

JMM 2016 LECTURE SAMPLER



From L-to-R: K. E. Lauter, K. E. Smith, P. Daskalopoulos, M. Lewicka, M. R. Pakzad, K. E. Lauter, T. A. Moore, T. Toro, A. Eskin.

Some of the Joint Mathematics Meetings invited speakers have kindly provided these introductions to their lectures in order to entice meeting attendants and to include nonattendants in the excitement.
—Frank Morgan

- page 8 — Lewicka and Mohammad Reza Pakzad, “Prestrained Elasticity: From Shape Formation to Monge-Ampère Anomalies”
10:05 am–10:55 am, Wednesday, January 6.
- page 11 — Daniel Alan Spielman, “Graphs, Vectors, and Matrices”
8:30 pm–9:30 pm, Wednesday, January 6.
- page 13 — Karen E. Smith, “Noether’s Legacy: Rings in Geometry”
10:05 am–10:55 am, Thursday, January 7.
- page 15 — Steve Zelditch, “Geodesics and Global Harmonic Analysis”
2:15 pm–3:05 pm, Thursday, January 7.
- page 17 — Alex Eskin, “The $SL(2, \mathbb{R})$ Action on Moduli Space”
10:05 am–10:55 am, Friday, January 8.
- page 18 — Kristin Estella Lauter, “Homomorphic Encryption for Private Genomic Computation”
11:10 am–12:00 pm, Friday, January 8.
- page 19 — Tanya A. Moore, “Why Mathematicians and Statisticians Are Needed to Create Lasting Social Impact”
7:45 pm–8:35 pm, Friday, January 8.
- page 20 — Panagiota Daskalopoulos, “Ancient Solutions to Parabolic Equations”
9:00 am–9:50 am, Saturday, January 9.
- page 21 — Tatiana Toro, “Analysis on Nonsmooth Domains”
1:00 pm–1:50 pm, Saturday, January 9.

Marta Lewicka and
Mohammad Reza Pakzad

Prestrained Elasticity: From Shape Formation to Monge-Ampère Anomalies



Marta Lewicka



Mohammad Reza Pakzad

Imagine an airplane wing manufactured in a hyperbolic universe and imported into our Euclidean space. The incompatibility of the two geometries would be an obstacle for the relative ideal hyperbolic distances in the wing to be realized in the ambient Euclidean space. As a consequence, the wing would take on a deformed shape and be subject to internal stresses, making it not suitable for flying. This scenario, though imaginary, describes an everyday phenomenon known as *prestrain* in nonlinear elasticity. Here, prestrain refers to an incompatible ideal metric, and, contrary to the above situation, it can play

a positive role in nature and in applications.

Figure 1 shows the optimal “relaxations” of a planar film allowed to freely seek a strain-minimizing deformation in space. Although the prescribed strain is radially symmetric, the resulting configurations are not; they exhibit large-scale buckling and multiscale wrinkling, and in fact they still retain residual strain albeit smaller than the original one.

How “good” are these relaxations in general? This problem can be studied through a variational model pertaining to the non-Euclidean version of nonlinear elasticity, which postulates formation of a target Riemannian metric resulting in the morphogenesis of the tissue that attains a configuration closest to being the metric’s isometric

Marta Lewicka is an associate professor of mathematics at the University of Pittsburgh. Her email address is lewicka@pitt.edu.

Mohammad Reza Pakzad is an associate professor of mathematics at the University of Pittsburgh. His email address is pakzad@pitt.edu

M.L. is supported by the NSF CAREER award DMS-0846996 and the NSF award DMS-1406730. R.P. is supported by the NSF Grant DMS-1210258.

For permission to reprint this article, please contact:
reprint-permission@ams.org.

DOI: <http://dx.doi.org/10.1090/noti1305>



Figure 1. The minimizing shapes of thin films with radially symmetric strains (target metrics). Reprinted from Klein et al. [5] with permission from AAAS.

immersion. It now turns out that the answer to the above question depends on the scaling of the energy minimizers in terms of the film’s thickness and a posteriori by the emerging isometry constraints on deformations with low regularity.

The study of mappings with weak regularity and the behavior of rough solutions to PDEs arising in geometry or physics has been an important part of analysis for decades. Many physical phenomena modeled by PDEs cannot be described by merely smooth solutions. On the other hand, lack of regularity can lead to nonphysical solutions or even to situations where generically every function is close to a solution. This kind of mathematical behavior goes back to early work by Nash and Kuiper on isometric embeddings, where a Riemannian surface can be C^1 isometrically embedded in \mathbb{R}^3 , while higher smoothness requires higher dimensions.

In practical applications, thin films can be residually strained by a variety of means, such as inhomogeneous growth, plastic deformation, swelling or shrinkage driven by solvent absorption, or opto-thermal stimuli in glass sheets. An interesting application, suggested by Kim et al. [4], creates curvy films by using light technology for the temperature-responsive flat gel sheets that transform into a prescribed curved surface when the in-built metric is activated (see Figure 2).

We hope that the study of thin films will lead to a better understanding of three-dimensional solids and such fundamentals as energy scaling laws, the role of curvature or symmetry breaking. Current disagreements between theory and experiment need also to be resolved.

Incompatible Elasticity and Residual Stresses

Let $\Omega \subset \mathbb{R}^n$ be a simply connected domain, and let G be a smooth Riemannian metric on Ω . It is well known that

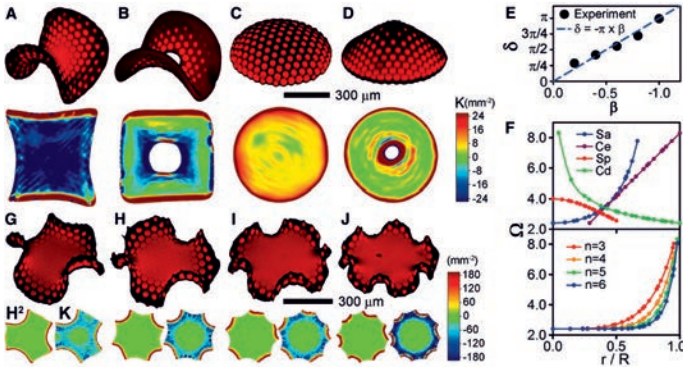


Figure 2. Halftone gel lithography from Kim et al. [4]: shapes obtained by photopatterning polymer films. Reprinted with permission from AAAS.

when the Riemann curvature tensor $Riem(G)$ vanishes in Ω , there exists a mapping u (in other words, a *deformation*) of Ω into \mathbb{R}^n which is an isometric immersion of G :

$$(1) \quad \nabla u(x)^T \nabla u(x) = G(x) \quad \forall x \in \Omega.$$

When the mentioned condition fails (as it fails for a generic choice of G), one proceeds by seeking an orientation-preserving deformation u which minimizes the difference between the tensor fields in the right and left hand sides of (1). This difference is measured by the energy functional, called the *prestrained (or incompatible) elasticity*:

$$(2) \quad E(u) = \int_{\Omega} \text{dist}^2(\nabla u(x) G(x)^{-1/2}, SO(n)) \, dx,$$

defined over the set of admissible deformations $u \in W^{1,2}(\Omega, \mathbb{R}^n)$ with square integrable derivatives of first order. The distance in matrix space $\mathbb{R}^{n \times n}$ is measured in terms of the Hilbert-Schmidt norm $\|A\|^2 = \text{trace}(A^T A)$. Note that $E(u) = 0$ if and only if u is orientation preserving and satisfies (1). In this case, a change of variable reduces (2) to a standard nonlinear elasticity functional of the type $\int_{\Omega} W(\nabla u) \, dx$, which has been largely studied in the literature.

In the incompatible case when $Riem(G) \neq 0$, existence of an energy gap phenomenon was shown in [8]. Namely, the equilibrium state of the body Ω must have a positive energy content, $\inf E > 0$, which we refer to as the *residual energy*. So far, only partial quantified estimates of this infimum in terms of $Riem(G)$ have been obtained. To better understand this problem, as well as to explore the relationship between the components of the target metric and the Riemann curvature as the driving force behind respectively the mechanical response and the residual stress, one is led to study models with reduced complexity, e.g., through dimension reduction.

