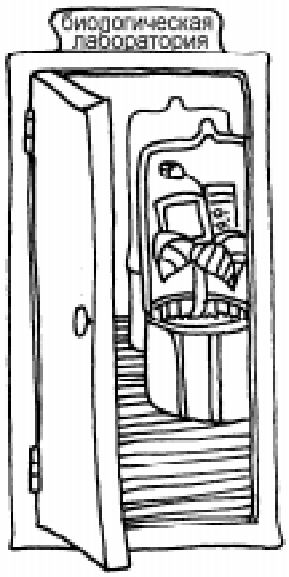
Слисенко Анатоль Олесьевич

ИНФОРМАТИКА И МАТЕМАТИЧЕСКОЕ ОБРАЗОВАНИЕ

Рассматривая взаимодействие информатики и математики, мы сразу же обнаруживаем, что, может быть, самое фундаментальное понятие информатики – понятие алгоритма – возникло в 30-е годы в математической логике (области математики, не слишком ценимой традиционными математиками даже и сейчас), то есть до появления информатики. После того, как в университетах появились компьютеры, исследования в информатике резко ускорились, и вслед за этим на математических факультетах университетов США началось изучение информатики. С тех пор университеты США остаются в целом лидерами в исследованиях и образовании в области информатики.

В первом приближении можно выделить три источника проблем для исследований в информатике: алгоритмика, программирование и вычислительная техника. Под алгоритмикой (термин, насколько я помню, был введен Д. Кнутом в 70-х годах) мы понимаем раздел, в котором исследуются методы построения эффективных алгоритмов. Проблемы сложности алгоритмов давно привлекали внимание математиков, которые внесли значительный вклад в эту область и продолжают это делать. Даже сейчас многие математические факультеты университетов США приглашают специалистов по алгоритмике и проблемам сложности алгоритмов для усиления своих отделов информатики.



Термин «биологические вычисления» может иметь разные значения...

В литературе по алгоритмике можно найти много примеров плодотворного участия математиков в алгоритмических исследованиях. Возьмем, например, быстрое умножение. Первый алгоритм, имеющий практическое значение и более быстрый, чем тот, который изучают в школе, был открыт А. Карацубой (научным сотрудником Математического Института им. Стеклова). Другой практически важный алгоритм был разработан позже математиками А. Шенхаге (A. Schoenhage) и Ф. Штрассеном (V. Strassen). Эти алгоритмы используются в системах символьной математики для умножения больших целых чисел.

Я бы сказал, что алгоритмика и проблемы сложности сейчас относятся в большей степени к математике, чем к информатике. Поэтому принципы исследований в этой области преподаются на математических факультетах. Дополнительным стимулом для этого является то, что различные системы символьной математики широко используются чистыми и прикладными математиками (во многих университетах на факультетах математики, физики и других преподаются курсы символьной математики, основанные на системах Maple или Mathematica).

Более современная область взаимодействия математики и информатики, важность которой постоянно растет, касается проблем, возникающих из развития компьютерной техники и про-

граммирования. Сами по себе эти отрасли, конечно, относятся к инженерному делу, а не к науке. Однако ясно, что нельзя ожидать заметного улучшения качества компьютеров и особенно программного обеспечения (качество которого довольно низко) без существенного улучшения их теоретической базы. Понятные и применимые на практике принципы верификации и тестирования чрезвычайно важны для развития этих областей. В настоящий момент имеются определенные подходы к проблеме верификации программ, в то время как тестирование, будучи основным инструментом проверки программ и компьютеров, остается чисто эмпирической деятельностью, чреватой существенными провалами (вспомним известную ошибку в процессоре Pentium). Ясно, что имеющиеся математические средства не могут быть применены непосредственно для получения необходимых основ тестирования. Это является стимулом для развития теории тестирования.

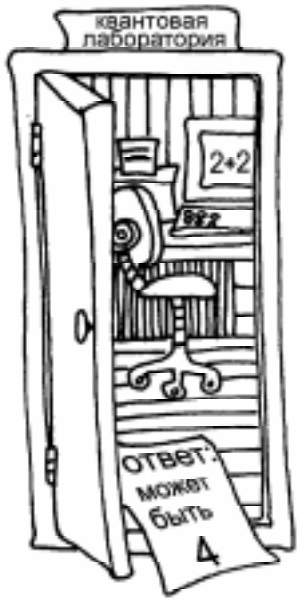
Что же касается верификации, то она тесно связана с математической логикой, которая за последние десятилетия испытала сильное влияние информатики. Прогресс очевиден, и он влияет на преподавание логики.

