JMM 2017 LECTURE SAMPLER

Barry Simon, Alice Silverberg, Lisa Jeffrey, Gigliola Staffilani, Anna Wienhard, Donald St. P. Richards, Tobias Holck Colding, Wilfrid Gangbo, and Ingrid Daubechies.

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***

Barry Simon

Spectral Theory Sum Rules, Meromorphic Herglotz Functions and Large Deviations

Barry Simon received the 2016 Steele Prize for Lifetime Achievement and was featured in the 2016 August and September issues of *Notices*.

Almost exactly forty years ago, Kruskal and collaborators revolutionized significant parts of applied mathematics by discovering remarkable structures in the KdV equation. Their main discovery was that KdV is completely integrable with the resulting infinite number of conservation laws, but deeper aspects concern the connection to the $1D$ Schrödinger equation

$$-\frac{d^2}{dx^2} + V(x) \tag{1}$$

where the potential, V, is actually fixed time data for KdV.

In particular, the conserved quantities which are integrals of polynomials in V and its derivatives can also be expressed in terms of spectral data. Thus one gets a *sum rule*, an equality between coefficient data on one side and spectral data on the other side. The most celebrated KdV sum rule is that of Gardner et al.:

$$\frac{1}{\pi}\int_0^\infty \log|t(E)|^{-1}E^{1/2}\,dE + \frac{2}{3}\sum_n |E_n|^{3/2} = \frac{1}{8}\int_{-\infty}^{\infty} V(x)^2\,dx \tag{2}$$

where $\{E_n\}$ are the negative eigenvalues and $t(E)$ the scattering theory transmission coefficient. We note that in this sum rule all terms are positive.

While these are well known, what is not so well known is that there are much earlier spectral theory sum rules, which, depending on your point of view, go back to 1915, 1920, or 1936. They go under the rubric Szegő's Theorem, which expressed in terms of Toeplitz determinants goes back to 1915. In 1920 Szegő realized a reformulation in terms of norms of orthogonal polynomials on the unit circle (OPUC), but it was Verblunsky in 1936 who first proved the theorem for general measures on $\partial\mathbb{D}$ ($=\{z \in \mathbb{C} \,|\, |z| = 1\}$)—Szegő had it only for purely a.c. measures—and who expressed it as a sum rule.

To explain the sum rule, given a probability measure, μ, on $\partial\mathbb{D}$ which is nontrivial (i.e. not supported on a finite set of points), let $\{\Phi_n(z)\}_{n=0}^\infty$ be the monic orthogonal polynomials for μ. They obey a recursion relation

$$\Phi_{n+1}(z) = z\Phi_n(z) - \overline{\alpha}_n\Phi_n^*(z);\ \Phi_0 \equiv 1;\ \Phi_n^*(z) = z^n\overline{\Phi_n\left(\frac{1}{\bar z}\right)} \tag{3}$$

where $\{\alpha_n\}_{n=0}^\infty$ are a sequence of numbers, called Verblunsky coefficients, in $\mathbb{D}$. $\mu \mapsto \{\alpha_n\}_{n=0}^\infty$ sets up a 1-1 correspondence between nontrivial probability measures on $\mathbb{D}$ and $\mathbb{D}^\infty$.

The Szegő-Verblunsky sum rule says that if

$$d\mu(\theta) = w(\theta)\frac{d\theta}{2\pi} + d\mu_s \tag{4}$$

then

$$\int \log(w(\theta))\,\frac{d\theta}{2\pi} = -\sum_{n=0}^\infty \log(1-\alpha_n|^2) \tag{5}$$

In particular, the condition that both sides are finite at the same time implies that

$$\sum_{j=0}^\infty |\alpha_j|^2 < \infty \iff \int \log(w(\theta))\frac{d\theta}{2\pi} > -\infty \tag{6}$$

Simon [3] calls a result like (6) that is an equivalence between coefficient data and measure theoretic data a *spectral theory gem*.

In 2000 Killip and I found an analog of the Szegő-Verblunsky sum rule for orthogonal polynomials on the real line. One now has nontrivial probability measures on $\mathbb{R}$, and $\{p_n\}_{n=0}^\infty$ are orthonormal polynomials whose recursion relation is

$$xp_n(x) = a_{n+1}p_{n+1}(x) + b_{n+1}p_n(x) + a_np_{n-1}(x); \quad p_{-1} \equiv 0 \tag{7}$$

where the Jacobi parameters obey $b_n \in \mathbb{R}$, $a_n \geq 0$. There is now a bijection of nontrivial probability measures of compact support on $\mathbb{R}$ and uniformly bounded sets of Jacobi parameters (Favard's Theorem).

If

$$d\mu(x) = w(x)dx + d\mu_s \tag{8}$$

then the gem of Killip-Simon says that

$$\sum_{n=1}^\infty (a_n-1)^2 + b_n^2 < \infty \tag{9}$$

$$\iff$$

$$\text{ess supp }(d\mu) = [-2,2],\ Q(\mu) < \infty \text{ and } \sum_m (|E_m|-2)^{3/2} < \infty$$

where

$$Q(\mu) = -\frac{1}{4\pi}\int_{-2}^2 \log\left(\frac{\sqrt{4-x^2}}{2\pi w(x)}\right)\sqrt{4-x^2}\,dx \tag{10}$$

The sum rule is

$$Q(\mu) + \sum_{\mu(\{E_n\})>0,\ |E_n|>2} F(E_n) = \sum_{n=1}^\infty \left[\tfrac{1}{4}b_n^2 + \tfrac{1}{2}G(a_n)\right] \tag{11}$$

Barry Simon is I.B.M. Professor of Mathematics and Theoretical Physics, Emeritus, at Caltech. His e-mail address is bsimon@caltech.edu.

DOI: http://dx.doi.org/10.1090/noti1461

where

(12)
$$F(\beta+\beta^{-1}) = \tfrac{1}{4}[\beta^2+\beta^{-2}-\log(\beta^4)], \qquad \beta \in \mathbb{R}\backslash[-1,1]$$

(13) $$G(a) = a^2 - 1 - \log(a^2)$$

The gem comes from $G(a) > 0$ on $(0,\infty)\backslash\{1\}$, $G(a) = 2(a-1)^2 + O((a-1)^3), F(E) > 0$ on $\mathbb{R}\backslash[-2,2], F(E) = \frac{2}{3}(|E|-2)^{3/2} + O((|E|-2)^{5/2})$. To get gems from the sum rule without worrying about cancellation of infinities, it is critical that all the terms are positive.

This situation changed dramatically in the summer of 2014

It was mysterious why there was any positive combination and if there was any meaning to the functions G and F which popped out of calculation and combination. Moreover, the weight $(4-x^2)^{1/2}$ was mysterious. Prior work had something called the Szegő condition with the weight $(4-x^2)^{-1/2}$, which is natural, since under $x = 2\cos\theta$ one finds that $(4-x^2)^{-1/2}\,dx$ goes to $d\theta$ up to a constant.

This situation remained for almost fifteen years, during which period there was considerable follow-up work but no really different alternate proof of the Killip-Simon result. This situation changed dramatically in the summer of 2014 when Gamboa, Nagel, and Rouault [1] (henceforth GNR) found a probabilistic approach using the theory of large deviations from probability theory.

