зования в квантовых компьютерах, за эти годы, конечно, расширился, но отнюдь не экспоненциально (будем считать, что хватит пальцев на руках – зависит от того, как считать: отдельные разновидности или классы). Но общая картина не поменялась. К чему у квантовых компьютеров были врожденные способности, то и осталось их сильным местом. Это трудно формализуемые задачи, среди которых комбинаторные, вроде проблемы коммивояжера. А также их математически близкие и немного более далекие родственники – задачи поиска совпадений (в том числе в базах данных), распознавание образов и разложение на простые множители (то есть шифрование и дешифровка).

Кванты в облаках

Есть некоторое число экспертов (и физиков – потенциальных пользователей, и специалистов HPC), вознесших такие квантовые компьютеры до небес – в облака. Именно там они смогут стать полезными и вести коммерчески вменяемое существование – квантовые сопроцессоры как дополнительная опция для тех, кому требуется эффективно решать весьма специфические задачи. Если опуститься с облаков на землю, то по некоторым, относительно оптимистичным прогнозам, лет через 10 полноценные, более универсальные квантовые компьютеры смогут позволить себе компании-гиганты, а еще через 15–20 и обычные пользователи.

Еще не догнали, но уже согрелись?

Сейчас стали слышны разговоры о квантовых вычислениях в сослагательном наклонении: если и не появятся коммерчески вменяемые квантовые компьютеры, то утешимся тем, что польза от них уже есть. Побочные эффекты разработок дают плоды. Квантовая криптография встает понемногу на коммерческие рельсы. Что до науки, то поиск алгоритмов, подходящих для квантовых компьютеров, подтолкнул развитие соответствующих разделов математики. Да и физики кое-что новое узнали.

Но с физикой не все так просто. Дело в том, что когда такая фирма, как D-Wave Systems, которую основывали, конечно, физики (кому же еще под силу разобраться в такой зауми), выходит на рынок, приходится умерить свои научные амбиции: ноу-хау надо припрятывать. Но физики-эксперты требуют доказательств «истинной квантовости» машин, корректности их работы. Приходится искать непростой компромисс открытости и проприетарности – обычная, впрочем, проблема для хайтек-фирм.

И здесь уместно вспомнить о других альтернативных путях развития вычислительной техники.

Нейроны из кремния

Идеи альтернативных принципов вычисления появлялись время от времени. Некоторые как бы подсказаны самой природой или всей историей физики, есть и совсем экзотические, которые и вычислениями-то трудно назвать – уж больно необычны. Ни естественность, ни экзотичность не стали критериями перспективности. Главный судья, говорят, Время. Но вместо «проверки временем» мы то и дело видим «проверку маркетингом» или «проверку экономикой», и в какой-то степени – «проверку политикой».

Один из «естественных» путей развития наметился давно: нейрокомпьютинг. Никто никогда не сомневался в возможностях – скрытых и уже явленных – нашего мозга. Было бы странно не пытаться воспроизвести его работу. Хотя бы грубо, приблизительно.

Мне вспоминается конференция по нейронным сетям более чем десятилетней давности. Это были сильные впечатления. Во-первых, огромное количество народу, битком набитые конференц-залы. Параллельные секции, экспериментальные аппаратные решения, широчайшая тематика приложений – от астрофизики до обнаружения хакерской активности. Инженеры из НТЦ «Модуль» рассказывали о нейрочипах собственной разработки. В общем, казалось, что пол-страны занято изучением и построением нейронных сетей.

Не пол-страны, но действительно многие. И прекрасно: столько людей занимались интересным и полезным делом, и казалось, что скоро станет понятно в общих чертах, как работает мозг. Для массовости была, конечно, более прозаическая причина, чем научная любознательность. Нейронные сети всегда считали перспективной технологией для распознавания образов и автоматического управления. А это важнейшая задача для военных. На них ресурсов не жалели, да и сейчас, кажется, не жалеют. Так или иначе, теория и практика цвела и ветвилась. Но дерево подсохло. Корни с трудом находят питание, фотосинтез еле теплится: света маловато.

