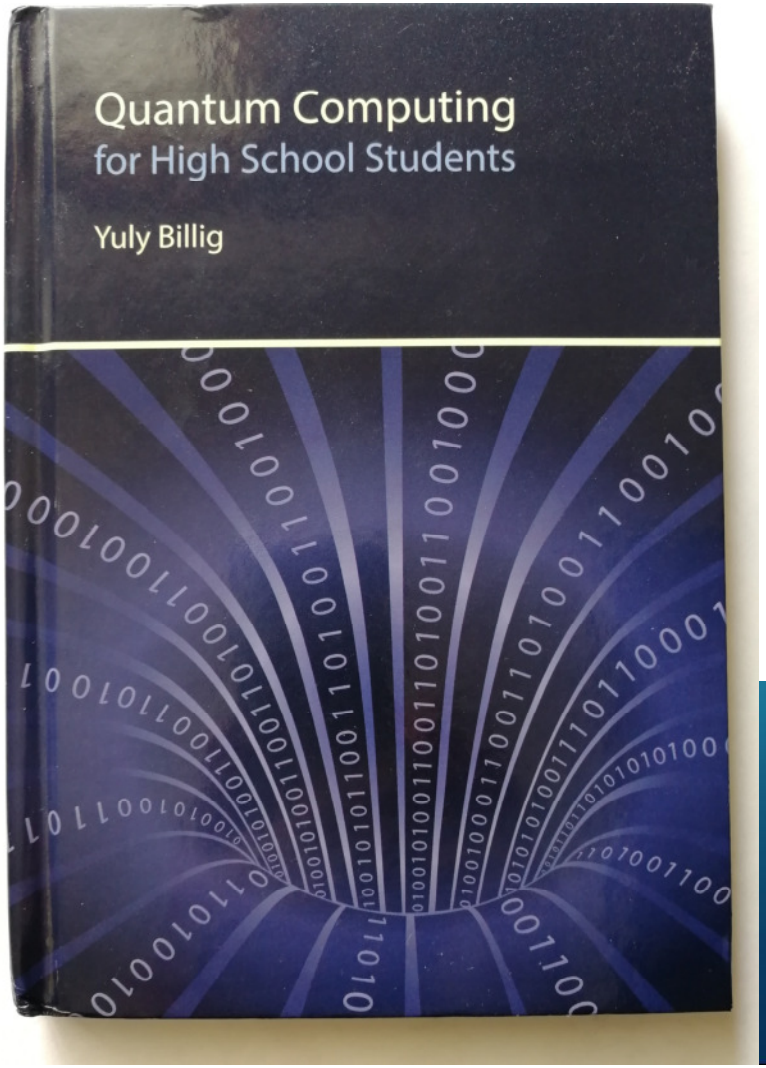
IMIR-

ия


Quantum Computing
for High School Students
Yuly Billig


КВАНТОВЫЕ
ВЫЧИСЛЕНИЯ
Юлий Биллиг

ОГЛА

- Предисл
- Блеск и н
- Квантовая
- Криптографи
- Линейные тран
- Квантовая телепор
- Теория групп (4 главы)
- Криптосистема RSA
- Классические вычисления на квантовом компьютере (3 главы)
- Преобразование Фурье (ДПФ, БПФ, КПФ – 3 главы)
- Алгоритм Шора
- За рамками книги

ПЛАН

- Введени
- Биты и ку
- Запутывани
- Квантовая теле
- Квантовый алгоритм и сических вычислений
- Квантовое преобразование Фурье
- Алгоритм Шора
- Итоги

ВВЕД

- Кванто
- Позволя трудные» для клас
- Программи нее классического
- Учить основам ква т уже сегодня.
- Блеск и нищета квантовых компьютеров
- Какие задачи уже сегодня можно решать на квантовом компьютере.

