

В.В. Ковальчук, Л.М. Мисеев, М.В. Кузнецов
НАНОМЕТРОВЫЕ КОММУНИКАЦИОННЫЕ КОМПЛЕКСЫ:
УЧЕБНО-МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ

Проведение исследований с целью усовершенствования преподавания курсов общей и теоретической физики, математики, где связывались бы вопросы систематизации знаний студентов и общеобразовательные аспекты, на наш взгляд, является сегодня чрезвычайно актуальным [1]. Именно популяризации современных достижений науки нами посвящены предыдущие публикации [1-3]. Настоящую статью можно рассматривать как методологически - поисковую работу, в которой предложен информационный блок о наиболее перспективном современном направлении науки – прикладной квантовой физике – теории квантового компьютера. И поскольку курс „Физика квантового компьютера” утвержден МОН Украины в качестве учебной дисциплины для магистров – физиков, то, вполне естественно, возникает необходимость в представлении системных сведений об этом новом образовательном курсе, что и является целью данной работы.

Ограниченность информации о современных приложениях и достижениях квантовой физики – это то, с чем сегодня сталкиваются будущие учителя физики. Поэтому решение поставленной нами просветительской задачи связано с разрешением актуальной методико-познавательной проблемы.

Исходя из выше сказанного, а также, основываясь на противоречиях, возникших на сегодняшнем этапе подготовки молодых специалистов – физиков, нами предлагается конкретный информационно-методический блок, который, как мы

надеемся, найдет отклик не только у студентов, но и у преподавателей педагогических ВУЗов.

Поскольку нами уже акцентировалось внимание на концептуальном подходе в изложении фундаментальных дисциплин [3], то данная статья, собственно, посвящена конкретизации, дополнению и углублению затронутой проблемы.

Как известно, существует множество систем, в работе которых квантовые эффекты играют существенную роль [5-8], примером одной из которых – лазер: поле излучения которого порождается спонтанным и индуцированным излучением света.

Другой не менее важный пример подобных систем – это современные микросхемы: непрерывное ужесточение проектных норм приводит к тому, что квантовые эффекты начинают играть в их поведении существенную роль. Так, в диодах Ганна возникают осцилляции электронных токов, в полупроводниках образуются слоистые структуры: электроны или дырки в различных запертых состояниях могут хранить информацию, а один или несколько электронов могут быть заперты в так называемых квантовых ямах.

В настоящее время ведутся разработки нового класса квантовых устройств – нанометровых коммуникационных комплексов, среди которых важнейшее место занимают компьютеры на атомно-молекулярной основе (КАМ), идея создания которых принадлежит Ричарду Фейнману [5].

Р. Фейнман рассмотрел, по крайней мере, два вопроса. Во-первых, он подошел к процессу вычисления как физик: есть чисто логические ограничения на то, что можно вычислить, т.е. можно придумать задачу, для которой вообще нет алгоритма и можно придумать задачу, для которой любой алгоритм будет долго работать. Возникает вопрос, существуют ли ограничения физические? Например, на основании закона сохранения энергии вечный двигатель построить, в принципе, невозможно. А спрашивается, есть ли какое-либо физическое ограничение на функционирование компьютера, которое накладывало бы некие запреты на реализуемость алгоритмов? И Фейнману удалось доказать, что термодинамических ограничений (типа второго начала термодинамики) не существует, т.е. если мы будем уменьшать потери энергии и шумы, то можно выполнять сколь угодно длинные вычисления со сколь угодно малыми затратами энергии. Последнее означает, что вычисления можно сделать обратимым образом, поскольку в необратимых процессах энтропия возрастает. Собственно, Фейнмана это и заинтересовало: ведь реальное вычисление на реальном компьютере необратимо. И полученный им результат свидетельствует в том, что можно так переделать (изменить) любое вычисление (без особой потери эффективности), чтобы оно стало обратимым.

