Distinguished Lecture Series

Avi Wigderson on *Randomness, Pseudorandomness, and Derandomization*

FROM SEPTEMBER 14 TO 16, FOR THE FALL 2010 Thematic Program on *Asymptotic Geometric Analysis*, the Institute was fortunate to have as Distinguished Lecturer Avi Wigderson, a Professor of Mathematics at the Institute for Advanced Study in Princeton.

Wigderson is a widely recognized authority in the diverse and evolving field of theoretical computer science. He has received the Rolf Nevanlinna Prize 1994, the Yoram Ben-Porat Presidential Prize for Outstanding Researcher, the Conant Prize 2008, and the Gödel Prize 2009. His research interests lie principally in complexity theory, algorithms, randomness, and cryptography. In his series of lectures, he generously gave us an overview on all topics mentioned here, with a strong emphasis on how they connect to the fundamental notion of randomness.

In Wigderson's first lecture, he reviewed the basic concepts of computational complexity. He started with the important distinction between *easy* versus *hard* problems. A problem is *easy* if it can be solved by an efficient algorithm, i.e., an algorithm that runs in polynomial time (polytime). The class of all problems that can be solved in polytime is denoted by *P*. A problem is *hard* if there is no polytime algorithm solving it. Consider the 3-colour problem, where we want to decide if a planar map is 3-colourable. Most complexity theorists believe that 3-colour is hard since it is *NP*-complete. *NP* stands for those problems solvable in *nondeterministic polytime*; a problem in *NP* is *NP*-complete if we can efficiently reduce any *NP* problem to it. The famous *P* vs. *NP* question in complexity theory can then be stated as: is the 3-colour problem (or any other *NP*-complete problem) easy? Or informally, can *creativity* be automated?

He then discussed the power of randomness in saving time. He gave many interesting examples (e.g., generating large primes, estimating the volume of a convex body) where we have *probabilistic polytime* algorithms, but (still) no deterministic ones. Surprisingly, recent progress suggests that randomness may not be as powerful as it seems. A remarkable theorem by Impagliazzo and Wigderson shows that a reasonable assumption about computationally difficult problems (i.e., a problem computable in exponential time requiring exponential circuit size) would imply the existence of *pseudorandom* distributions, which cannot be distinguished from the uniform distribution by efficient algorithms, and thus can be used to derandomize any probabilistic polytime algorithms.

He concluded the first lecture by discussing other computational settings, primarily probabilistic proof systems, where randomness is essential. He mentioned the PCP theorem, a striking result by Arora, Lund, Motwani, Safra, Sudan and Szegedy in the '90s, showing that every proof of a statement in a formal system can be efficiently converted into another proof in a special format that is verifiable with high probability by a randomized verifier that inspects only $\mathcal{O}(1)$ letters of that proof. In a rather different direction, instead of verifying a proof quickly, one can consider the prover's desire of having his or her proof verified without allowing the verifier to learn enough of the proof to publish it first. Strikingly, this is also possible using *zero-knowledge* proofs (under a plausible assumption, e.g., factoring integers is hard).

Wigderson's second lecture introduced the world of modern cryptography. He emphasized that the goals of modern cryptography are more than just secret communications. We want to deal with many situations where there are requirements for both privacy and resilience without trusted third parties, e.g., proving a person's identity, money transfer, public bids, playing poker on the phone, etc. It turns out that these goals can be achieved based on two main assumptions. First, every agent participating in the communication is computationally bounded (say, to polytime). Second, *one-way functions* exist; a function is *one-way* if it can be easily computed on every input, but hard to invert. He also formally defined the notion of *computational indistinguishability*, and showed how it can be used to define cryptographic protocols and pseudorandom distributions.

Avi Wigderson (IAS)

Before finishing the second lecture, Wigderson reviewed *zero-knowledge* proofs and demonstrated how they work through an interesting experiment, where he played the role of the prover, who wanted to convince the audience, the verifier, that he had a correct 3-colouring of a map. The key observation is that we can permute the colours around and convert any given 3-colouring into one of 3! = 6 colourings, and for every round, the speaker would randomly shuffle the colours, and then the audience was only allowed to check one edge of the claimed 3-colourable map. Thus, eventually, the audience is convinced that the map is 3-colourable, but learned nothing about how to colour it.