Один из относительно удачных исходов той ситуации был путь «вниз»: нисхождение ученых к практическим, коммерческим проектам, основание небольших хайтек-компаний. В общем, то, что наблюдалось и в фирме D-Wave Systems, и в многих тысячах других.

Примерно на рубеже тысячелетия я посетил компанию НейрОК, ее сотрудники занимали помещение в одном из корпусов МГУ, рядом с ботаническим садом на Воробьевых горах. Там занимались очень интересными технологиями: разрабатывали замысловатые алгоритмы для 3D-дисплеев, совершенствовали текстовый поиск, занимались и оффшорным программированием, конечно. У консалтингового подразделения были клиенты в финансовой, фармацевтической, нефтегазовой отраслях. По поводу последней из них невозможно удержаться от заезженного выражения «Last but not least». С «нефтегазом» как раз у холдинга все в порядке до сих пор.

Что касается самых интересных и

Классические и квантовые генераторы случайных чисел

Текст Виктор Задков, Юлия Владимирова
Иллюстрация Владимир Камаев

Генерация действительно случайных чисел играет очень важную роль в самых разных приложениях – в криптографии, в области численного моделирования, в игровой индустрии и других областях. В последние пятьдесят лет, в связи с расширением области применения компьютеров и быстрым развитием электронных сетей связи, число таких приложений постоянно растет. Высокое качество генерации случайных чисел играет жизненно важную роль. Это обстоятельство подчеркивает известный афоризм Роберта Р. Кавью из ORNL: «Генерация случайных чисел слишком важна, чтобы оставлять ее на волю случая».

К сожалению, этот факт зачастую упускается из виду. Здесь можно привести пример алгоритма RANDU, десятилетиями использовавшегося на мейнфреймах, но оказавшегося впоследствии очень плохим, что вызвало сомнения в достоверности результатов многих исследований, использовавших этот алгоритм.

Остановимся кратко на основных приложениях. Сначала рассмотрим криптографию.

Криптография может быть определена как «наука и искусство сохранения сообщения в безопасности». Она состоит из алгоритмов и протоколов, которые могут быть использованы для обеспечения конфиденциальности, подлинности и целостности передаваемой информации. Криптографические алгоритмы различны, и выбор конкретного алгоритма зависит от поставленной задачи. Некоторые из них трудно взломать, но для их работы требуются существенные вычислительные мощности и сложное управление ключами. Другие алгоритмы легче взломать, но они и менее требовательны, а следовательно, лучше подходят для некоторых приложений. Однако общим является тот факт, что все они требуют генерации истинно случайных чисел для создания ключей, и их количество зависит от схемы шифрования. Многие приложения безопасности потерпели неудачу или были серьезно нарушены, поскольку их генераторы случайных чисел не были достаточно случайными.

Для того чтобы гарантировать конфиденциальность передаваемого сообщения, отправитель создает зашифрованный текст путем сочетания текста, который необходимо передать, с ключом с помощью алгоритма шифрования. Затем этот зашифрованный текст передается по незащищенному каналу связи получателю, который использует алгоритм расшифровки и ключ для расшифровки, чтобы восстановить исходный текст. В идеале злоумышленник не может расшифровать зашифрованный текст без ключа. Таким образом, сила системы шифрования в конечном итоге зависит от силы ключа или, что эквивалентно, от сложности для перехватчика угадать его. Эта трудность заметно увеличивается с длиной ключа – типичные размеры ключа, используемые в настоящее время, составляют 56 бит (DES), 168

самых, видимо, наукоемких разработок, которые впитали в себя и применение нейросетевых алгоритмов в том числе, то с ними, как и следовало ожидать, не все так благополучно, как с околонефтяными проектами. 3D-проект заморожен, потому что инвестирования, достаточного для новых разработок, да и на реализацию старых, найти, судя по объявлениям на сайте фирмы, не удалось. Этому можно огорчиться, но стоит ли удивляться? Как работает мозг, еще не разобрались, города на Марсе не построили, но жизнь продолжается.