Таким образом вычисления, которые можно считать необратимыми – это те рост необратимости которых при этом пренебрежимо мал по сравнению с шумами в современном компьютере, т.е. необратимость – это довольно тонкий эффект и вопрос это

не практический, а принципиальный. Следовательно, если технология достигнет такого уровня, что этот эффект станет существенным, то представится реальная возможность таким образом перестроить вычисления, чтобы добиться обратимости.

И в этой же работе [6] Фейнман обратил внимание на то, что если имеется устройство квантовое, т.е. подчиняющееся законам квантовой механики, то его вычислительные возможности совершенно не обязательно должны совпадать с возможностями обычного устройства – возникают некоторые дополнительные возможности. Однако, пока непонятно, как утверждает Фейнман [6], позволяют они получить какой-то выигрыш или нет.

Впрочем, выясняется, что не только классическая, но и квантовая криптография (наука о шифровании сообщений) часто не способна противостоять квантовой криптоаналитике (науке о расшифровке), т.е. некоторые важные криптографические протоколы, такие, например, как «подбрасывание монеты по телефону», рушатся при переходе к квантовым вычислениям. Точнее, гарантией их надежности является отныне не сложность тех или иных алгоритмов, а сложность задачи создания квантового компьютера.

Таким образом, возникает новая отрасль вычислений – квантовые вычисления (КВ). КВ - это вычисления на КАМ. До сих пор неясно, когда появятся практически полезные конструкции КАМ и появятся ли они вообще. Тем не менее, КВ - предмет, чрезвычайно модный сейчас и в математике, и в физике, как теоретической, так и экспериментальной, и

занимается им довольно много исследователей. Судя по всему, именно интерес стимулировал первопроходцев: Ричарда Фейнмана, в пионерской работе которого поставлен вопрос о вычислительных возможностях устройств на квантовых элементах; Дэвида Дойча, формализовавшего этот вопрос в рамках современной теории вычислений, а также Питера Шора, придумавшего первый нетривиальный квантовый алгоритм [6-8].

Строго говоря, можно выделить два типа КАМ, которые основаны на квантовых явлениях, однако разного порядка [9-11].

Представителями первого типа являются, например, КАМ, в основе которых лежит квантование магнитного потока на нарушениях сверхпроводимости - Джозефсоновских переходах. На эффекте Джозефсона уже сейчас делают линейные усилители, аналого-цифровые преобразователи, СКВИДы и корреляторы. Другой тип – квантовые когерентные компьютеры (ККК) требует поддержания когерентности волновых функций используемых кубитов в течение всего времени вычислений - от начала и до конца. Кубитом может быть любая квантомеханическая система с двумя выделенными энергетическими уровнями. Следует заметить, что именно последний тип устройств имеется в виду, когда речь идёт о КАМ.

Рассмотрим вкратце математические основы функционирования КАМ. Классический компьютер состоит, грубо говоря, из некоторого числа битов, с которыми можно выполнять арифметические операции. Основным элементом КАМ являются квантовые

биты, или кубиты (от Quantum Bit, qubit). Обычный бит - это классическая система, у которой есть только два возможных состояния. Можно сказать, что пространство состояний бита - это множество из двух элементов, например, из нуля и единицы. *Кубит* же – это квантовая система с двумя возможными состояниями, так, например, электрон, у которого спин может быть равен либо $+1/2$ либо $-1/2$, атомы в кристаллической решетке при некоторых условиях и т.д. Но, поскольку система квантовая, то ее пространство состояний будет несравненно богаче. Кстати, математически *кубит* - представляет двумерное комплексное пространство.

В такой системе можно выполнять унитарные преобразования пространства состояний системы. С точки зрения геометрии, такие преобразования – это прямой аналог вращения и симметрий обычного трехмерного пространства. Согласно принципу суперпозиции, можно складывать состояния, вычитать их и умножать на комплексные числа. Эти состояния образуют фазовое пространство. При объединении двух систем полученное фазовое пространство будет их тензорным произведением. Эволюция системы в фазовом пространстве описывается унитарными преобразованиями фазового пространства.

