

# Учебные семинары

Черновая версия конспектов материалов учебных семинаров лаборатории квантовых вычислений.

## ВВЕДЕНИЕ В КВАНТОВУЮ ИНФОРМАЦИЮ

### Введение

Лаборатория квантовых вычислений работает с программным обеспечением в области квантовых технологий. Наша задача заключается в том, чтобы соединить научный мир квантовых вычислений с обычным потребителем. Для повышения качества разработки начали свою работу учебные семинары. Основная технология научных семинаров в настоящий момент — это технология квантового отжига. Квантовый отжиг довольно сложная технология для понимания которой нужно изучить различные дисциплины. А именно

- Квантовая механика.
- Квантовые вычисления.

Для комфортного владения квантовой механикой и квантовых вычислений необходимо знание математического аппарата. А именно

- Линейная алгебра.
- Математический анализ.
- Теория вероятностей.
- Дифференциальные уравнения.

### Классическая информация

Начнём наш первый семинар с введения в квантовую информацию. Но чтобы понимать принципы работы квантовой информации, необходимо понимать принципы работы классической информации. Центральным объектом изучения классической информации является бит. Слово «*bit*» произошло от английского слова «*bit*», которое расшифровывается как **b**inary **d**igit. В настоящее время слово бит является уже вполне привычным и очевидным. Но это ранее не было так очевидно.

Всё началось с задачи передачи информации. Пусть Алиса хочет передать сообщение Бобу. Сообщение — это некоторая последовательность символов некоторого языка. Пусть  $M$  — это количество символов алфавита некоторого языка. И пусть  $N$  — это длина последовательности. В 1928 году Ральф Хартли предложил свой способ измерения информации [1], которая в настоящее время известна как формула Хартли.

$$I = N \cdot \log_2 M,$$

где  $I$  — это *количество информации*, а величина  $H = \log_2 M$  была названа *информационной энтропией*.



**Ральф Винтон Лайон Хартли** (30 ноября 1888 – 1 мая 1970) — американский исследователь в области электротехники. В 1928 году предложил свой способ измерения количества информации в передаваемом сообщении в работе «Transmission of information» в журнале «Bell System technical journal». Родился в городе Спрингмонт, штат Невада. В 1909 году окончил университет Юты. В 1913 закончил Оксфордский университет. В 1915 году руководил разработкой радиоприемника для испытаний трансатлантической радиотелефонной системы Bell System.

Рис. 1. Ральф Хартли

Здесь важно прокомментировать такой способ измерения информации. Пусть у нас есть два символа  $a, b$ . Их можно закодировать с помощью нуля и единицы:  $a \mapsto 0, b \mapsto 1$ . Пусть теперь у нас есть три символа  $a, b$  и  $c$ . Закодировать нулём и единицей их мы уже не сможем. Здесь будет нужна последовательность из двух нулей/единиц. Например,

$$a \mapsto 00, b \mapsto 01, c \mapsto 10.$$

Для 4 символов также хватит последовательности длины 2. Но для 5 символов уже нужна будет последовательность длины 3.

$$a \mapsto 000, b \mapsto 001, c \mapsto 010, d \mapsto 011, e \mapsto 100.$$

На этом этапе может возникнуть вопрос: почему мы кодируем только нулём и единицей? На самом деле, кодировать можно и большим количеством цифр. Но удобнее всего использовать две цифры.

Исходя из представленных примеров можно сделать вывод, что  $M \leq 2^n$ , где  $n$  — минимальное количество цифр в последовательности, удовлетворяющее неравенству. Отсюда несложно получить выражение для  $n$ :

$$n = \lceil \log_2 M \rceil,$$

где  $\lceil x \rceil$  — это операция округления вверх. Важно отметить, что Хартли ещё не использовал термин бит, хотя уже ввёл двоичную систему измерения информации.

У формулы Хартли был важный недостаток. Его формула не учитывала шумы и внешнее воздействие на канал передачи информации. Спустя два десятилетия Клод Шеннон предложил несколько иной способ измерения информации [2]. Пусть теперь у

каждого символа алфавита есть вероятность появления  $p_i$  при получении сообщения. Тогда информационная энтропия по Шеннону примет вид

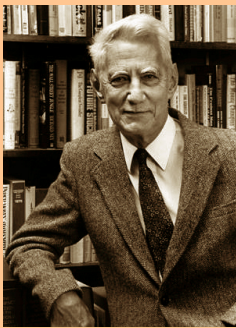
$$H = - \sum_{i=1}^M p_i \log p_i.$$

Оказывается, формула Хартли является частным случаем формулы Шеннона. Докажем это утверждение.