A thin film can be modeled by the Cartesian product $\Omega^h = \omega \times (-\frac{h}{2}, \frac{h}{2})$, with the *mid-plate* $\omega \subset \mathbb{R}^2$ and small thickness $h \ll 1$. In what follows, we are concerned with analyzing the infimum energy and the structure of

minimizers of the energy functional below, now also in relation to the vanishing thickness $h \rightarrow 0$:

$$(3) \quad E^h(u^h) = \frac{1}{h} \int_{\Omega^h} \text{dist}^2((\nabla u^h)(G^h)^{-1/2}, SO(3)) \, dx$$

$$\forall u^h \in W^{1,2}(\Omega^h, \mathbb{R}^3).$$

Γ -Convergence

A major difficulty in studying the functionals (3) is that the frame invariance of the energy density spoils convexity. Thus, in general, direct methods of calculus of variations cannot be applied, and the minimizing sequences to (3) must be studied through asymptotic analysis, exploiting the small thickness of the domain. Namely, one first hopes to establish compactness properties for approximate minimizers of E^h as $h \rightarrow 0$. These, naturally, vary among different ranges of the scaling exponent β in $\inf E^h \sim h^\beta$, which is in its turn induced by the prestrain G^h . Having found the admissible set of the limiting deformations, one then looks for suitable “dimensionally reduced” energies that would carry the structure of E^h . The method of Γ -convergence is one of the strategies available for this purpose in the variational toolbox.

In the present set-up for thin films, proving Γ -convergence of $h^{-\beta} E^h$ consists of deriving two inequalities. The first inequality establishes a lower bound: $\mathcal{I}_\beta(u) \leq \liminf_{h \rightarrow 0} h^{-\beta} E^h(u^h)$ for any sequence u^h converging to a mapping u . The second inequality shows that the previous bound is optimal in the sense that for any given admissible u , we have $\mathcal{I}_\beta(u) = \limsup_{h \rightarrow 0} h^{-\beta} E^h(u^h)$ for a particular recovery sequence u^h converging to u .

The main feature of this definition, which in fact justifies its applicability, is that the limits of any converging sequence of minimizers of E^h coincide with the minimizers of \mathcal{I}_β . Again, the results vary and depend on the chosen scaling β ; in general, larger energies admit larger deformations, while smaller energies (induced by G^h with small Riemann curvatures in terms of h) admit only more restrictive deformations that need to preserve certain stringent curvature constraints.

Curvature-Driven Energy-Scaling Quantization

We start by a short excursion in the context of compatible prestrains satisfying $Riem(G) \equiv 0$. In this case, a change of variable brings the energy (3) to the standard nonlinear elasticity functional defined on deformations u^h of a tubular neighborhood S^h of a surface $S \subset \mathbb{R}^3$, with trivial prestrain $G = Id_3$. When $S = \omega \subset \mathbb{R}^2$, the quantitative geometric rigidity estimate established in [3] leads to the rigorous study of the dimensionally reduced thin models in low-energy scalings. For more general geometries, a conjecture has been put forward [9] concerning an infinite hierarchy of limiting thin shell models, each valid in its respective energy-scaling regime induced by the scaling of the applied body forces. In each case, the Γ -limit of $h^{-\beta} E^h$ consisted of a computable combination of bending and stretching.

In certain situations, the geometry of S allows for the matching of lower-order infinitesimal isometries to higher-order ones, whereas the corresponding theories collapse to one and the same theory, valid under the lower-order infinitesimal isometry constraint. The conjecture and this “collapse phenomenon” is so far consistent with all the rigorously established analytical results.

The picture in the prestrained elasticity scenario, where $\text{Riem}(G) \neq 0$, is richer in as much as it does not generate one sequential hierarchy but rather a network of limiting models, differentiated by the scaling of the components of the curvatures of G^h when $h \rightarrow 0$.

When $G^h = G$ is independent of thickness parameter, an energy gap phenomenon can be observed [1]. Namely, the only possible scaling after the nonzero energy drops below h^2 is that of order h^4 . In the first case, the Γ -limit of $h^{-2}E^h$ consists of a curvature functional defined over the $W^{2,2}$ isometric immersions of the two-dimensional manifold $(\omega, G_{2 \times 2})$ into \mathbb{R}^3 . In the second case, the three Riemann curvatures R_{1212}, R_{1213} , and R_{1223} of G vanish identically. The Γ -limit of $h^{-4}E^h$ is then given in terms of *stretching*, i.e. the change of metric, and *bending* that is the induced change of the second fundamental form with respect to the unique isometric immersion that gives the zero energy in the prior Γ -limit, plus a new term that quantifies exactly the remaining three possibly nonzero Riemann curvatures.

The Monge-Ampère Constrained Energy

The Monge-Ampère equation:

$$(4) \quad \det \nabla^2 v = f \quad \text{in } \omega \subset \mathbb{R}^2$$

can be seen as a “small slope” variant of the isometric immersion equations, and it naturally arises in the thin limit residual theories of the model (3). Indeed, for the incompatibility tensor of the form $G^h = \text{Id}_3 + 2h^\gamma S$ where $0 < \gamma < 2$, the Γ -limit \mathcal{I} of $h^{-(\gamma+2)}E^h$ is effectively defined [7], [6] on the deformations of regularity $W^{2,2}$ for which the pull-back of the Euclidean metric coincides with the prestrain G^h at the first order of expansion of their Gauss curvatures. This condition is precisely equivalent to (4) with $f = -\text{curl}^T \text{curl } S_{2 \times 2}$, whereas we have $\mathcal{I}(v) = \int_\omega |\nabla^2 v|^2$.

For future purposes, let us note that the above discussion motivates the following weak form of the two-dimensional Monge-Ampère equation (4):

$$(5) \quad \boxed{\mathcal{D}et \nabla^2 v := -\frac{1}{2} \text{curl}^T \text{curl} (\nabla v \otimes \nabla v)} = f.$$

The Monge-Ampère constrained variational problem \mathcal{I} is the source of a wide range of questions: from the technical obstacles in deriving the model as a Γ -limit to the study of regularity and multiplicity of minimizers or critical points, of which many remain open. Along these lines, we recently demonstrated the surprising existence of a class of anomalous solutions to (5). The rest of this article is dedicated to this line of inquiry.

Convex Integration for the Monge-Ampère Equation

When f is nonnegative, any $v \in W^{2,2}(\omega)$ satisfying (4) must actually be C^1 and *convex*. Once the convexity is established, the path opens up for applying the standard results in the theory of nonlinear PDEs to obtain better interior regularity of v depending on the given regularity of f . For the “flat case” $f \equiv 0$, any such v must be *developable*: it is C^1 , and for every point $x \in \omega$ there exists either a neighborhood of x or a segment passing through it and joining $\partial\omega$ at both its ends, on which ∇v is constant.

The same assertions of convexity/developability are true [10] for solutions $v \in C^{1,\alpha}(\omega)$ of (5) with $\frac{2}{3} < \alpha < 1$. Let us point out that a crucial step in proving results for the weak Hölder regular solutions is a commutator estimate that yields a degree formula for the Hölder continuous mapping ∇v . Such commutator estimates were used for the Euler equations by Constantin, E, and Titi and for the isometric immersion problem by Conti, Delellis, and Székelyhidi. This relationship is not surprising in view of the presence of a quadratic term in the equations in all three cases.

The parallels with the isometric immersions and Euler’s equations do not stop here. In both cases, the known *rigidity* statements are contrasted with existence of anomalous *flexible* solutions in lower regular regimes. It is perhaps surprising that similar statements on existence of anomalous solutions to the Monge-Ampère equation (4) have been missing in the literature. Indeed, the reformulation (5) leads to the following counterintuitive result [10]. Fixing an exponent $\alpha < \frac{1}{7}$ and the right-hand side $f \in L^{7/6}(\omega)$, the set of $C^{1,\alpha}(\bar{\omega})$ solutions to (5) is dense in $C^0(\bar{\omega})$.

The critical value of Hölder’s exponent at the threshold of rigidity and flexibility is not yet clear; it has been conjectured to be $\frac{1}{3}, \frac{1}{2}$ or $\frac{2}{3}$, relying on various intuitions. Here and also in the case of isometries, the Nash-Kuiper iteration method cannot yield anomalous solutions with regularity better than $C^{1,1/3}$, but on the other hand, there seems to be little indication of how to prove the rigidity for the regimes $\frac{1}{3} \leq \alpha \leq \frac{2}{3}$. This situation is, again, parallel with the recent results in the context of fluid dynamics (see Delellis and Székelyhidi [2] and the references therein), where the famous Onsager’s conjecture puts the Hölder regularity threshold for the energy conservation of the weak solutions to the Euler equations at exactly $C^{0,1/3}$.