Their approach shed light on all the mysteries. The measure $(4-x^2)^{1/2}\,dx$ is just (up to scaling and normalization) the celebrated Wigner semicircle law for the limiting eigenvalue distribution for GUE. The function G of (13) is just the rate function for averages of sums of independent exponential random variables, as one can compute from Cramér's Theorem, and the function F of (12) is just the logarithmic potential in a quadratic external field which occurs in numerous places in the theory of random matrices.

In the first half of my lecture, I'll discuss sum rules via meromorphic Herglotz functions and in the second half the large deviations approach of GNR.

References

[1] F. Gamboa, J. Nagel, and A. Rouault, Sum rules via large deviations, *J. Funct. Anal.* **270** (2016), 509–559. MR3425894

[2] R. Killip and B. Simon, Sum rules for Jacobi matrices and their applications to spectral theory, *Ann. Math.* **158** (2003), 253–321. MR1999923

[3] B. Simon, *Szego's Theorem and Its Descendants: Spectral Theory for L^2 Perturbations of Orthogonal Polynomials*, Princeton University Press, Princeton, NJ, 2011. MR2743058

Alice Silverberg

Through the Cryptographer's Looking-Glass, and What Alice Found There

Alice Silverberg

Mathematicians and cryptographers have much to learn from one another. However, in many ways they come from different cultures and don't speak the same language. I started as a number theorist and have been welcomed into the community of cryptographers. Through joint research projects and conference organizing, I have been working to help the two communities play well together and interact more. I have found living and working in the two worlds of mathematics and cryptography to be interesting, useful, and challenging. In the lecture I will share some thoughts on what I've learned, both scientifically and otherwise.

Can more than three parties efficiently create a shared secret?

A primary scientific focus of the talk will be on the quest for a Holy Grail of cryptography, namely, cryptographically useful multilinear maps.

Suppose that Alice and Bob want to create a shared secret, for example to use as a secret key for encrypting a credit card transaction, but their communication channel is insecure. Creating a shared secret can be done using public key cryptography, as follows. Alice and Bob fix a large prime number p and an integer g that has large order modulo p. Alice then chooses a secret integer A, computes $g^A \bmod p$, and sends it to Bob, while Bob similarly chooses a secret B and sends $g^B \bmod p$ to Alice. Note that Eve, the eavesdropper, might listen in on the transmissions and learn $g^A \bmod p$ and/or $g^B \bmod p$. Alice and Bob can each compute their

Alice Silverberg is professor of mathematics and computer science at the University of California, Irvine. Her e-mail address is `asilverb@math.uci.edu`.

DOI: http://dx.doi.org/10.1090/noti1453

Can Alice, through the cryptographer's looking glass, find an efficient way for many parties to create a shared secret key?

Mathematicians and cryptographers at a 2015 conference on the Mathematics of Cryptography.

shared secret $g^{AB} \bmod p$, Alice computing $(g^B \bmod p)^A \bmod p$ and Bob computing $(g^A \bmod p)^B \bmod p$. It's a secret because it is believed to be difficult for Eve to compute $g^{AB} \bmod p$ when she knows $g^A \bmod p$ and $g^B \bmod p$ but not A or B (this belief is called the Diffie-Hellman assumption). This algorithm is known as Diffie-Hellman key agreement.

Can more than two parties efficiently create a shared secret? It's a nice exercise to think about why naïvely extending the above argument doesn't work with only one round of broadcasting (in the above, the broadcasting consists of Alice sending $g^A \bmod p$, while Bob sends $g^B \bmod p$).

Here's an idea for how $n+1$ people could create a shared secret. Suppose we could find finite cyclic groups G_1 and G_2 of the same size and an efficiently computable map

$$e : G_1^n \to G_2$$

such that (with g a generator of G_1):

(a) $e(g^{a_1}, \dots, g^{a_n}) = e(g, \dots, g)^{a_1 \cdots a_n}$ for all integers $a_1, \dots, a_n$ (multilinear),

(b) $e(g, \dots, g)$ is a generator of G_2 (nondegenerate), and

(c) it is difficult to compute $e(g, \dots, g)^{a_1 \cdots a_{n+1}}$ when $a_1, \dots, a_{n+1}$ are unknown, even given $g^{a_1}, \dots, g^{a_{n+1}}$ (the multilinear Diffie-Hellman assumption).

A multilinear version of Diffie-Hellman key agreement would go as follows. Alice chooses her secret integer a_1 and broadcasts g^{a_1}, Bob chooses his secret a_2 and broadcasts $g^{a_2}, \dots$, and Ophelia chooses her secret a_{n+1} and broadcasts $g^{a_{n+1}}$. Then all $n+1$ people can compute the group element $e(g, \dots, g)^{a_1 \cdots a_{n+1}}$; for example, Bob computes $e(g^{a_1}, g^{a_3}, \dots, g^{a_{n+1}})^{a_2}$. By (c), it's hard for anyone else to learn this group element. In this way, $n+1$ people can create a shared secret. When $n = 1$ and e is the identity map on a (large) subgroup of the multiplicative group of the finite field with p elements, this is the Diffie-Hellman key agreement algorithm described above, which allows two parties to share a secret. For three parties, such maps e can be constructed from pairings ($n = 2$) on elliptic curves. For more than three parties, finding such cryptographically useful multilinear maps e is a major open problem in cryptography and an area of current research.

In [1], Dan Boneh and I raised this question; gave applications to broadcast encryption, digital signatures, and key agreement; and gave evidence that it would be difficult to find very natural mathematical structures, like "motives," giving rise to such maps e when $n > 2$. (As my coauthor generously allowed me to include in the introduction to our paper, "We have the means and the opportunity. But do we have the motive?") Events since then have led us to become more optimistic that a creative solution can be found, and we are hopeful that the combined efforts of mathematicians and cryptographers will lead to progress on this problem.

References

[1] Dan Boneh and Alice Silverberg, Applications of multilinear forms to cryptography, in *Topics in Algebraic and Noncommutative Geometry: Proceedings in Memory of Ruth Michler*, Contemporary Mathematics **324**, American Mathematical Society, Providence, RI, 2003, pp. 71–90. MR1986114

Lisa Jeffrey

The Real Locus of an Antisymplectic Involution

Lisa Jeffrey

Suppose M is a compact symplectic manifold equipped with an antisymplectic involution. Then the fixed point set of the involution is a Lagrangian submanifold.

A prototype example is complex projective space $\mathbf{CP^n}$, with the involution complex conjugation. The fixed point set of the involution is then real projective space $\mathbf{RP^n}$. In the case $n = 1$, $\mathbf{CP^1}$ is the same as the 2-sphere S^2, and the fixed point set of the involution is the equator (which is $\mathbf{RP^1}$, which is a circle).

Suppose in addition M has a Hamiltonian torus action. It is possible to define what it means for the torus action to be compatible with the involution. In the above example, the torus action is the standard action of $U(1)^n$ on $\mathbf{CP^n}$. (For $n = 1$ this is the rotation action of $U(1)$ rotating around the vertical axis.)

In 1983 Hans Duistermaat [1] proved many results in this situation, among them that the image of the moment map restricted to the fixed point set of the involution is the same as the image of the moment map for the symplectic manifold (in particular it is a convex polyhedron, as shown by Atiyah and Guillemin-Sternberg).

Numerous symplectic manifolds fit into this picture. In particular some character varieties (spaces of conjugacy classes of representations of the fundamental group) are naturally equipped with Hamiltonian torus actions. Jeffrey and Weitsman [2] developed Hamiltonian torus actions on open dense subsets in $SU(2)$ character varieties for orientable 2-manifolds, following a groundbreaking 1986 article by Goldman that describes Hamiltonian flows of a natural class of functions on these character varieties.

