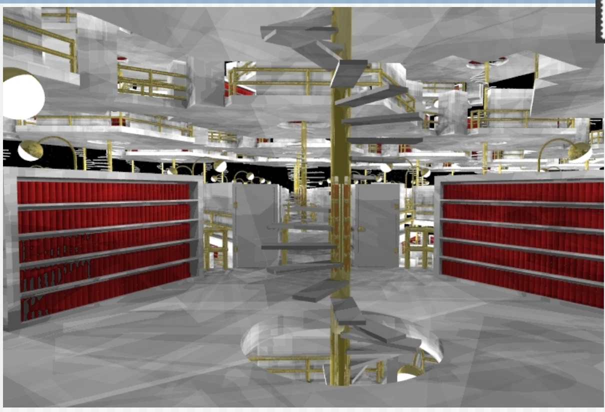
Overview

- Information is what remains after one abstracts from the material aspect of the physical reality ...
- How to do it?

The Library of Babel



- The universe (which others call the Library) is composed of an indefinite and perhaps infinite number of hexagonal galleries, with vast air shafts between, surrounded by very low railings
  - Jorge Luis Borges (1899-1986)

What is an „A“ ?

- What makes something similar to something else (specifically what makes, for example, an uppercase letter 'A' recognisable as such)

- Metamagical Themas, Douglas Hoffstader, Basic Books, 1985

- First law of thermodynamics: conservation of energy
  - The change in the internal energy of a closed thermodynamic system is equal to the sum of the amount of heat energy supplied to the system and the work done on the system
- Second law: entropy
  - The total entropy of any isolated thermodynamic system tends to increase over time, approaching a maximum value

- Entropy is a measure of disorder of the configuration of states of the atoms or other particles, which make up the system

- Any physical system that is made up of many, many tiny parts will have **microscopic** details to its physical behavior that are not easy to observe (*Matt McIrvin*)
- There are various **microscopic** states the system can have, each of which is defined by the state of motion of every one of its atoms, for instance
- But all we can measure easily are its **macroscopic** properties like density or pressure

Secend Law of Thermodynamics

- The Second Law of Thermodynamics can be nicely stated as follows
- A physical system will, if isolated (that is, if energy cannot get in or out), tend toward the available **macroscopic** state in which the number of possible **microscopic** states is the *largest*

- Suppose that the "macrostate" is the total of the dice
  - There are six ways to get a total of 7 from the "microstates" of the two dice
  - Only one way to get a total of 2 or 12
  - *7 is more likely*

$$S = k \log W$$

- In statistical thermodynamics, Boltzmann's equation is a probability equation relating the entropy *S* of an ideal gas to the quantity *W*, which is the number of **microstates** corresponding to a given **macrostate**
- *k* is Boltzmann's constant equal to *1.38062 x 10-23 joule/kelvin* and

- Boltzmann formula shows the relationship between entropy and the *number of ways the atoms or molecules of a thermodynamic system can be arranged*
- Entropy has to do with the *number of ways* that the microstate can rearrange itself without affecting the macrostate
  - Stated in terms of this quantity, the Second Law says that isolated systems tend toward an equilibrium macrostate with as large a total entropy as possible, because then the number of microstates is the largest

- We define the real entropy:

- for one experiment as $H_0(F^1)$
- for two experiments as $H_0(F^2)$
- ..
- For k experiments as $H_0(F^k)$

- The mean number of question for one experiment in the sequence of *k* experiments is
- $1/k \, {}^*H_0(F^k)$

- For four cards of which one is the joker the probability of a joker is *0.25* and of other cards *1-0.25=0.75*
- $H_0(F^1)=1$
- $H_0(F^1)=1= 1{}^*0.75 + 1{}^*0.25=1$
- $k=1,\ 1/k \, {}^*H_0(F^k)=1/1{}^*H_0(F^1)=1$
-

- What is the size of $H_0(F^2)$?