БИТЫ

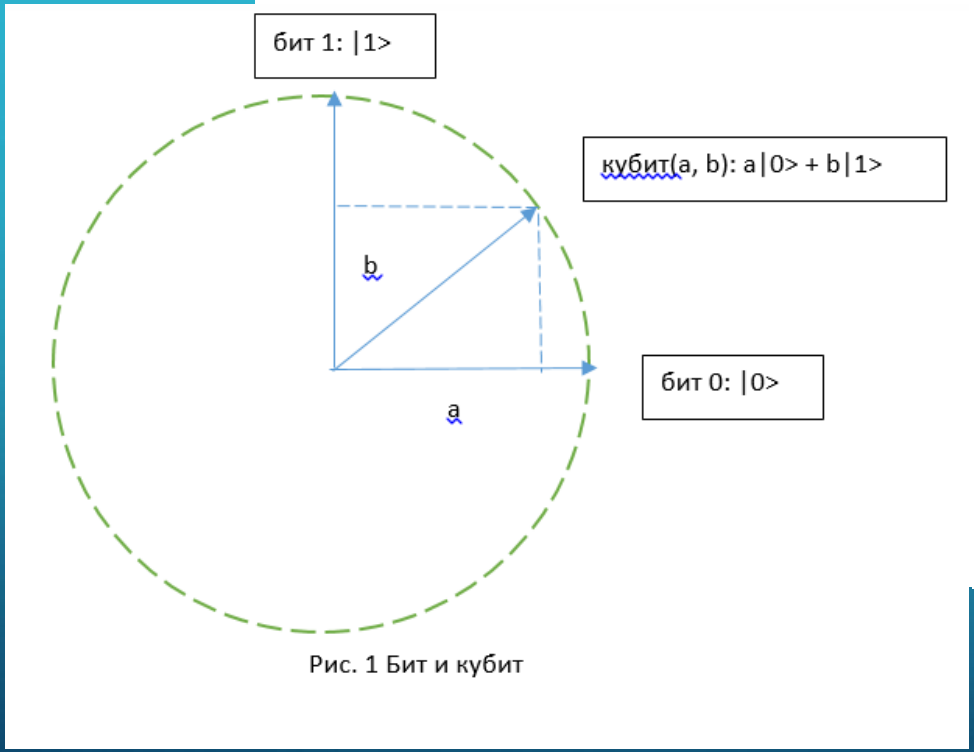


Рис. 1 Бит и кубит

ы

ины

ой длины
. a^2 + b^2 = 1

единичной длины в
е размерности 4

A0|00> + A1|01> + A2|10> + A3|11>

- N-Кубит – вектор единичной длины в пространстве размерности 2^N
- Sum(Ak |k>) k = 0 … 2^N

ИЗМЕР

- Измер
  состоя ми
  кубита.
- В N-куби льких
  кубитов.
- 3-кубит: 0,3|0 |101> -0,2|110>
  Измеряя первые получим 00 и
  новое состояние p(0,3| е p = 1/корень(0,45)
- N-кубит, в котором присутствуют все коэффициенты может быть факторизован – представлен в виде тензорного произведения N независимых кубитов.
- Запутанное состояние , когда факторизация невозможна

КВАН

- Кванто
- Нельзя
- Нельзя т
- Можно тел ояние кубита A)
- Проблема: Нев так что нужно телепортировать с ния.
- Создаем 3-кубит. В точке тным состоянием и кубит P запутанной пары. В точку B посылаем другой кубит Q запутанной пары.
- Над парой кубитов (S, P) в точке A выполняется некоторое преобразование и измеряется его результат. В точке B кубит Q перейдет в новое состояние.

КЛАС
АЛГО

- N-куби
- Класси торами.
- Квантов ического алгоритма тями.
- Элементарны ействуют над одним – двумя би
- Квантовые аналоги элем раций классического компьютера
  QAND, QOR, QNOT
- Специфические операции
- Преобразование Адамара, управляемое отрицание

КВАН ЬЕ

- Широк и f(t), измере тот, сокраща
- ДПФ – дис O(N^2), где N = 2^n.
- БПФ – быстрое пр сть O(N*logN) = O(n*N)
- КПФ – квантовое преобразование Фурье. Сложность O(logN*logN) = O(n^2)

АЛГО

- Алгори рафию, основа
- Пусть N ча факториз компьютер .
- Порядок групп -1).
- M является делите пы g
- Строится (1/2^n) Sum|k> |g^k mod N (k = 0.. 2^(2n))
- g^k – периодическая функция. КПФ позволяет определить порядок элемента g, что в конечном итоге позволяет за полиномиальное время решить задачу.

ИТОГ

- Можно … ьютеры станут … одня.
- Квантовы… решать ряд важны… ассических компьютерах…
- Программирован… – новый вызов теории и практике прогр…
- Данный курс позволяет понять основы квантовых вычислений.
- Курс доступен продвинутым школьникам и студентам факультетов ИТ.