Со скоростью света, с неловкостью динозавра

Оптические вычисления – тоже вполне естественный путь развития вычислительной техники. Если мы хотим, чтобы устройство работало быстро, то как не использовать свет, который быстрее всех? Казалось, что через десяток лет оптические вычислители если не вытеснят, то хотя бы выступят достойно. Я говорю здесь не об оптике вообще, не о волноводах, а об оптических арифметических устройствах. И этим занимались у нас давно.
Мне запомнилась первая встреча с одним из пропонентов оптических вычислений. Я проверил, есть ли пленка в диктофоне, свежа ли батарейка. Я надеялся, что обойдется без Powerpoint-презентаций, будет непринужденная беседа. Но встреча требовала явно других средств запечатления. Видеокамеры у меня не было. Руководитель группы оптиков принес небольшой деревянный ящичек, вроде сильно выросшего ноутбука. В ящичке, оказалось, был макет с детальками и табличками, поясняющими: вот «призма», вот «диод», а это «нелинейный оптический элемент». Форма подачи материала была настолько для меня неожиданна, что мне запомнилось только общее впечатление – ни фамилий, ни названия НИИ я, увы, не запомнил.
Живы ли идеи оптических вычислений? Живы, но как-то подспудно. С очень большой вероятностью оптические элементы в ближайшие годы будут интегрированы в кремниевые чипы, но это будут, скорее всего, контроллеры сетевых устройств. Данными будут все чаще обмениваться по волокну. Самая заметная попытка использовать оптику в суперкомпьютерах – узлы IBM Power 775 с оптическими межсоединениями. На основе такой архитектуры собирались строить Blue Waters для Университета Иллинойса, но высокая себестоимость оптических трансиверов, то есть устройств, преобразующих оптический сигнал в электрический и обратно, вынудила даже IBM выйти из проекта, расчистив путь для Cray.
Время играет на оптику. Она будет дешеветь и вытеснять медь.
А кремний? Об арифметических устройствах на оптических элементах речь не идет – вычислять будут по-прежнему рабочие кремниевые лошадки-транзисторы. Но кто знает, возможно, с распространением волоконной оптики в межсоединениях вопрос о чисто оптических вычислениях снова станет уместным?
Другие гиганты брались за оптические вычисления. В знаменитой Bell Labs, принадлежащей AT&T, в 1980-е разработали оптический компьютер на квантово-размерных полупроводниковых элементах, использующих нелинейные оптические эффекты. В нем была реализована двоичная логика, система имела разрядность 32 бита. До коммерческой системы дело не дошло: не выдержала проверку временем (долларом) или не дождалась своего времени, как и многие удивительные проекты Bell Labs. Ни тебе оптических компьютеров, ни такси на воздушной подушке. Это была отнюдь не последняя попытка создания оптического компьютера. Например, компания Lenslet создала оптический процессор Enlight 256. Сейчас домен lenslet.com выставлен на продажу.
Но и в университетских лабораториях, и в больших и небольших компаниях исследования продолжаются. Регулярно проводятся международные конференции по оптическим вычислениям, причем HPC там обязательный пункт повестки дня.