Я предпочитаю не касаться проблем вычислительной техники в силу недостаточных знаний в этой области. Лучше упомянуть два сравнительно недавно возникших источника постановки задач в информатике, которые, по крайней мере, косвенно связаны с математикой. Я имею в виду биологические и квантовые вычисления.

Термин «биологические вычисления» может иметь разные значения, но одно из направлений исследований связано с новой вычислительной техникой, основанной на молекулярных структурах, специфические свойства которых могут быть использованы для вычислений. Если бы удалось развить такую нано-технологию (1 метр = 10^9 нанометров), это обеспечило бы гигантскую плотность памяти и других элементов с революционными последствиями. В результате этих исследований появляются интересные математические задачи.

«Квантовые вычисления» используют принципы квантовой механики, реализация которых создает совершенно новые вычислительные возможности, хотя и вероятностного характера. Я узнал об этой идее от Ю.И. Манина в 1979 году, который пришел к ней, видимо, независимо от других. В то время Ю.И. Манин был научным сотрудником Математического Института им. Стеклова, сейчас он содиректор Института Макса Планка в Бонне. Он упомянул о ней на международном симпозиуме по теории алгоритмов, посвященном Аль-Хорезми (от имени которого произошел термин «алгоритм»).

Существует «квантовый» алгоритм разложения на множители целых чисел, созданный П. Шором (P. Schore), имеющий степенную сложность, в то время как все традиционные алгоритмы (даже вероятностные, но в традиционном смысле) имеют экспоненциальную сложность. За этот и другие результаты по квантовым вычислениям автор был удостоен премии Неванлинна, аналога Филдсовской медали.



«Квантовые вычисления» используют принципы квантовой механики...

Насколько мне известно, в США физикам удалось реализовать эти вычисления, но с числом битов, недостаточным для факторизации представляющих интерес чисел. Очевидно, что квантовые алгоритмы, использующие

разнообразные математические средства, могут оказать значительное влияние на математику и информатику.

Квантовые алгоритмы могут кардинально изменить современную криптографию – еще одну область, преобразованную (около 25 лет назад) благодаря информатике, использующую глубокие результаты из теории чисел и комбинаторики. Интересно, что А. Тьюринг, который ввел, возможно, наиболее популярное и простое понятие алгоритма – «машину Тьюринга» – был одним из основателей современной криптографии (он работал в Блэчли Парке (Blatchley Park) во время Второй мировой войны, и криптография была основной темой его работы). Поскольку математика, используемая в криптографии, довольно сложна, эта дисциплина (мы говорим о ее аспектах, относящихся к информатике) преподается на математических факультетах.

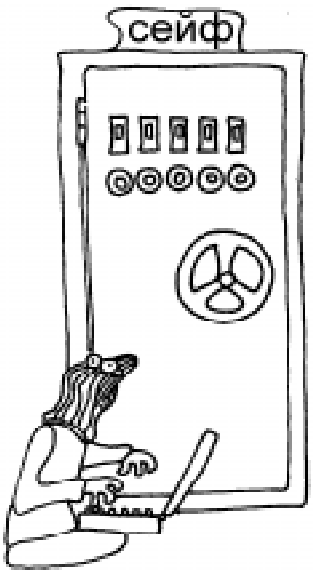
Влияние информатики на математику и математическое образование хорошо заметно в США, демонстрирующих динамизм в этой области. Европа, особенно континентальная, отстает, причем отставание доходит до 10 лет.

Теоретическая информатика в бывшем Советском Союзе была на относительно высоком уровне. Если измерять этот уровень числом цитирований в различных книгах и числом международных премий (например, А.Разборов из Математического Института Стеклова получил премию Неванлинна), то советская теоретическая информатика была, очевидно, на более высоком уровне, чем в любой из стран континентальной Европы. Значительные усилия по введению информатики в математическое образование были предприняты в университетах Москвы, Ленинграда и других городов. Относительно высокий уровень советской информатики кажется удивительным, если вспомнить постоянно снижавшийся с 70-х годов уровень разработок в вычислительной технике. Я вижу этому только одно объяснение – традиционно высокий уровень математики в бывшем Советском Союзе. Конечно, наличие незаурядных людей в этой области также было необходимо.

К несчастью, многие (возможно, даже все) достижения советской эпохи в информатике были сведены на нет последующими событиями – массовым отъездом российских ученых за границу, упадком исследований и университетского образования.

Можно ли объяснить школьникам такие понятия, как алгоритмы вообще и, в частности, квантовые алгоритмы?

Я не знаю, можно ли объяснить школьникам принципы квантовых вычислений. Может быть, в школах с углубленным изучением физики и математики (которые существуют, возможно, только в России). Что же касается классического понятия алгоритма, то, конечно, возможно, причем, по-моему, не только в старших классах, но и раньше. Попытки представить понятие алгоритма в простой и привлекательной форме предпринимались в прошлом и продолжаются сейчас.