References

[1] J.J. Duistermaat, Convexity and tightness for restrictions of Hamiltonian functions to fixed point sets of an antisymplectic involution. *Trans. Amer. Math. Soc.* **275** (1983), no. 1, 417–429. MR678361

[2] L. Jeffrey and J. Weitsman, Bohr-Sommerfeld orbits in the moduli space of flat connections and the Verlinde dimension formula. *Commun. Math. Phys.* **150** (1992), no. 3, 593–630. MR1204322

Lisa Jeffrey is professor of mathematics at the University of Toronto. Her e-mail address is `jeffrey@math.toronto.edu`.

DOI: http://dx.doi.org/10.1090/noti1456

Gigliola Staffilani

The Many Faces of Dispersive and Wave Equations

Gigliola Staffilani

One of the most beautiful effects of dispersion is a rainbow, as in Figure 1, or, more prosaically, the refraction of a ray of light through a prism, as in Figure 2.

While looking at this timeless phenomenon it is hard to believe it is connected to Vinogradov's Mean Value Theorem, one of several deep theorems in number theory. The mathematical nature of dispersion is the starting point of a very rich mathematical activity that has seen incredible progress in the last twenty years and that has involved many different branches of mathematics: Fourier and harmonic analysis, analytic number theory, differential and symplectic geometry, dynamical systems and probability. It would take a very long book to explain all these interactions and consequences, so here we just give a small sample, which we hope can still suggest the wealth of what has been accomplished and what is still there to discover.

Let us start with one of the best-known equations of dispersive type, the nonlinear Schrödinger equation (NLS), the quantum analog of Newton's $F = ma$. We consider the Cauchy problem: that is, given initial data $u(0,x)$ at time $t = 0$:

$$\begin{cases} i\partial_t u + \Delta u = \lambda u|u|^2, \\ u(0,x) = u_0(x), \end{cases} \tag{1}$$

where $\lambda = \pm 1$ and $x \in \mathbb{R}^2$. If we want a periodic solution, then we take $x \in \mathbb{T}^2$, the torus of dimension two. Usually we measure the smoothness of the initial data by assuming that it is in a Sobolev space of order s, that is, $u_0 \in H^s$. This problem plays a fundamental role in physics that we will not discuss here, but certainly once the Cauchy problem

Gigliola Staffilani is the Abby Rockefeller Mauze Professor of Mathematics at MIT. Her e-mail address is `gigliola@mit.edu`.

DOI: http://dx.doi.org/10.1090/noti1459

Figure 1. An Alaskan rainbow.

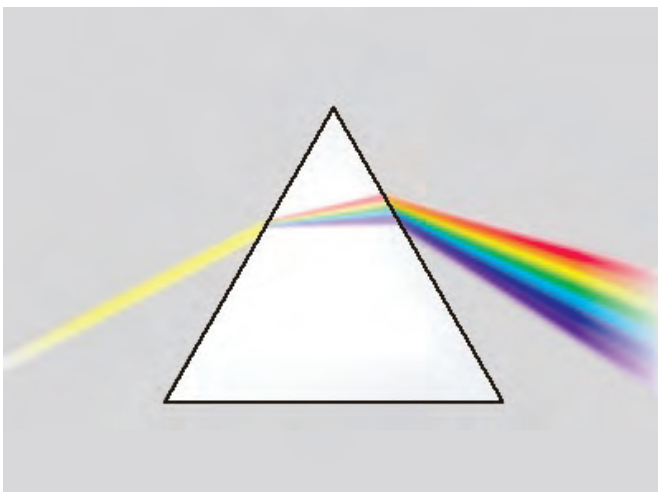

Figure 2. The dispersion in a prism has deep connections to number theory.

is set up one wants to prove existence and uniqueness of solutions, together with stability properties that allow us to say that if, for example, the initial data $u_0(x)$ changes a little, then the solution changes also only a little. This can be summarized as *well-posedness of the initial value problem*. As a physical problem (1) satisfies conservation of mass

$$M = \int |u(t,x)|^2\,dx \tag{2}$$

and of energy

$$E = \frac{1}{2}\int |\nabla u(t,x)|^2\,dx - \frac{\lambda}{4}\int |u(t,x)|^4\,dx. \tag{3}$$

Hence natural sets of initial data are the spaces L^2 and H^1. Clearly at this level of regularity not even the equation in (1) makes sense; hence we reformulate (1) via the Duhamel principle into the integral equation

$$u(t,x) = S(t)u_0(x) + \lambda \int S(t-t')u(t',x)|u(t',x)|^2\,dt', \tag{4}$$

where $S(t)$ is the Schrödinger group and $S(t)u_0(x)$ is the linear solution with initial data u_0. Since H^1 and in particular L^2 are spaces of relatively low regularities, a classical energy method based on a priori bounds such as (2) and (3) is not enough to prove well-posedness. An extremely efficient and successful way to show well-posedness instead is via (4) and a fixed point method. For this it is important to establish a function space in which a fixed point theorem can be set up. Such a function space is dictated by estimates for the linear solution $S(t)u_0$, since as a first try we can think of the nonhomogeneous term $\int_0^t S(t-t')|u|^2u(t')\,dt'$ as a perturbation. This brings us to the famous Strichartz estimates that in $\mathbb{R}^2$ read as

$$\|S(t)u_0\|_{L_t^q L_x^p} \le C\|u_0\|_{L^2}, \tag{5}$$

where the couple (q,p) is *admissible*; that is, it satisfies

$$\frac{2}{q} = 2\left(\frac{1}{2} - \frac{1}{p}\right).$$

The proof of (5) is a direct consequence of (2) and of the dispersive estimate

$$|S(t)u_0(x)| \le C\frac{\|u_0\|_{L^1}}{|t|}, \tag{6}$$

which in turn follows from the explicit formula

$$S(t)u_0(x) = \frac{c_1}{t}\int u_0(y)e^{i\frac{|x-y|^2}{c_2 t}}\,dy,$$

where c_1 and c_2 are two given complex numbers. From (6) we learn that in spite of the fact that the signal $S(t)u_0(x)$ conserves mass, it is dispersive: its intensity dies off as long as no obstacles or boundaries are present.

When we consider the periodic version of the problem (1), the situation is much more subtle, because in fact the dispersion is interrupted by the boundary conditions. It is in this case that Bourgain used tools from analytic number theory to prove that

$$\|S(t)u_0\|_{L^4_{[0,1]}L^4_{\mathbb{T}^2}} \le C\|u_0\|_{H^s(\mathbb{T}^2)}, \tag{7}$$

where $\mathbb{T}^2$ is a *rational torus*[1] and $s > 0$. The main ingredient from analytic number theory used in the proof is that on a circle of radius R there are at most $\exp C\frac{\log R}{\log R \log R}$ many lattice points sitting on it. It took about twenty years to obtain (7) for a generic torus. It was proved by Bourgain and Demeter as a consequence of their proof of the L^2 decoupling conjecture using classical harmonic analysis tools and elements from incidence geometry, initially introduced in this context by Guth. Here no analytic number theory is used, quite the opposite: Bourgain, Demeter, and Guth used harmonic analysis to prove an outstanding conjecture related to the famous Vinogradov's Mean Value Theorem.