Мокрые технологии

Перечисленные пути развития выглядят почти естественным ходом развития технологий и человеческой мысли. Во всяком случае, на фоне линии «мокрых вычислений» (wet computing). Эти идеи, откровенно выражаясь, звучали и звучат просто безумно.
К тому же это не такие уж свежие идеи. Во времена советского нейробума, первых дискуссий о квантовых и оптических компьютерах об этом уже говорили. Грубо идея такова: если у нас есть комбинаторная задача, зачем делать работу за саму Природу? Не поместить ли в колбу смесь длинных молекул (полимеров, например), способных образовывать цепочки, соединяться разнообразными способами, а мы лишь «подсмотрим» решение, которое найдет сама природа, отберем, используя химические методы, цепочки, удовлетворяющие условиям комбинаторной задачи? В нескольких граммах реактива молекул достаточно, чтобы они «перебрали» все возможные комбинации. Получаются весьма своеобразные параллельные вычисления: все молекулы участвуют в вычислениях (в химической реакции), но лишь немногие из них «вычислят» правильный ответ, «склеившись» нужным образом.
Сначала речь шла о длинных полимерных молекулах. Теперь этот принцип применяют к молекулам ДНК, про «мокрый», wet computing, почти забыли, зато говорят про DNA computing. ДНК-компьютеры можно найти исключительно в лабораториях. На них уже научились решать вполне «обычные» задачи. Например, уже создана система из 74 молекул, которая умеет вычислять квадратные корни. Но, дойдя до этого пункта, надо бы вернуться к тому, с чего началось это повествование,

бит (3-DES) и 256 бит (IDEA и AES). Непредсказуемость ключа является функцией от степени случайности генерируемых чисел, используемых для генерации ключа. Следовательно, необходимо использовать достаточно длинные последовательности истинно случайных чисел для генерации ключа.
Другим примером служит процедура аутентификации (authentication) – проверка подлинности. Эта процедура необходима, например, для того, чтобы при подключении клиента к серверу система удостоверилась в том, что он на самом деле имеет право на доступ к данным. Не обсуждая деталей данной процедуры, отметим, что на практике она часто использует случайные числа.
Для моделирования и имитации сложных систем ученые разработали методы, опирающиеся на случайные числа. Эти методы являются быстрыми и ведут к высокой степени точности получаемых результатов. Они имеют большое значение для современного численного моделирования (метода Монте-Карло, имитационного моделирования и т. д.). Случайные числа необходимы и в лотереях и азартных играх. Здесь должна отсутствовать возможность для игроков увеличить вероятность выигрыша, обнаружив склонность к определенным результатам в процессе игры. Поэтому современные лотереи и игровые автоматы основаны на использовании случайных чисел, чтобы гарантировать одинаковую вероятность выигрыша.
Как мы видим, случайные числа окружают нас повсюду. Что же такое случайные числа?
Хотя на первый взгляд ответ на этот вопрос интуитивно понятен каждому, дать точное определение оказывается довольно сложно. Случайное число – это число, порожденное процессом, исход которого непредсказуем и который не может быть впоследствии воспроизведен надежно. Это определение хорошо работает при условии, что имеется некий «черный ящик» — называемый, как правило, генератором случайных чисел, – который выполняет эту задачу. Если мы имеем какое-то одно число, то невозможно проверить, является ли оно результатом генератора случайных чисел или нет. С целью изучения случайности на выходе такого генератора необходимо рассматривать последовательности чисел. Определить, является ли последовательность бесконечной длины случайной или нет, довольно просто. Последовательность является случайной, если количество содержащейся в ней информации – в смысле теории информации Шеннона – тоже бесконечно. Интересно, что бесконечная случайная последовательность содержит все возможные конечные последовательности.
Если мы имеем конечную последовательность чисел, то формально невозможно проверить, является ли она случайной или нет. Можно только проверить, что она имеет статистические свойства случайных последовательностей, т. е. все числа в последовательности равновероятны, однако это трудная и непростая задача. Для преодоления этих сложностей были предложены различные способы, на которых мы не будем останавливаться. Важным является тот факт, что цифры в случайной последовательности не должны быть связаны. Знание одного из чисел последовательности не должно помогать в прогнозировании других. Далее речь будет идти именно о таких числах.
Таким образом, имея последовательность случайных чисел, созданную генератором случайных чисел, нам надо определить, является ли она действительно случайной и в какой степени. Для этого разрабатываются статистические тесты случайности, основанные на вычислении определенных статистических величин и сравнении их со средними значениями, которые были бы получены в случае случайной последовательности. Эти средние значения получаются из расчетов по модели идеального генератора случайных чисел. Тестирование случайности является эмпирической задачей. Необходимо провести множество испытаний, каждое из которых выявляет определенный тип несовершенства в последовательности.
Одним из примеров является частотный тест. В случае двоичной последовательности при помощи него определяется относительная частота выпадения 1 по отношению к выпадению 0. Другой пример – автокорреляционный тест, исследующий корреляции между соседними битами. Как видно, задача определения случайности числа нетривиальна, поэтому важное значение имеет выбор адекватного генератора для получения случайных чисел. Рассмотрим теперь различные типы генераторов случайных чисел.