Conclusion

In this article, we motivated how the prestrain metric problem can be formulated for three-dimensional elastic bodies and showed how it leads to problems in geometry and analysis. In particular, rigidity properties of the weak solutions to geometric PDEs come to the frontline, including the discovery of the anomalous solutions to the Monge-Ampère equation. The investigation of the dimensionally reduced models can also shed light on the

precise role which is played by the curvature tensor in the stress distribution within a three-dimensional body and can eventually lead to a better understanding of the shape formation phenomena through growth, plasticity, etc. Coming back to the energy (3), a direct consequence of the existence of the anomalous $C^{1,\alpha}$ solutions in the regime $\alpha < 1/7$, is that for all given $G^h = \text{Id}_3 + 2h^\gamma S$ one has: $\inf E^h \ll h^{1/2}$. This could be improved to: $\inf E^h \ll h$, if the anomalous regime was extended to $\alpha < 1/3$. Finally, scaling regimes between h^2 and $h^{1/2}$, and the corresponding behaviour of thin prestrained films, are not yet well understood. Other largely unexplored related topics include homogenization, symmetry and symmetry breaking, inverse prestrain analysis (useful, e.g., in tumor detection) and randomly generated prestrain. These avenues of research connect between theory of elasticity, differential geometry, analysis, and PDEs. We also hope that a thorough theoretical understanding of the phenomena discussed in this article could help in engineering sheets or bodies with finely controlled shapes, dynamics, structural resistance to loads, and elastic properties such as rigidity and flexibility.

References

- [1] K. BHATTACHARYA, M. LEWICKA, and M. SCHAFFNER, Plates with incompatible prestrain, to appear in *Arch. Rational Mech. Anal.*
- [2] C. DELELLIS and L. SZEKELYHIDI JR., The h-principle and Onsager's conjecture, *EMS Newsletter*, March 2015.
- [3] G. FRIESECKE, R. JAMES, and S. MÜLLER, A hierarchy of plate models derived from nonlinear elasticity by gamma-convergence, *Arch. Ration. Mech. Anal.* **180** (2006), no. 2, 183–236.
- [4] J. KIM, J. A. HANNA, M. BYUN, C. D. SANTANGELO, and R. C. HAYWARD, Designing responsive buckled surfaces by halftone gel lithography, *Science* **335** (2012), 1201–1205.
- [5] Y. KLEIN, E. EFRATI, and E. SHARON, Shaping of elastic sheets by prescription of non-Euclidean metrics, *Science* **315** (2007), 1116–1120.
- [6] M. LEWICKA, L. MAHADEVAN, and M. R. PAKZAD, The Monge-Ampère constrained elastic theories of shallow shells, *Annales de l'Institut Henri Poincaré (C) Nonlinear Analysis* (2015).
- [7] M. LEWICKA, P. OCHOA, and M. R. PAKZAD, Variational models for prestrained plates with Monge-Ampère constraint, *Diff. Int. Equations* (2015).
- [8] M. LEWICKA and M. R. PAKZAD, Scaling laws for non-Euclidean plates and the $W^{2,2}$ isometric immersions of Riemannian metrics, *ESAIM: Control, Optimisation and Calculus of Variations* **17**, no. 4 (2011), 1158–1173.
- [9] ———, The infinite hierarchy of elastic shell models: some recent results and a conjecture, *Fields Institute Communications*, Volume **64**, Springer, New York, 2013, pp. 407–420.
- [10] ———, Convex integration for the Monge-Ampère equation in two dimensions, to appear.

Daniel Alan Spielman

Graphs, Vectors, and Matrices

Algebraic Graph Theory



Daniel Alan Spielman

Graphs are the quintessential objects of study in discrete mathematics. They are usually described as a set of vertices, V , that are connected by a set of edges, E , each of which is a pair of vertices. Graphs encode connections and

are one of the most commonly used representations of data. While we first learn to prove theorems about graphs through local arguments and combinatorial manipulations, much of what I want to know about a graph is revealed through the more continuous approach of algebraic graph theory.

We define the Laplacian quadratic form of a weighted, undirected graph with positive edge weights $w_{a,b}$ to be the function from $x \in \mathbb{R}^V$ to real numbers given by

$$\phi_G(x) \stackrel{\text{def}}{=} \sum_{(a,b) \in E} w_{a,b} (x(a) - x(b))^2.$$

So, the coefficient of $x(a)x(b)$ in $\phi_G(x)$ is $-w_{a,b}$ if (a,b) is an edge and zero otherwise. The coefficient of $x(a)^2$ is the weighted degree of vertex a : $\sum_{(a,b) \in E} w_{a,b}$. The Laplacian matrix of G , denoted L_G , is the symmetric matrix such that

$$\phi_G(x) = x^T L_G x.$$

To build intuition for why the eigenvalues and eigenvectors of L_G should reveal combinatorial properties of G , in my talk I'll present Hall's spectral graph drawing algorithm [Hal70]. When we introduce graphs to students, we often do so through pictures. We draw the vertices as little circles and the edges as lines or curves connecting the circles representing their endpoints. While we obtain the same graph wherever we put the circles, some drawings reveal the structure of the graph much better than others. For example, consider the two drawings in Figure 1. They both represent the same graph, but the second reveals its structure much better than the first. As suggested by Hall, it was drawn by using two eigenvectors of the Laplacian matrix of the graph to determine the coordinates of the vertices.

Daniel Alan Spielman is the Henry Ford II Professor of computer science, applied mathematics, and mathematics at Yale University. His email address is spielman@cs.yale.edu.

DOI: <http://dx.doi.org/10.1090/noti1306>



Figure 1. An arbitrary drawing of a graph and a spectral drawing of that graph.

Sparsification

Sparsification is the approximation of a graph by a graph with fewer edges. We say that a graph G is an ϵ -approximation of a graph H with the same vertex set if for all $x \in \mathbb{R}^V$,

$$(1) \quad (1 + \epsilon)\phi_G(x) \geq \phi_H(x) \geq (1 + \epsilon)^{-1}\phi_G(x).$$

We may express this condition in a linear algebraic manner by introducing the notation $A \succcurlyeq B$ to indicate that $x^T A x \geq x^T B x$ for all vectors x . For symmetric matrices A and B , this is equivalent to saying that $A - B$ has no negative eigenvalues. With this notation, (1) becomes

$$(1 + \epsilon)L_G \succcurlyeq L_H \succcurlyeq (1 + \epsilon)^{-1}L_G.$$

For small ϵ this is a very strong condition. Among other things, it implies that L_G and L_H have approximately the same eigenvalues.

Every graph may be approximated by a sparse graph, where the number of edges in the sparse graph depends on the quality of the approximation. The strongest result of this form that we presently know comes from the following theorem of [BSS12].

Theorem 1. *For every graph G on n vertices and every $\epsilon > 0$, there is a graph H having at most $\lceil n/\epsilon^2 \rceil$ edges so that*

$$(1 + \epsilon)^2 L_G \succcurlyeq L_H \succcurlyeq (1 - \epsilon)^2 L_G.$$

The proof of this theorem is purely linear-algebraic and relies on the association of vectors with the edges of a graph. We define the *vector associated with edge (a, b)* to be the vector

$$u_{a,b} \stackrel{\text{def}}{=} e_a - e_b,$$

where e is the elementary unit vector in direction a . That is, $u_{a,b}$ has a 1 in position a , a -1 in position b , and is zero everywhere else. For a vector $x \in \mathbb{R}^V$,

$$x(a) - x(b) = u_{a,b}^T x,$$

and thus

$$(x(a) - x(b))^2 = (u_{a,b}^T x)^2 = x^T (u_{a,b} u_{a,b}^T) x.$$

So, we can write L_G as

$$\sum_{(a,b) \in E} w_{a,b} u_{a,b} u_{a,b}^T.$$

In [BSS12] we derive Theorem 1 as a consequence of the following theorem about collections of vectors.

