THE ABEL PRIZE 2021

Академия Наук Норвегии приняла решение присудить Абелевскую премию за 2021 год

Ласло Ловасу

Университет имени Ло́ранда Э́твёша, Будапешт, Венгрия, и

Ави Вигдерсону

Институт перспективных исследований, Принстон, США,

«за их фундаментальный вклад в теоретическую информатику и дискретную математику, и их ведущую роль в том, что они стали центральными областями современной математики».

Теоретическая информатика (Theoretical Computer Science – TCS) – это учение о возможностях и пределах информатики. Своими корнями она восходит к фундаментальным трудам Курта Гёделя, Алонцо Чёрча, Алана Тьюринга и Джона фон Неймана, которые привели к созданию настоящих, физических компьютеров. Теоретическая информатика включает в себя два взаимодополняющих раздела: теорию алгоритмов, которая разрабатывает эффективные методы решения вычислительных задач; и теорию сложности, изучающую принципиальные ограничения на эффективность алгоритмов. Понятие алгоритма полиномиального времени, сформулированное в 1960 году Аланом Кобхэмом, Джеком Эдмондсом и другими, и знаменитая гипотеза P≠NP Стивена Кука, Леонида Левина и Ричарда Карпа оказали сильное влияние на эту область и на деятельность Ловаса и Вигдерсона.

Кроме своего колоссального влияния на информатику и на практическое применение компьютеров, теоретическая информатика является основой для криптографии, и в последнее время оказывает все большее влияние на многие другие науки, ведя к новому пониманию, «преломленному через вычислительную призму». Дискретные структуры, такие, как графы, строки, перестановки, являются центральными в теоретической информатике, естественно тесно связанной с дискретной математикой. Обе эти области подчерпнули много полезного из более традиционных разделов математики, но одновременно наблюдается всё возрастающее влияние в обратном направлении. Приложения, понятия и методы, взятые из теоретической информатики, стали стимулами к постановке новых задач, открыли новые научные направления и привели к решению важных проблем в чистой и прикладной математике.

Ласло Ловас и Ави Вигдерсон были ведущими фигурами этого прогресса в течение последних десятилетий. Их труды во многом переплетаются друг с другом, в частности, они оба внесли фундаментальный вклад в понимание роли случайности в вычислениях и в поиск границ эффективности вычислений.

Вместе с Арьеном Ленстра и Хендриком Ленстра Ласло Ловас разработал ЛЛЛ-алгоритм (Алгоритм Ленстры - Ленстры – Ловаса) – алгоритм редукции базиса решетки. Для многомерной целочисленной решетки, этот алгоритм находит кратчайший почти ортогональный базис. В дополнение к многим применениям, таким, как алгоритм факторизации рациональных многочленов, ЛЛЛ-алгоритм является любимым инструментом крипто-аналитиков, использующимся для успешного взлома многих предложенных криптосистем. Весьма неожиданно, анализ ЛЛЛ-алгоритма также используется для создания и обеспечения безопасности новейших криптосистем, основанных на решетках, которые могут выдержать даже атаки квантовых компьютеров. Для некоторых экзотических криптографических схем, таких, как гомоморфное шифрование, единственные известные конструкции создаются посредством этих криптосистем, основанных на решетках.