Генерация случайных чисел

Генератор случайных чисел представляет собой устройство, которое

– к незадачливому коммивояжеру, о котором читатель, не ровен час, вообще забыл.

Вспомним о коммивояжере

Что объединяет способы вычисления, о которых шла речь? Очевидно, что это – перспективность и смелость идей при полной, если не безнадежной удаленности от мейнстрима вычислительной техники.
Но не только. У всех этих способов вычислений есть свои «предпочтения» по части алгоритмов, и вкусы здесь если не совпадают, то сильно пересекаются. В некотором смысле точка их пересечения – тот самый коммивояжер и его знаменитая проблема, точнее, задачи похожего класса – очень сложные и совершенно не похожие на те, что решают суперкомпьютеры, чтобы попасть в список TOP500 (Linpack проверяет эффективность решения огромной системы линейных уравнений). И квантовые, и оптические, и ДНК-компьютеры хороши там, где нужен перебор возможностей, а не там, где правит бал принцип SIMD, то есть Single Instruction Multiple Data – одна команда и много данных, когда хорошо бы никаких «если». А первое, что поручили «рассчитывать» молекулам – это путь коммивояжера. Он может ликовать: никто из «альтернативщиков» о нем не забыл, его проблему упоминают в этих кругах часто.
В списке задач, которые решали в одной из лабораторий, где занимаются оптическими вычислениями, используя задержки, были такие алгоритмы:

- *Гамильтонова проблема пути* (привет нашему коммивояжеру).
- *Проблема суммы подмножеств.*
- *Диофантовы уравнения.*
- *Задача о точном покрытии.*

На таких задачах можно получить выигрыш по сравнению с традиционными вычислениями.
Это отнюдь не отвлеченные проблемы, и выиграет от них не один коммивояжер. Они, например, имеют отношение к обнаружению паттернов, а в этом уже заинтересованы не только ученые и силовики, но и биржевые брокеры, финансовые аналитики.
В распознавании образов надеялись на нейронные сети. Но одна из проблем состояла в эффективном обучении сети. И как раз одна из идей применения квантовых компьютеров была в том, чтобы приспособить их, в том числе нынешние, а не только будущие их воплощения, для обучения нейронной сети, которая уже дальше будет сама распознавать то, то от нее потребуют.
Для обучения нейронных сетей нередко используют генетические алгоритмы, в которых найденные «случайным» образом решения («мутанты») борются за выживание, подобно живым существам в процессе эволюции.
Генетические алгоритмы и ДНК-вычисления сочетаются не только тематически, но и технически. Кто знает, может, на каком-то витке развития вычислительной техники генетические алгоритмы будут все-таки воплощать на генетических машинах. Или на оптических. Или на квантовых. Во всяком случае, ясно, что традиционные архитектуры, тем более современные «молотилки», создавались и оптимизировались не для таких задач.
Но предсказать Путь развития вычислительной техники – задача почти безнадежная. Уж лучше помогать в поиске пути окончательно растерявшемуся коммивояжеру.

