THE ABEL PRIZE 2021

# 挪威科学和文学院决定将 2021 年阿贝尔奖授予

## 来自匈牙利，布达佩斯 罗兰大学的 László Lovász 和

## 来自美国，普林斯顿高等研究院的 Avi Wigderson，

“表彰其在理论计算机科学和离散数学方面做出的杰出贡献，以及在将之塑造为现代数学中心领域中发挥的主导作用”。

理论计算机科学 (TCS) 是研究计算的能力和局限性的科学。其根源可追溯至 Kurt Gödel、Alonzo Church、Alan Turing 和 John von Neumann 所做的基础性研究，这些研究推动了真正的物理计算机的发展。TCS 包含两个互补的分支学科，即算法设计（为大量计算问题开发有效方法）和计算复杂性（证明算法效率的固有限制）。20 世纪 60 年代，Alan Cobham、Jack Edmonds 等人提出的多项式-时间算法的概念，以及 Stephen Cook、Leonid Levin 和 Richard Karp 提出的著名的 P≠NP 猜想，都对该领域和 Lovász 与 Wigderson 的研究产生了重要影响。

除了对更广泛的计算机科学和实践产生的巨大影响外，TCS 还为密码学奠定了基础，现在对其他几门科学产生的影响也在日益增大，通过“使用计算镜头”，让人们对其有了新的认识。离散结构（如图、字符串、排列）是 TCS 的核心，自然离散数学和 TCS 一直是紧密联系的两个领域。虽然这两个领域都从更传统的数学领域中获益匪浅，但其对传统数学领域的反向影响也越来越大。 TCS 的应用、概念和技术带来了新的挑战，开辟了新的研究方向，解决了纯数学和应用数学中的重要开放性问题。

在过去几十年中，Lászlé Lovász 和 Avi Wigderson 一直是推动实现相关发展的主导力量。他们的研究在很多方面是相互交错的，特别是，他们都对理解计算中的随机性和探索高效计算的边界做出了巨大贡献。

Lászlé Lovász 与 Arjen Lenstra 和 Hendrik Lenstra 一起开发出了 LLL 格基约减算法。给定一个高维整数格（网格），此算法可以为之找到一个不错的近乎正交基。除了因式分解有理多项式的算法等一些应用之外，LLL 算法也是一个受密码专家欢迎的工具，并成功破解了所提出的几个加密系统。令人惊讶的是，LLL 算法的分析还用于设计和保证较新的格基加密系统的安全性，这些系统甚至能够抵御量子计算机的攻击。对于一些外来的加密基元（如同态加密），它们已知的唯一构造正是通过这些格基加密系统获得的。

LLL 算法只是 Lovász 许多富有远见的贡献之一。他证明了局部引理，这是一种独特的工具，可以证明罕见的组合对象的存在，与当对象大量存在时使用的标准概率方法截然不同。他与 Martin Grötschel 和 Lex Schrijver 一起证明了如何有效地解半正定规划，从而在算法设计领域引发了一场革命。他对随机游走理论

做出了贡献，并将其应用于欧几里德等周问题和高维体的近似体积计算。他与 Uriel Feige、Shafi Goldwasser、Shmuel Safra 和 Mario Szegedy 共同发表的有关概率可验证证明(PCP)的论文提出了早期版本的 PCP 定理，这是一个极具影响力的结果，它表明，只需读取少量符号，就可以在概率上验证数学证明的正确性，且可信度很高！此外，他还解答了长期存在的问题，如完美图猜想、Kneser 猜想、确定五边形图的香农容量，近年来，他还发展了图极限理论（与 Christian Borgs、Jennifer Chayes、Lex Schrijver、Vera Sós、Balázs Szegedy 和 Katalin Vesztergombi 合作）。这项研究将极图理论、概率理论和统计物理学等要素结合在了一起。

Avi Wigderson 对计算复杂性的各个方面，特别是随机性在计算中的作用，做出了广泛而深刻的贡献。随机算法是指通过抛硬币的方法，以高概率计算正确解的算法。几十年来，研究人员发现了许多问题确定性算法，而在以前，人们只知道用随机算法来解答这些问题。由 Agrawal、Kayal 和 Saxena 提出的用于素性测试的确定性算法就是这种去随机化算法的一个突出示例。这类去随机化的结果提出了一个问题，即随机性是否真的必不可少。通过与László Babai, Lance Fortnow, Noam Nisan 和 Russell Impagliazzo 的合作，Wigderson 证明了上述问题的答案很可能是否定的。正式地，他们证明了一个计算猜想，其实质与 P≠NP 猜想类似，即 P=BPP。这意味着每一种随机算法都可以去随机化，并转化为一种效率相当的确定性算法；此外，去随机化具有通用性和普遍性，并不依赖于随机算法的内在细节。

看待这项研究的另一种方式是在难解性和随机性之间做出权衡：如果存在一个足够难解的问题，就可以通过有效的确定性算法来模拟随机性。Wigderson 与 Impagliazzo 和 Valentine Kabanets 的后续研究证明结论恰恰相反：即使是对于有已知的随机算法的具体问题，有效的确定性算法也意味着必须存在这样一个难解的问题。

这项研究与伪随机（看似随机）对象的构造密切相关。Wigderson 的研究构建了将少量真正的随机位转换为许多伪随机位的伪随机生成器，从不完美的随机性源中提取近乎完美的随机位的提取器，稀疏但仍然具有高连接性的 Ramey 图和扩展图。 他与 Omer Reingold 和 Salil Vadhan 一起引入了之字形图积，提出了构建扩展图的基本方法，并启发了 Irit Dinur 对 PCP 定理的组合证明以及 Reingold 对图连通性问题的记忆有效算法。后者提出了一种方法，可以在大型迷宫中穿行，同时记住迷宫中仅有的恒定数量的交点的特征！

Wigderson 的其他贡献包括零知识证明，这些证明可以为主张提供证据，但除了主张的有效性之外，不透露任何额外信息; 以及通信协议、电路和正式证明系统效率的下限。

由于 Lovász 和 Wigderson 发挥的领导力作用，离散数学和相对"年轻"的理论计算机科学领域现已成为现代数学的中心领域。