В КАМ аналогичная ситуация. Он тоже работает с нулями и единицами. Но его функциональные элементы реализуют действия прямо в фазовом пространстве некоторой квантовой системы при помощи унитарных преобразований этого пространства.

Фазовое пространство КАМ есть тензорное произведение кубитов. Если в каждом кубите фиксирован базис (он будет состоять из двух векторов), то

фазовое пространство – это комплексное линейное пространство, базис которого индексирован словами из нулей и единиц. Таким способом двоичное слово на входе определяет базисный вектор.

Итак, вход – двоичное слово, определяющее один из базисных векторов. Сам же алгоритм – предписанная последовательность элементарных операторов. Применяем эту последовательность к вектору на входе, в результате него получаем некоторый вектор на выходе.

Так вот, согласно квантовой механике (КМ), пока система эволюционирует под действием наших унитарных операторов, невозможно сказать, в каком именно классическом состоянии она находится. Другими словами, она находится в каком-то квантовом состоянии, однако, согласитесь, что измеряем-то мы, когда общаемся с системой, все равно какие-то классические значения. Как это понимается в КМ? В фазовом пространстве фиксируется некоторый базис, и вектор состояния разлагается по этому базису. Это математическая формализация процедуры измерения в КМ, т.е. если мы имеем дело с системой, у которой «то ли спин влево, то ли спин вправо», и если мы все-таки посмотрим, какой спин, то мы получим одно из двух в любом случае. А вот вероятности того, что мы получим тот или другой результат, – это как раз квадраты модуля коэффициентов разложения. КМ утверждает, что точно предсказать результат измерения нельзя, но вероятности возможных результатов вычислить можно.

Вероятность возникает в процессе измерения. А пока система живет, для нас является существенным тот факт, что там есть сам этот вектор.

Другими словами, существенным является то, что система «находится одновременно во всех возможных состояниях». Как пишут многие авторы популярных введений в КВ, возникает совершенно чудовищный параллелизм вычисления: к примеру, в случае нашей системы из двух кубитов мы как бы оперируем одновременно со всеми возможными ее состояниями: 00, 01, 11, 10.

Чтобы интерпретировать ответ, надо заранее условиться, что какой-то бит, допустим, первый – это бит ответа. Пусть алгоритм проработал, у нас получился какой-то вектор, не обязательно базисный. Тогда мы можем сказать, что первый бит с некоторой вероятностью равен 1. И требование к алгоритму такое: если ответ «да», то вероятность того, что первый бит равен 1, должна быть больше двух третей. А если ответ «нет», то вероятность того, что будет ноль, должна быть тоже больше двух третей.

Какие реальные проблемы создания КАМ. Когда начался бум вокруг квантовых вычислений, физики высказывались об этом более чем скептически. Модель квантовых вычислений не противоречит законам природы, но это еще не значит, что ее можно реализовать. К примеру, можно вспомнить создание атомного оружия и управляемый термоядерный синтез.

А если говорить о КАМ, надо отметить одну очень серьезную проблему. Дело в том, что любая физическая реализация будет приближенной. Во-первых, мы не сможем сделать прибор, который будет давать нам произвольный вектор фазового пространства. Во-вторых, работа любого устройства подвержена случайным ошибкам. А уж в квантовой системе – пролетит

какой-нибудь фотон, взаимодействует с одним из спинов, и все поменяется. Поэтому сразу возник вопрос, можно ли, хотя бы в принципе, организовать вычисления на ненадежных квантовых элементах, чтобы результат получался со сколь угодно большой достоверностью. Такая задача для обычных компьютеров решается довольно просто, и например, за счет введения дополнительных битов.

В случае КАМ эта проблема гораздо глубже. То место, где возникает новое качество КВ по сравнению с обычными вычислениями, - это как раз сцепленные состояния – линейные комбинации базисных векторов фазового пространства. У вас есть биты, но они не сами по себе живут в каких-то состояниях - это был бы просто вероятностный компьютер (компьютер, дающий тот или иной ответ с определенной вероятностью), - а они находятся в некоем смешанном состоянии, причем согласованно-смешанном. Из-за этого в КАМ нельзя, например, просто взять и скопировать один бит в другой! Обычная интуиция из теории алгоритмов здесь неприменима.