создает последовательности чисел, описанные выше. Существуют два основных вида генераторов: программное обеспечение и физические генераторы. С общей точки зрения программного обеспечения генераторы производят так называемые псевдослучайные числа. Хотя они могут быть полезны в некоторых случаях, они не должны использоваться в большинстве приложений, где требуется истинная случайность. Рассмотрим эти два класса генераторов.

ГПСЧ

Компьютер – это детерминированная система. Получая на входе определенные данные, программа всегда будет давать на выходе один и тот же результат. Отсюда вытекает фундаментальное свойство, а именно: невозможно при помощи программы получить последовательность истинно случайных чисел.
Полученная последовательность может иметь некоторые свойства случайных последовательностей и, таким образом, пройти несколько статистических тестов случайности, но ее всегда можно воспроизвести. Никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства. Такие генераторы называют генераторами псевдослучайных чисел (ГПСЧ).

Любой ГПСЧ с ограниченными ресурсами рано или поздно зацикливается – начинает повторять одну и ту же последовательность чисел. Длина циклов ГПСЧ зависит от самого генератора и составляет около 2n/2, где n – размер внутреннего состояния в битах (линейные конгруэнтные и LFSR-генераторы обладают максимальными циклами порядка 2n). Если порождаемая ГПСЧ последовательность сходится к слишком коротким циклам, то такой ГПСЧ становится предсказуемым и непригодным для практических приложений.
Большинство простых арифметических генераторов хотя и обладают большой скоростью, но страдают от многих серьезных недостатков.

- *Слишком короткий период/периоды.*
- *Последовательные значения не являются независимыми.*
- *Некоторые биты «менее случайны», чем другие.*
- *Неравномерное одномерное распределение.*
- *Обратимость.*

ГПСЧ состоит из алгоритма, в котором вводится некоторое начальное значение и затем методом итераций производится последовательность псевдослучайных чисел. Хотя период последовательности может быть очень длинным, но она всегда будет периодической. Одним из свойств таких последовательностей является тот факт, что, как только один из элементов последовательности известен, все остальные элементы – и предшествующие, и последующие, – могут быть определены. Очевидно, что это свойство особенно важно учитывать при использовании таких последовательностей в криптографии для генерации ключа. Хорошие ГПСЧ выдерживают большинство статистических тестов, но тем не менее важно понимать, что если последовательность считается достаточно долго, то при проведении некоторых тестов вы всегда потерпите неудачу, поскольку последовательность все-таки периодична.
Может показаться, что ГПСЧ бессмысленны, поскольку имеют много ограничений, но это не так. Несмотря на то, что они не производят истинно случайные числа, эти генераторы имеют ряд преимуществ. Во-первых, их стоимость практически равна нулю, так как они могут быть реализованы в программном обеспечении и многочисленные библиотеки находятся в свободном доступе. Во-вторых, их главный недостаток – а именно что последовательности, которые они производят, воспроизводимы – может в некоторых случаях представлять собой преимущество. При использовании случайных чисел для научных расчетов иногда бывает полезно иметь возможность воспроизвести последовательность чисел при отладке программы моделирования. Это одна из причин – другая причина состоит в отсутствии хороших физических генераторов случайных чисел, – вот почему эти генераторы широко используются в этих приложениях. Тем не менее даже в этой области важно быть осторожным при использовании псевдослучайных чисел. Они, как было показано, ведут к появлению артефактов в определенных моделях. Хороший подход заключается в использовании псевдослучайных чисел при отладке, а затем, при расчетах, – в использовании физического генератора для уточнения и подтверждения моделирования.