Пусть вероятности появления символов одинаковые. То есть  $\forall i \ 1 \leq i \leq M \ p_i = 1/M$ . Подставим эти вероятности в формулу Шеннона.

$$H = - \sum_{i=1}^M p_i \log p_i = - \sum_{i=1}^M \frac{1}{M} \log \frac{1}{M} = -M \cdot \frac{1}{M} \log \frac{1}{M} = \log M.$$

□



**Клод Элвуд Шеннон** (30 апреля 1916 – 24 февраля 2001) — американский инженер и математик. В 1948 году в работе «A mathematical theory of communication» ввёл обобщенное понятие информационной энтропии. Начал использовать термин «бит» в научной литературе. Родился в городе Петоски, штат Мичиган, США. В 1936 году окончил Мичиганский университет.

Рис. 2. Клод Шеннон

История термина «бит» довольно примечательна. Его начал использовать Клод Шеннон в работе, в которой он ввёл обобщенную информационную энтропию. Причём в этой работе он пишет: «The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly bits, a word suggested by J. W. Tukey» [2]. Таким образом, термин «бит» впервые использовал Джон Тьюки.

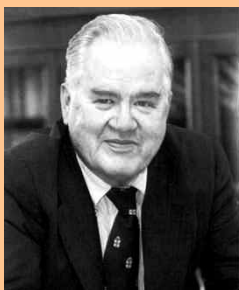


Рис. 3. Джон Тьюки

**Джон Уайлдер Тьюки** (16 июня 1915 – 26 июля 2000) — американский математик. Автор термина «бит». Родился в городе Нью-Бедфорд, штат Массачусетс, США. Высшее образование получил в Брауновском университете. Докторскую степень получил в Принстонском университете. Во время Второй мировой войны работал в Bell Labs.

### Физические основы информации

Информация нам интересна с точки зрения вычислений. Поэтому важно понять, каким образом происходят классические вычисления. А для этого нужно изучить физические основы кодирования классической информации. Самый распространённый способ кодирования информации — это электричество. Интуитивный способ кодирования:  $0 \mapsto$  тока нет,  $1 \mapsto$  ток есть. В начале XX века был изобретён *триод*.

Триод представляет из себя газоразрядную лампу, в которой ток проходит от катода к аноду. А напряжение на сетке позволяет контролировать силу тока между анодом и катодом. Если выставить некоторую границу для силы тока, то можно получить закодированное бинарное значение. То есть, если сила тока меньше порогового значения, то кодируется ноль; если же сила тока больше порогового значения, то кодируется единица. С помощью подобных газоразрядных ламп и были созданы первые ЭВМ. Главный недостаток такого подхода заключался в сложности масштабирования. Для работы требовалось тысячи ламп. Но если сломаются хотя бы несколько из них, вероятность чего достаточно велика, то вся система перестанет работать.

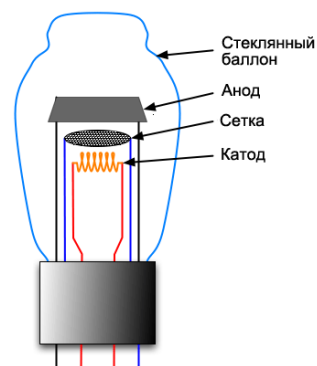


Рис. 4. Триод

Ситуация радикально изменилась после полупроводниковой революции. В конце 50-60-х годов были открыты материалы полупроводники. С помощью полупроводников удалось сделать устройство, по назначению схожее с триодом — транзистор. Во-первых, эти устройства были на порядки компактнее. Во-вторых, они были более надёжными, чем газоразрядные лампы. Таким образом, изобретение полупроводников позволило масштабировать объёмы информации, которые способны обрабатывать ЭВМ.

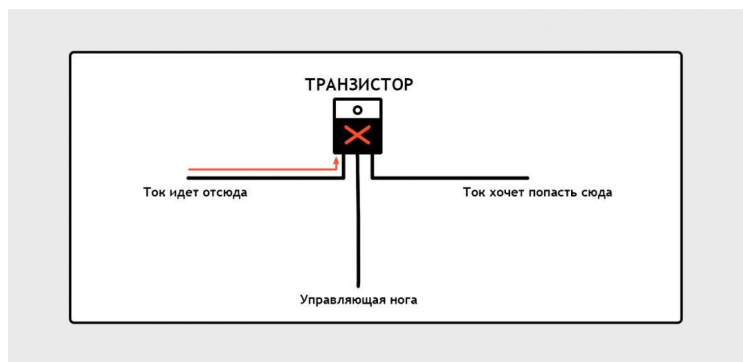


Рис. 5. Транзистор

Важно отметить, что выше был описан только способ кодирования информации. На практике в настоящее время транзисторы используются в качестве вентилях. Способы постоянного хранения информации отличаются от описанного.

