ISSN 0002-9920 (print)
ISSN 1088-9477 (online)

Notices

of the American Mathematical Society

January 2017 Volume 64, Number 1

JMM 2017 Lecture Sampler
page 8

Hodge Theory of Matroids
page 26

Charleston Meeting
page 80

2017 Mathematical Congress of the Americas (MCA 2017)
page 88


Donald St. P. Richards


Gigliola Staffilani


Barry Simon


Tobias Holck Colding


Lisa Jeffrey


Alice Silverberg


Anna Wienhard


Wilfrid Gangbo


Ingrid Daubechies

AMS
American Mathematical Society

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

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}, ..., 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