Физические источники случайных чисел

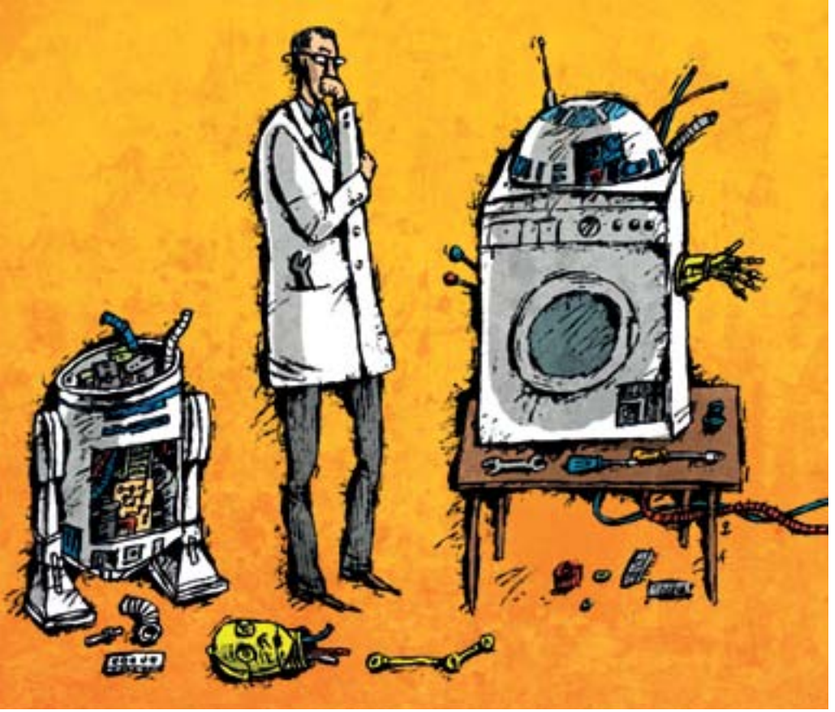
В случаях, когда использование псевдослучайных чисел не подходит, необходимо прибегать к использованию физического (аппаратного) генератора случайных чисел. Аппаратный генератор случайных чисел — устройство, которое генерирует последовательности случайных чисел на основе измеряемых параметров протекающего физического процесса. Процесс может описываться либо классической, либо квантовой физикой. Классическая физика, разработанная физиками до начала XX века, описывает макроскопические системы. Квантовая физика описывает микроскопические системы, такие как атомы, молекулы, элементарные частицы и т. п.
Проблема, возникающая с физическими генераторами случайных чисел, состоит в том, что такие генераторы могут производить смещенные последовательности (когда определенная последовательность чисел повторяется чаще). Смещение возникает из-за трудностей в разработке точно сбалансированных физических процессов. Однако существуют алгоритмы пост-обработки, которые могут быть использованы для удаления смещения в последовательности случайных чисел.

Классическая физика

Макроскопические процессы, описываемые классической физикой, можно использовать для генерации случайных чисел. Самый известный генератор случайных чисел – бросание монеты – принадлежит к этому классу. Несмотря на свою популярность, бросание монеты, очевидно, не очень удобно, когда требуется большое число случайных событий.
Другие примеры – физические генераторы случайных чисел на основе хаотических процессов – включают мониторинг электрических шумов тока в резисторе. Формально эволюция таких генераторов не является случайной, однако очень сложна. Можно сказать, что детерминизм скрывается за сложностью.
В качестве генератора шума используют шумящее тепловое устройство, например транзистор. Существуют физические генераторы случайных чисел, использующие различные физические процессы, такие как радиоактивный распад, шумы аналоговых сетей, космическое излучение, фотоэлектрический эффект, другие квантовые явления.