Что касается технической стороны, то появились сообщения о создании реальных квантовых систем (экспериментальных) с небольшим числом битов, например, с двумя.

Так что эксперименты имеются,

однако они очень далеки от реальности. Дело в том, что два бита - это и для классического и для КАМ слишком мало! Чтобы моделировать молекулу белка, например, нужно порядка ста тысяч кубитов. Для ДЛ, чтобы вскрывать шифры, достаточно примерно тысячи кубитов.

Подводя итог, заметим, что физической системе, реализующей КАМ, можно предъявить определённые требования. Первое. Система должна состоять из точно известного числа частиц. Второе. Должна быть возможность привода системы в точно известное начальное состояние. Третье. Степень изоляции от внешней среды должна быть достаточно высокой. Четвертое. Надо уметь менять состояние системы согласно заданной последовательности унитарных преобразований ее фазового пространства. Необходимо иметь возможность выполнять «сильные измерения» состояния системы (то есть такие, которые переводят ее в одно из чистых состояний). Не исключено, что в информационном обществе появление КАМ сыграет ту же роль, что, в свое время, в индустриальном, - изобретение атомной бомбы. Действительно, если последняя является средством «уничтожения материи», то КАМ может стать средством «уничтожения информации» - ведь очень часто то, что известно всем, не нужно никому.

ЛИТЕРАТУРА

1. Ковальчук В.В., Моїсєєв Л.М. Сучасні нанометрові технології: наукові й освітні аспекти // Наука і освіта. – 2001. – № 1. – С. 120-123.
2. Дроздов М.О., Ковальчук В.В., Моїсєєв Л.М., Моїсєєва В.О., Ройлян В.О. Студентам - про інтуїцію, здогади, аналогії у фізиці // Наука і

освіта. – 2002. – № 6. – С. 99-103.

3. Ковальчук В.В., Моїсєєв Л.М., Царенко М.О. Методичні зауваження щодо визначення деяких фізичних понять // Наука і освіта. – 2002. – № 5. – С. 120-123.

4. Дроздов В.О. Ковальчук В.В., Моїсєєв Л.М., Бобошко В.В. та ін.

Концептуальний метод у навчанні // Наука і освіта. – 2004. – № 1. – С.45-51.

5. Манин Ю.И. Вычислимое и невычислимое. – М.: Советское радио, 1980. – 145 с.

6. Feynman R. Quantum mechanical computers// Optics News, February 1985.-V. 11. - P.11-15.

7. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. - Proc. R. Soc. London A 400, 97, 1985 – P.23-38.

8. Shor P.W. Algorithms for Quantum Computation: Discrete log and Factoring. // Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S.

Goldwasser, IEEE Computer Society Press, Los Alamitos, CA, 1994.- P.124.

9. Grover L. A fast quantum mechanical algorithm for database search. //Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, P. 212-219.

10. Дроздов В.О., Ковальчук В.В. Електронні процеси в наноструктурах з субфазим кремнієм // Журнал фізичних досліджень. – 2003. – Т.7, – № 4. – С.393-401.

11. Дроздов В.А., Ковальчук В.В., Мусеев С.Л. Фрактальная размерность наночастиц // Физика аэродисперсных систем. - 2003. – № 39. – С. 55-67.

Подано до редакції 29.11.06

РЕЗЮМЕ

Статтю присвячено популяризації досягнень сучасної прикладної квантової теорії. Пропонуються системні відомості у форматі конкретного інформаційного блоку з курсу „Фізика квантового

комп'ютера”, затвердженого МОН України, як навчальна дисципліна для майбутніх вчителів фізики, – випускників педагогічного університету.

SUMMARY

The article is devoted to popularization of achievements of the modern applied quantum theory. The authors suggest some system data in the format of a concrete information block of the course „Physics of the quantum computer ” approved by the Ministry of Education and Science of Ukraine as a subject for future teachers of physics - graduates from pedagogical university.