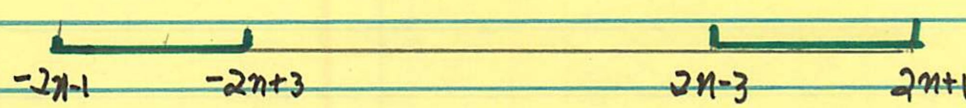


$R_{1,n}(E) =$



$R_{1,1}(F) = M_1(G_1)$

$R_{1,n}(F) =$



$n \geq 2$

$$R_{1,n}(E) = R_{1,n}(N)$$

$$\mathrm{PROB}(R_{1,1}(E)) = 0.18$$

$$\mathrm{PROB}(R_{1,n}(E)) \ll \exp(-\delta n \log n)$$

FOR $\delta > 0$

(FOLLOWS FROM JOHANSSON – COURTREAUT – LAMBERT SEE BELOW)

THRESHOLDS FOR RECOVERY ($n \to \infty$)

RANGE OF k, n	RECOVERY PROBABILITIES
$k \gg \frac{n}{\sqrt{\log n}}$	PROB(R(E)), PROB(R(F)), PROB(R(N)) ALL TEND TO 1. ALMOST SURE RECOVERY WITH A POLYNOMIAL TIME CERTIFICATE.
* $k \gg \sqrt{n}$ AND θ'S CHOSEN RANDOMLY INSTEAD OF AEG RANDOM	* ALMOST SURE RECOVERY OF THE ABOVE WITH A POLYNOMIAL TIME ALGORITHM.
$k = n^{\alpha}$ WITH $0 < \alpha \leq \frac{1}{3}$	$\text{PROB}(R(E)) \ll \exp(-n^{1-\alpha})$
FOR $\frac{1}{3} < \alpha < 1$	? BUT EXPECT THE SAME.
$\alpha = 0$; $k = n^{0}$ (BOUNDED)	$\text{PROB}(R(E)) \ll \exp(-\delta n \log n)$

THE MOMENT SETS

LET C_k BE THE CURVE

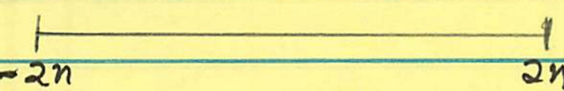
$$C_k: \left\{ \left(2\cos\theta, 2\cos 2\theta, \ldots, 2\cos k\theta\right) : 0 \le \theta \le \pi \right\} \subset \mathbb{R}^k$$

FOR $k \geq 1$, $n \geq 1$ THE BASIC MOMENT SET IS

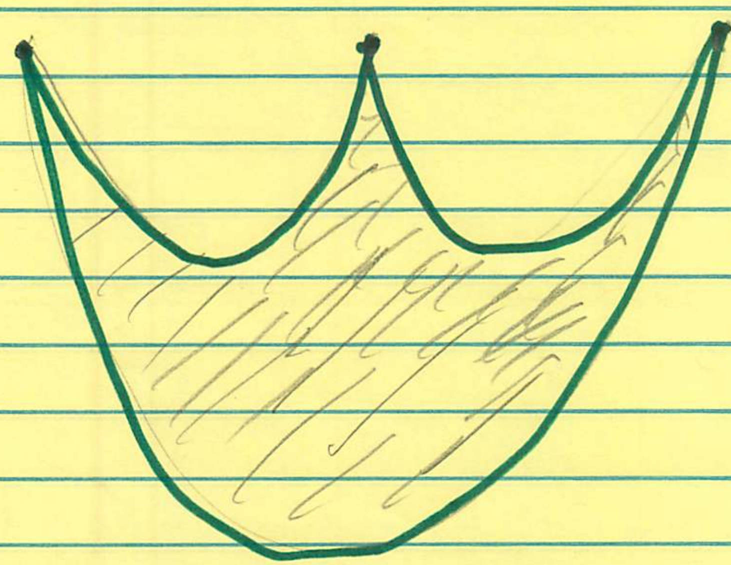
$$A(k,n) = C_k + C_k + \cdots + C_k \quad n\text{-times}.$$

$A(k,n)$ IS (REAL) SEMIALGEBRAIC IN $\mathbb{R}^k$

$k=1$: $A(1,n) =$



$k=2$, $n=2$ $A(2,2) =$



EQUATIONS FOR $A(2, n)$ ARE GIVEN IN
BIK – CZAPLINSKI – WAGERINGEL

2. Main results

Let $n \geq 3$ be a positive integer. Our first result describes the boundary of $\mathcal{A}_{3,n}$. We need this result in order to prove the Main Theorem. However, it also provides us with a piecewise parametrization, which is useful for rendering a visualization of $\mathcal{A}_{3,n}$. See Figure 1 for an example.

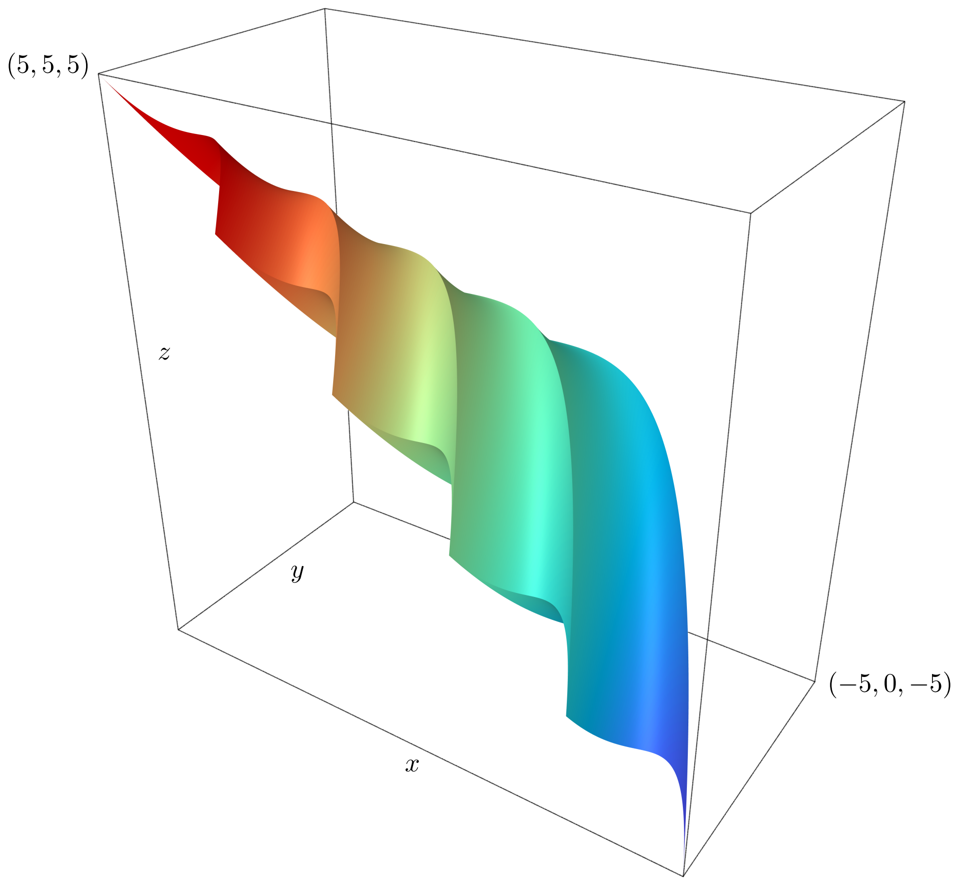


Figure 1. A rendering of the semi-algebraic set $\mathcal{A}_{3,5}$. Interactive 3D models of $\mathcal{A}_{3,n}$ are available at `https://mathsites.unibe.ch/bik/A3n.html` for $n = 1, \ldots, 20$.

Before we give the semi-algebraic description of $\mathcal{A}_{3,n}$, we first discuss the intuition behind it. As Figure 1 for $n = 5$ and the interactive 3D models for $n = 3, \ldots, 20$ demonstrate, the set $\mathcal{A}_{3,n}$ looks like an oyster with an upper and lower shell forming the boundary. We call these upper and lower shells $\mathcal{B}_n^+$ and $\mathcal{B}_n^-$ respectively. These two shells have identical projections to the (x, y)-plane, which we denote by $\mathcal{B}_n^\flat$, and both projection maps are one-to-one. This yields a first description of $\mathcal{A}_{3,n}$: for a point $(x, y, z) \in \mathbb{R}^3$ to lie in $\mathcal{A}_{3,n}$, it is necessary that (x, y) lies in $\mathcal{B}_n^\flat$. When this is the case, the point lies in $\mathcal{A}_{3,n}$ precisely when it lies below $\mathcal{B}_n^+$ and above $\mathcal{B}_n^-$.