### Квантовые системы

В XX веке исследователи думали об альтернативных способах кодирования информации. В частности была гипотеза, что возможно использовать квантовые системы для кодирования информации. Примеры квантовых систем: поляризация фотона, спин электрона, энергетические уровни иона и так далее.

В квантовых системах способы кодирования появляются естественным образом, о чём мы поговорим чуть позже. Сейчас важно обсудить некоторые свойства квантовых систем. Например, *корпускулярно-волновой дуализм*. Дуализм (то есть двойственность) заключается в том, что квантовая система может обладать свойствами как волны, так и частицы (корпускулы). В качестве примера волнового свойства можно рассмотреть интерференцию. Пусть есть два источника гармонических колебаний. Тогда волны от двух источников складываются и появляются области, в которых волны достигают своего максимума и минимума.

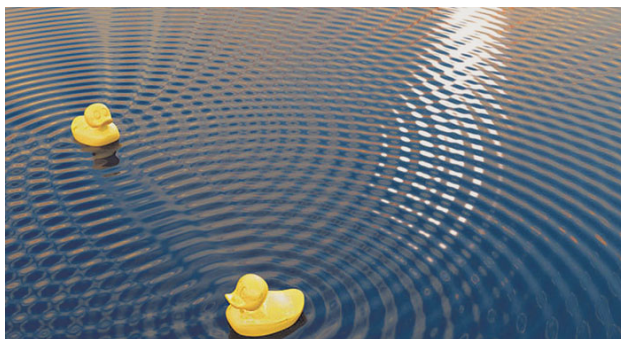


Рис. 6. Интерференция волн на воде

В качестве проявления свойства частицы достаточно рассмотреть частицу, как очень маленькое тело. То есть оно обладает массой, импульсом. Также частица может оставить точечный след на некоторой поверхности. Важнейшим опытом, доказывающим наличие корпускулярно-волнового дуализма был двухщелевой опыт Юнга. Изначально этот опыт был продемонстрирован на свете. Но сейчас нам будет интересен этот эксперимент на электронах. С одной стороны, электрон является частицей. В этом сомнения нет. Но вот как понять, что электрон является волной?

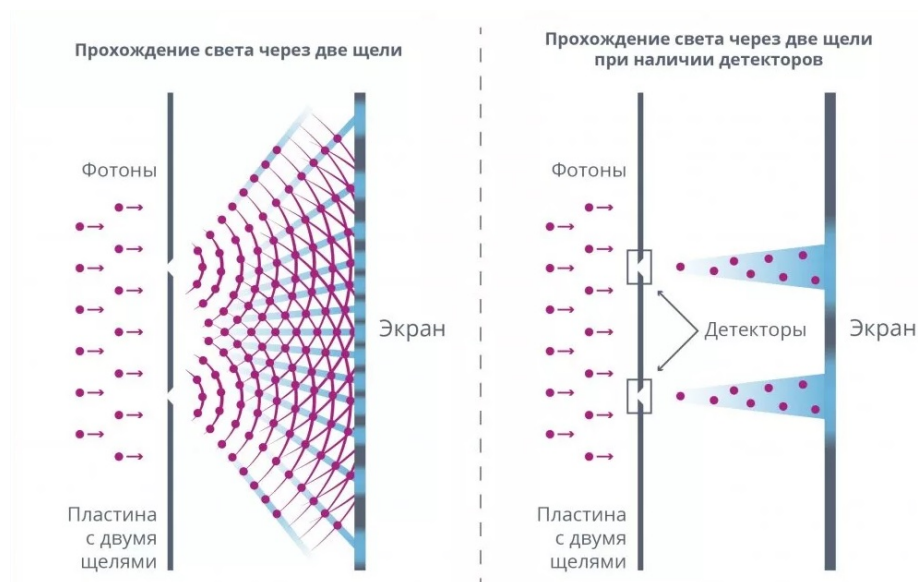


Рис. 7. Двухщелевой опыт Юнга

Схема установки следующая. Есть два экрана. На одном из экранов имеются две прорези. Слева от экрана есть источник электронов. Электроны вылетают из источника, проходят через щели и попадают на второй экран. Если бы электрон был классической частицей, то мы бы увидели только две полоски. Но на самом деле мы видим целую череду полосок. Эта чередка полос и есть интерференционная картина, то есть фиксированные области максимумов и минимумов попадания электронов. Таким образом, электрон проявляет как свойства частицы, так и волны.