Theorem 2. *Let u_1, \dots, u_m be vectors in \mathbb{R}^n , and let $\epsilon > 0$. Then, there exists a subset $S \subseteq \{1, \dots, m\}$ of size at most $\lceil n/\epsilon^2 \rceil$ and real numbers $s_i > 0$ so that for*

$$A = \sum_{i=1}^m u_i u_i^T \quad \text{and} \quad B = \sum_{i \in S} s_i u_i u_i^T, \\ (1 + \epsilon)^2 A \succcurlyeq B \succcurlyeq (1 - \epsilon)^2 A.$$

Even the problem of sparsifying the complete graph is interesting. Recall that the complete graph on n vertices is the graph with every possible edge. Sparse approximations of the complete graph are expander graphs (see [HLW06]), and they have proved incredibly useful in computer science and combinatorics. The best sparse approximations of the complete graphs are the Ramanujan graphs constructed by Margulis (1988) and Lubotzky, Phillips, and Sarnak (1988).

Weaver's Conjecture and the Kadison-Singer Problem

The Kadison-Singer problem [KS59], which comes from the study of C^* algebras and quantum physics, has been shown to be related to problems in many branches of mathematics (see [CFTW06]). We [MSS15] solve this problem by proving a conjecture in discrepancy theory that Weaver (2004), using results of Akemann and Anderson (1991), proved would give a positive solution to the Kadison-Singer problem.

Weaver's conjecture concerns a collection of complex vectors, u_1, \dots, u_m , such that

$$(2) \quad \sum_{i=1}^m u_i u_i^* = I.$$

For most purposes, it suffices to consider the outer products of real vectors with their transposes. Collections of vectors that satisfy (2) are said to be in “isotropic position” and are also called a “Parseval frame”. The sum in this expression is also known as a “decomposition of the identity”. For example, the vectors in an orthonormal basis are in isotropic position, as are the set of vectors associated with the edges of a complete graph. The vectors in Figure 2 are in isotropic position.

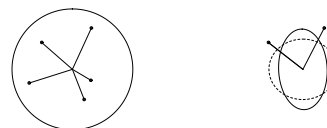


Figure 2. The vectors on the left are in isotropic position and are drawn along with their moment ellipse—the unit circle. The right image depicts a subset of those vectors with their moment ellipse—the image of the unit circle under multiplication by $\sum_{i \in S} u_i u_i^T$. The dotted line is the circle of radius $1/2$.

We would like to know conditions under which a set of vectors in isotropic position is guaranteed to contain a subset whose sum of outer products approximates half the identity. The most obvious obstacle to this happening is if one of the vectors, u_i , has large norm. For example, if u_i has norm 1, then the sum will have an eigenvalue of 1 if $i \in S$ and an eigenvalue of 0 if $i \notin S$. Weaver conjectured that vectors of large norm are the only obstacle.

Conjecture 1. There are positive constants α and ϵ so that for every collection of vectors u_1, \dots, u_m in isotropic position such that $\|u_i\|^2 \leq \alpha$ for all i , there exists a subset $S \subseteq \{1, \dots, m\}$ so that

$$(1 - \epsilon)I \succcurlyeq \sum_{i \in S} u_i u_i^* \succcurlyeq \epsilon I.$$

This conjecture has a provocative resemblance to Theorem 2. Using some ideas from the proof of that theorem, along with the theory of real stable polynomials and an elementary but new proof technique that we call the *method of interlacing families of polynomials*, we [MSS15] prove a strong version of this conjecture.

Theorem 3. For every constant $\alpha > 0$ and every collection of vectors u_1, \dots, u_m in isotropic position such that $\|u_i\|^2 \leq \alpha$ for all i , there exists a subset $S \subseteq \{1, \dots, m\}$ so that

$$(1/2 + \beta)I \succcurlyeq \sum_{i \in S} u_i u_i^* \succcurlyeq (1/2 - \beta)I,$$

for $\beta = \sqrt{2\alpha} + \alpha$.

Editor's Note: Daniel Spielman's use of the discrete Laplacian is complemented by Steve Zelditch's use of the continuous Laplacian; see page 15.

References

- [BSS12] JOSHUA BATSON, DANIEL A. SPIELMAN, and NIKHIL SRIVASTAVA, Twice-Ramanujan sparsifiers, *SIAM Journal on Computing*, 41(6):1704–1721, 2012.
- [CFTW06] PETER G. CASAZZA, MATTHEW FICKUS, JANET C. TREMAIN, and ERIC WEBER, The Kadison-Singer problem in mathematics and engineering: a detailed account, *Contemp. Math.*, 414, Amer. Math. Soc., 2006, pp. 299–355.
- [Hal70] K. M. HALL, An r -dimensional quadratic placement algorithm, *Management Science*, 17:219–229, 1970.
- [HLW06] SHLOMO HOORY, NATHAN LINIAL, and AVI WIGDERSON, Expander graphs and their applications, *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.
- [KS59] RICHARD V. KADISON and ISADORE M. SINGER, Extensions of pure states, *American Jour. Math.*, 81:383–400, 1959.
- [MSS15] ADAM W. MARCUS, DANIEL A. SPIELMAN, and NIKHIL SRIVASTAVA, Interlacing families II: Mixed characteristic polynomials and the Kadison-Singer problem, *Annals of Mathematics*, 182:327–350, 2015.

Karen E. Smith

Noether's Legacy: Rings in Geometry



©Eric Bronson, Michigan Photography.

Karen E. Smith

I am deeply honored to lecture in the name of my mathematical idol, Emmy Noether.

Emmy Noether is responsible for the modern definition of commutative *rings* and their *homomorphisms*. Her 1921 paper “Idealtheorie in Ringbereichen” laid out the foundations of modern algebra and continues to impact mathematics well beyond algebra nearly a century later.

Rings of functions provide natural examples of abstract rings, an example as relevant today as it was in Noether's time.



Public Domain.

Even in high school, we add and multiply real-valued functions of the real line, quickly absorbing the basic properties (such as distributivity of multiplication over addition) that make up the axioms of Noether's definition.

Then as now, rings of functions help us understand the geometry of spaces on which those functions are defined. Remarkably, deep geometric discoveries often arise from purely algebraic investigations of rings.



Public Domain.

Portraits of Amalie Emmy Noether, who has been described by some as the most important woman in the history of mathematics.

This is especially true in algebraic geometry, where geometric objects called varieties turn out to be more or less equivalent to the rings of polynomial functions on them. Some relatively concrete questions about a variety V include the following: Is V smooth? How can we tell if it is smooth?

Even if V is not smooth, how damaging are its singularities? Can we perhaps ignore them for some computations or purposes? Can we measure the singularities precisely? All these questions can be answered

Karen E. Smith is Keeler Professor of Mathematics at the University of Michigan. Her email address is kesmith@umich.edu.

She did not realize that one could have a career as a mathematician until college, when her freshman calculus teacher, Charles Fefferman, suggested it. After teaching high school for a year, she discovered that schools will pay for you to get a PhD. In 2001 she won the Ruth Lyttle Satter Prize for her work in commutative algebra. She is especially proud of her record of mentoring, already with sixteen completed PhD students.

DOI: <http://dx.doi.org/10.1090/noti1307>

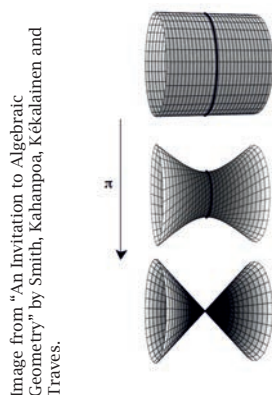


Figure 1. Desingularizing the cone.

by studying the algebraic features of rings of functions on V .

Precisely, an affine algebraic *variety* V is the common zero set, in \mathbb{C}^n , of a (possibly infinite) collection of polynomials. Its *coordinate ring*, denoted $\mathbb{C}[V]$, is the \mathbb{C} -algebra of complex valued functions on V generated by the (restrictions to V of the) coordinate functionals z_1, \dots, z_n . Noether's famous *First Isomorphism Theorem* gives a concrete presentation of the coordinate ring. Indeed, the natural restriction mapping

$$\mathbb{C}[z_1, \dots, z_n] \xrightarrow{\rho} \mathbb{C}[V]$$

sending each polynomial to its restriction to V is easily seen to be a surjective ring homomorphism. So the First Isomorphism Theorem implies that

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[z_1, \dots, z_n]}{\text{kernel } \rho},$$

where the kernel of the restriction map, of course, consists of the polynomials vanishing at every point of V . So, for example, the coordinate ring of the cone in \mathbb{C}^3 defined by $x^2 + y^2 = z^2$ is the ring $\mathbb{C}[x, y, z]/(x^2 + y^2 - z^2)$.