FUNDAMENTAL COMPLEXITY PROBLEM:

IS THE RECOGNITION PROBLEM; "GIVEN $y \in \mathbb{R}^k$ IS $y \in A(k,n)$??" IN $\underline{P}$?

NB: FOR $n \leq k$ AND IN PARTICULAR FOR $n = k$ IT IS. THE COMPONENTS c_j's FOR $k = n$ ARE THE ROOTS OF THE CORRESPONDING POLYNOMIAL.

- $A(n,n)$ IS THE REGION IN $\mathbb{R}^n$ FOR WHICH THE ROOTS OF THE CORRESPONDING POLYNOMIAL ARE IN $[-2,2]$ AND IT HAS BEEN STUDIED IN CONNECTION WITH 'WEIL NUMBERS AND 'HONDA-TATE' THEORY (DIPIPPO-HOWE, HOWE-KEDLAYA ...)

- THE CASE OF INTEREST TO US IS $n > k$ WHICH IS THE UNDER DETERMINED PROBLEM: RECOVERING INFORMATION ABOUT THE SUMMANDS IN

$$c_1 + c_2 \dots + c_n = y \quad \in \mathbb{R}^k.$$

$$G_n = O(2n+1) \quad , \quad M_k : G_n \longrightarrow R^k$$

$$\text{IMAGE } M_k = M_k(G_n) = M_k^+(G_n) \cup M_k^-(G_n)$$

$$M_k^+(G_n) = A(k,n) + (1,1,\ldots,1)$$

$$M_k^-(G_n) = A(k,n) + (-1,1,-1,1,\ldots).$$

WITH THESE WE HAVE

$$R_{k,n}(\varepsilon) = \left(M_k^+(G_n) \cup M_k^-(G_n)\right) \setminus \left(M_k^+(G_n) \cap M_k^-(G_n)\right)$$

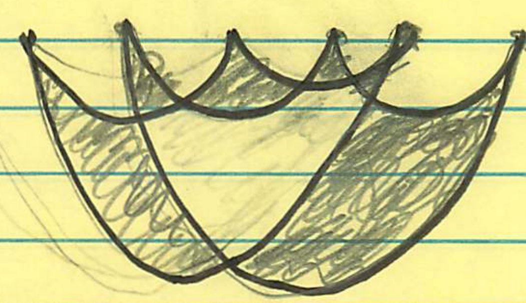
~~AND~~

$$R_{k,n}(F) = \left\{ y \in M_k(G_n) : y + C_k \cap \left[M_k(G_{n-1})\right]^{\text{COMP}} \neq \phi \right\}.$$

AND IF $y \in R_{k,n}(F)$ THEN $F(y)$ CONSISTS OF THE CONNECTED INTERVALS IN C_k FOR WHICH $y + C_k \notin M_k(G_{n-1})$.

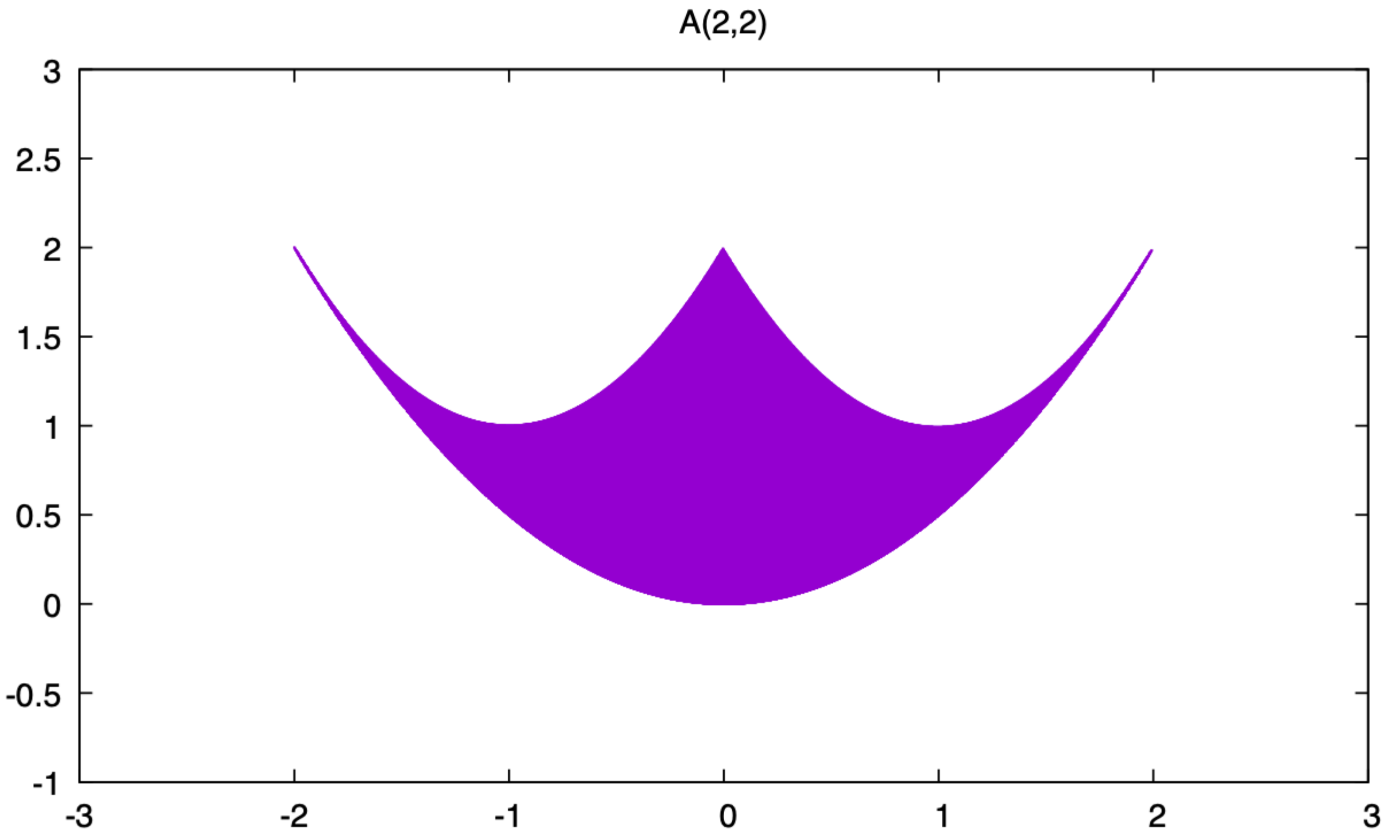
EG:

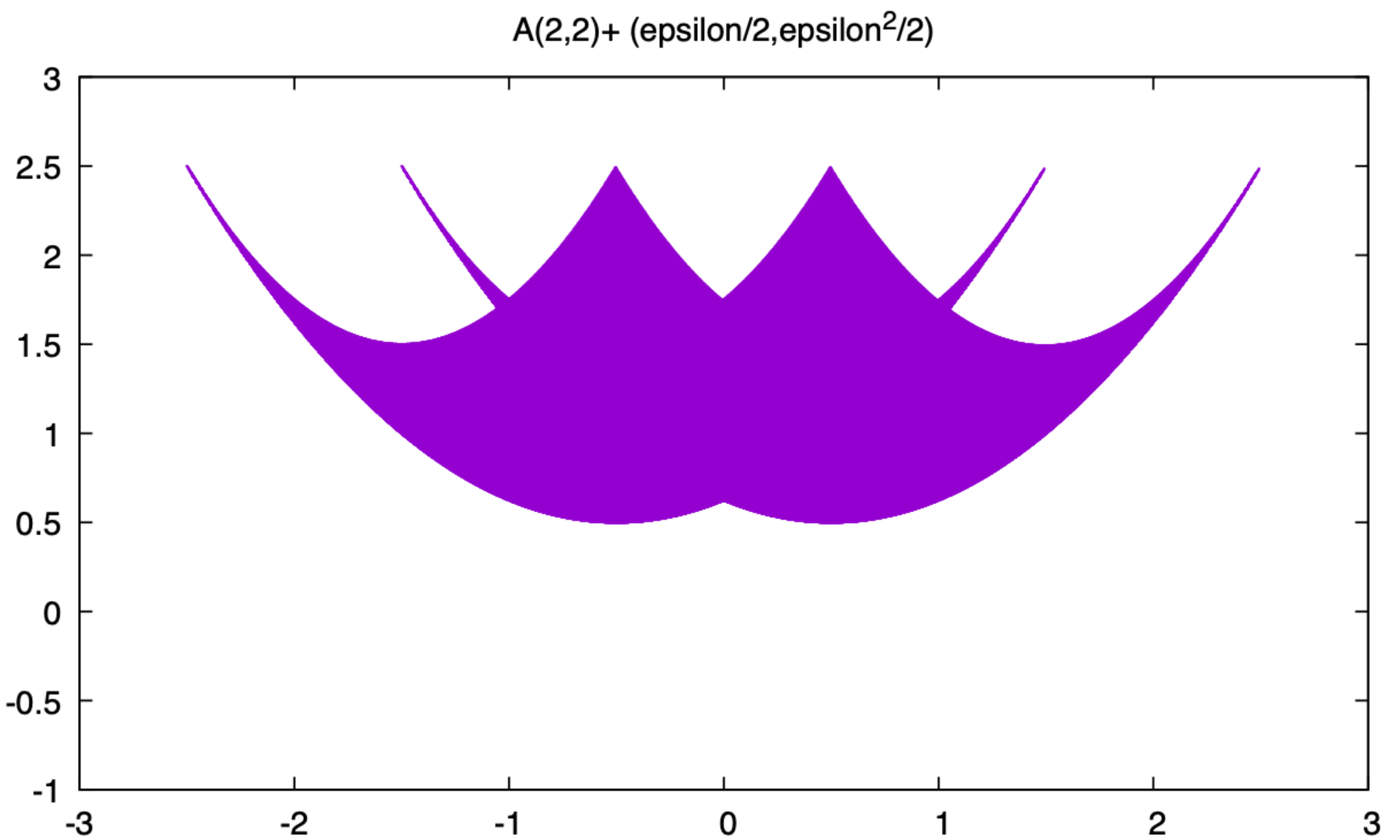
$$M_2(G_2) =$$



$R_{2,2}(\varepsilon)$ = SHADED REGION

$$\text{PROB}(R_{2,2}(\varepsilon)) = 0.37$$


A(2,2)
3
2.5
2
1.5
1
0.5
0
-0.5
-1
-3
-2
-1
0
1
2
3


A(2,2)+ (epsilon/2,epsilon^2/2)
3
2.5
2
1.5
1
0.5
0
-0.5
-1
-3
-2
-1
0
1
2
3

OUR ALGORITHM:

IT IS BASED ON LINEAR PROGRAMS FOR HYPERPLANES USED TO SEPARATE POINTS y FROM $A(k,n)$.

- USING A SINGLE HYPERPLANE IS TOO RESTRICTIVE BUT IS INSTRUCTIVE.
  IN THIS CASE ONE IS SEPARATING y FROM THE CONVEX HULL OF $A(k,n)$ AND THE LINEAR PROGRAM CAN BE SOLVED EXPLICITLY

  (CHEBYSHEV, MARKOV, HAMBURGER).

- STARTING WITH TWO HYPERPLANES AND AN ITERATION SCHEME TURNS OUT TO BE DECISIVE IN GIVING A NON-TRIVIAL LOWER BOUND FOR $F(y)$ ALMOST SURELY AS $n \to \infty$ IN THE RANGE $k \gg n/\sqrt{\log n}$.

THE ITERATION

GIVEN $y \in M_k(G_n)$

AT ν-TH STEP WE HAVE A LOWER APPROXIMATION $F_\nu(y)$ FOR $F(y)$.

FOR $J = [\alpha, \beta] \subset [0, \pi]$ RUN THE LINEAR PROGRAM IN $c_0, c_1, \ldots, c_k, b_0, b_1, \ldots, b_k$:

$$\min [U - L] := m_J$$

WHERE $U = (2n+1)c_0 + y_1 c_1 + \cdots + y_k c_k$; $L = (2n+1)b_0 + y_1 b_1 + \cdots + y_k b_k$

SUBJECT TO

$$b_0 + 2b_1 \cos\theta + \cdots + 2b_k \cos k\theta \leq \chi_J(\theta) \leq c_0 + 2c_1\cos\theta + \cdots + 2c_k \cos(k\theta)$$

FOR $\theta \notin F_\nu(y)$.

$\Rightarrow$ FOR ANY $A \in G_n$ WITH $M_k(A) = y$

$$L \leq \chi_J(\varepsilon) + 2\sum_{j=1}^{n} \chi_J(\theta_j) \leq U$$

- GIVEN ε THIS DETERMINES AN EXACT COUNT OF θ_j's IN J IF $\boxed{m_J < 2}$ (AND IF THE INTERVAL IS FREE OF ADMISSIBLE INTEGERS THEN THIS IS A CERTIFICATE THAT ε IS FORBIDDEN) ALSO THE ENDPOINTS α, β ARE IN $F(y)$.

$(\nu+1)$-ST STEP:

UPDATE $F_\nu(y)$ TO $F_{\nu+1}(y)$ WHICH CONSISTS OF $F_\nu(y)$ TOGETHER WITH THE NEWLY UNCOVERED α, β's IN $F(y)$ FROM THE ν-TH STEP.

- FOR $\nu = 1$ SET $F_1(y) = \phi$.

ITERATING WE ARRIVE AT AN INCREASING SEQUENCE OF LOWER APPROXIMATIONS TO $F(y)$, $N(y)$ AND $\mathcal{E}(y)$.

ANALYSIS OF THE ALGORITHM

RESULTS FROM RANDOM MATRIX THEORY SHOW THAT ASYMPTOTICALLY AS $n \to \infty$ THE RANDOM $A \in G_n$ HAS LARGE GAPS OF SIZE

$$\frac{\sqrt{\log n}}{n}$$

BETWEEN SOME OF ITS CONSECUTIVE θ_j'S.

THIS ALLOWS US TO ANALYSE THE ALGORITHM AND SHOW THAT ALREADY AFTER ONE ITERATION THE PROBABILITIES OF RECOVERING $\mathcal{E}$, F AND N ALL TEND TO 1, IN THE RANGE $R \gg n/\sqrt{\log n}$.

SOME RESULTS FROM RANDOM MATRIX THEORY

AS $n \to \infty$

(I) THE MINIMUM SPACING BETWEEN THE θ_j's OF A RANDOM $A \in G_n$ IS $\boxed{n^{-4/3}}$

(VINSON)

(II) THE MAXIMUM SPACING BETWEEN THE θ_j's OF A RANDOM $A \in G_n$ IS $\boxed{\frac{\sqrt{\log n}}{n}}$

(BOURGADE-BEN AROUS)

(III) STRONG SZEGO LIMIT THEOREM

(COURTREAUT-JOHANSSON)

FOR $\varepsilon = +, -$

$$X^{\varepsilon}_{n,k}(A) = \left(S_1(A), \frac{S_2(A)}{\sqrt{2}}, \dots, \frac{S_k}{\sqrt{k}}(A) \right); \text{ FOR } A \in O^{\varepsilon}(2n+1)$$

THEN

$$\text{TOTAL VARIATION}\left(X^{\varepsilon}_{n,k}, \text{NORMAL}\right) \ll \exp\left(-n^{1-\alpha}\right)$$

FOR $k = n^{\alpha}$ AND $0 \leq \alpha \leq 1/3$.

HERE NORMAL IS THE STANDARD CENTERED GAUSSIAN ON $\mathbb{R}^k$.