Квантовая физика

В отличие от классической физики квантовая физика принципиально вероятностна. Поэтому при выборе процесса, лежащего в основе генератора истинно случайных чисел, выбор естественным образом падает на квантовые процессы как источники случайности. Формально квантовые генераторы случайных чисел являются единственно верными генераторами случайных чисел, однако обладают и другими преимуществами. Вероятностная природа (внутренняя случайность) квантовой физики позволяет выбрать очень простой процесс как источник случайности. Это означает, что такой генератор легко моделировать и его функцио-



нирование можно контролировать для того, чтобы подтвердить, что он работает правильно и на самом деле производит случайные числа. До недавнего времени единственный существующий квантовый генератор случайных чисел был основан на наблюдении радиоактивного распада некоторых элементов. Хотя подобные генераторы создают последовательности высокой степени случайности, эти генераторы являются весьма громоздкими, а использование радиоактивных материалов может быть вредно для здоровья. Современное развитие науки и техники позволило ученым создать простые и недорогие квантовые генераторы случайных чисел, использующие квантовый оптический процесс как источник случайности. Рассмотрим их работу подробнее.

Свет состоит из элементарных «частиц», называемых фотонами. В определенной ситуации фотоны демонстрируют случайное поведение. Одна из таких ситуаций, которая очень хорошо подходит для генерации бинарных случайных чисел, заключается в следующем. На полупрозрачное зеркало направляются фотоны, генерируемые источником одиночных фотонов. Фотон может отразиться, а может пройти через полупрозрачное зеркало с вероятностью 50%. Выбор, который «делает» фотон, абсолютно случаен. На выходе системы стоят два счетчика фотонов, регистрирующих прошедшие и отраженные фотоны и формирующих выходные электрические сигналы.

Кроме оптической части – «сердца» генератора случайных чисел – система включает в себя подсистему, которая управляет синхронизацией, а также сбором и обработкой данных, поступающих с детекторов, выполняет статистические и аппаратные проверки последовательности. Как отмечалось выше, физические процессы трудно точно сбалансировать. Таким образом, трудно гарантировать, что вероятность записи 0 и 1 в точности равна 50%. Например, в генераторе Quantis разница между этими двумя вероятностями меньше 10%, что эквивалентно вероятностям от 45% до 55%. Поскольку это смещение не может быть приемлемым для некоторых приложений, то обязательно выполняется алгоритм постобработки для удаления смещения в последовательности случайных чисел. Как уже говорилось выше, одним из главных преимуществ квантовых генераторов случайных чисел на оптических фотонах является то, что они основаны на простом и принципиально случайном процессе, который легко моделировать и контролировать. Подобные квантовые генераторы имеют высокую скорость выходного потока – до 10-16 Мбит/с, – при которой не наблюдается никаких корреляций и выполняются все статистические тесты. Еще одним примером является генератор случайных чисел с использованием полупроводникового лазера с короткими и резкими пиками интенсивности. Лазер пропускается через среду с обратной связью с задержкой, то есть интенсивность излучения на выходе определяется интенсивностью сигнала на входе и состоянием среды, которое зависит от интенсивности на входе. Известно, что изменение интенсивности – процесс квазипериодический, то есть с течением времени почти повторяется, поэтому напрямую использовать его в качестве генератора случайных чисел нельзя.

Для того чтобы избавиться от квазипериодичности, интенсивность излучения замеряется примерно 2.5 миллиарда раз в секунду. Результат каждого измерения записывается в строку длиной в 8 бит. Он вычитается из значения предыдущего измерения, а результат усекается. Таким образом, удается избавиться от квазипериодичности и добиться генерации случайного потока нулей и единиц со скоростью примерно 12.5 Гигабит в секунду.

В заключение можно с уверенностью сказать, что генерация случайных чисел необходима для решения задач безопасности и надежности передачи и хранения данных, численного моделирования и многих других приложений. Благодаря своей вероятностной природе квантовая физика является идеальным источником случайности.

Математический экспансионер

Текст Владимир Тучков

Он стремился создать математическую модель всего сущего на свете, уподобившись Творцу.

Разнообразие научных направлений, которыми занимался и которые активно развивал за свою относительно короткую жизнь математик Алексей Андреевич Ляпунов (1911–1973) в определенной степени проистекает из многообразия научных, культурных и педагогических поприщ, на которых добились впечатляющих результатов его многочисленные родственники.