The How and Why of Partial Period Matrices

J. Wolper

AMS Special Session, Boulder

Outline

The Information-Theoretic Schottky and Torelli Problems

Using Partial Period Matrices

Constructing Partial Period Matrices

Point Clouds and Period Matrices

Acknowledgments, etc

- Many applications of algebraic curves in coding and cryptography
- What about using ideas from coding and cryptography (*i.e.* information theory) to study curves?
- Do information–theoretic properties of periods of curves “look different" from properties of general Abelian Varieties?
- Working analytically, over $\mathbb{C}$
- Primarily interesting for *very large* genus

Information Theoretic Schottky Problem I

- Alice wants to tell Bob about a compact Riemann Surface of genus g
- Alice knows that the moduli space has dimension $3g-3$
- But she sends Bob the whole period matrix, size $\infty^{g(g+1)/2}$
- Much more data than information content
- Can she do better?
- This is the *Information Theoretic Schottky Problem*

Information Theoretic Schottky Problem II

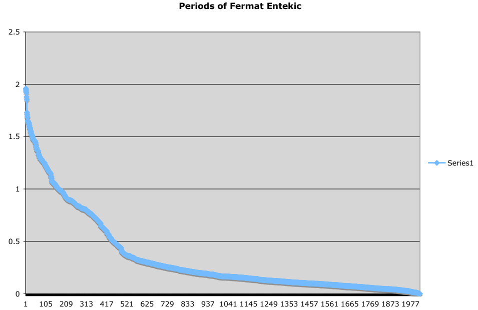
- Eve overhears Alice and Bob discuss a large symmetric matrix with positive definite imaginary part
- *Is it a period matrix?*
- *Is it a period matrix of a hyperelliptic curve?*

Information Theoretic Torelli Problem

- Bob wants to do something with the curve
- *eg,* find its automorphism group, decide if it is hyperelliptic, solve a K–P equation, . . .
- The way we do things with Torelli's Theorem is using Riemann's θ–function
- What if the period matrix he received is corrupted by noise?
- What if he only knows part of the period matrix?
- This is the *Information Theoretic Torelli Problem*

Compressibility

Coefficients of compressible or sparse signals (any basis) have a characteristic shape



[computed by Maple]

Partial Period Matrices

- What good is part of a period matrix?
- *THEOREM [Rauch, 1955]* Some sets of $3g - 3$ periods form moduli.
- *THEOREM [W–, 2012]* For a smooth plane curve, four columns suffice.
- *THEOREM [W–, 2012]* After random change of basis of $H^{(1,0)}$, first three columns suffice (whp).
- (Note that due to symmetry this constitutes $3g - 3$ entries)

Constructing Partial Period Matrices

- When and why would one only have part of a period matrix?
- • Incomplete knowledge of the differentials
- • Incomplete knowledge of the cycles
- • Desire to avoid computing all those integrals. . .

- Can one recover the period matrix for a curve from a point cloud ($=$ large sample of points?)
- Likely tool: *Persistent Homology*
- Construct a sequence of simplicial complexes from the point cloud governed by a size parameter t
- Many spurious cycles for small and large values of t, but those that *persist* more likely to represent cycles on the underlying surface
- Represent as a *bar code*

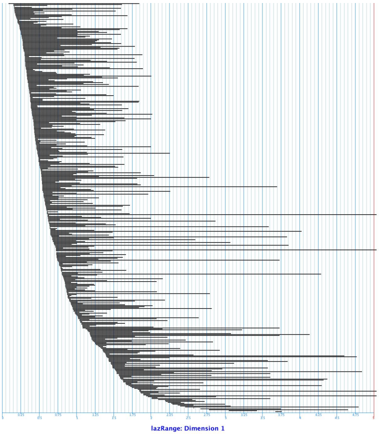
Bar Code for Fermat Curve of Genus 3

[Software from http://comptop.stanford.edu/programs/]

- THEOREM (Niyogi, Smale, Weinberger 2008) For compact submanifolds of Euclidean Space, persistent homology finds all of the topology.
- But what about affine curves, a more likely source of point clouds?

- Constructing point clouds of canonical curves of genus 4
- By Riemann–Roch, intersection of a quadric and a cubic
- Take cubic with random coefficients
- Quadric is Segré embedding of $\mathbb{P}^1 \times \mathbb{P}^1$

- 1. Choose random cubic C
- 2. Choose random point of $\mathbb{P}^1 \times \mathbb{P}^1$
- 3. Choose random ruling through that point
- 4. Use Newton's method to find an intersection with the cubic C
- Repeat until desired number of points found



Bar Code for Space Sextic

- Took many tweaks
- Points are *very* spread out
- *BUT:* do get some genuine cycles on the curve, so can construct *part* of the period matrix.

ACKNOWLEDGEMENTS

Theresa L. Ross, PhD PA
JETNet, LLC