What one can prove about the global dynamics of the problem is all linked to the focusing or defocusing nature of the equation, respectively $\lambda = 1$ and $\lambda = -1$, and then to the fact that (1) is mass critical, in the sense that the

[1] *That is, the ratio of the two periods is a rational number.*

L^2 is invariant with respect to the natural scaling of the problem. A very short analysis follows below.

The Defocusing NLS in $\mathbb{R}^2$

Global well-posedness for smooth ($s \geq 1$) data is a straightforward consequence of the fact that the local time of existence depends on the norm H^s of the data when $s > 0$, and when $s = 1$ the energy conservation (3) bounds this norm, since $\lambda = -1$. By using the I-method, global well-posedness can be shown for $s < 1$, but close to 1 serious obstructions do not allow this method to reach L^2. In fact, L^2 is a very special case, due to the criticality of the problem at this level, and a global well-posedness in L^2 was only recently proved by Dodson. This settles completely the long-time dynamics of the problem in this case.

The Focusing NLS in $\mathbb{R}^2$

In this case, the long-time dynamics is much richer since blowup is possible and solitons exist. It is in cases like these that one would like to show that a generic solution is made up by finitely many solitons and a radiation that ultimately behaves as a linear solution. In very general terms, this goes under the name of the *Soliton Resolution Conjecture*. At the moment we are far from proving this conjecture for the NLS, but a series of recent works by Duyckaerts, Kenig, and Merle proved the conjecture for certain nonlinear wave equations. On top of the usual Strichartz estimates, a large number of new tools had to be implemented in order to obtain this result. Among these tools we recall the *profile decomposition*, initially introduced by Gerard and collaborators in order to study the failure of compactness of Strichartz inequalities, and *channels of energy*.

The periodic case is much more delicate

The question of blowup for NLS equations instead has been studied in great detail in a series of works by Raphäel and Merle. In an astonishing result, they confirmed mathematically what is now known as the $\log - \log$ blow-up regime, which had been previously numerically identified by Papanicolaou, C. Sulem, and P.-L. Sulem.

The Defocusing NLS in $\mathbb{T}^2$

As mentioned above, the periodic case is much more delicate since boundary effects amplify the nonlinear nature of the problem. As recalled above, using the Strichartz estimate (7), Bourgain proved local well-posedness for rational tori in H^s for $s > 0$. Now that (7) is also available for irrational tori, Bourgain's result can be extended. Local well-posedness in L^2 is still an open, difficult, and extremely interesting question. Again in the defocusing case the energy estimate (3) is enough to show global well-posedness in H^s for $s \geq 1$. For rational tori also in this case the I-method can be used to show global well-posedness slightly below H^1. For irrational tori this should still hold, but no proof has been published yet. In any case, we now know that smooth solutions are global, and for these global solutions a very interesting and physically meaningful problem is to study the transfer of energy from low to high frequencies. This concept is linked to the notion of *weak turbulence* and *forward cascade*, on which we will not elaborate here. What we will say, though, is that one possible way to study if such a transfer of energy occurs is to analyze the growth in time of the norm H^s, for s large, of a smooth solution u. So far, we know that this growth cannot be more than polynomial. Although this result is concerned with smooth data, the tools used to obtain it are fundamentally based on very fine estimates of wave packets at a very low regime of regularity. Also as of now the proofs of these results have been presented for rational tori. One should be able to repeat them also in the irrational case. In fact, for irrational tori, one may expect a lower degree for the polynomial growth, since the set of frequencies that are in resonance, believed to be responsible for the transfer of energy, can be proved to be smaller in the irrational case. As for exhibiting solutions that actually have an H^s norm that grows in time at least logarithmically, at the moment no such result is available. It has been proved, though, by Colliander, Keel, Takaoka, Tao, and the author of this note, with techniques that resemble those used in dynamical systems, that there are solutions that start small but grow arbitrarily large.

Finally, we would like to touch upon the fact that the periodic NLS can also be viewed as an infinite-dimensional Hamiltonian system by rewriting equation (1) for $u(t,x)$ as a system for its Fourier coefficients $a_k(t) + ib_k(t)$ for $k \in \mathbb{Z}^2$. For such a system, a Gibbs measure can be defined with support in $H^{-\epsilon}$, and Bourgain proved that a global NLS flow can be defined on the support of the Gibbs measure (almost sure global well-posedness), and the Gibbs measure ultimately can be proved to be invariant. Note that such a result is the first in proving generically global well-posedness in a space of supercritical regularity with respect to the intrinsic scaling of the equation. In order to prove this result elements of probability had to be introduced, and many generalizations have now been considered and not only for NLS.

Let us now conclude by introducing one last concept associated with dispersive equations that can be viewed as infinite-dimensional Hamiltonian systems: the nonsqueezing theorem. In finite dimensions this is a celebrated theorem of Gromov. It states that a Hamiltonian flow that is also a symplectomorphism cannot squeeze a ball into a cylinder of smaller radius. Kuksin has investigated quite extensively how to extend this theorem to the infinite-dimensional case. For the infinite-dimensional Hamiltonian system associated to (1) the L^2 space can be equipped with a symplectic structure, but unfortunately, as recalled above, for now we do not know if a global NLS

flow in L^2 can be defined. Nevertheless, nonsqueezing theorems have been proved in the periodic case for the 1D cubic and NLS, for the KdV equation, and conditionally for other systems. Moreover, recently Killip, Visan, and Zhang proved that in the appropriate sense the global flow for (1) in $\mathbb{R}^2$ is indeed nonsqueezing.

You will not find here a section on the global dynamics of the focusing periodic NLS, since it remains wide open.

Anna Wienhard

A Tale of Rigidity and Flexibility—Discrete Subgroups of Higher Rank Lie Groups

Anna Wienhard

In 1872 Felix Klein proposed to approach geometry as the study of symmetry. Instead of starting with geometric quantites, he considered the geometric properties of a space to be those that are invariant under a certain group of transformations. This gave a unified approach to various geometries that had been studied extensively in the nineteenth century, in particular, to classical Euclidean geometry, spherical geometry, the newly discovered hyperbolic geometry, and projective geometry, the geometry of perspective art. In fact, Klein interpreted all three—Euclidean geometry, spherical geometry, and hyperbolic geometry—as subgeometries of projective geometry. Felix Klein's approach to geometry has deeply influenced our understanding of geometry in modern mathematics and theoretical physics.

The key role in Klein's approach is played by Lie groups, which arise as continuous groups of symmetries. Examples of Lie groups are $\mathbb{R}^n$ (as translations of Euclidean space $\mathbb{E}^n$), invertible matrices $\mathrm{GL}(n,\mathbb{R})$, matrices of determinant one $\mathrm{SL}(n,\mathbb{R})$, symplectic matrices $\mathrm{Sp}(2n,\mathbb{R})$, and orthogonal matrices $\mathrm{SO}(p,q)$. It has since become an important endeavor in mathematics to understand the structure of Lie groups and also of their subgroups, in particular, their discrete subgroups.