The points of an affine algebraic variety V are in one-one correspondence with the maximal ideals of its coordinate ring $\mathbb{C}[V]$; this is the content of Hilbert's Nullstellensatz, or *zero set theorem*. Indeed, all the algebro-geometric features of the variety—for example, its dimension, its subvarieties, its singular set—have algebraic characterizations in the coordinate ring. This idea was greatly expanded by Grothendieck, who taught us to view every commutative ring, no matter how abstract, as the ring of functions on some corresponding space.

In my Noether lecture, I will explain one surprisingly effective method for understanding varieties with ring theory: reduction to prime characteristic. In the case of the cone, the idea is to go beyond the coordinate ring $\mathbb{C}[x, y, z]/(x^2 + y^2 - z^2)$ and study instead the family of “reductions modulo p ”,

$$\mathbb{F}_p[x, y, z]/(x^2 + y^2 - z^2),$$

as \mathbb{F}_p ranges through all the fields of p elements, p prime.

Why would one do so? Why would one throw away the tools of analysis, such as integration and differentiation, and instead look at algebras over finite fields? What do we gain?

The point is that the ring $\mathbb{F}_p[x, y, z]/(x^2 + y^2 - z^2)$ has characteristic p . A commutative ring R of prime characteristic p has the property that the p th power map

$$R \rightarrow R \text{ sending } f \mapsto f^p$$

is a ring homomorphism. This homomorphism, called the Frobenius map, turns out to be a tremendous tool. In particular, it sheds light on the singularities of algebraic varieties in many ways.

Already half a century ago, Ernst Kunz characterized smoothness of complex varieties using Frobenius: smoothness turns out to be equivalent to a simple algebraic property called flatness of Frobenius in the corresponding family of modulo p reductions. More recent theorems characterize the so-called rational singularities of complex varieties, again, as a property of the modulo p reductions defined using Frobenius. This technique has found many applications throughout mathematics, including, for example, to cluster algebras in combinatorics.

In another direction, numerical invariants for measuring the “badness” of complex singularities have been defined with Frobenius. Starting with a complex variety defined by a single polynomial f with integer coefficients, for example, the so-called F -pure threshold of f is a different rational number for each choice of p ; interestingly, as p grows to infinity, these F -pure thresholds converge to (the reciprocal of) a well-known invariant of complex singularities called the analytic index of singularities, defined by integration.

My hope is that my audience will glimpse the beauty of this blooming field of “Frobenius techniques” in commutative algebra and grasp a small part of our collective mathematical indebtedness to Emmy Noether's profound contribution to algebra.

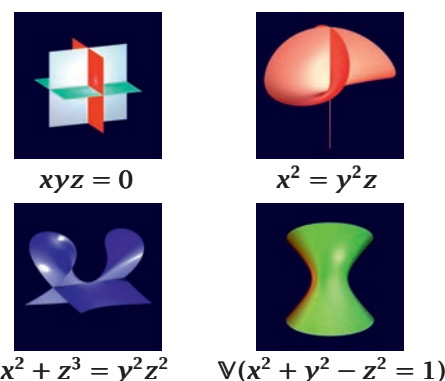


Figure 2. The real points of four different varieties in \mathbb{C}^3 , each defined by one polynomial.

Steve Zelditch

Geodesics and Global Harmonic Analysis



Steve Zelditch

Harmonic analysis originates with the exponential functions $e_k(x) = e^{2\pi i \langle k, x \rangle}$ of Fourier analysis on \mathbb{R}^n (with $k \in \mathbb{R}^n$) or on the torus $= \mathbb{R}^n / \mathbb{Z}^n$ (with $k \in \mathbb{Z}^n$). The idea is to express any function (or distribution) as a linear combination of the exponentials,

$$(1) \quad f(x) \sim \sum_{k \in \mathbb{Z}^n} a_k e^{2\pi i \langle k, x \rangle},$$

and to relate properties of f to the dual properties of the Fourier coefficients a_k . As eigenfunctions of the Laplacian $\Delta = \sum_{j=1}^n \frac{\partial^2}{\partial x_j^2}$ on \mathbb{R}^n , the exponentials $e^{2\pi i \langle k, x \rangle}$ form a (generalized) orthonormal basis of eigenfunctions of L^2 .

In the case of the flat torus, the exponentials (i) have uniformly bounded L^∞ -norms, $|e^{2\pi i \langle k, x \rangle}| \leq 1$, (ii) have the ‘WKB form’ of $a(x)e^{ikS(x, \omega)}$ where the amplitude $a = 1$ and $S(x) = \langle x, \frac{k}{|k|} \rangle$.

These properties reflect the flatness of the Euclidean metric and are rarely found on other Riemannian manifolds (M, g) where $g = \{g_{ij}\}$ is the metric tensor. The main theme of this article is that eigenfunctions of the Laplacian Δ_g of the metric in general reflect the geometry of geodesics. Henceforth we drop g from the notation for a Riemannian manifold M , but it should be kept in mind that eigenfunctions and geodesics depend on the metric g .

A round 2-sphere provides an opposite extreme where certain eigenfunctions are ‘as large as possible’. The zonal (rotationally invariant) spherical harmonics Y_ℓ^0 of eigenvalues $\ell(\ell+1)$ have the possible largest L^∞ norm of size $\sqrt{\ell}$. There is a universal estimate

$$(2) \quad \|\phi_\lambda\|_{L^\infty} \leq C_g \lambda^{\frac{n-1}{2}}, \quad (\|\phi_\lambda\|_{L^2} = 1, n = \dim(M)),$$

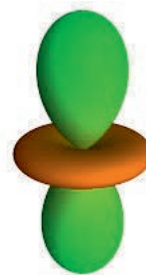
where C_g depend only on g and not on the eigenvalue λ^2 . [Sogb]

An illustration of “global harmonic analysis” is the following recent result of the author with C. D. Sogge (building on prior results of Y. Safarov, the authors, and J. Toth).

Steve Zelditch is the Wayne and Elizabeth Jones Professor of Mathematics at Northwestern University. His email address is zelditch@math.northwestern.edu.

This research partially supported by NSF grant DMS-1206527.

DOI: <http://dx.doi.org/10.1090/noti1308>



©W. Jarosz, used with permission.
www.cs.dartmouth.edu/wjarosz/
publications/dissertation/
appendixB.pdf

Figure 1. An intensity plot of the zonal spherical harmonic, i.e., the graph of $|Y_\ell^0|^2$. It has huge peaks at two poles. Theorem 1 says that any eigenfunction with comparable sup norm must have at least one pole. Are there always two?

Theorem 1. Let M be a real-analytic Riemannian surface. If M possesses a sequence of Δ_g -eigenfunctions ϕ_{λ_j} achieving the bound (2) for some $C_g > 0$, then $M = S^2$ (topologically) and must possess a “pole”, i.e., a point such that every geodesic leaving p is a closed geodesic of period 2π .

Examples of surfaces with poles are surfaces of revolution, the poles being the obvious poles (fixed points of the S^1 action). Every point of the round S^2 is a pole. On the other hand, every geodesic leaving one of the four umbilic points p of a tri-axial ellipsoid is a “self-focal” point, but none are poles (every geodesic $\gamma(t)$ leaving p returns to p at time 2π , but $\gamma'(0) \neq \gamma'(2\pi)$ in general). Theorem 1 is a corollary of a general result valid in all dimensions, but as yet the existence of a “pole” is proved only in dimension 2.