SAMPLE IMPLEMENTATIONS OF THE ALGORITHMS

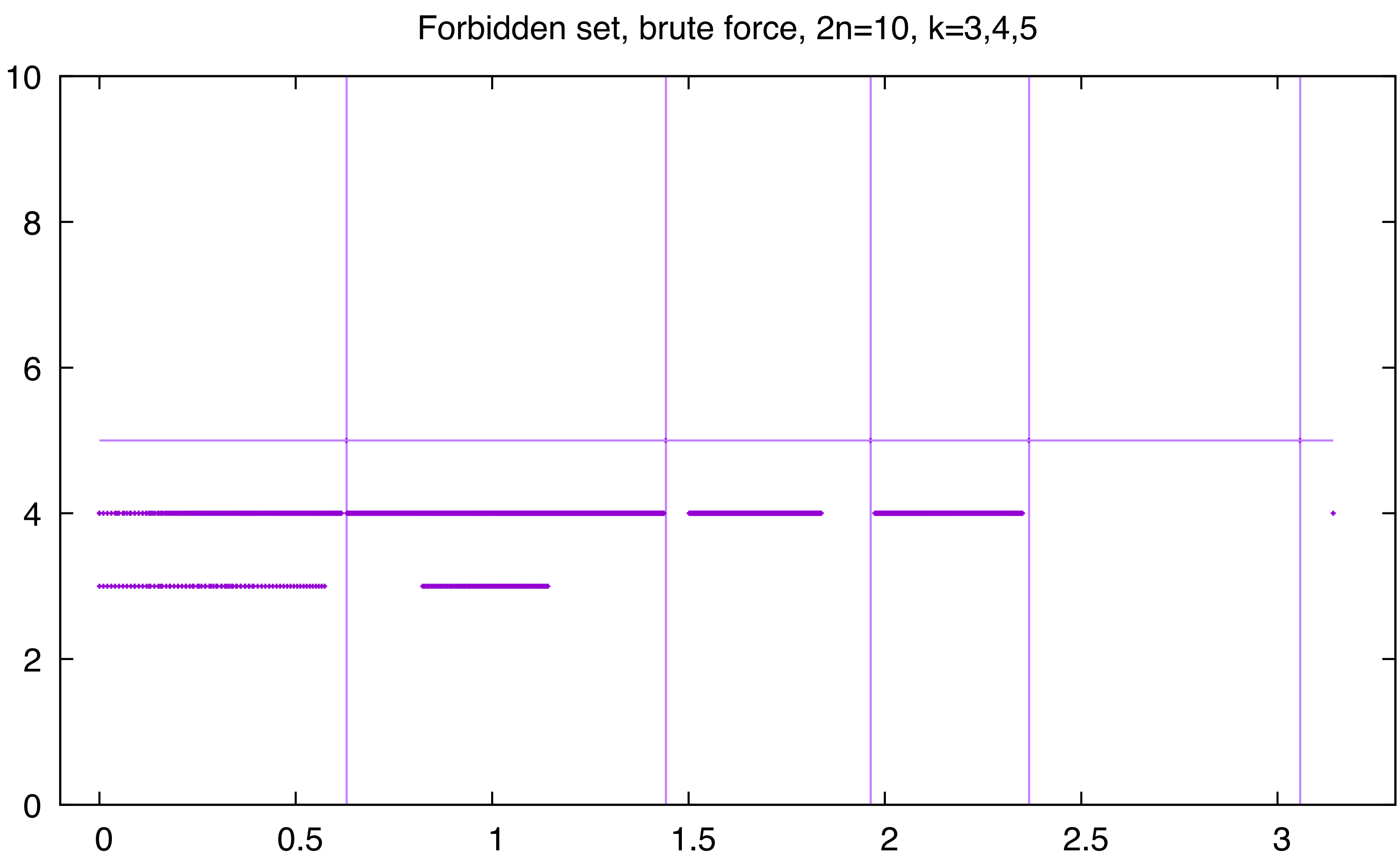
THE CASE $k=n$: $G = O(2n+1)$

IN THIS EXTREME CASE GIVEN ε, θ IS DETERMINED.
HENCE $(\varepsilon, \theta_1, \ldots, \theta_n) \to y$ IS EITHER 1-1 (IF $y \in R_{n,n}(\varepsilon)$) OR 2-TO 1.
WE MONTE CARLO' THESE PROBABILITIES

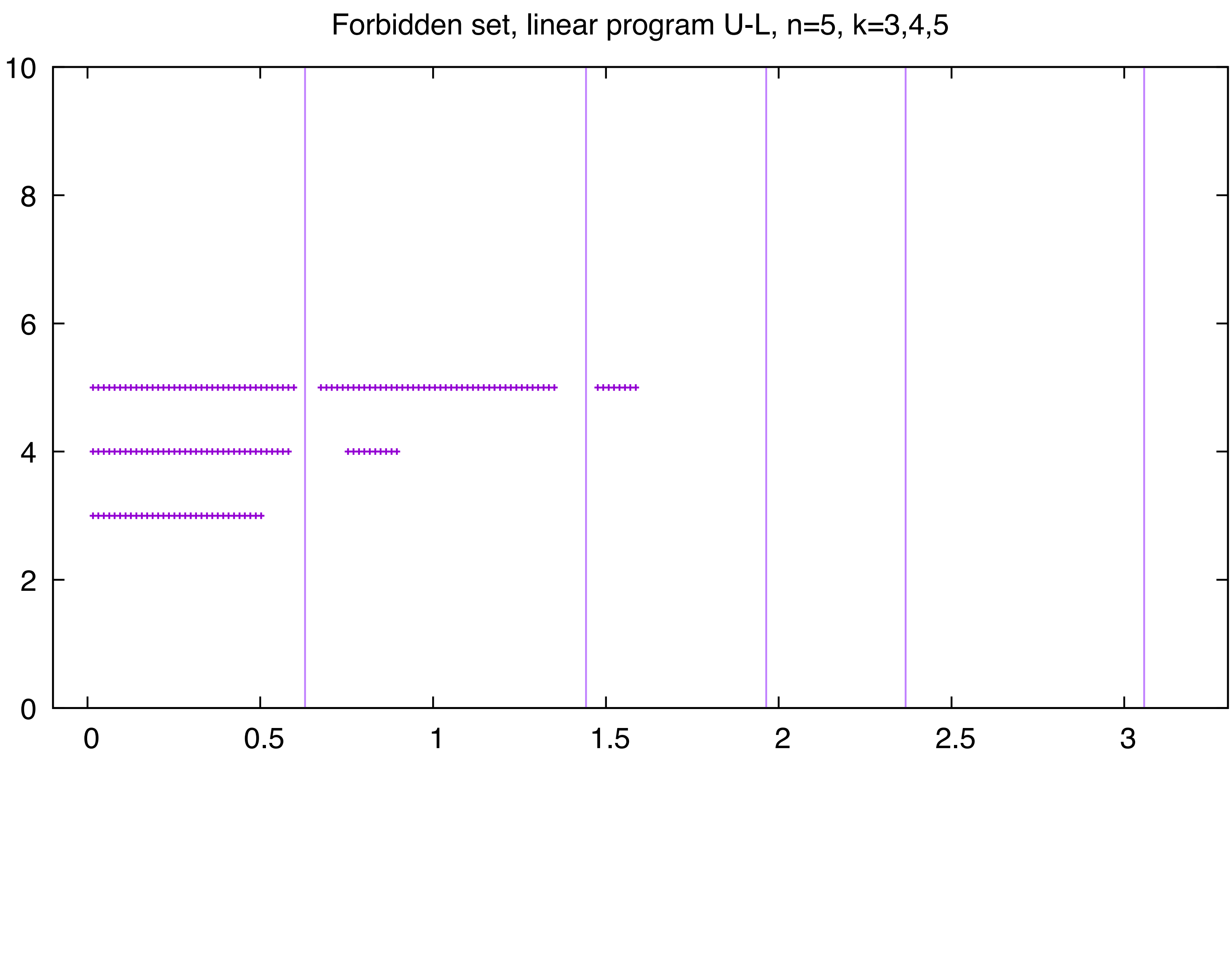
n	PROB$(R_{n,n}(\varepsilon))$; IE FULL RECOVERY
3	0.18
5	0.37
7	0.49
9	0.58
11	0.64
15	0.76
17	0.81
51	0.99

WE DETERMINED $F(y)$ FOR $G_n = SO(2n)$ FOR VARIOUS n's AND k's NEAR n USING THE BRUTE SEARCH REDUCTION.