Discrete subgroups of Lie groups preserve additional structure of the space. This additional structure breaks the continuous symmetry preserved by the ambient Lie group. For example, the group of translations $\mathbb{R}^n$ preserves $\mathbb{E}^n$ with all its geometric properties. But if we consider inside $\mathbb{E}^n$ the set of points with integer coordinates, then this set of points is not preserved under translation by an element in $\mathbb{R}^n$, but only by elements in the discrete subgroup $\mathbb{Z}^n$. The subgroup $\mathbb{Z}^n$ is an example of a lattice in $\mathbb{R}^n$; it has finite volume fundamental domain, namely, the unit square. Figure 1 shows a planar pattern with symmetry group $\mathbb{Z}^2$. Figure 2 shows a pattern in the hyperbolic Poincaré disk with symmetry group a lattice in $\mathrm{SL}(2,\mathbb{R})$.

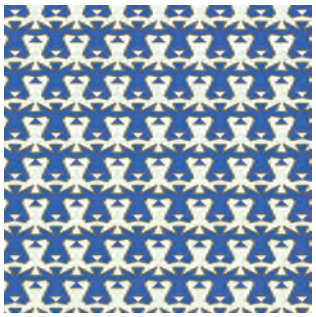

Figure 1. The group of symmetries preserving this pattern is the lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$.

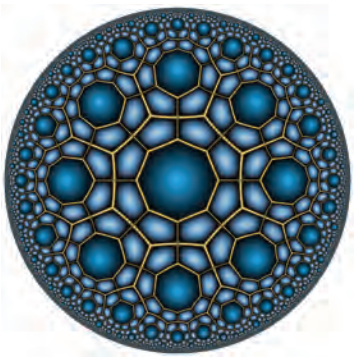

Figure 2. The group of symmetries preserving this pattern in the hyperbolic Poincaré disk is a lattice in $\mathrm{SL}(2,\mathbb{R})$.

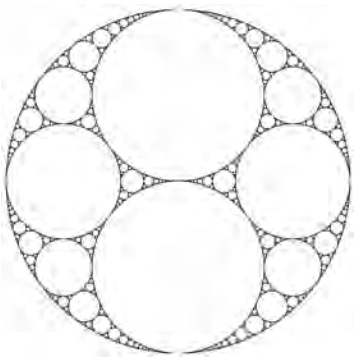

Figure 3. The group of symmetries preserving this circle packing is a nonlattice ("thin") subgroup of SO(1,3). Thin subgroups are generally harder to understand than lattice subgroups.

Anna Wienhard is a professor at Mathematisches Institut, Ruprecht-Karls-Universität Heidelberg. Her e-mail address is wienhard@mathi.uni-heidelberg.de.

DOI: http://dx.doi.org/10.1090/noti1455

Discrete subgroups also arise as monodromies of differential equations or from geometric, dynamical, or number-theoretic constructions. A special case of discrete subgroups is lattices. Lattices are very "big" discrete subgroups: they have finite covolume with respect to a natural measure on the Lie group. Discrete subgroups that are not lattices are sometimes called thin or small subgroups of the Lie groups, as in Figure 3. Whereas lattices in Lie groups are fairly well understood, it is rather difficult to get a handle on discrete subgroups that are not lattices.

For lattices there is a big difference between Lie groups of rank one, which are those whose associated geometry exhibits strictly negative curvature, and Lie groups of higher rank, which are those whose associated geometry exhibits only nonpositive curvature. For example, $\mathrm{SL}(n, \mathbb{R})$ is of rank one if and only if $n = 2$, in which case it is the group of symmetries of the hyperbolic plane. A series of celebrated rigidity results of G. Margulis implies that every lattice in a higher rank Lie group arises from a number-theoretic construction and that many questions about these lattices can be answered by considering the ambient Lie group, which is much easier to understand. Since then rigidity has been the overarching paradigm when studying subgroups of Lie groups of higher rank. In the rank one situation, in particular for $\mathrm{SL}(2, \mathbb{R})$, lattices are essentially free groups or fundamental groups of surfaces, and these groups are rather flexible. They allow for a continuous space of deformations within $\mathrm{SL}(2, \mathbb{R})$.

In recent years new developments in geometry, low-dimensional topology, number theory, analysis, and representation theory have led to the discovery of several interesting examples of discrete subgroups that are thin (i.e., not lattices) but—quite surprisingly—admit an interesting structure theory, which arises from a combination of the flexibility of free groups, surface groups, and more generally hyperbolic groups with the rigidity of higher rank Lie groups. One particularly exciting development is the discovery of higher Teichmüller spaces and their relation to various areas in mathematics, such as analysis, algebraic geometry, geometry, dynamics, and representation theory.

Wienhard discusses projective deformations of a hyperbolic 3-manifold with postdoctoral fellow Dr. Gye-Seon Lee.

Donald St. P. Richards

Distance Correlation: A New Tool for Detecting Association and Measuring Correlation between Data Sets

Donald St. P. Richards

The difficulties of detecting association, measuring correlation, and establishing cause and effect have fascinated mankind since time immemorial. Democritus, the Greek philosopher, emphasized well the importance and the difficulty of proving causality when he wrote, "I would rather discover one cause than gain the kingdom of Persia."

To address problems of relating cause and effect, statisticians have developed many inferential techniques. Perhaps the most well-known method stems from Karl Pearson's coefficient of correlation, which Pearson introduced in the late nineteenth century based on ideas of Francis Galton. The Pearson coefficient applies only to scalar random variables, however, and it is inapplicable generally if the relationship between X and Y is highly nonlinear; this has led to the amusing enumeration of correlations between pairs of unrelated variables, e.g., "Median salaries of college faculty" and "Annual liquor sales in college towns."

Székely et al. [3] defined a new *distance covariance*, $\mathcal{V}(X, Y)$, and related correlation coefficient, $\mathcal{R}(X, Y)$. These entities are defined for random vectors X and Y of any dimension. Moreover, X and Y are mutually independent if and only if $\mathcal{R}(X, Y) = 0$. These properties provide advantages of $\mathcal{R}(X, Y)$ over the Pearson coefficient and other measures of correlation.

Donald St. P. Richards is professor of statistics at Penn State University. His e-mail address is `richards@stat.psu.edu`.

This research was supported in part by National Science Foundation grants AST-0908440 and DMS-1309808, and by a Romberg Guest Professorship at the University of Heidelberg Graduate School for Mathematical and Computational Methods in the Sciences, funded by German Universities Excellence Initiative grant GSC 220/2.