In the final lecture, Wigderson focused on *expander graphs*. Expander graphs are sparse *d*-regular graphs (for some fixed *d*), but highly connected. In other words, any two disjoint sets of vertices cannot be disconnected from each other without removing many edges. Expander graphs are widely

'Avi Wigderson' continued on page 18

The Challenge of Multiple Scales in the Biological Sciences: Applications in Cerebro-vascular Perfusion

TIMOTHY DAVID IS DIRECTOR OF THE CENTRE for Bioengineering at the University of Canterbury and a Director of Blue Fern, a supercomputing unit, comprising both SMP and a Blue Gene. On November 26, 2010 at the Fields Institute, David spoke about how he uses Blue Fern to model blood flow within the human brain, a complex problem defined on a complex geometric physical space. There are pressures placed on the arterial system of the human brain when one stands up from a sitting or lying position. Nevertheless, the flow of blood and oxygen is kept quite constant by subtle and marvelous features of the arterial geometry. In an adult, 15 percent of the cardiac output is fed to the brain, but it is regulated to meet the brain's demands. Too much or too little brain blood pressure or flow creates serious health problems. David models the brain's response to pressure variation to maintain a virtually constant supply of blood to the tissue.

His numerical models describe both the vascular tree and a dynamic model of how small arteries constrict and dilate. Simulating this phenomenon as a "lumped" connection of arteries is inadequate since different parts of the arterial tree respond differently. The perfusion of blood to the brain, from the outside in, is modeled using the full complexity of fluid dynamics, including considerations of viscous and turbulent flow, Reynolds numbers, etc. He deals with the pressures and flows at the boundaries of the blood vessels. The brain blood network has a range of length scales, ranging in size from 1-25 millimetres in major arteries down to 10-20 microns in the blood vessel network of arteries, arterioles and capillaries. Arteries perfuse the cerebral cortex from the "outside in" where "penetrating" arteries spread perpendicularly into the cortex.

One of David's major contributions is the realization of the need to distinguish these scales, and integrate them into a single cohesive model.

The arteries are built in layers like coaxial cables, but they have the capacity to stretch when pressure changes quickly.

Timothy David (Canterbury) and Siv Sivaloganathan (Waterloo and CMM)

Consciousness depends on this capability. Models of calcium levels in the smooth muscle cells that surround the arteries provide mechanisms that change arterial diameters. Biochemical pathways from glutamate and potassium perfusion seem to explain dilation.

David models how the brain manages autoregulation by using conservation of CO_2. There is a vascular tree process of blood vessels that have up to four million segments and two million leaves in current models. Each leaf connects to a capillary bed. There are six major connected trees that form a network of arteries, arterioles and capillaries. All of this information, plus biochemical reactions are integrated into a single model. David has learned how to create asymmetric 3-D binary trees whose bifurcation is controlled by conservation of energy. He determines the ratio of daughter to parent using simple models. His models are tested against MRIs of human brains, which can measure the flows in major blood vessels. He notes that the pathology of the Alzheimer brain shows amyloid clumps that could possibly be the result (instead of the cause) of poor perfusion.

Tim David might be described as a Renaissance man or polymath; a scholar whose expertise spans a significant number of different complex subject areas. He is attempting to model a nearly intractable object—the human brain—using deep knowledge of Medicine, Anatomy, Biology, Biochemistry, Mathematics and Computer Science. We wish him success.

Irwin Pressman (Carleton)

'Gordon Slade' continued from page 14

function" (a Fourier-analytic way of counting the walks from o to x) decays as $\sim c\,|\,x\,|^{-2}$ This is the formulation Brydges and Slade succeeded in proving. Results of this kind had been established for weakly self-avoiding walks on a "4-dimensional hierarchical lattice" (which has a built-in self-similarity designed for renormalization arguments). Brydges and Slade work instead with the weakly self-avoiding walk in $\mathbb{Z}^4$ in continuous time. Using a rigorous renormalization group approach and Grassmann integrals, they succeed in showing the above asymptotics, at least when the penalty for non-self-avoidance is small.

The talk provided a rich survey of a deep and difficult area of probability theory. It raised hopes that tools are emerging to finally tame these models in dimension 4.

Neal Madras and Tom Salisbury (York)

'Avi Wigderson' continued from page 15

used in computer science and have many applications in derandomization, circuit complexity, error correcting codes, network design, etc. Expander graphs also have many interesting applications in various areas of pure mathematics: topology, group theory, measure theory, number theory and especially graph theory. He discussed some applications in detail and then surveyed explicit algebraic and combinatorial constructions of expander graphs.

As one of the principal contributors of many of the achievements mentioned above, Wigderson brought many new insights to his lectures. His ability to make so many sophisticated ideas accessible to a diverse audience within only three hours of lecturing was truly remarkable.

Dai Tri Man Lê (Toronto)