results	probability
card, card	$0.75 \cdot 0.75$
joker, card	$0.25 \cdot 0.75$
card, joker	$0.75 \cdot 0.25$
joker, joker	$0.25 \cdot 0.25$

$$H_0(F^2) = 1 \cdot 0.75 \cdot 0.75 + 2 \cdot 0.75 \cdot 0.25 + 3 \cdot 0.25 \cdot 0.75 + 3 \cdot 0.25 \cdot 0.25$$

$$H_0(F^2) = 1.6875$$

$$\frac{H_0(F^2)}{2} = 0.84375$$

results	probability
card, card, card	$0.25 \cdot 0.25 \cdot 0.25$
joker, card, card	$0.25 \cdot 0.75 \cdot 0.75$
card, joker, card	$0.25 \cdot 0.75 \cdot 0.25$
joker. joker, card	$0.75 \cdot 0.75 \cdot 0.25$
card, card, joker	$0.25 \cdot 0.25 \cdot 0.75$
joker, card, joker	$0.75 \cdot 0.25 \cdot 0.75$
card, joker, joker	$0.25 \cdot 0.75 \cdot 0.75$
joker, joker, joker	$0.75 \cdot 0.75 \cdot 0.75$

$$H_0(F^3) = 1 \cdot 0.42188 + 3 \cdot 0.14062 + 3 \cdot 0.14062 + 3 \cdot 0.14062 +$$

$$+ 5 \cdot 0.046875 + 5 \cdot 0.046875 + 5 \cdot 0.046875 + 5 \cdot 0.015625$$

$$H_0(F^3) = 2.4688$$

$$\frac{H_0(F^3)}{3} = 0.82292$$

Ideal Entropy

$$H(F) := \lim_{k \to \infty} \frac{H_0(F^k)}{k} \leq H_0(F)$$

$$H(F) = -\sum_i p_i \log_2 p_i$$

$$H(F) = -0.25 \cdot \log_2 0.25 - 0.75 \cdot \log_2 0.75 = 0.81128$$

- An experiment is described by probabilities $p=(p_1,p_2,\ldots,p_n)$
- Does the distribution of these probabilities have an effect on the ideal entropy?
- It turns out that the ideal entropy is maximal in the case all probabilities are equal, means $p=(1/n,1/n\ldots,1/n)$

- In this case the maximal ideal Entropy is

$$H(F) = -\sum_i p_i \log_2 p_i = -\log_2 1/n = \log_2 n$$

- The is nearly similar Boltzmann's equation, in which W is number of microstates corresponding to a given macrostate
- It follows that then number number of microstates is evenly distributed, each microstate has the same probability of appearance.

$$H(F) = -\sum_i p_i \log_2 p_i = -\log_2 1/n = \log_2 n$$

$$S = k \cdot \log \cdot W$$

- Instead of measuring the information in bits, yes no questions, it measure the information in nepit (nat), it is the power of the Euler's number *e=2.7182818…* (sometimes also called Napier's constant).
  - Euler's number is irrational and can not be attributed to any questions
  - Euler's number is the ideal number which minimizes the depth of an idealistic search tree….

Relationship to *log₂*

$$-\frac{1}{\log 2}\sum_i p_i \log p_i = -\sum_i p_i \log_2 p_i$$

- Differs by a constant, *1.4427*

$$-\frac{1}{\log_{10} 2}\sum_i p_i \log_{10} p_i = -\sum_i p_i \log_2 p_i$$

- Differs by a constant, *3.3219*

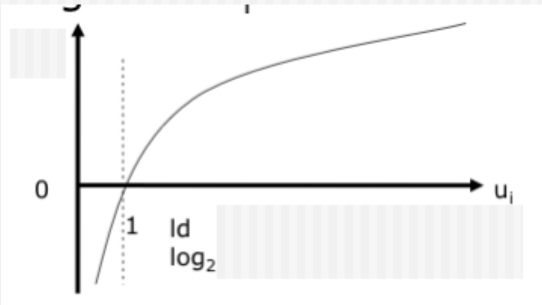
Information

- Information is the uncertainty which declines through the appearance of a character
- The information content is defined by the probability that this character appears
- Information is the gain of knowledge
- Information can be transmitted

- Noiseless communications:
- The decoder at the receiving end receives exactly the characterssent by the encoder
- The transmitted characters are typically not in the original message's alphabet.

