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 1*D* 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 $b_n\in\mathbb{R}$, $a_n\ge 0$. 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

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

$$\iff$$

ess supp $(d\mu)=[-2,2]$, $Q(\mu)<\infty$ 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, *Szegő'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