DOI: http://dx.doi.org/10.1090/noti1457

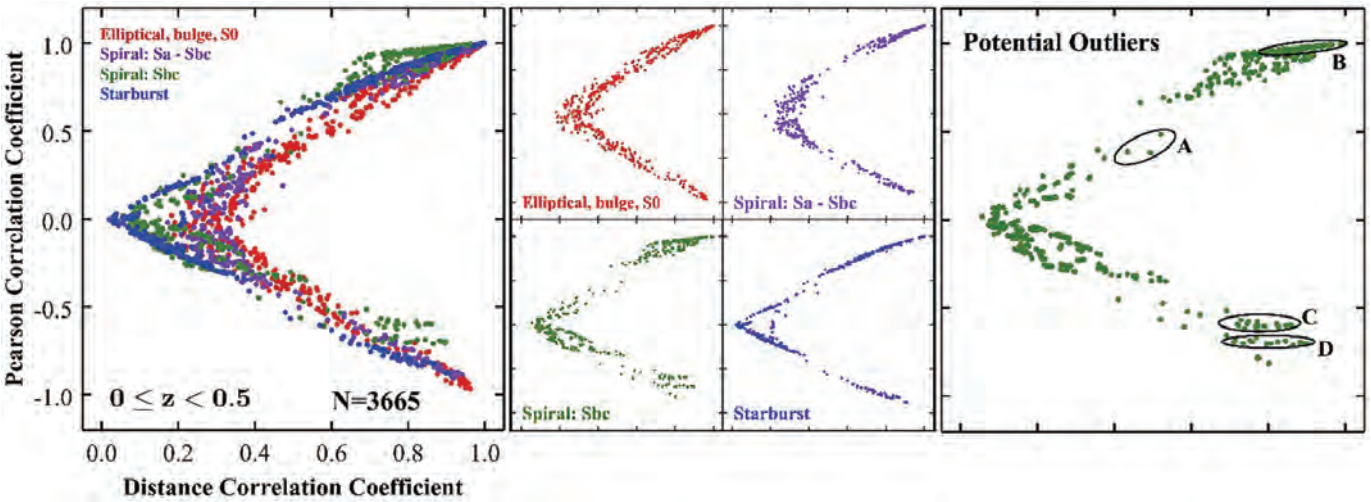

Figure 1. The distance correlation coefficient exhibited a superior ability to resolve astrophysical data into concentrated horseshoe- or V-shapes and led to more accurate classification of galaxies and identification of outlying pairs. The subplots for each galaxy type are shown in four middle frames, their superposition in the large left frame. Potential outlying pairs in the scatter plot for Type 3 galaxies are circled in the large right frame.

For a pair of jointly distributed random vectors (X, Y), it is nontrivial to calculate $\mathcal{V}(X, Y)$. Recent work of Dueck et al. [1] calculates $\mathcal{V}(X, Y)$ for the Lancaster distributions.

The distance correlation coefficient has now been applied in many contexts. It has been found to exhibit higher *statistical power*, i.e., fewer false positives, than the Pearson coefficient, to find nonlinear associations that were undetected by the Pearson coefficient, and to locate smaller sets of variables that provide equivalent statistical information.

The distance correlation coefficient has now been applied in many contexts. It has been found to exhibit higher statistical power, i.e., fewer false positives, than the Pearson coefficient

In the field of astrophysics, large amounts of data are collected and stored in publicly available repositories. The COMBO-17 database, for instance, provides numerical measurements on many astrophysical variables for more than 63,000 galaxies, stars, quasars, and unclassified objects in the Chandra Deep Field South region of the sky, with brightness measurements over a wide range of redshifts. Current understanding of galaxy formation and evolution is sensitive to the relationships between astrophysical variables, so it is essential in astrophysics to be able to detect and verify associations between variables.

Mercedes Richards et al. [2] applied the distance correlation method to 33 variables measured on 15,352 galaxies in the COMBO-17 database. For each of the $\binom{33}{2} = 528$ pairs of variables, the Pearson and distance correlation coefficients were graphed in Figure 1 for galaxies with redshift $z \in [0, 0.5)$. We found that, for given values of the Pearson coefficient, the distance correlation had a greater ability than other measures of correlation to resolve the data into concentrated horseshoe- or V-shapes. These results were observed over a range of redshifts beyond the Local Universe and for galaxies ranging in type from elliptical to spiral.

The greater ability of the distance correlation to resolve data into well-defined horseshoe- or V-shapes leads to more accurate classification of galaxies and identification of outlying pairs of variables. As seen in Figure 1, the Type 2 and Type 3 groups of spiral galaxies appear to be contaminated substantially by Type 4 starburst galaxies, confirming earlier findings of other astrophysicists. Our study found further evidence of this contamination from the V-shaped scatter plots for galaxies of Type 2 or 3.

I will also explore data on the relationship between homicide rates and the strength of state gun laws.[1] A *Washington Post* columnist has claimed that there is "zero correlation between state homicide rate and state gun laws" [4]. Although the Pearson coefficient detects no statistically significant relationship between those variables, a distance correlation analysis discovers strong evidence of a relationship when the states are partitioned by region.

[1] *As sure as my first name is "Donald," this portion of the talk will be* Huge!

Distance correlation applications rest on a curious singular integral: For $x \in \mathbb{R}^p$ and $0 < \mathrm{Re}(\alpha) < 1$,

$$\int_{\mathbb{R}^p} \frac{1 - e^{i\langle s,x\rangle}}{\|s\|^{p+2\alpha}} \mathrm{d}s = \frac{\pi^{p/2}\Gamma(1-\alpha)}{\alpha 2^{2\alpha}\Gamma(\alpha + \frac{1}{2}p)} \|x\|^{2\alpha},$$

with absolute convergence for all x. We shall describe generalizations of this singular integral arising in the theory of spherical functions on symmetric cones.

References

[1] J. Dueck, D. Edelmann, and D. Richards, Distance correlation coefficients for Lancaster distributions, (2016), http://arxiv.org/abs/1502.01413.

[2] M. T. Richards, D. St. P. Richards, and E. Martínez-Gómez, Interpreting the distance correlation results for the COMBO-17 survey, *Astrophys. J. Lett.* **784**:L34 (2014) (5 pp.).

[3] G. J. Székely, M. L. Rizzo, and N. K. Bakirov, Measuring and testing independence by correlation of distances. *Ann. Statist.* **35** (2007), 2769–2794. MR2382665

[4] E. Volokh, Zero correlation between state homicide rate and state gun laws. *The Washington Post*, October 6, 2015.

Tobias Holck Colding

Arrival Time

Tobias Holck Colding

Modeling of a wide range of physical phenomena leads to tracking fronts moving with curvature-dependent speed. A particularly natural example is where the speed is the mean curvature. If the movement is monotone inwards, then the arrival time function is the time when the front arrives at a given point. It has long been known that this function satisfies a natural differential equation in a weak sense, but one wonders what is the regularity. It turns out that one can completely answer this question. It is always twice differentiable, and the second derivative is only continuous in very rigid situations that have a simple geometric description. The proof weaves together analysis and geometry. For more, see my article with Bill Minicozzi, "Level Set Method: For Motion by Mean Curvature," in the November 2016 issue of the *Notices*.
(See `www.ams.org/journals/notices/201610/rnoti-p1148.pdf`).

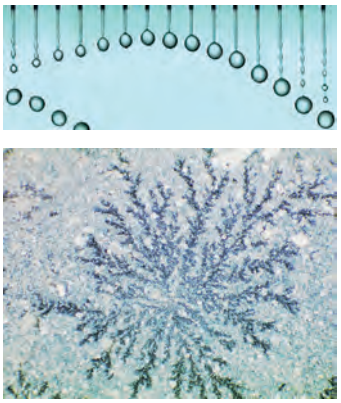

Figure 1. Droplets and crystal growth can be modeled as moving fronts.

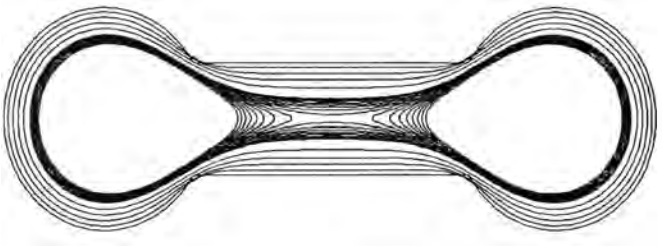

Figure 2. Cross-sections of a dumbbell moving by mean curvature. Curves are level sets of the arrival time function.

