



Введение в квантовую информатику

Алексей Борисович Курдинов

10-11 класс

«Возможно, вскоре квантово-информационная картина мира отправит привычную нам физику [речь идет ни много ни мало как о всемогущей Квантовой Теории Поля!] вслед за алхимией, флогистоном и тремя китами.»

Херард 'т Хоофт, Нобелевский лауреат по физике

Что такое «кубит»?

Как из них построить сеть?

Какие алгоритмы могут реализовывать эти сети?

Как с их помощью можно решать некоторые задачи неизмеримо быстрее, чем обычными компьютерами?

Эти и другие вопросы мы сможем подробно (с примерами и упражнениями!) обсудить в ходе предлагаемого с/к.

А заодно и поубавить священный трепет перед словом «квантовый», который давно уже стал анахронизмом.

За тридцать лет своего существования Квантовая Информатика сумела превратиться в полноценную, бурно развивающуюся научную дисциплину, которой занимаются сотни тысяч специалистов во всем мире.

И хотя до аппаратной реализации квантового компьютера еще не близко, Нобелевская Премия 2012 года недвусмысленно подтверждает серьезность намерений мировой науки двигаться в этом направлении!

Из предварительной математики нам потребуется, пожалуй, только уравнение единичной окружности, да линейные замены двух переменных.

Так что если вам приходилось слышать о синусах и косинусах – то с математикой проблем не будет ☺.

А вот физику, которую мы с помощью этих элементарных средств сможем описывать, до недавних пор считали доступной не раньше, чем курсе на третьем физических факультетов!

*Историческая справка: с 80-х годов набирает силу новая, пока в основном чисто математическая, дисциплина – **Квантовая Информатика**. В основе ее лежит довольно простой – но абсолютно квантовый! – объект под названием «кубит». Из них по специальным правилам можно строить «вычислительные сети», подобно тому как из классических логических элементов (типа И-НЕ) строятся обычные вычислительные сети. Замечательным свойством этих сетей – и алгоритмов, для них написанных («квантовых алгоритмов») – служит колоссальное ускорение большинства вычислений. К примеру, задача разложения числа на простые множители (в реальных системах шифрования – скажем 300-цифрового числа на 150-цифровые множители) по классике решается за астрономические времена, тогда как квантовый алгоритм Шора позволяет решить ее за время, сопоставимое со временем перемножения.*

Схема курса:

1. Квантовые постулаты и их мотивация. Эксперимент с двумя щелями
2. Интерпретации Фейнмана и Эверетта. Мультиверс
3. Кубит. Принцип суперпозиции. Различные базисы в 2-мерии. Принцип неопределенности
4. Два кубита. Запутанные состояния. Парадокс Эйнштейна-Подольского-Розена
5. Теорема Белла и опыты Аспе
6. Клонирование и квантовая телепортация
7. Квантовые вентили. Простейшие сети. Понятие квантового алгоритма. Тезис Дойча.
8. Квантовое преобразование Фурье. Алгоритм Саймонса
9. Алгоритм Шора для факторизации.
10. Алгоритм Гровера. Перспективы квантовых компьютеров

Пробное занятие

сентября,

, каб.