ЛЛЛ-алгоритм – лишь один из многих провидческих вкладов Ловаса в науку. Локальная лемма Ловаса (также сокращающаяся ЛЛЛ) позволяет доказывать существование редких комбинаторных объектов, в отличие от стандартного вероятностного метода, который применяется, когда объекты существуют в изобилии. Вместе с Мартином Грётшелем и Лексом Шрийвером Ловас показал, как эффективно решать задачи полуопределенного программирования, что привело к революции в дизайне алгоритмов. Он внёс вклад в теорию случайных блужданий, включая приложения к эвклидовым изопериметрическим задачам и приблизительным вычислением объема тел большой размерности. Его совместная работа с Уриэлем Фейге, Шафи Голдвассером, Шмуэлем Сафра и Марио Шегеди о вероятностно проверяемых доказательствах дала раннюю версию теоремы PCP – очень влиятельного результата, показывающего, что правильность математических доказательств может быть проверена вероятностным методом с высокой степенью надежности, даже если прочесть лишь несколько символов! Кроме того, Ловас решил несколько давно известных задач – гипотезу о совершенных графах, гипотезу Кнесера, задачу определения ёмкости Шеннона пятиугольника, и в последние годы развил теорию пределов графов (совместно с Кристианом Боргсом, Дженнифер Чейес, Лексом Шривером, Верой Сос, Балаш Шегеди и Каталин Вестергомби). Эта работа связывает вместе элементы экстремальной теории графов, теории вероятностей и статистической физики.

Ави Вигдерсон внес обширный и глубокий вклад во все аспекты теории вычислительной сложности, и в особенности в роль случайности в вычислениях. Вероятностный (рандомизированный) алгоритм – это алгоритм, который может подбрасывать монету и использовать выпавшее значение для расчета решения, которое будет правильным с высокой вероятностью. За последние десятилетия ученые открыли детерминированные алгоритмы для многих задач, которые ранее решались только с применением вероятностного алгоритма. Детерминированный алгоритм Агравала-Каяла-Саксены для проверки простоты чисел (тест AKC) является поразительным примером такого «дерандомизированного» алгоритма. Дерандомизированные результаты поднимают вопрос о том, играет ли вообще вероятность существенную роль. В своих работах с Ласло Бабаи, Лэнсом Фортноу, Ноамом Нисаном и Расселом Импальяццо, Вигдерсон показал, что ответ скорее всего отрицательный. Точнее, что гипотеза о сложности вычислений, похожая по своему характеру на гипотезу P≠NP, влечёт равенство P = BPP. Это означает, что каждый вероятностный алгоритм, может быть «дерандомизирован» и превращен в детерминированный алгоритм с сопоставимой эффективностью; кроме того, дерандомизация носит общий и универсальный характер, и не зависит от внутренних свойств вероятностного алгоритма.

Можно также рассматривать эту работу как демонстрирующую компромисс

между трудностью и случайностью: если существует достаточно сложная задача, тогда случайность может быть смоделирована эффективными детерминированными алгоритмами. Последующая работа Видгерсона с Р. Импальяццо и Валентайном Кабанэ показывает обратное: эффективные детерминированные алгоритмы даже для решения конкретных задач с известными вероятностными алгоритмами, будут означать, что такая вычислительно трудная задача существует.

Эта работа тесно связана с конструированием псевдослучайных (похожих на случайные) объектов. Работы Видгерсона привели к построению псевдослучайного генератора, превращающего несколько истинно случайных битов в множество псевдослучайных битов; экстракторов, которые извлекают почти совершенные случайные биты из несовершенного источника случайности; графов Рамсея и экспандеров – разреженных, но всё же имеющих сильную связность, графов. С Омером Рейнголдом и Салилом Вадханом он ввел понятие зиг-заг произведения графов, предложив простой метод построения экспандеров, и вдохновив Ирит Динур на комбинаторное доказательство теоремы PCP, а Рейнголда – на построение эффективного (по использованию памяти) алгоритма для проблем связности графа. Этот алгоритм дает метод прохождения огромного лабиринта, помня лишь фиксированное количество точек пересечения в нём!

Другие вклады Видгерсона в науку включают в себя доказательства с нулевым разглашением, которые позволяют показать, что доказываемое утверждение верно, не предоставляя никакой дополнительной информации, кроме достоверности утверждения; и доказательство нижних границ эффективности протоколов передачи данных, схем и формальных систем доказательств.

Благодаря ведущей и направляющей роли Ловаса и Видгерсона, дискретная математика и такая сравнительно молодая наука, как теоретическая информатика, уверенно стали центральными областями современной математики.