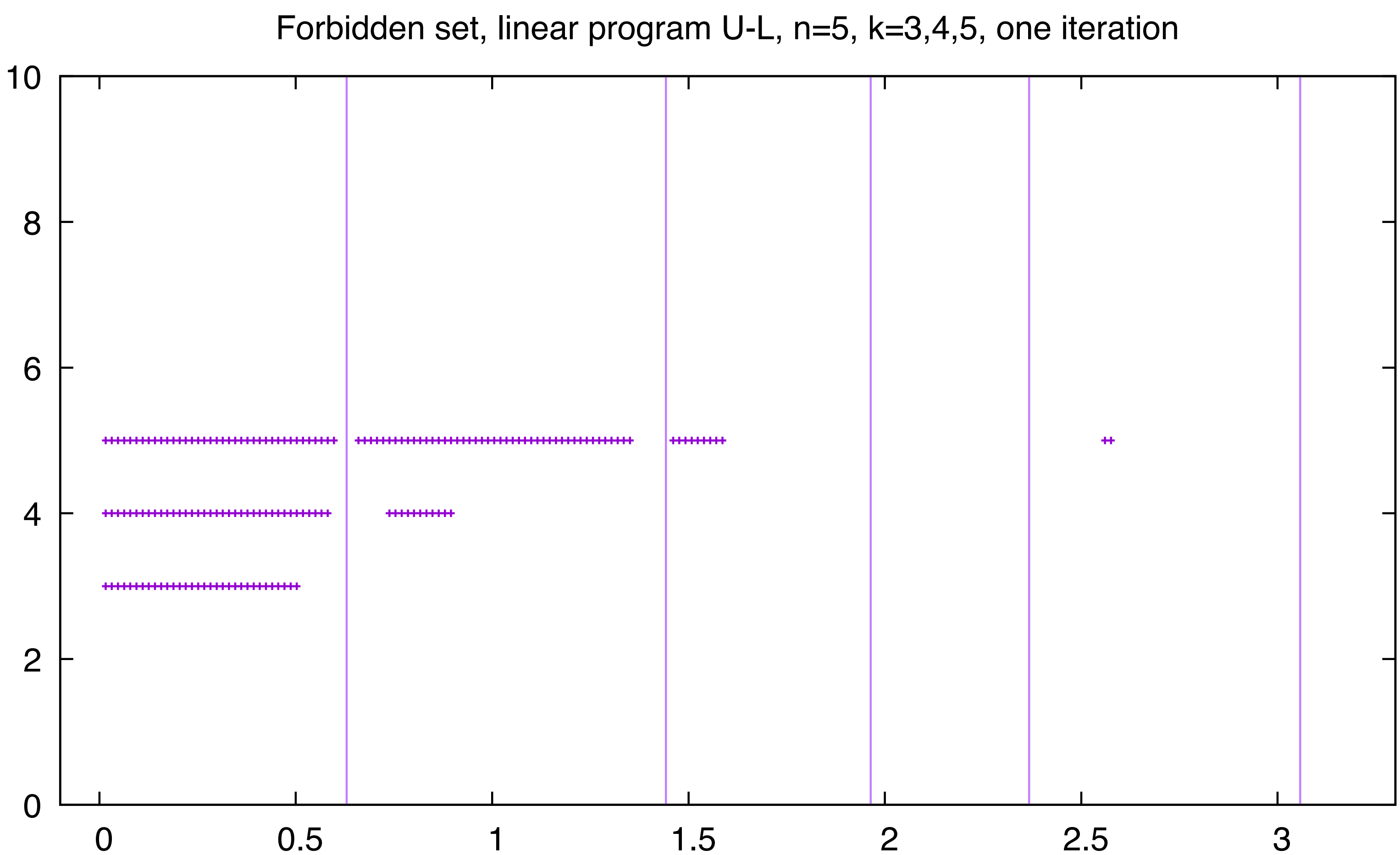
THESE WERE USED TO BENCHMARK OUR ITERATIVE APPROXIMATION $F_\infty(y)$ IN THESE CASES.

