

**В.Н. Ручкин, В.А. Романчук, В.А. Фулин**

## **ЕСТЕСТВЕННЫЙ ПАРАЛЛЕЛИЗМ КВАНТОВЫХ КОМПЬЮТЕРОВ И НЕЙРОВЫЧИСЛИТЕЛЕЙ \***

Анализируются физические основы одно- и двухбитовых логических операций «И», «НЕТ», «ДА», 2И-НЕ, построения RS-триггеров и структуры квантового компьютера на основе кубитов с суперпозицией квантовых состояний и использованием квантового параллелизма.

*суперпозиция квантовых состояний, квантовый параллелизм, кубит, логические операции, RS-триггер, структура квантового компьютера.*

Согласно гипотезе М. Минского производительность параллельной системы растет (примерно) пропорционально логарифму числа процессоров, то есть намного медленнее, чем линейная функция, что указывает на необходимость развития не только классических технологий, но и принципиально новых подходов. Одним из направлений роста производительности является повышение уровня параллелизма и отход от *фон-неймановской архитектуры* с последовательным выполнением команд.

Квантовые компьютеры и нейровычислители являются вычислительными системами с естественным параллелизмом [1–3; 8]. Квантовый параллелизм заключается в том, что данные в процессе вычислений представляют собой квантовую информацию, которая по окончании процесса преобразуется в классическую путем измерения конечного состояния квантового регистра. Повышение производительности в квантовых алгоритмах достигается за счет того, что при применении одной квантовой операции большое число коэффициентов суперпозиции квантовых состояний преобразуется одновременно.

Электрон или любой другой квантовый объект частично будет находиться в одной точке, частично в другой, частично в третьей и т. д. Такое состояние электрона, когда он находится сразу в нескольких точках пространства, называют *суперпозицией квантовых состояний* [2] и описывают обычно волновой функцией, введенной в 1926 году немецким физиком Э. Шредингером. Модуль значения волновой функции в любой точке, возведенный в квадрат, определяет вероятность найти частицу в этой точке в данный момент. После измерения положения частицы ее волновая функция как бы стягивается (коллапсирует) в ту точку, где частица была обнаружена, а затем вновь

---

\* Работа выполнена в рамках гранта РФФИ №12-07-97516/12.

начинает расплываться. Свойство квантовых частиц быть одновременно во многих состояниях, называемое *квантовым параллелизмом*, успешно используется в квантовых вычислениях.

### Кубит ( $q$ -бит) и логические основы квантового компьютера

Основная ячейка квантового компьютера (квантовый бит, или сокращенно *кубит* ( $q$ -бит) [3]) – это квантовая частица, имеющая два базовых состояния, которые обозначаются, как принято в квантовой механике, 0 и 1. Двум значениям кубита могут соответствовать, например, основное и возбужденное состояния атома, направления вверх и вниз спина атомного ядра, направление тока в сверхпроводящем кольце, два возможных положения электрона в полупроводнике и т. п.

Квантовый регистр устроен почти так же, как и классический. Он состоит из цепочки квантовых битов, над которыми можно проводить одно- и двухбитовые логические операции, подобно операциям НЕ, 2И-НЕ и т. п.

К базовым состояниям квантового регистра, образованного  $L$  кубитами, относятся все возможные последовательности нулей и единиц длиной  $L$ . Всего может быть  $2^L$  различных комбинаций, которые можно считать записью чисел в двоичной форме от 0 до  $2^L - 1$ . Однако эти базовые состояния не исчерпывают всех возможных значений квантового регистра (в отличие от классического), поскольку существуют еще и состояния суперпозиции, задаваемые комплексными амплитудами, связанными условием нормировки. Классического аналога у большинства возможных значений квантового регистра за исключением базовых просто не существует, а его состояния лишь малая часть всего богатства состояний квантового компьютера.