We intend Theorem 1 as an illustration of a result of global harmonic analysis. The existence of closed geodesics through p cannot be proved using small time behavior of waves and geodesics or by nonwave methods. Analogous problems may be posed for L^p norms with $p < \infty$. For instance, it is known that certain eigenfunctions on the round S^2 known as the highest weight spherical harmonics Y_ℓ^ℓ are Gaussian beams which “blow up” on the equatorial geodesic but have Gaussian decay in the normal directions. They achieve the maximum possible L^p norms on S^2 for $p \leq 6$; the analogue of (2) for other L^p norms is due to C. D. Sogge (see [Sogb]). It is natural to conjecture that a surface can have a sequence of eigenfunctions achieving the maximal L^p bound with $p < 6$ only if it has a stable elliptic closed geodesic, somewhat like the equator, and if the eigenfunctions are something like Gaussian beams concentrating on that closed geodesic. This is a very good open problem in the field.

On any complete Riemannian manifold, geodesics depend on curvature and so do eigenfunctions of the Laplacian, but the key link is through the wave equation and dynamics of the long-time global geodesic flow. The title of this article, “Global harmonic analysis”, is

meant to indicate how global properties of the geodesic flow are related to the asymptotics of eigenfunctions. Experts will recognize that the relations are between classical and quantum mechanics in the semiclassical or high-frequency limit. The author has not seen a proof of (2) using the standard elliptic estimates of geometric analysis; it is a good illustration of the power of wave equation methods.

Let us compare how local and global harmonic analysts approach a problem on eigenfunctions. The local harmonic analyst works with the partial differential equation

$$(3) \quad \Delta\phi(x) = -\lambda^2\phi(x), \quad x \in B \subset M,$$

locally in a ball B . When $\lambda = 0$, the equation says that ϕ is harmonic. Even when $\lambda > 0$, a local harmonic analyst sees this as constraining just how far the eigenfunction is from being a harmonic function. Dilating a “small ball” $B(p, \frac{C_g}{\lambda_j})$ by the factor λ_j stretches out the eigenfunction to a nearly harmonic one and allows one to use the tools of local harmonic analysis (such as mean value inequalities). By comparison, the global harmonic analyst works with the “wave equation”

$$e^{it\sqrt{-\Delta}}\phi = e^{it\lambda}\phi,$$

which is only valid if (3) holds globally on M . The “propagator” $e^{it\sqrt{-\Delta}}$ or solution operator of the wave equation propagates singularities along geodesics. The global harmonic analyst doesn’t want to suppress oscillations in ϕ by stretching them out, but rather exploits the ever more rapid oscillations as $\lambda \rightarrow \infty$. Ultimately, this leads to relations between asymptotics of eigenfunctions as $\lambda \rightarrow \infty$ and the long-time behavior of geodesics, e.g., whether they are periodic (as on round spheres) or wind around uniformly in the unit cosphere bundle (as for negatively curved manifolds).

Another rich area for global harmonic analysis is the asymptotic behavior of nodal sets of eigenfunctions. To contrast again local versus global properties of eigenfunctions, it is a classical local result that there exists a zero of ϕ_λ in every ball $B(p, \frac{C_g}{\lambda_j}) \subset M$; i.e., the nodal set $\mathcal{N}_{\phi_\lambda} = \{x : \phi_\lambda(x) = 0\}$ is $\frac{1}{\lambda}$ -dense. The proof uses only that $\Delta\phi_\lambda = -\lambda^2\phi_\lambda$ in a ball $B(p, r)$ and not globally on (M, g) , and in this sense is a model of local harmonic analysis of eigenfunctions. Putting together local arguments, Donnelly-Fefferman (1987) proved that for real-analytic (M, g) , the hypersurface measure $\mathcal{H}^{n-1}(\mathcal{N}_{\phi_\lambda})$ of the nodal sets satisfies the bounds

$$(4) \quad c_g\lambda \leq \mathcal{H}^{n-1}(\mathcal{N}_{\phi_\lambda}) \leq C_g\lambda,$$

for some $c_g, C_g > 0$. The inequality was earlier conjectured by S. T. Yau for general C^∞ metrics, but that remains a very open problem.

A further well-known nodal problem is to count the number of nodal domains. A nodal domain is a connected

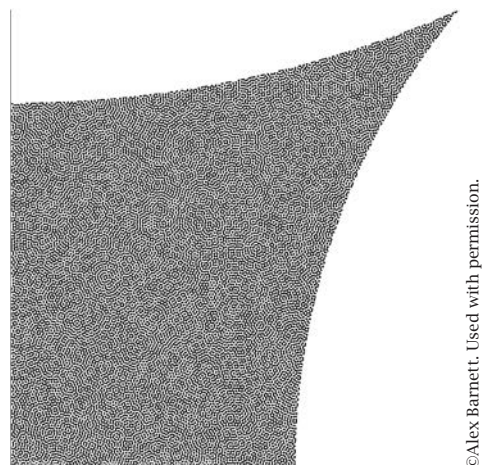


Figure 2. Nodal domains of a high-frequency Neumann eigenfunction of the Laplacian on a billiard table with chaotic billiards. The number of nodal domains is roughly the eigenvalue. Theorem 2 sees only the nodal domains touching the boundary, which cannot number more than the square root of the eigenvalue. And it does not even prove there are that many!

component of $M \setminus \mathcal{N}_{\phi_\lambda}$. The nodal domains partition M into disjoint open sets:

$$M \setminus \mathcal{N}_{\phi_\lambda} = \bigcup_{j=1}^{\mu(\phi)} \Omega_j.$$

When 0 is a regular value of ϕ_λ , the level sets are smooth curves. When 0 is a singular value, the nodal set is a singular (self-intersecting) curve. The question is: how many connected components does the nodal set have? The classical Courant bound is that the number $N(\phi_j)$ of the j th eigenfunction in an orthonormal basis is bounded by j ; in general, $N(\phi_\lambda)$ is bounded by $N(\lambda)$ (the number of eigenvalues $\leq \lambda$). It is known that there is no nontrivial lower bound for $N(\phi_\lambda)$ that holds for every sequence of eigenfunctions on every (M, g) ; for example, it was shown by H. Lewy that there exist (M, g) and sequences of $\phi_j, \lambda_j \rightarrow \infty$ with only two or three nodal domains. An obvious question is whether any (M, g) possesses at least *one* sequence of eigenfunctions for which $N(\phi_{j_k}) \rightarrow \infty$ as $k \rightarrow \infty$. It was pointed out by T. Hoffman-Ostenhof that this is (apparently) an open problem. At first, it seems obviously true: on S^2 , for instance, such a sequence exists for the standard metric (e.g., the zonal harmonics). Connect any metric g on S^2 by an analytic path g_t of metrics with $t \in [0, 1]$ and “analytically continue” the eigenfunctions $\phi_j(t)$ along the path (this is possible). Then show that that number of nodal domains does not change for a “generic” path. Unfortunately, this outline overlooks the fact that for a generic path of metrics and the associated paths of eigenfunctions $\phi_j(t)$, two nodal domains will collide (i.e.,

intersect) at some times t_k at a *singular point* of $\phi_j(t_k)$, and two nodal domains can merge into one. By the time $t = 1$, the λ_j nodal domains may have merged into just a fixed number of domains independent of λ_j . Although such a conspiratorial situation seems unlikely, there is no proof that it does not occur for any path g_t between the standard metric and another given metric. In fact, it is a challenge to prove the existence of any reasonably large class of metrics which possess a sequence ϕ_{j_k} of eigenfunctions for which $N(\phi_{j_k}) \rightarrow \infty$. The following result with Junehyuk Jung gives a reasonably large class.

Theorem 2. *Let (X, g) be a surface with curvature $k \leq 0$ and with concave boundary. Then for any orthonormal eigenbasis $\{\phi_j\}$ of Dirichlet (or Neumann) eigenfunctions, one can find a density 1 subset A of \mathbb{N} such that*

$$\lim_{\substack{j \rightarrow \infty \\ j \in A}} N(\phi_j) = \infty.$$

A density one subset $A \subset \mathbb{N}$ is one for which $\frac{1}{N} \#\{j \in A, j \leq N\} \rightarrow 1$, $N \rightarrow \infty$. An example of a nonpositively curved surface with concave boundary is a Sinai-Lorentz billiard in which one removes a small disc C from X .

The proof is based on proving that there are “many” zeros and critical points of eigenfunctions of Neumann eigenfunctions (or of normal derivatives of Dirichlet eigenfunctions) along the boundary ∂M . That is, the proof very much depends on the existence (and concavity) of a boundary. The results were inspired by one of Ghosh-Reznikov-Sarnak for Hecke eigenfunctions.