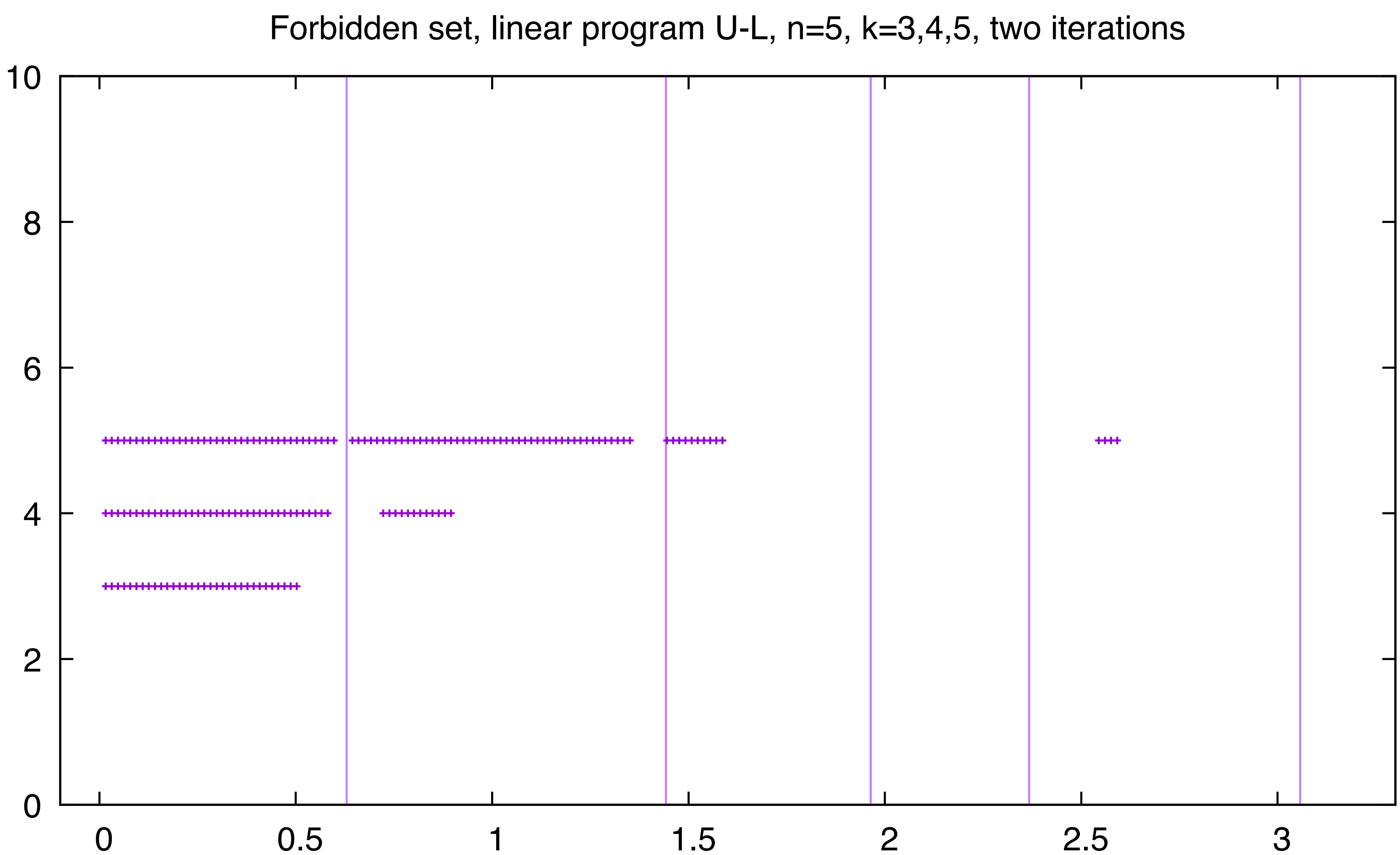


Forbidden set, brute force, 2n=10, k=3,4,5
10
8
6
4
2
0
0
0.5
1
1.5
2
2.5
3

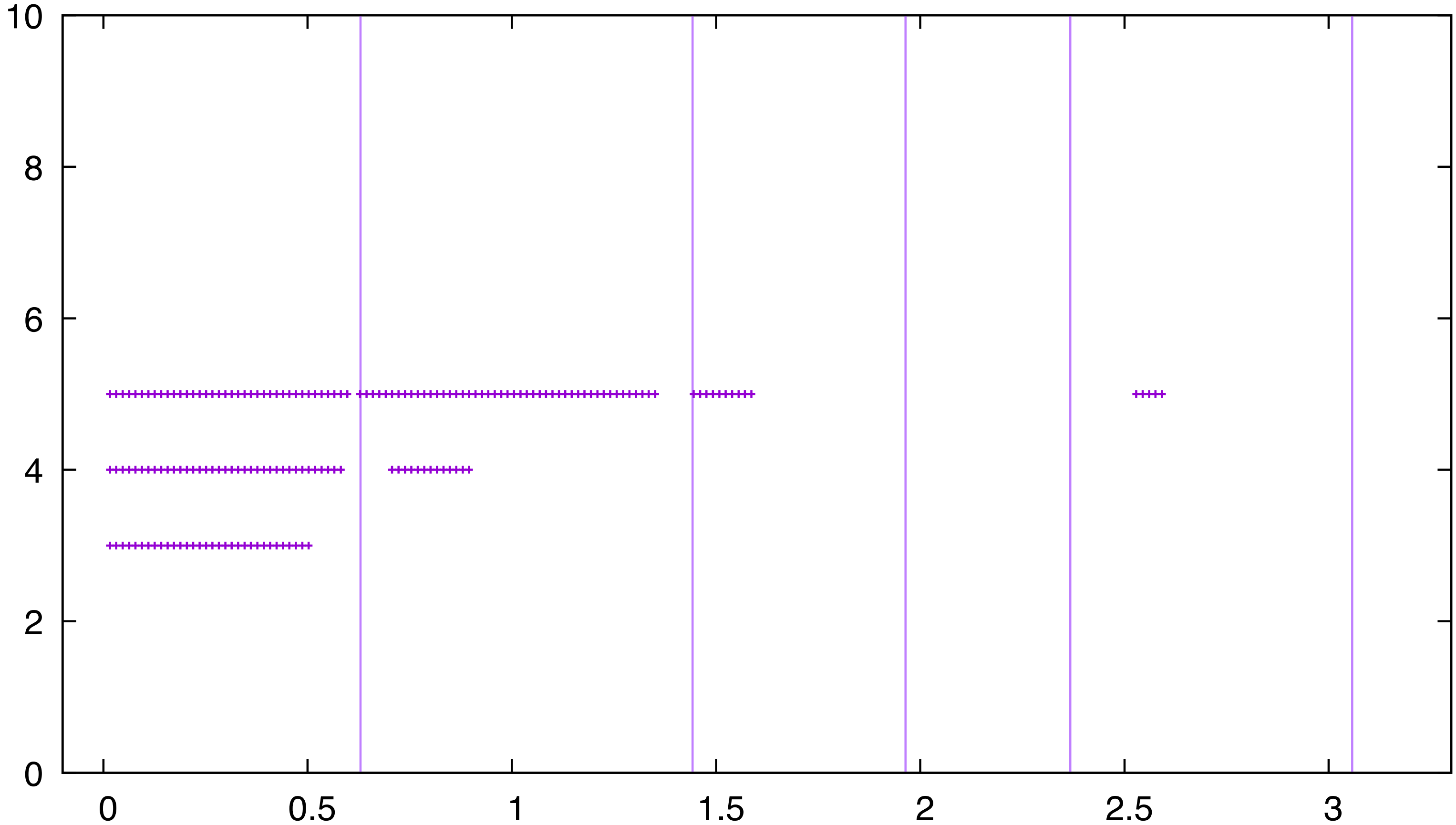


Forbidden set, linear program U-L, n=5, k=3,4,5
10
8
6
4
2
0
0
0.5
1
1.5
2
2.5
3

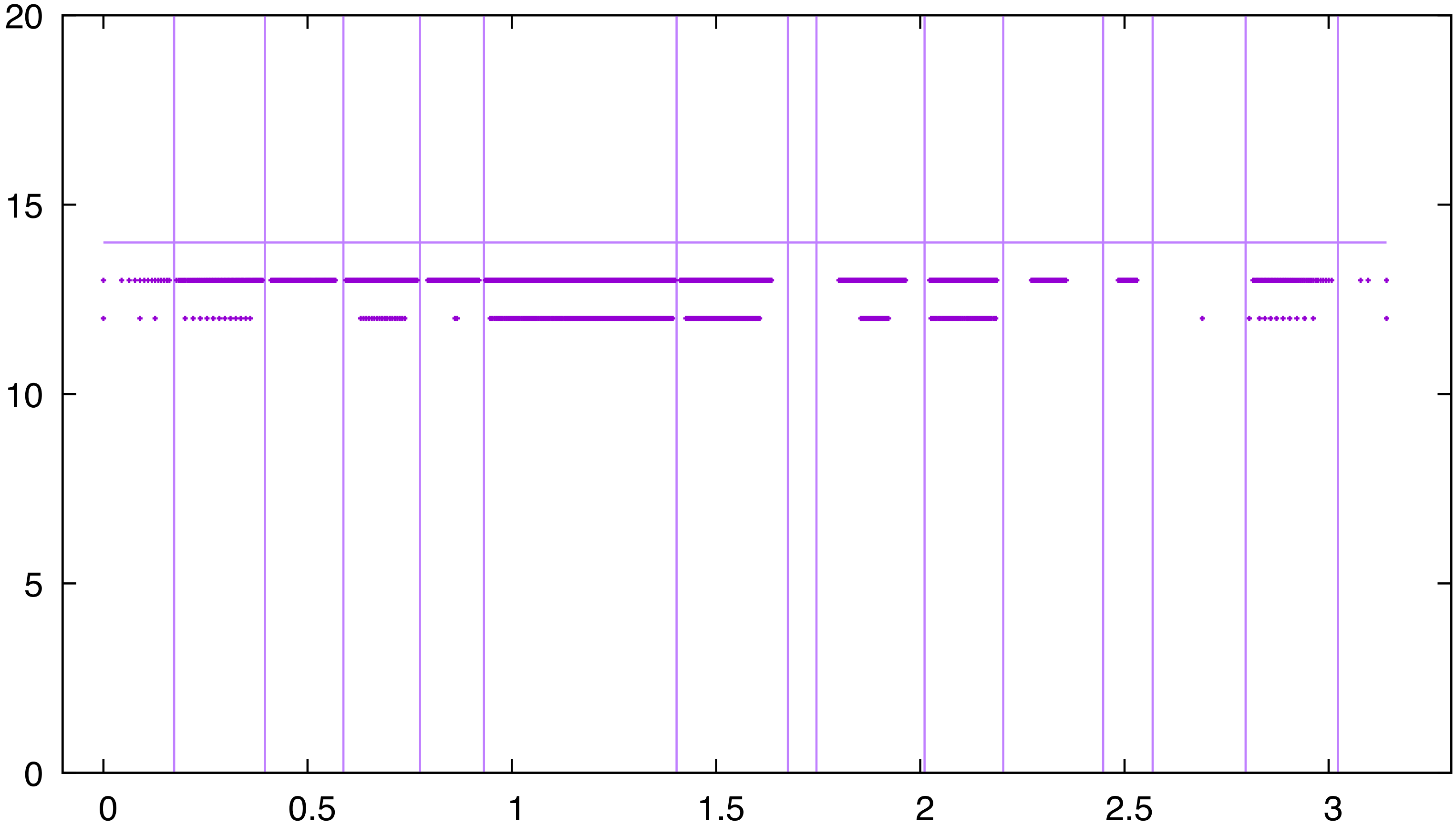

Forbidden set, linear program U-L, n=5, k=3,4,5, one iteration
10
8
6
4
2
0
0
0.5
1
1.5
2
2.5
3