Идея квантовых вычислений, впервые высказанная Ю.И. Маниным и Р. Фейнманом, состоит в том, что квантовая система из  $L$  двухуровневых кубитов (квантовых элементов) имеет  $2^L$  линейно независимых состояний, а значит вследствие принципа квантовой суперпозиции пространством состояний такого квантового регистра является  $2^L$ -мерное гильбертово пространство [3]. Операция в квантовых вычислениях соответствует повороту вектора состояния регистра в этом пространстве. Таким образом, квантовое вычислительное устройство размером  $L$  кубит может выполнять параллельно  $2^L$  операций. В общем случае системы из  $L$  кубитов имеют  $2^L$  классических состояний (00000 ( $L$ -нулей), 00001 ( $L$ -цифр), ... , 11111 ( $L$ -единиц)), каждое из которых может быть измерено с вероятностями 0–100 %

$$|\Psi\rangle = \sum_{n=0}^{2^L-1} c_n |n\rangle ,$$

где  $|n\rangle$  – базисные квантовые состояния (например, состояние  $|001101\rangle$ ), а  $|c_n|^2$  – вероятность нахождения в базисном состоянии  $|n\rangle$ .

Таким образом, одна операция над группой кубитов затрагивает все значения, которые она может принимать в отличие от классического бита, что и обеспечивает беспрецедентный параллелизм вычислений.

Полный набор полностью оптических логических устройств для синтеза более сложных блоков реализуется, например, на основе пассивных нелинейных резонаторов-интерферометров, в которых в результате светоиндуцированного изменения оптической длины происходит сдвиг пика пропускания (резонанса) относительно длины волны падающего излучения. В зависимости от начальных условий (начало положения пика пропускания и начало интенсивности) в пассивном нелинейном резонаторе нелинейный процесс завершается установлением одного из двух устойчивых состояний пропускания (отражения) падающего излучения.

На рисунках 1а и 2а приведены передаточные характеристики бистабильного интерферометра [7] – зависимости интенсивности выходного сигнала, отраженного  $I_{отр.}$  и прошедшего  $I_{пр.}$ , от интенсивности сигнала на входе  $I_{вх.}$ , складывающегося из сигнала подсветки  $I_0$  и информационного сигнала  $I_1$  или  $I_1$  и  $I_2$ . Если  $I_0 + I_1 = I_{вкл.}$  – порогу переключения – происходит переход системы из состояния с высокой интенсивностью на выходе «1» в состояние с низкой интенсивностью на выходе «0» (рис. 1а) или наоборот (рис. 2а).

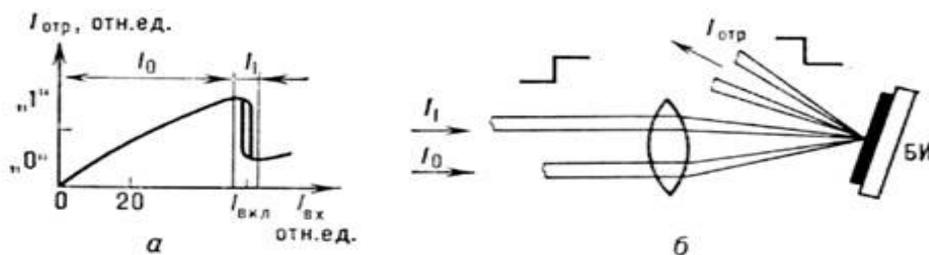


Рис. 1. Передаточная характеристика бистабильного интерферометра в отраженном пучке (а) и «НЕ» (б)

Вообще говоря, гистерезис, характерный для оптической бистабильности, в данном случае не обязателен. Важно лишь обеспечить достаточно большой перепад между высокой и низкой выходными интенсивностями по отношению к изменению входной интенсивности, вызвавшей этот перепад.