Квантовые алгоритмы могут кардинально изменить современную криптографию...

Алгоритмическая культура является решающим элементом в информатике и в культуре программирования. Среди первых советских виртуозов программирования было много людей, хорошо знавших теорию, в частности, понятие машины Тьюринга. Можно вспомнить, напри-

мер, Г. Адельсона-Вельского, одного из создателей компьютерной шахматной программы – первого чемпиона мира среди таких программ, или Г. Цейтина, который внес выдающийся вклад в теоретическую информатику, лишь частично известный на Западе. К этим именам я могу добавить группу математической логики из Ленинградского отделения Математического Института им. Стеклова (С. Маслов, Г. Минц, В. Оревков, Ю. Матиясевич и другие). Насколько я помню, производительность программирования в нашей группе была, по крайней мере, в 30 раз выше средней производительности в то время.

Во многих российских школах есть курсы информатики, оправдано ли наличие в школах таких курсов?

Эти курсы, по моим сведениям, заполнены в основном довольно примитивным практическим изучением популярных компьютерных систем, иногда с элементами программирования. Конечно, программирование или знание популярных программных систем полезны, но они не заменяют основ культуры в информатике. Низкое качество широко используемых программ (таких, как изделия фирмы Microsoft) и низкая производительность программирования приводят к мысли, что было бы разумно ввести базовый курс информатики в школах. Я здесь упомянул низкое качество программ фирмы Microsoft, но это не является исключительно недостатком этой фирмы. В компании есть блестящие сотрудники, она внесла важный вклад в улучшение технологии программного обеспечения, ее продукция содержит много оригинальных новинок. Однако в целом индустрия программирования еще не достигла достаточной зрелости, которая вряд ли может быть достигнута без высокой культуры в области информатики.

Известен ли вам достаточно хороший школьный курс информатики где-нибудь в мире?

Насколько я знаю, такого нет. Например, во Франции чиновники от образования только начинают говорить об этом. Так что можно прождать лет десять, прежде чем будут видны какие-то изменения.

Еще один вопрос – о соотношении непрерывной и дискретной математики. Существует много курсов, посвященных непрерывной математике, но выпускники школ и университетов имеют дело в основном с дискретными задачами. Чем можно пожертвовать в этой ситуации?

Соотношение между непрерывной и дискретной математикой должно зависеть от целей обучения. Скажем, студенты, собирающиеся работать в области аэродинамики, должны изучать непрерывную математику в достаточном объеме, хотя они, наверняка, будут активно использовать компьютеры для моделирования. В целом, информатика требует в большей степени дискретной математики. Поэтому для развития соответствующей культуры мышления целесообразно ввести в школах элементы дискретной математики. Например, логику можно изучать с помощью логических головоломок. Для этого не требуется никакой техники, хотя владение техникой может значительно упростить поиск решения. Также можно использовать некоторые понятия комбинаторики для оптимизации опытов, например, при поиске фальшивой монеты с помощью весов без гирь. Эта же задача дает пример несложного алгоритма. Все упомянутые вопросы недостаточно представлены в школьных программах.

Что же касается университетов, то, как я уже говорил, проблема заключается в понимании того, кто и чем будет заниматься после окончания. У меня сложилось впечатление, что российские университеты в этом отношении ориентируются на устаревшую ситуацию. Поэтому дискретной математике не уделяется должного внимания.

С. Смейл (S. Smale), отвечая на предложение В.И. Арнольда сформулировать задачи, которые предстоит решать в будущем веке, сформулировал 18 задач, часть которых связана с его идеей обобщения машины Тьюринга для работы с вещественными числами. Интересна последняя из этих задач: каковы границы возможностей машинного и человеческого интеллекта?

Последняя из задач Смейла – о границах машинного и человеческого интеллекта – имеет вековую историю. Достаточно вспомнить Декарта или Лейбница с его автоматом для решения задач. Этой теме посвящена блестящая книга Тьюринга, переведенная на русский язык. Кстати, машины Тьюринга, оперирующие с вещественными числами, называемые BSS-машинами (Blum-Shub-Smale), были введены не Блумом, Шубом и Смейлом. Этот факт согласуется с тезисом В.И. Арнольда о том, что математические понятия получают названия не по имени их создателей (понятие машины, оперирующей с вещественными числами, было четко сформулировано, например, в книге Шеймоса (Shamos) по вычислительной геометрии). Блум, Шуб и Смейл развили теорию, показывающую важность этих понятий.

Слисенко Анатоль Олесьевич, профессор Университета Париж-12, сотрудник Института Информатики и Автоматизации РАН.

НАШИ АВТОРЫ