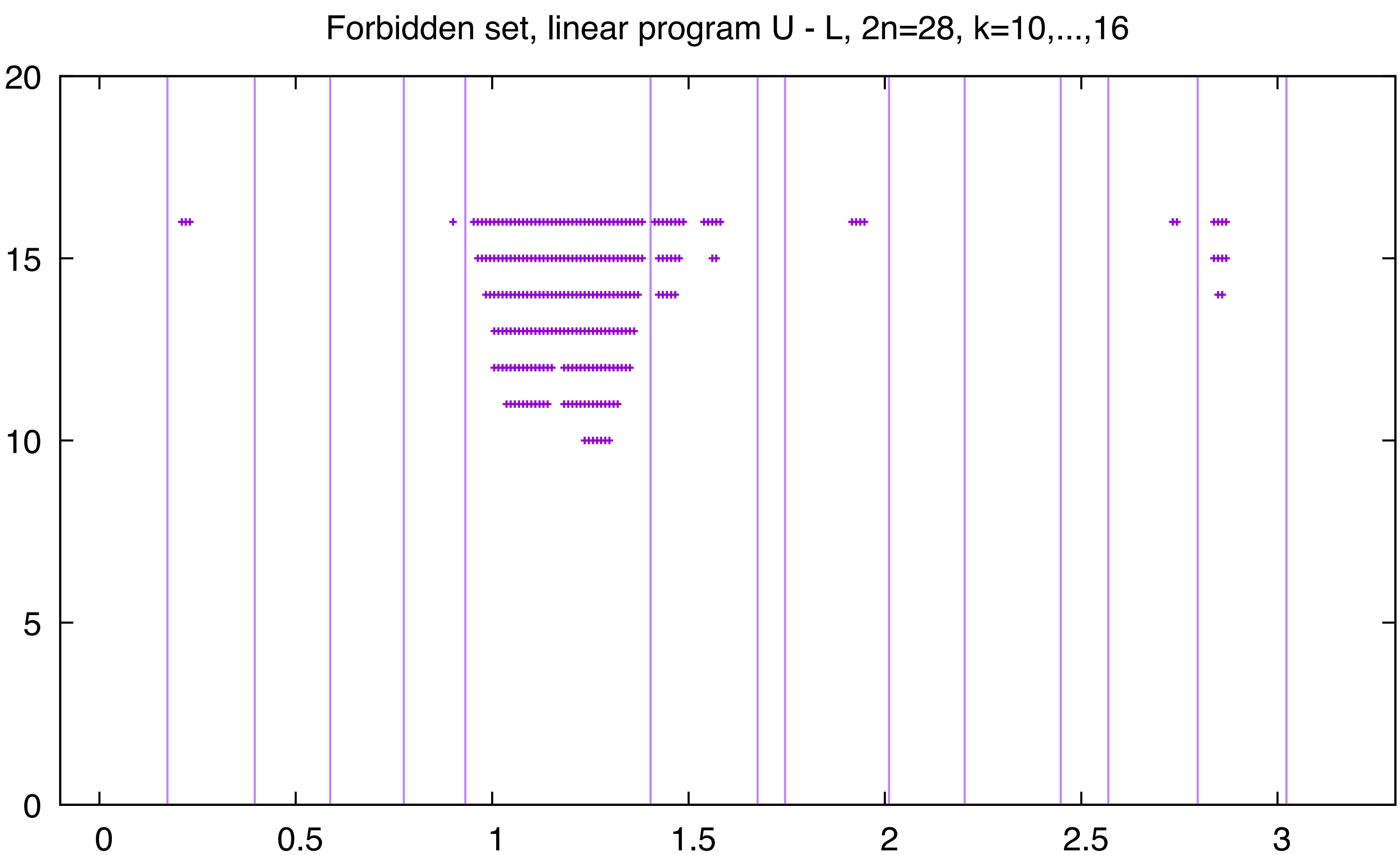

Forbidden set, linear program U-L, n=5, k=3,4,5, two iterations
10
8
6
4
2
0
0
0.5
1
1.5
2
2.5
3

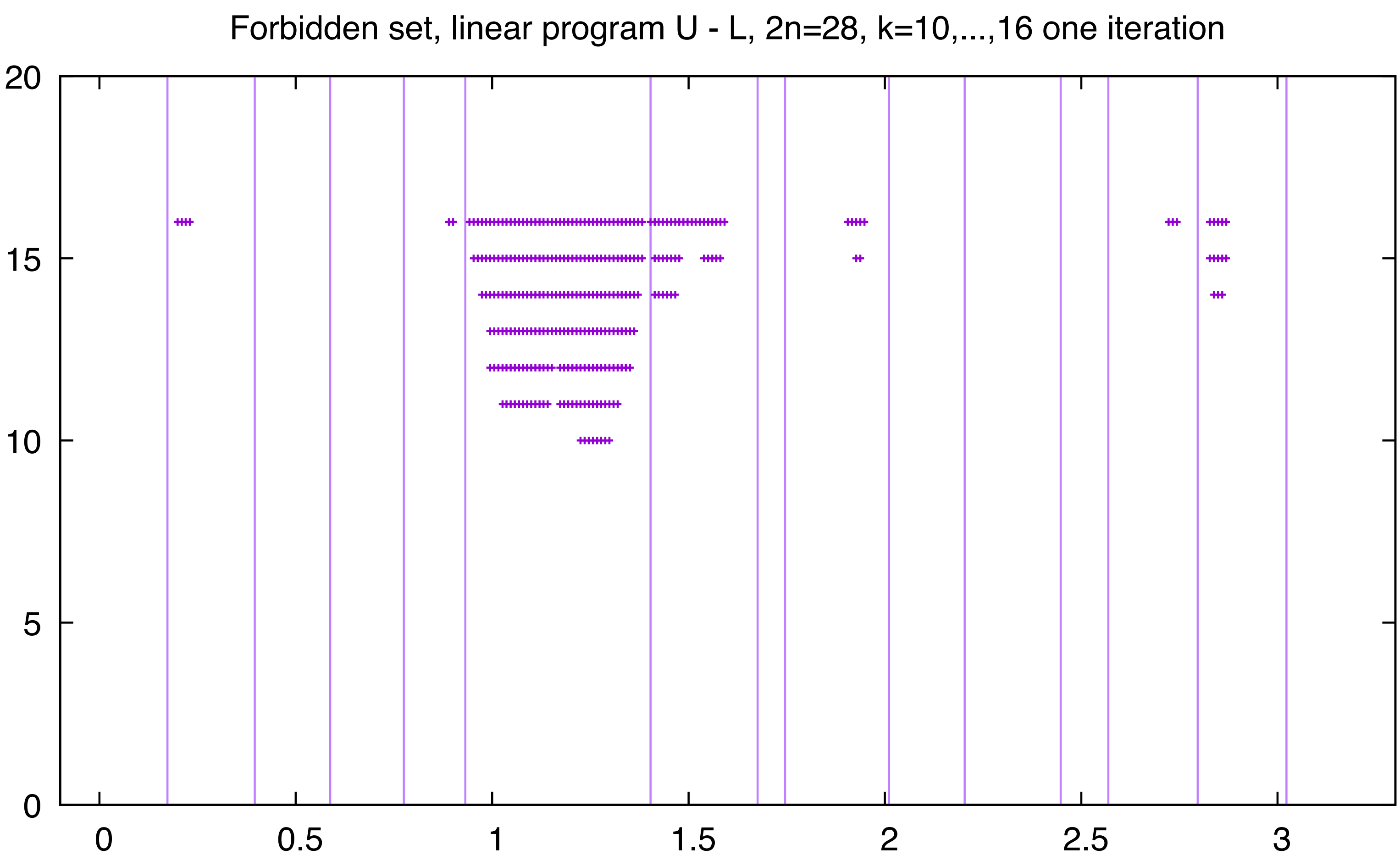
Forbidden set, linear program U-L, n=5, k=3,4,5, three iterations