Рис. 8. Томас Юнг

**Томас Юнг** (13 июня 1773 – 10 мая 1829) — английский физик, механик, астроном и филолог. Родился в городе Милвертон, Англия. В конце XVIII – начале XIX веков занимался изучением волновой природы света. В 1803 году опубликовал работу, в которой описал двухщелевой опыт со светом.

Помимо корпускулярно-волнового дуализма квантовые системы обладают такими свойствами как *суперпозиция* и *запутанность*. Таким образом, квантовые системы обладают различными свойствами, которыми не обладают классические системы. Здесь может возникнуть закономерный вопрос. Есть ли у квантовых систем преимущество с точки зрения кодирования информации? Ответ: да, имеют.

### Квантовая информация

Пусть необходимо закодировать классическую информацию (то есть обычные биты) в какой-нибудь квантовой системе. Какое количество информации мы сможем закодировать? Квантовые системы дают некоторое преимущество перед классическими, но не безграничное. Именно этот результат получил советский математик А. С. Холево [3]. Таким образом, можно сказать, что было получено количественное соотношение между классической и квантовой информацией.



Рис. 9. А. С. Холево

**Александр Семёнович Холево** (род. 2 сентября 1943) — советский математик, юниор квантовой информации. Определил верхнюю границу классической информации, которую можно передать в квантовом канале. В настоящее время работает в Математическом институте им. В.А. Стеклова РАН. Читает курс «Квантовая информация».

Работа Холево дала толчок к изучению квантовой информации. Обратите внимание, что теория классической информации зародилась из задачи коммуникации. Теория квантовой информации берёт своё начало также из задачи коммуникации. В 1984 году впервые был разработан протокол квантовой коммуникации. Мы не будем его детально



обсуждать сейчас. Но мы обсудим ключевые идеи оттуда.

Мы до сих пор не обсудили как всё-таки можно кодировать информацию с помощью квантовой системы. В качестве физической системы возьмём *фотон*. Фотону также характерен корпускулярно-волновой дуализм. Поэтому фотон мы можем легко рассматривать как волну. Это является корректным допущением, поскольку свет имеет электромагнитную природу. Электромагнитная волна представляет из себя колебания векторов напряженности электрического и магнитного полей.

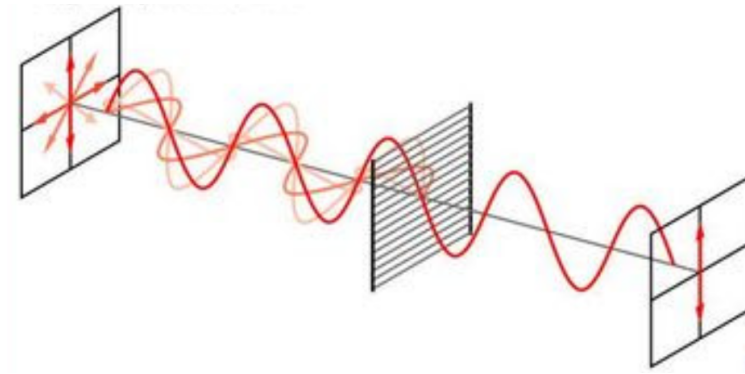


Рис. 10. Электромагнитная волна

В общем виде волна может быть произвольно ориентирована в пространстве. В частном случае, она может колебаться только в горизонтальной или вертикальной плоскостях. Это называется *поляризацией* электромагнитной волны. Введём обозначения. Пусть  $|\leftrightarrow\rangle$  — горизонтальная поляризация,  $|\updownarrow\rangle$  — вертикальная поляризация. Суть обозначения  $|\cdot\rangle$  мы поясним позже. Идея кодирования следующая:  $0 \mapsto |\leftrightarrow\rangle$  и  $1 \mapsto |\updownarrow\rangle$ . Но помимо горизонтальной и вертикальной поляризации могут быть и промежуточные. Это можно описать с помощью комбинации

$$\alpha |\leftrightarrow\rangle + \beta |\updownarrow\rangle.$$

Суть коэффициентов  $\alpha$  и  $\beta$  мы обсудим на следующем занятии. Но даже сейчас видно, что квантовая система может описать очень много разных *состояний*. Причём бесконечно много. В следующий раз мы обсудим математический формализм квантовой информации.

- 
- [1] R. V. Hartley, Transmission of information 1, Bell System technical journal **7**, 535 (1928).
  - [2] C. E. Shannon, A mathematical theory of communication, The Bell system technical journal **27**, 379 (1948).
  - [3] А. С. Холево, Некоторые оценки для количества информации, передаваемого квантовым каналом связи, Проблемы передачи информации **9**, 3 (1973).