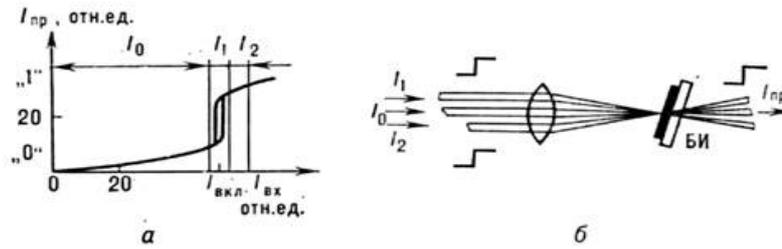


Рис. 2. Передаточная характеристика бистабильного интерферометра в проходящем пучке (а) и схема устройства с логическими функциями «И», «НЕТ», «ДА» (б)

Элемент «НЕ» реализуется с использованием отраженного от бистабильного интерферометра потока (рис. 1б). Интенсивность  $I_{вх.}$  устанавливается несколько ниже порога переключения  $I_{вкл.}$ , что соответствует высокой интенсивности отраженного сигнала. Незначительная добавка  $I_1$  приводит к резкому уменьшению интенсивности  $I_{отр.}$ , а снятие  $I_1$  – к восстановлению высокого уровня  $I_{отр.}$ .

На рисунке 2б дана схема устройства, представляющего собой по сути оптически программируемый элемент процессора, в котором тот или иной вид логической операции задается значением интенсивности подсветки  $I_0$ . На бистабильный интерферометр, кроме подсветки, подаются еще два информационных пучка  $I_1$  и  $I_2$  и на выходе рассматривается интенсивность проходящего пучка. Если интенсивность подсветки выбрана такой, что  $I_0 = I_{вкл.} - 0,5I_1$  (рис. 2а), то наличие сигнала хотя бы в одном из информационных пучков переводит элемент в единичное состояние для проходящего луча («ИЛИ»). При установке  $I_0 \approx I_{вкл.} - 1 > 5 I_1$  элемент включается лишь при одновременной подаче сигнала «1» в обоих информационных каналах (функция «И»). Если выполняется условие  $I_0 < I_{вкл.} - (I_1 + I_2)$ , то при любой комбинации состояний  $I_1, I_2$  на выходе имеет место низкий уровень интенсивности («НЕТ»). Наконец, при  $I_0 > I_{вкл.}$  бистабильный интерферометр всегда остается при включенном состоянии («ДА»). Для отраженного потока в этой же схеме обеспечиваются также функции «ИЛИ – НЕТ» и «И – НЕТ». Такой набор элементов является достаточным для синтеза более сложных блоков. На рисунке 3 даны некоторые примеры организации взаимодействия между отдельными элементами. Бистабильный интерферометр с гистерезисной зависимостью (рис. 3а) действует как оптический триггер с отдельными инверсными входами и выходами (рис. 3б).

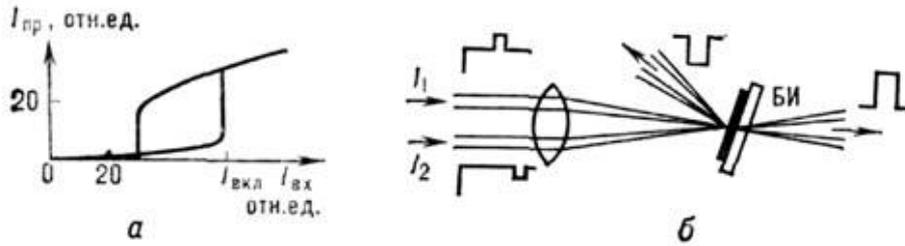


Рис. 3. Передаточная характеристика (а) и схема триггера (б)

Чтобы получить *RS*-триггер, один из входных сигналов в схеме рисунка 3б необходимо инвертировать. *RS*-триггер имеет два входа и два устойчивых состояния, которые меняются под действием входных сигналов, при этом обязательно попеременно то с одного, то с другого входа. Инвертирование можно сделать с помощью дополнительного элемента «НЕ» (рис. 4а). В исходном состоянии интенсивность  $I_2$  выбрана чуть ниже порога переключения элемента «НЕ» и уровень сигнала, отраженного в направлении основного пучка<sub>1</sub>, высок. Его сумма с начальной интенсивностью  $I_1$  за счет регулировки последней соответствует примерно центральной области гистерезиса.