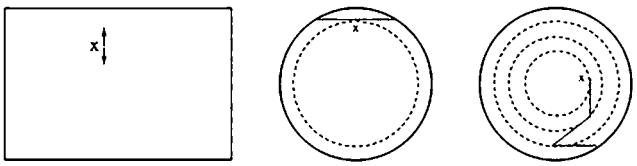

Figure 3. Kohn and Serfaty have given a game theoretic interpretation of arrival time.

Tobias Holck Colding is Cecil and Ida B. Green Distinguished Professor of Mathematics at MIT. His e-mail address is `colding@math.mit.edu`.

DOI: http://dx.doi.org/10.1090/noti1462

Wilfrid Gangbo

Paths of Minimal Lengths on the Set of Exact k-forms

Wilfrid Gangbo

Let $\Omega \subset \mathbb{R}^n$ be a bounded contractible domain with smooth boundary $\partial\Omega$. The (linear) Hodge decomposition of vector fields states that any smooth vector field $\mathbf{v}$ of Ω into $\mathbb{R}^n$ can be decomposed into

$$\mathbf{v} = \nabla\phi_0 + \mathbf{v}_0, \tag{1}$$

where $\mathbf{v}_0$ is a differentiable divergence-free vector field, parallel to $\partial\Omega$, and $\phi_0 : \Omega \to \mathbb{R}$ is a differentiable function.

A very influential paper by Y. Brenier revealed that any square integrable vector field satisfying a certain nondegeneracy condition is, up to a change of variables that preserves Lebesgue measure, the gradient of a real-valued function. This remarkable result, termed "the polar factorization of a vector field," led to the mathematical renaissance of the Monge-Kantorovich theory, now called "optimal mass transportation theory."

Since vector fields can be identified with differential 1-forms, roughly speaking, the polar factorization states that any differential 1-form is exact up to a change of coordinates that preserves Lebesgue measure. A natural mathematical question is whether there exists an analogous result for differential k-forms.

It is now time to justify why the polar factorization of a vector field can be interpreted as a nonlinear Hodge factorization and motivate the optimal transport of differential forms.

Synopsis: Renaissance of the Monge-Kantorovich Theory

Any vector field $\mathbf{u} : \Omega \to \mathbb{R}^n$ transports any measure on Ω to another measure on $\mathbb{R}^n$. For instance, the transport of μ_0, Lebesgue measure on Ω, produces the measure μ_1 on $\mathbb{R}^n$ defined by

$$\mu_1(B) := \mu_0(\mathbf{u}^{-1}(B))$$

for any $B \subset \mathbb{R}^n$. If $\mathbf{u}$ is nondegenerate, then μ_1 must be absolutely continuous with respect to Lebesgue measure on $\mathbb{R}^n$. In fact, by definition, $\mathbf{u}$ is nondegenerate means that μ_1 vanishes on any $(n-1)$-rectifiable set.

Assume without loss of generality that $\mu_0(\Omega) = 1$, μ_0 represents the distribution of a fluid occupying Ω at time $t = 0$, and μ_1 represents the distribution at time $t = 1$. The fluid consists of infinitely many particles evolving over time. Assume that at time t the velocity of the particle located at $x \in \mathbb{R}^n$ is $\mathbf{v}(t,\cdot) =: \mathbf{v}_t(x)$. At each time t, the positions of the particles are represented by a probability measure σ_t. The total kinetic energy of the system at time t is then

$$||\mathbf{v}_t||^2_{L^2(\sigma_t)} := \int_{\mathbb{R}^n} |\mathbf{v}_t(x)|^2 \sigma_t(dx).$$

Formally, one views the set of probability measures of bounded second moment as a manifold $\mathcal{M}$. The tangent space to $\mathcal{M}$ at $\sigma \in \mathcal{M}$ includes vector fields $\mathbf{v} \in C_c^\infty(\mathbb{R}^n, \mathbb{R}^n)$. The metric at σ is such that $\langle \mathbf{v}; \mathbf{v}\rangle = ||\mathbf{v}||^2_{L^2(\sigma)}$.

The square Wasserstein distance between μ_0 and μ_1 is the minimal kinetic energy required by the fluid to evolve from its initial to its final configuration. By a reparametrization argument, the Wasserstein distance between μ_0 and μ_1 is

$$\begin{aligned} W_2(\mu_0,\mu_1) &:= \min_{(\sigma,\mathbf{v})}\Big\{\int_0^1 ||\mathbf{v}_t||_{L^2(\sigma_t)} dt \mid \partial_t\sigma + \nabla\cdot(\sigma\mathbf{v}) = 0, \\ &\qquad \sigma_0 = \mu_0, \sigma_1 = \mu_1\Big\}. \end{aligned} \tag{2}$$

Here, the minimum is performed over the set of paths $t \to (\sigma_t, \mathbf{v}_t)$ satisfying some measurability conditions for the expression in (2) to make sense.

There exists a Lipschitz convex function $\psi : \mathbb{R}^d \to \mathbb{R}$ such that the optimal σ is given by

$$\sigma_t(B) = \mu_1\Big(\{y \in \mathbb{R}^n \mid ty + (1-t)\nabla\psi(y) \in B\}\Big), \ \forall\, t \in [0,1]. \tag{3}$$

When $t = 0$, (3) means that $S := \nabla\psi \circ \mathbf{u}$ preserves μ_0. Applying $\nabla\phi$ to both sides of the identity $S = \nabla\psi \circ \mathbf{u}$ with ϕ the Legendre transform of ψ, we have

$$\mathbf{u} = \nabla\phi \circ S. \tag{4}$$

The pair $(\nabla\phi, S)$ is uniquely determined in (4). Pick any $\mathbf{v} \in C^\infty(\overline{\Omega})$ and apply the previous factorization to obtain

$$\mathbf{id} + \epsilon\mathbf{v} = \nabla\phi_\epsilon \circ S_\epsilon. \tag{5}$$

The uniqueness of the pair $(\nabla\phi_\epsilon, S_\epsilon)$ yields for $\epsilon = 0$ that both $\nabla\phi_0$ and S_0 are the identity map. Thus,

$$S_\epsilon = \mathbf{id} + \epsilon\mathbf{v}_0 + o(\epsilon), \quad \nabla\phi_\epsilon = \mathbf{id} + \epsilon\nabla\phi_0 + o(\epsilon). \tag{6}$$

Observe that for S_ϵ to preserve Lebesgue measure for every ϵ small enough, $\mathbf{v}_0$ must be a divergence-free vector. Combining (5) and (6), one concludes that

$$\mathbf{id} + \epsilon\mathbf{v} = \mathbf{id} + \epsilon(\nabla\phi_0 + \mathbf{v}_0) + o(\epsilon),$$

and so the decomposition (1) holds.

Wilfrid Gangbo is professor of mathematics at UCLA. His e-mail address is `wgangbo@math.ucla.edu`.

DOI: http://dx.doi.org/10.1090/noti1458

There is another characterization of the map S in (4). It is the unique minimizer of

$$\left\{||\mathbf{u} - S||_{L^2(\mu_0)} \mid S_\# \mu_0 = \mu_0\right\}. \tag{7}$$

In summary, the geodesic problem (2), the projection problem (7), and the nonlinear factorization of vector fields are all linked.

