Photo credit: Andrea Kane, Institute for Advanced Studies, Princeton, NJ, USA / Abel Prize

Биография Ави Вигдерсона

Когда Ави Вигдерсон начал свою академическую карьеру в конце 1970-х, теория вычислительной сложности, изучающая принципиальные ограничения на эффективность алгоритмов, тогда еще только зарождалась. Вклад, который внёс Вигдерсон в расширение и углубление этой отрасли математики, неоспоримо более велик, чем личный вклад любого другого человека, и наука, которая только стояла на пороге своего развития, сейчас является общепризнанной областью как математики, так и теоретической информатики. Вычислительная сложность неожиданно стала очень важной областью, создающей теоретический фундамент для обеспечения безопасности в Интернете.

Вигдерсон родился в 1956 г. в Хайфе, в Израиле. В 1977 г. он поступил в Технион, Изра́ильский технологи́ческий институ́т, и закончил его в 1980 г., получив степень бакалавра в области информатики (B.Sc.). Он отправился в Принстонский университет для работы над дисертацией, и получил докторскую степень (PhD) в Принстонском университете за выполненную под руководством Ричарда Липтона работу «*Исследования в области комбинаторной сложности*». В 1986 г. Вигдерсон вернулся в Израиль, где он через год получил постоянную работу, а в 1991 г. должность полного профессора в Еврейском университете в Иерусалиме.

В 1970 г. теоретики информатики сформулировали некоторые основополагающие идеи относительно характера вычислений, а именно, понятия P и NP. P – это множество задач, которые компьютер может легко решить, скажем, за несколько секунд, тогда как NP тоже содержит задачи, но которые компьютеру решить сложно, то есть, известные методы смогут найти ответ через, допустим, миллионы лет. Вопрос, можно ли все эти сложные задачи сделать легкими, то есть вопрос может или нет P = NP, является фундаментальным вопросом теории вычислительной сложности. И действительно, эта задача включена в список самых главных нерешенных задач всей математики.

Вигдерсон сделал поразительные успехи, исследуя роль случайности в компьютерных вычислениях. Некоторые сложные задачи

могут быть облегчены с помощью алгоритмов, когда компьютер может подбрасывать монету в процессе вычисления. Однако, если алгоритм основывается на подбрасывании монеты, всегда существует возможность того, что в решение вкрадется ошибка. Вигдерсон, вначале вместе с Ноамом Нисаном, а позднее с Расселом Импальяццо, показал, что на любой быстрый алгоритм, который может решить сложную задачу используя метод подбрасывания монеты, имеется почти такой же быстрый алгоритм, который не использует метод подбрасывания монеты, при условии наличия определенных условий.

Вигдерсон руководил исследованиями, касающимися каждой главной нерешенной проблемы в области теории сложности. Во многих аспектах эта область эволюционировала вокруг него, не только благодаря широте его интересов, но также и открытости его характера и энтузиазму, которые он проявлял в общении с коллегами. Он создал научные труды в соавторстве с более чем сотней других ученых, и был научным руководителем и наставником многих молодых исследователей в области теории сложности. «Я считаю, что мне невероятно повезло, что я живу в это время, – говорит он. – [Вычислительная сложность] – это молодая область науки. Это очень демократичная область. Это очень доброжелательная область, в которой очень легко сотрудничать, она подходит моей натуре. И, наконец, она до предела набита интеллектуальными задачами и проблемами».

В 1999 году Ави Вигдерсон получил место в Институте перспективных исследований (IAS) в Принстоне, США, и с тех работает там на постоянной основе. На одном из мероприятий, посвященных празднованию 60-летия Вигдерсона в 2016 г., директор IAS Робберт Дийкграаф сказал, что Вигдерсон дал старт золотой эре теоретической информатики в институте.

Вигдерсон известен своей способностью видеть связи между никак не связанными на первый взгляд областями. Он углубил связи между математикой и вычислительной наукой. Одним из примеров является понятие зиг-заг произведения графов, которое он ввел вместе с Омером Рейнголдом и Салилом Вадханом, и которое объединяет теорию групп, теорию графов и теорию сложности вычислений, и получила неожиданные области применения, например, как наилучшим образом выбраться из лабиринта.

Наиболее важной областью применения теории сложности в настоящее время является использование криптозащиты для обеспечения безопасности информации в интернете, такой, как номера кредитных карт и пароли. Создатели криптосистем, например, должны добиться того, чтобы задача декодирования в их системах относились к задачам класса NP, то есть, чтобы на её решение компьютеру понадобились бы миллионы лет. На ранней стадии своей карьеры Вигдерсон внес фундаментальный вклад в новый концепт в криптографии, доказательство с нулевым разглашением, которое сегодня, спустя более 30 лет, успешно используется в технологии блокчейн. В доказательстве с нулевым разглашением двое должны доказать, что доказываемое утверждение верно, не предоставляя никакой дополнительной информации, кроме достоверности утверждения. Как в примере о двух миллионерах, которые хотят доказать, кто из них богаче, не разглашая, сколько денег имеется у каждого из них. Вигдерсон, всесте с Одедом Голдбрейхом и Сильвио Микали, показал, что доказательства с нулевым разглашением могут быть использованы, чтобы доказать, секретно, любой доступный результат, касающийся секретных данных. Представим себе, что вы, например, хотите доказать кому-то, что нашли доказательство математической теоремы, не раскрывая никаких деталей относительно сущности доказательства. В этом случае доказательство с нулевым разглашением поможет вам это сделать.

В 1994 г. Вигдерсон стал лауреатом премии Рольфа Неванлинны за выдающиеся достижения в области информатики и вычислительной математики, присуждаемой Международным математическим союзом раз в 4 года на Международном конгрессе математиков. Среди многих других его наград есть также Премия Гёделя, полученная в 2009 г. и Премия Кнута, полученная в 2019 г.

Вигдерсон женат на Эдне, в которой встретился во время учебы в Технионе, и работает в Институте перспективных исследований на факультете информатики. У них трое детей и двое внуков.

Источник цитаты: Heidelberg Laureate Foundation Portraits, интервью с Ави Вигдерсоном, 2017 г.