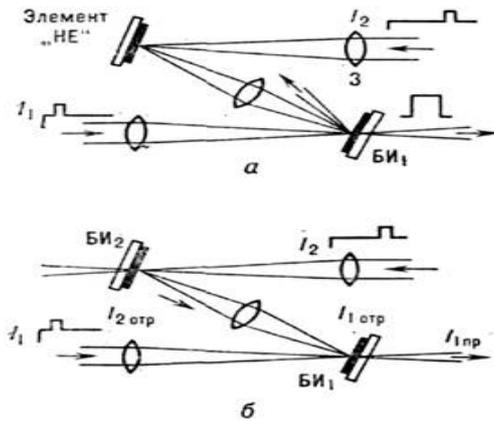


Рис. 4. Схемы оптических *RS*-триггеров

*RS*-триггер реализуется также и на основе двух «скрещенных» устройств с функциями «НЕ» (рис. 4б). Введенная в систему жесткая положительная обратная связь приводит к тому, что первый из элементов устойчиво находится во включенном состоянии, если второй в выключенном, и наоборот. По сравнению с предыдущей эта схема полностью симметрична, но требует более тщательной юстировки.

### Структура квантового компьютера

В квантовом процессоре введенные данные подвергаются последовательности квантовых логических операций, которые с математической точки зрения описываются унитарным преобразованием  $\hat{U}_{\text{опл}}$ , воздействующим на состояние всего регистра (рис. 5). В результате через некоторое количество тактов работы квантового процессора исходное квантовое состояние системы становится новой суперпозицией вида

$$|\psi(t)\rangle = \sum_{n, n_2=0}^{2^i-1} c_n \hat{U}_{\text{опл}} |n\rangle$$

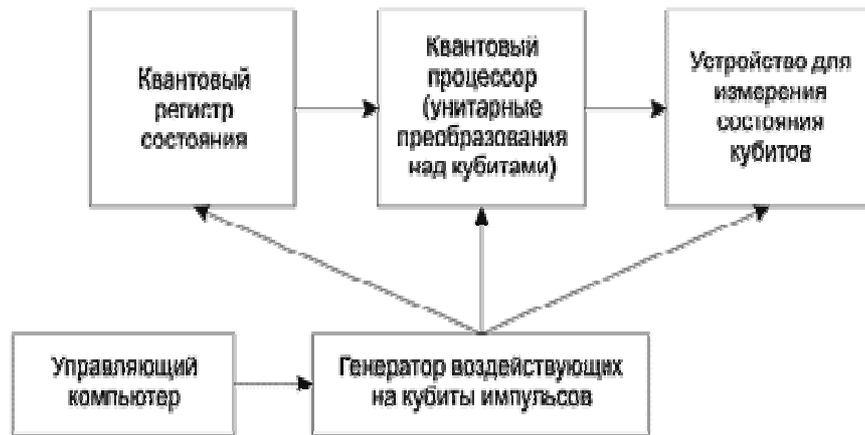


Рис. 5. Структура квантового компьютера

Первый квантовый компьютер, который был реализован на практике, – это импульсный ядерный магнитно-резонансный (ЯМР) компьютер. К его потенциальным преимуществам можно отнести: 1) в линейной среде световые потоки не взаимодействуют между собой, проходя в непосредственной близости или даже пересекаясь друг с другом; 2) световые потоки могут быть локализованы в поперечном направлении до субмикронных размеров и передаваться как по световодам, так и по свободному пространству; 3) скорость распространения светового сигнала выше скорости электрического, зависящего от соотношения активных и реактивных компонент проводимости тракта передачи; 4) взаимодействие световых потоков с нелинейными средами не локализовано, а распределено во всей среде, что дает новые степени свободы организации связей и создания параллельных архитектур.