An Open Problem

An outstanding open problem is to know if we can invent an optimal transport of k-forms, linked to a nonlinear factorization of differential forms, that yields the classical Hodge decomposition of differential k-forms by a linearization procedure as above. Unfortunately, we need to introduce some notation to state a meaningful result. For instance, assume $n = 2m$ and $\mathbf{u} \in C^1(\overline{\Omega})$ is one-to-one. Let

$$\omega_m = \sum_{i=1}^{m} dx^i \wedge dx^{i+m}$$

and consider the maps $S : \Omega \to \Omega$ that pull ω_m back to itself; in other words,

$$\sum_{i=1}^{m} dS^i \wedge dS^{i+m} = \sum_{i=1}^{m} dx^i \wedge dx^{i+m}. \tag{8}$$

For any minimizer S of

$$\left\{||\mathbf{u} - S||_{L^2(\mu_0)} \mid S \text{ satisfies (8)},\ S \in \mathrm{Diff}^1(\overline{\Omega}, \mathbf{u}(\overline{\Omega}))\right\}, \tag{9}$$

there exists a closed 2-form Φ such that

$$\mathbf{u} = (\delta\Phi \rfloor \omega_m) \circ S, \quad d\Phi = 0, \quad \text{and} \quad \nabla(\delta\Phi \rfloor \omega_m) \geq 0.$$

Here, $\rfloor$ is the interior product operator, and the interior derivative δ is defined as minus the adjoint of the exterior derivative operator d. In an ongoing collaborative research program with B. Dacorogna and O. Kneuss, we study extensions and variants of the projection problem (9) and search for geodesics of minimal length.

Ingrid Daubechies

Reunited: Francescuccio Ghissi's St. John Altarpiece

Ingrid Daubechies

Over a century ago, a fourteenth-century altarpiece was removed from its church in the Marche region in Italy and dismantled. The nine individual scenes—eight smaller pictures featuring St. John the Evangelist flanking a larger central crucifixion—had been sawn apart; the resulting panels ended up in different collections. In the process, the last of the eight smaller scenes was lost.

In preparation for an exhibition that opened on September 10, 2016, the North Carolina Museum of Art (NCMA) commissioned Dutch artist and art reconstruction expert Charlotte Caspers to paint a replacement panel. Together with NCMA curator David Steel, she designed a composition in Ghissi's style; the subject of the scene could be determined from the Golden Legend, a medieval bestseller chronicling lives of saints that was the source for the first seven small panels.

The new panel demonstrated how bright and sparkling these altarpieces were in their own time. But it became

Ingrid Daubechies is James B. Duke Professor of Mathematics and Electrical and Computer Engineering at Duke University. Her e-mail address is `ingrid@math.duke.edu`.

DOI: http://dx.doi.org/10.1090/noti1460

Figure 1a. The reunited altarpiece at the exhibition comprises all of the old panels, in their present condition, together with the aged version of panel 9.

Figure 1b. All of the rejuvenated panels of the St. John Altarpiece by Francescuccio Ghissi, together with Caspers's panel 9.

Figure 2a. Panel 1, *The Resurrection of Drusiana*, shown here in its present physical condition.

Figure 2b. With cracks removed and colors remapped, the painted portion of *The Resurrection of Drusiana* is rejuvenated.

clear that the new Caspers panel could not simply be displayed next to the eight other panels in the same frame: vivid and bright, it would lure the viewer's attention away from the faded originals, even though it was an imposter next to the real panels.

The Duke IPAI (Image Processing for Art Investigation) group, however, could help with this. By studying the old

Figure 3. A "crack map" (right) for a detail of panel 3 (left).

as well as the new panels, we could "virtually age" the new panel, i.e., make a digital copy in which the gold would look duller, the colors would be altered to mimic 650 years of aging of the pigments, small cracks would be added. A printout could then "complete" the reunited Ghissi Altarpiece (as in Figure 1a) without distracting from its authentic siblings.

The whole project was really a triumph of "how math can help"

The same technical analysis can also be applied in the reverse direction. From the correspondence between "old" and "new" for each pigment mixture used in the altarpiece, and after fine-tuning the digital image manipulations to make the transition from new to old, we can also take a high-resolution image of the old panels and map their old, aged colors to corresponding "freshly painted" versions, thus rejuvenating the fourteenth-century panels (see Figure 2a and 2b).

The exhibition at NCMA features a printout of the virtually aged panel, completing the others in a reunited altarpiece, and showcases the bright new panel separately, with a documentary on its painting process. It also shows "old" and "new" versions of all panels and short videos on the different image-processing and analysis steps that made the reconstruction possible. Some of the image processing we did was fairly standard and could be carried out by means of programs like GIMP or Photoshop. Other steps—such as automatically identifying cracks (see Figure 3) so they could then be inpainted or removing cradling artifacts from X-ray images of the paintings—involved the development of new or very recently developed approaches.

For instance, graduate student Rachel (Rujie) Yin first carried out a nifty combination of a 2D Radon transform with a wavelet transform in order to locate cradle artifacts

and then later used new machine-learning techniques based on sparse expansions and dictionary identification, which themselves emerged only in the last decade, to remove from the X-ray images the woodgrain stemming from the early twentieth-century cradle supports while leaving intact the woodgrain from the original panels.

Since even the more established image-processing tools we used are also based on very nice mathematical analysis, the whole project was really a triumph of "how math can help." In fact, we now have several more projects with the NCMA conservation and curatorial staff. When they suggest a new collaboration, they preface it with, "We wonder, could math help us with the following?"

For more information, see `dukeipai.org/projects/ghissi` and `ncartmuseum.org/exhibitions/view/13698`.

Photo Credits

Simon: Photo of Barry Simon is courtesy of the California Institute of Technology/Bob Paz.

Silverberg: Photos of Alice Silverberg, mathematicians and cryptographers at the conference are courtesy of Alice Silverberg.

Illustration from *Alice's Adventures in Wonderland* is in the public domain.

Jeffrey: Photo of Lisa Jeffrey is courtesy of Radford Neal.

Staffilani: Photo of Gigliola Staffilani is courtesy of Brye Vickmark.

Figure 1 (source: `https://commons.wikimedia.org/wiki/File:Prism-rainbow.svg`).

Figure 2 (public domain: `https://commons.wikimedia.org/wiki/File:Rainbow10_-_NOAA.jpg`).

Wienhard: Photos of Anna Wienhard are courtesy of Heidelberg Institute for Theoretical Studies.

Figures 1, 2, and 3 are by Jos Leys—`www.josleys.com`.

Richards: Photo of Donald St. P. Richards is courtesy of the University of Heidelberg.

Colding: Photo of Tobias Holck Colding is courtesy of Bryce Vickmark/MIT.

Figure 1 was created by Matthew Kuo and Christian Clasen (`https://www.flickr.com/photos/cambridgeuniversity-engineering/5957374384/in/photostream/`.

Figure 2 is courtesy of James A. Sethian.

Figure 3 is courtesy of R. V. Kohn.

Gangbo: Photo of Wilfrid Gangbo is courtesy of Wilfrid Gangbo.

Daubechies: Photo of Ingrid Daubechies is courtesy of Ingrid Daubechies.

Figure 1a is courtesy of Portland Art Museum, NCMA, Metropolitan Museum in NYC, and the Art Institute in Chicago.

Figure 1b is courtesy of IPAI group, Duke University, and museums listed in Figure 1a.

Figure 2a is courtesy of Portland Art Museum.

Figure 2b is courtesy of IPAI group, Duke University, and Portland Art Museum.

Figure 3 is courtesy of North Carolina Museum of Art and IPAI group, Duke University; and North Carolina Museum of Art.