Let us outline the proof in the Neumann case. The geodesic billiard flow of M is ergodic under the assumption that the curvature is ≤ 0 and the boundary is concave. Hence the eigenfunctions are “quantum ergodic”. Without going into the details, ergodicity of eigenfunctions means that they oscillate a lot and in all directions as $\lambda_j \rightarrow \infty$.¹ We then restrict the eigenfunctions to the boundary ∂M . The main point is to prove that the Neumann eigenfunctions ϕ_j have a growing number of zeros on ∂M as $\lambda_j \rightarrow \infty$. In fact, this is true for any curve on M , not just the boundary.

The last step is a topological argument (based on the Euler inequality for embedded graphs in surfaces). Suppose that a Neumann eigenfunction vanishes at N points and that the genus of M is h . Each nodal line emanating from the boundary must return to the boundary at some other point. In general, the curve together with the boundary might not bound a domain. But an Euler inequality for graphs in M shows that there must exist at least $\frac{1}{2}N - C_h$ nodal domains formed this way, where $C_h = h + h_M$ where h_M is the number of components of ∂M .

In conclusion, the global results use long-time dynamical properties of the geodesic flow, such as its ergodicity (or, at the opposite extreme, its integrability or periodicity) to prove results about eigenfunctions and waves that are often invisible to the more traditional local harmonic analysis in small balls.

¹Ergodicity of eigenfunctions originates in work of A. I. Shnirelman and has a long history of results, for which we refer to [Ze08], [Ze13], [Zw].

References

- [AN] N. ANANTHERAMAN and S. NONNENMACHER, Chaotic vibrations and strong scars, *Eur. Math. Soc. Newsl.* No. 74 (2009), 19–24.
- [Sogb] C. D. SOGGE, *Fourier Integrals in Classical Analysis*. Cambridge Tracts in Mathematics, 105, Cambridge University Press, Cambridge, 1993.
- [Ze08] S. ZELDITCH, Local and global analysis of eigenfunctions on Riemannian manifolds, *Handbook of Geometric Analysis*, No. 1, Adv. Lect. Math. (ALM), 7, Int. Press, Somerville, MA, 2008, pp. 545–658.
- [Ze13] ———, *Park City Lectures on Eigenfunctions*, to appear in the PCMI volume (AMS) (arXiv:1310.7888).
- [Ze12a] ———, Eigenfunctions and nodal sets, *Surveys in Differential Geometry*, volume 18, Int. Press, Somerville, MA, 2013, pp. 237–308 (arXiv:1205.2812).
- [Zw] M. ZWORSKI, *Semiclassical Analysis*, Graduate Studies in Mathematics, 138, American Mathematical Society, Providence, RI, 2012.

Alex Eskin

The $SL(2, \mathbb{R})$ Action on Moduli Space



Courtesy of The Simons Foundation.

Alex Eskin

Alex Eskin, Compton Distinguished Service Professor at the University of Chicago, will talk about ergodic theory with applications to billiards (just the math; won't help you win, but applies on any polygonal table, convex or not). *His recent breakthrough work with Mirzakhani and Mohammadi on $SL(2, \mathbb{R})$ actions on moduli space has as an application this new result by

Lelievre, Monteil, and Weiss: If the angles are rational multiples of π , from every point on the table you can shoot the cue ball to all but finitely many other points.

*See Alex Wright's elementary introduction to the study of dynamics on certain moduli spaces and, in particular, the recent results of Eskin, Mirzakhani, and Mohammadi in the January issue of the *Bulletin of the American Mathematical Society*: www.ams.org/journals/bull/2016-53-01/S0273-0979-2015-01513-2/

Editor's Note: See the related “WHAT IS ...an Ergodic Transformation?” on page 26.

Alex Eskin is Compton Distinguished Service Professor at the University of Chicago. His email address is eskin@math.uchicago.edu. DOI: <http://dx.doi.org/10.1090/noti1309>

Kristin Estella Lauter

Homomorphic Encryption for Private Genomic Computation



Kristin Estella Lauter

The capacity to sequence the human genome has opened up a treasure chest of possibilities for understanding human disease, searching for cures, and providing personalized medicine. But it also raises both important privacy challenges and questions about how to securely store and handle genomic data for computation. Just as data on individual preferences and behavior is a valuable economic commodity in the present, human genomic data has been called the “currency of the future.” Protecting

access to it is crucial.

Mathematics provides important infrastructure and tools for solving a host of problems in genomic computation. Mathematical modeling and machine learning algorithms help scientists learn from data to do predictive analysis, and pattern matching is used for sequence alignment. The mathematics of cryptography has recently provided an important new tool for protecting privacy in genomic computation: homomorphic encryption.

Homomorphic encryption keeps genetic data private but still allows another party to do computations on it. Consider a patient or a consumer who has his or her genome sequenced and stores the result locally on a personal computer or device. To obtain a private prediction—such as the likelihood of having a disease associated with a known genotype—from a Cloud service, the client first encrypts the genomic data homomorphically, then sends the encrypted data to the Cloud for processing without sending the decryption key. The Cloud computes on the encrypted data and returns an encrypted result to the client. The client then decrypts the result locally.

Here’s an analogous classroom-related example: A professor stores her students’ encrypted grades in the Cloud and keeps the decryption key, which may be shared with the university administration, for example. The Cloud service can compute an encrypted version of the mean and standard deviation of the final exam or other statistical functions of students’ grades without knowing the grades. The encrypted results can be decrypted by anyone who has the decryption key.

Construction of a homomorphic encryption scheme that allows computation of **any** circuit was an open problem for several decades until Craig Gentry provided



istock/©s-cphoto.



Photographer: Hai Yang.



Photographer: Hai Yang.

In March 2015, the Secure Genome Analysis Competition was hosted by the National Center for Biomedical Computing at UCSD with teams competing from around the world. The tasks consisted of statistical analyses and sequence comparison on SNPs from databases of human genomic data. Teams from Microsoft Research, IBM Research, and Stanford/MIT were the winners of the three tasks in the Homomorphic Encryption Challenge.

Kristin Estella Lauter is a Principal Researcher and Research Manager of the Cryptography Group at Microsoft Research. Her email address is klauter@microsoft.com.

DOI: <http://dx.doi.org/10.1090/noti1310>



Photographer: Kate Stange.



Photographer: Kate Stange.



iStock.

Private medical predictions: A demo of our cryptographic system to predict the likelihood of having a heart attack was demoed live to reporters in the AAAS Newsroom. I input age, weight, height, and other private data on my laptop, where it was encrypted. Then it was sent to a Cloud computing service, where the risk was computed on the encrypted data. The encrypted result was then sent back to my laptop and decrypted. The computation on the encrypted data took about 0.2 seconds.

the blueprint for a solution in 2009. Solutions evolved quickly over the subsequent five years, and current systems are based on the hardness of a problem called “Learning With Errors” (LWE) and its ring variants (RLWE). The LWE problem is to find a secret vector \mathbf{s} given only samples consisting of a random vector, \mathbf{a} , of the same

length, along with the inner product of the two vectors obscured by some Gaussian noise, \mathbf{e} (error). (Sample: $(\mathbf{a}, \mathbf{a}\mathbf{s} + \mathbf{e})$.) These problems are believed to be hard due to security reductions, proved by Regev and coauthors Lubashevsky and Peikert, to other known problems on lattices, such as certain approximate versions of the Shortest Vector Problem (SVP), which has been studied for decades.

The vectors in the above description are thought of as elements of a lattice, but they can also be viewed as coefficients of a polynomial in a polynomial ring, and this is the point of view in the Ring Learning With Errors setting. For cryptosystems based on RLWE, the polynomial ring which we use in practice is the ring of integers in a cyclotomic number field, presented as

$$\mathbb{Z}[\zeta_m] = \mathbb{Z}[X]/\Phi_m(X).$$

In fact, the question of the hardness of the RLWE problem in general number rings raises many interesting new questions in number theory which we are only beginning to investigate.

Cryptographic systems based on number theoretic constructions provide a surprising potential solution for ensuring privacy in outsourced genomic computation. This is a beautiful example of several apparently unrelated branches of science intersecting to provide coherent solutions to human problems.