Эти свойства делают квантовые компьютеры способными преодолеть ограничения по быстродействию и параллельной обработке информации. Например, цифровой оптический процессор с числом параллельных каналов  $\sim 10^5 - 10^6$

может совершать до  $10^{13}$ – $10^{15}$  операций в секунду (при времени переключения в одном канале  $\sim 10^{-8}$  –  $10^{-9}$  с), что значительно превосходит число операций в секунду в электронных системах.

На практике пассивные нелинейные резонаторы-интерферометры являются вакуумно-напыленными тонкопленочными многослойными полупроводниковыми структурами с несколькими промежуточными слоями из арсенида галлия (GaAs), фосфида индия (InP) или селенида цинка (ZnSe), формирующими в тонкопленочном элементе полупроводниковую сверхрешетку. Такие резонаторы обладают временами переключения  $\sim 10^{-8}$ – $10^{-9}$  с и удельными энергиями переключения  $\sim 10^{-12}$ – $10^{-14}$  Дж/мкм<sup>2</sup>. Элементы памяти оптического компьютера представляют собой полупроводниковые нелинейные оптические интерферометры, в основном созданными из арсенида галлия (GaAs). Минимальный размер составляет  $\sim 1000$  атомов или 1–10 нм.

### **Области применения квантового компьютера**

Перспективность квантовых вычислений заключается в достаточно быстром решении целого класса задач. Однако в настоящее время они достаточно сложные и трудно обрабатываемые.

Первой областью применения является квантовая криптография, которая устанавливает, что перехват посланного сообщения сразу же становится известным. Перехваченное сообщение, зашифрованное квантовым компьютером, утрачивает свою структуру и становится непонятным для адресата. Поскольку квантовая криптография эксплуатирует природу реальности, а не человеческие изыски, то скрыть факт шпионажа становится невозможно. Это должно окончательно решить проблему криптографов по наиболее надежным способам шифрования сообщений.

Другая сфера применения гигантской вычислительной мощи квантового компьютера позволит переложить на плечи машины самую разнообразную интеллектуальную деятельность. В результате можно будет создавать экспертные системы нового поколения по использованию знаний одного или нескольких экспертов в формализованном виде, а также логику принятия решений. Эти системы предназначены для принятия обоснованного решения в тяжелых условиях, когда не хватает времени, опыта, знаний, информации. На введенный запрос машина дает квалифицированную консультацию или подсказку.

Третья сфера применения предоставляется компьютером Orion фирмы D Wave, который был создан в 2007 году в виде 16-кубитового квантового компьютера. Он был признан самым мощным и является первым коммерчески значимым приложением.

Особо следует отметить оптические нейронно-сетевые компьютеры [5; 7], которые могут решать нерегулярные (случайные) задачи, для которых трудно, практически невозможно, задать алгоритм. Выполнение случайных задач по сути сводится к выбору одного из множества готовых решений, которое является наилучшим при имеющихся входных данных. Для этого в памяти должна храниться совокупность таких решений. Обычный компьютер не обладает способ-