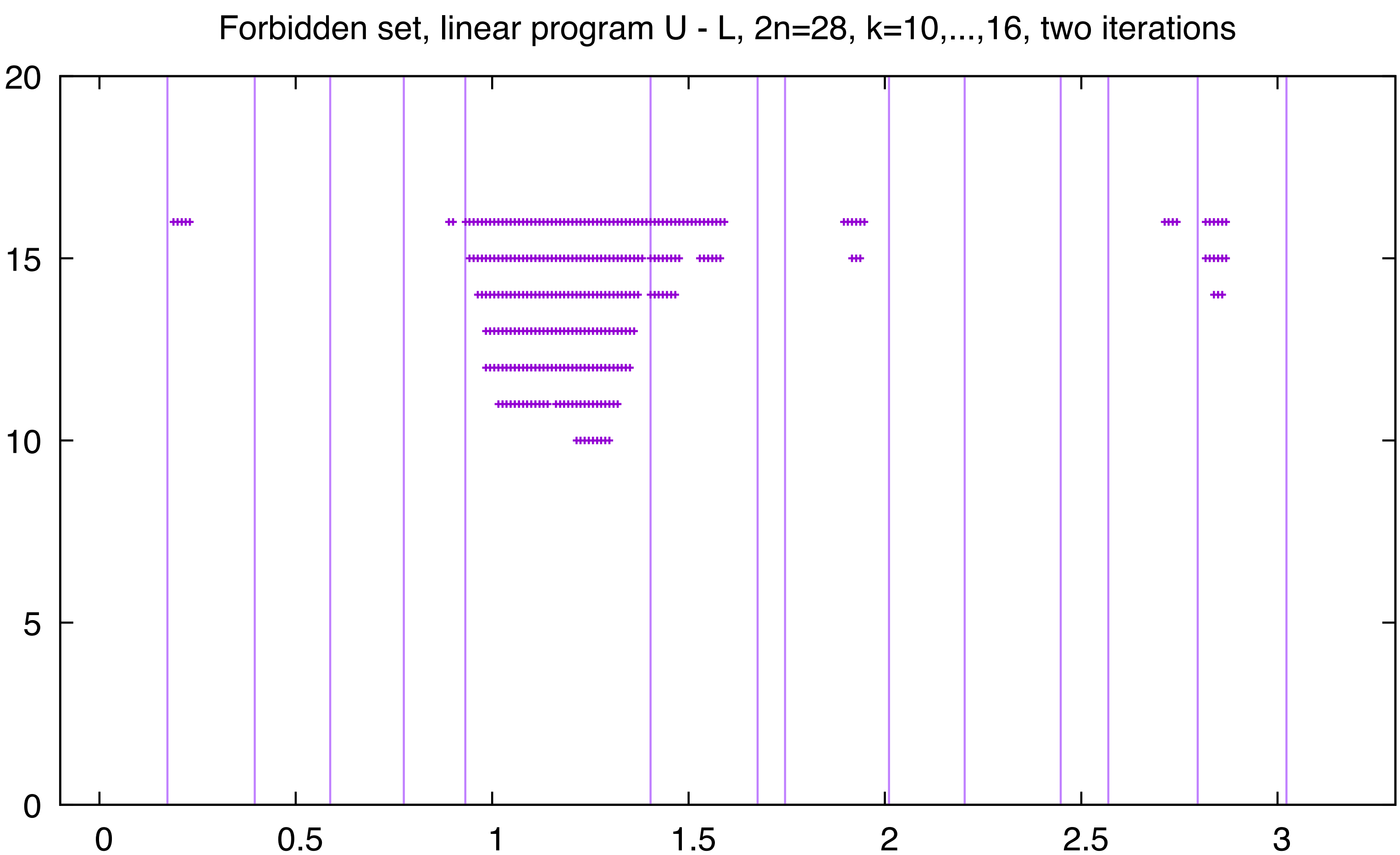


Forbidden set, brute force, 2n=28, k=12,13,14




Forbidden set, linear program U - L, 2n=28, k=10,...,16
20
15
10
5
0
0
0.5
1
1.5
2
2.5
3


Forbidden set, linear program U - L, 2n=28, k=10,...,16 one iteration
0
5
10
15
20
0
0.5
1
1.5
2
2.5
3


Forbidden set, linear program U - L, 2n=28, k=10,...,16, two iterations
20
15
10
5
0
0
0.5
1
1.5
2
2.5
3

ROOT NUMBERS AND ZEROS OF L-FUNCTIONS

$L(s,\pi)$ A SELF-DUAL AUTOMORPHIC L-FUNCTION OF DEGREE ν COMING FROM GEOMETRY (HASSE-WEIL TYPE EG ELLIPTIC CURVE $/\mathbb{Q}$)

- FOR PRIMES p THE LOCAL ZETA FACTOR $L(s,\pi_p)$ THAT IS "$a_p(\pi)$" CAN BE COMPUTED IN POLY$(\log p)$ STEPS (FOR OUR ASYMPTOTIC RESULTS POLY IN p ALSO SUFFICES!)

- WE ASSUME THAT WE KNOW THE CONDUCTOR $Q(\pi)$ OF π, BUT NOT THE GLOBAL ROOT NUMBER $\varepsilon(\pi) = \pm 1$ (WHICH CAN BE COMPUTED ON FACTORING $Q(\pi)$)

<u>NB:</u> ASSUMING THE RIEMANN HYPOTHESIS, WHICH WE DO FROM NOW ON; THE $a_p(\pi)$'S FOR $p \ll (\log Q(\pi))^2$ DETERMINE π AND HENCE ALSO $\varepsilon(\pi)$ AND THE ZEROS $\frac{1}{2}+i\gamma_\pi$ OF $L(s,\pi)$.

- THE PROBLEM IS WHAT CAN ONE COMPUTE EFFICIENTLY FROM THE $a_p(\pi)$'S.

RIEMANN'S GOLD STANDARD: SQUARE ROOT OF CONDUCTOR

THE "APPROXIMATE FUNCTIONAL EQUATION" SHOWS THAT IF WE KNOW $\mathcal{E}(\pi)$ WE CAN COMPUTE THE ZEROS OF $L(s,\pi)$ TO ANY ACCURACY IN

$$O\left(Q(\pi)^{1/2+o(1)} \right) \quad \text{STEPS.}$$

• CAN ONE DO BETTER AND RECOVER INFORMATION IN $Q(\pi)^{o(1)}$ STEPS ?
(IE SUBEXPONENTIAL IN $\log Q(\pi)$).

THE IDEA IS TO USE THE EXPLICIT FORMULA (RIEMANN-GUINAND-WEIL)

NOTE: THE EXPLICIT FORMULA IS DERIVED FROM THE LOGARITHMIC DERIVATIVE OF $L(s,\pi)$ SO IS FREE OF $\mathcal{E}(\pi)$ AND INVOLES ONLY THE $a_p(\pi)$'S .

IT IS A FOURIER TRASFORM DUALITY INVOLVING

- $Q(\pi)$ AND THE $a_p(\pi)$'s ON ONE SIDE
- THE ZEROS $\frac{1}{2} + i\,\gamma_\pi$ ON THE OTHER.

THE LOCAL DENSITY OF THE ZEROS IS

$$\log Q(\pi)$$

LOG OF THE CONDUCTOR!

GIVEN SAY $K = Q(\pi)^{\alpha/2}$ OF THE $a_p(\pi)$'s THE DETERMINATION OF THE ZEROS REDUCES TO OUR UNDERDETERMINED MOMENT PROBLEM WITH

$$2n = \log Q(\pi)$$

AND $k = \alpha n$ MOMENTS.

SO RIEMANN'S GOLD STANDARD $\alpha = 1 + o(1)$ REDUCES TO $k = n + 1$ WHEN WE RECOVER EVERYTHING EFFICIENTLY !

THE LINEAR PROGRAM ITERATION PROCEDURE APPLIES EQUALLY WELL IN THIS SETTING AND LEADS TO:

- AN ASYMPTOTIC SUBEXPONENTIAL IN $\log Q(\pi)$ ALGORITHM TO COMPUTE $\mathcal{E}(\pi)$ AND THE EXACT COUNT SET FOR t's

$$N(t) = \#\{\gamma_\pi \in [-t, t]\}$$

WHICH SUCCEEDS ALMOST SURELY IN ANY FAMILY.

- IF THE ABOVE FAILS TO GIVE $\mathcal{E}(\pi)$ THEN BY TWISTING π BY RANDOM QUADRATIC CHARACTERS χ_D; $\mathcal{E}(\pi \otimes \chi_D)$ CAN BE COMPUTED RAPIDLY IN TERMS OF $\mathcal{E}(\pi)$ AND RUNNING THE ABOVE FOR $L(s, \pi \times \chi_D)$ FOR A FEW χ_D's WILL QUICKLY YIELD $\mathcal{E}(\pi)$.

IN A FOLLOW-UP PAPER WE ARE IMPLEMENTING THE ALGORITHM FOR ELLIPTIC CURVES $E/\mathbb{Q}$.

TO DETERMINE THE CONDUCTOR $Q(E)$ ONE COMPUTES THE DISCRIMINANT OF E IN A WEISTRASS AFFINE MODEL. TO GET THE SQUARE-FREE PART OF D (AND THE CONDUCTOR) ONE CAN USE THE

- BOOKER – HIARY – KEATING ALGORITHM WHICH DETECTS SQUARE-FREE NUMBERS:

IT IS SIMILARLY BASED ON THE EXPLICIT FORMULA FOR DIRICHLET L-FUNCTIONS AND LINEAR PROGRAMS AND SAMPLING BY TWISTING (ALL WITHOUT FACTORING THE GIVEN NUMBER!)

THE UNDERDETERMINED MOMENT PROBLEM HAS TAUGHT US A COUPLE OF BASIC FEATURES IN CONNECTION WITH THE USE OF THE EXPLICIT FORMULA TO COMPUTE $\mathcal{E}$ AND ZEROS

(1). THAT WHILE THE ALGORITHM IS SUBEXPONENTIAL IN $\log Q(\pi)$ AS FAR AS COMPUTING $\mathcal{E}(\pi)$ IT GETS STUCK THERE JUST LIKE FACTORING ALGORITHMS DO AND THE REASON IS THE RIGIDITY OF THE EIGENVALUES OF RANDOM MATRICES

(2) ASYMPTOTICALLY IN n THE ALGORITHMS ARE FAST ~~M~~; BUT TO APPLY THESE FOR FEASIBLE Q'S ONE NEEDS THE THEORY FOR MODERATE n'S WHICH THE RUNS FOR G_n YIELD.