References and links to articles in the popular press can be found on my webpage: research.microsoft.com/en-us/people/klauter/default.aspx

Tanya A. Moore

Why Mathematicians and Statisticians Are Needed to Create Lasting Social Impact



Courtesy of Albina Khazan.

Tanya A. Moore

Tanya Moore, Presidio Graduate School, is cofounder of the Infinite Possibilities Conference, a national biennial conference designed to support, promote, and empower underrepresented minority women in mathematics and statistics. She has been featured in *Black Enterprise* and *O, The Oprah Magazine*. Her talk will highlight the obvious and not-so-obvious ways mathematicians and statisticians are today's change agents.

Tanya A. Moore, *Building Diversity in Science*. Her email address is Tanya.Moore@presidio.edu.

DOI: <http://dx.doi.org/10.1090/noti1311>

Panagiota Daskalopoulos

Ancient Solutions to Parabolic Equations



Panagiota Daskalopoulos

Some of the most important problems in geometric partial differential equations are related to the understanding of singularities. Focusing in on a singularity, a certain “blow-up” procedure yields special solutions defined for all time $-\infty < t \leq T$, for some $T \leq +\infty$. We refer to such solutions as *eternal* if $T = +\infty$ and *ancient* if $T < +\infty$. The classification of such solutions, when possible, often sheds new insight into singularity analysis.

Common examples of singularities are *solitons*, which maintain their shape as time advances. Shrinking solitons are often examples of ancient solutions, while steady solitons are examples of eternal solutions. One often sees other ancient or eternal solutions which come from the gluing of solitons. The main question is whether these special solutions and the solitons are the only nontrivial ancient or eternal solutions of the flow.

We will focus on an area of active research: ancient solutions to *geometric flows*, such as the *Ricci flow*, the *Mean Curvature flow*, or the *Yamabe flow*.

Under the Ricci flow, the metric of an n -dimensional Riemannian manifold M shrinks by its Ricci curvature, a natural intrinsic curvature of the manifold. The Ricci flow was introduced by R. Hamilton in his seminal 1981 paper and developed by him in a series of subsequent breakthrough works leading to G. Perelman’s 2002 seminal works on the resolution of the Poincaré Conjecture.

In 2012, in joint work with R. Hamilton and N. Sesum, we proved that there are just two types of ancient solutions on a compact surface ($n = 2$). The simplest type is a round sphere contracting to a point. The second type, due to J. R. King and P. Rosenau, is two cigars glued together, as in Figure 1, the so-called *sausage model* of quantum field theory.

The proof relies on both analytical and geometric tools, such as a priori estimates, monotonicity of nonstandard Lyapunov functionals, geometric blow-up arguments, geometric estimates on isoperimetric ratios, and the application of the maximum principle on a rather complex quantity which vanishes on the King-Rosenau solutions.

A similar conjecture holds for 3-dimensional compact manifolds under a noncollapsing condition: that the only ancient non-collapsed solutions to the Ricci flow are

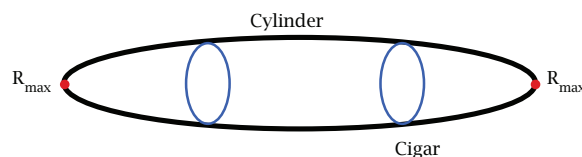


Figure 1. The King-Rosenau ancient solution to the Ricci flow consists of two cigars glued together.



Figure 2. A new ancient solution to the Yamabe flow on S^3 consists of moving towers of spheres with evolving necks.

contracting spheres and analogues of the King-Rosenau solutions due to G. Perelman. The noncollapsing condition is necessary due to the existence of other collapsed examples discovered by V. A. Fateev and related to quantum field theory.

One of the remarkable features of the 2-dimensional Ricci flow is its *conformal invariance*, because in 2D it coincides with the Yamabe flow, in which the metric shrinks in a given conformal class by a rate proportional to its scalar curvature. The Yamabe flow was introduced by Hamilton in 1989 as a parabolic approach to the resolution of the so-called Yamabe problem, solved by S. Brendle in 2005–2007.

It turns out that for the Yamabe flow there are more types of ancient solutions. In a recent work with M. del Pino and Sesum, we constructed ancient solutions of the Yamabe flow on, for example, the 3-dimensional sphere as moving towers of 2-spheres joined by thin necks, as in Figure 2.

The appearance of the towers of bubbles shows that the classification of ancient solutions to the compact Yamabe flow on S^n poses a rather difficult task. On the other hand, it gives a new way for constructing special solutions. It shows how one may glue two or more ancient solutions of a parabolic equation to construct a new ancient solution of the same equation. More recently, in joint work with del Pino, J. King, and Sesum, we have constructed a four-parameter family of ancient solutions which converge, as $t \rightarrow -\infty$, to two self-similar solutions moving in opposite directions. The picture that one has is very similar to that in Figure 1, where the cigar solution is replaced by a one-parameter family of self-similar solutions (solitons) which may be viewed as traveling waves in cylindrical coordinates. Our solutions are not given in closed form, except for one (the analogue of the sausage model in the Ricci flow), which was previously discovered by King.

One of the best-known extrinsic geometric flows is the *Mean Curvature flow*, in which a hypersurface in \mathbf{R}^{n+1}

Panagiota Daskalopoulos is a professor of mathematics at Columbia University. Her email address is pdaskalo@math.columbia.edu.

DOI: <http://dx.doi.org/10.1090/noti1312>

moves in the normal direction at a rate proportional to the mean curvature. Since this flow is known for its many exotic examples of singularities, one expects to have many ancient solutions. The simplest ancient solution is a contracting sphere. One hopes to provide a classification of ancient solutions by imposing natural geometric conditions, such as convexity or noncollapsedness. The latter condition is necessary due to “pancake”-type solutions, which collapse as $t \rightarrow -\infty$.

For the case $n = 1$ of the *curve-shortening flow* in the plane, S. Angenent found interesting compact noncollapsing solutions: two “Grim Reapers” that approach each other from opposite ends of the plane, so named because of the way they sweep away all other possibilities as they come together. In joint work with Hamilton and Sesum, we proved that there are no other convex ancient solutions.

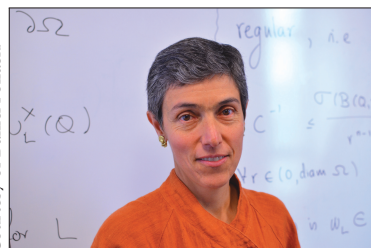
It is unknown how much of this generalizes to higher dimensions. B. White has found noncollapsing convex and compact ancient solutions. In joint work with Angenent and Sesum we have made some partial progress toward proving that these are the only ones by providing the detailed asymptotic analysis of rotational symmetric solutions as $t \rightarrow -\infty$.

The results above are only a small step forward towards understanding ancient solutions to parabolic equations. All the existing classification results are based on knowing all the candidates as either being solitons or given in closed form. The next big step forward would be to classify other ancient solutions, including the examples mentioned above. In that respect the classification of all ancient noncollapsed and compact solutions to the mean curvature flow would be the first result in this direction.

For more information come to our talk and see our recent papers at arXiv.org and references therein.

Tatiana Toro

Analysis on Nonsmooth Domains



Tatiana Toro

Tatiana Toro, Robert R. and Elaine F. Phelps Professor in Mathematics at the University of Washington in Seattle, will deliver the NAM Claytor-Woodard Lecture this year. Toro is a mathematician working at the interface of

geometric measure theory, harmonic analysis, and partial differential equations. The cross-pollination between these three areas has been one of the pillars of her research. Her work focuses on understanding mathematical questions that arise in environments where the known data is very rough. The main premise of her work is that objects that at first glance appear to be very irregular do in fact exhibit quantifiable regular characteristics when viewed through the right lens.

In her lecture Toro will focus on the deep interplay between the geometry of a domain and the boundary regularity of solutions to elliptic partial differential equations. This will allow her to illustrate the way in which ideas and tools from geometric measure theory, harmonic analysis, and partial differential equations come together to produce interesting and surprising results. It will also provide a concrete example of an instance in which the right magnifying glass reveals a precise structure that would have otherwise remained invisible.

Tatiana Toro is the Robert R. and Elaine F. Phelps Professor in Mathematics at the University of Washington. Her email address is toro@math.washington.edu.

DOI: <http://dx.doi.org/10.1090/noti1313>