ностью запоминать и извлекать из памяти информацию в виде готовых решений. Это свойственно только человеческому мозгу и проявляется при решении задач, связанных с распознаванием образов (такие задачи относятся к случайным). Для моделирования процессов работы мозга человека путем имитации его анатомических нейронных структур предназначены разрабатываемые с 80–90-х годов XX века нейронные (нейронно-сетевые) компьютеры. Подобно мозгу, такие компьютеры должны состоять из большого числа несложных процессорных элементов, между которыми имеются многочисленные перекрестные связи. Такие системы так же, как и мозг, должны обладать ассоциативной памятью, способной при наличии на входе части всех признаков некоторого объекта воспроизвести на выходе всю информацию о данном объекте. Вычисления в нейронных сетях выполняются одновременно в результате простых операций отдельными нейронами, при этом вся сеть в целом реализует более сложную функцию. Информация при такой организации процесса вычислений может кодироваться и запоминаться не в отдельных ячейках, а установлением определенной структуры связей между ними. Нейронно-сетевые компьютеры состоят из двух основных компонентов. Первый компонент – это двумерная матрица оптически переключающих (бистабильных) элементов (искусственных аналогов нейронов), состояние которых изменяется в зависимости от подсоединенных связей с помощью световых пучков. Второй компонент – голограмма, с помощью которой задаются различные связи между элементами: объем в  $1 \text{ см}^3$  задает более  $10^9$  связей. Нейронно-сетевые компьютеры способны также к самопроизвольному обучению, что целесообразно в информационной деятельности, свойственной человеческому мозгу.

Как показывают исследования, естественный параллелизм квантовых компьютеров и нейровычислителей позволяет преодолеть ограничения по быстродействию за счет параллельной обработки информации с огромным числом каналов  $\sim 10^5$ – $10^6$  и совершать до  $10^{13}$ – $10^{15}$  операций в секунду, что значительно превосходит число операций в секунду в современных существующих электронных системах. В свою очередь применение квантовых компьютеров позволит решать сложные задачи в таких областях, как криптография, мощные экспертные системы, приближающие нас к возможностям человеческого мозга.

#### СПИСОК ЛИТЕРАТУРЫ И ЭЛЕКТРОННЫХ РЕСУРСОВ

1. Абу-Мостафа, Я.С. Оптические нейронно-сетевые компьютеры [Текст] / Я.С. Абу-Мостафа, Д. Псалтис // В мире науки. – М., 1987. – № 5.
2. Гиббс, Х.М. Оптическая бистабильность. Управление светом с помощью света [Текст] : пер. с англ. С. П. Апанасевича, Ф. В. Карпушко ; под ред. Ф.В. Карпушко. – М. : Мир, 1988. – 518 с.
3. Квантовый\_компьютер [Электронный ресурс] // Википедия. Свободная энциклопедия. – Режим доступа : <http://ru.wikipedia.org/wiki/> (дата обращения: 01.12.2012).

4. Мембрана. Люди. Идеи. Технологии [Электронный ресурс]. – Режим доступа : <http://www.membrana.ru/particle/3333> (дата обращения: 01.12.2012).
5. Нейрокомпьютер [Электронный ресурс] // Википедия. Свободная энциклопедия. – Режим доступа : <http://ru.wikipedia.org/wiki/> (дата обращения: 01.12.2012).
6. Синицын, Г.В. Полностью оптические элементы дискретной логики на основе бистабильных тонкопленочных интерферометров [Текст] // Квантовая электроника. – М., 1987. – Т. 14. – № 3.
7. Шумский, С.А. Нейрокомпьютинг – состояние и перспективы [Текст] / Физический институт РАН им. П.Н. Лебедева. – М., 2002.
8. Эйбрэхом, А. Оптический компьютер [Текст] / А. Эйбрэхом, К.Т. Си-тон, С.Д. Смит // В мире науки. – М., 1983. – № 4.

**V.N. Ruchkin, V.A. Romanchuk, V.A. Fulin**

### **NATURAL PARALLELISM OF QUANTUM COMPUTERS AND NEURONAL COMPUTERS**

The article analyzes the physical basis of logical bitwise operations ‘and’, ‘no’, ‘yes’, ‘2and-no’, which create RS-triggers and are used in quantum computers based on quantum bits in quantum superposition states and employ quantum parallelism.

*quantum superposition states, quantum parallelism, quantum bit, logical operation, RS-trigger, quantum computer*