- For example, in Morse Code appropriately spaced short and long electrical pulses, light flashes, or sounds are used to transmit the message

Information



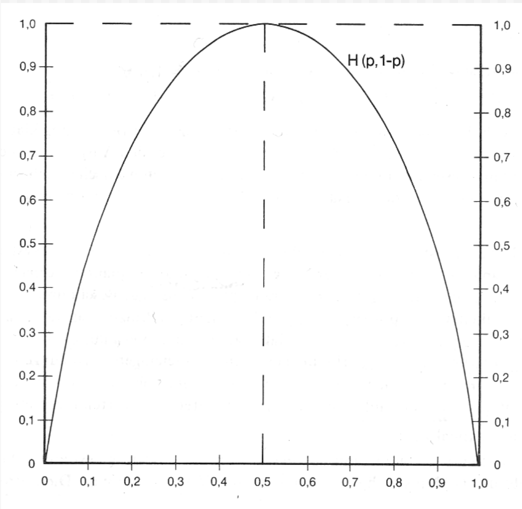
$$I_i = \log_2(u_i) = \log_2(1/p_i) = -\log_2(p_i)$$

Entropy in Information since

- Entropy measured in bits

$$I = H(F) = -\sum_i p_i \log_2 p_i$$

Only two characters



Probabilities, where do the come?

- Humans can believe is a subjective viewpoint
- *Form any finite sample, we can estimate the true fraction and also calculate how accurate our estimation is likely to be.*
  - *This approach is called frequentist.*
- True nature of the universe, for example for a fair coin the probability up heads 0.5.

. If Ω is a set of all possible events, $P(\Omega) = 1$

$$P(a) = card(a)/card(\Omega).$$

$$P(a|b) = card(P(a \wedge b))/card(b).$$

$$P(a|b) = \frac{P(a \wedge b)}{P(b)}$$

$$P(b|a) = \frac{P(a \wedge b)}{P(a)}$$

$$P(b|a) = \frac{P(a|b) \cdot P(b)}{P(a)}$$

Conditional Entropy

$$P(b|a) = \frac{P(a|b) \cdot P(b)}{P(a)}$$

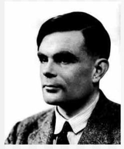
$$H(B \mid A) = -\sum_{a \in A} p(y) \sum_{b \in B} p(b \mid a) \log(p(b \mid a) = -\sum_{a,b} p(b,a) \log \frac{p(b,a)}{p(a)}$$

$$H(B \mid A) = H(B,A) - H(A)$$

Entscheidungsproblem
(German for 'decision problem')

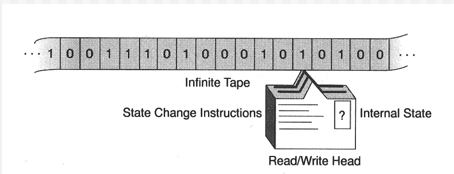
- Is there a general algorithm to determine whether a mathematical conjecture is true or false?

  - The origin of the Entscheidungsproblem goes back to Gottfried Leibniz, who in the seventeenth century, after having constructed a successful mechanical calculating machine, dreamt of building a machine that could manipulate symbols in order to determine the truth values of mathematical statements
  - As late as 1930 Hilbert believed that there would be no such thing as an unsolvable problem



- In 1936, Alonzo Church and Alan Turing published independent papers showing that it is impossible to decide algorithmically whether statements in arithmetic are true or false, and thus a general solution to the Entscheidungsproblem is impossible
- This result is now known as Church's Theorem or the Church-Turing Theorem

- The Turing machine consists of infinitely long tape that is marked off into a sequence of cells which may be written a *0*, a *1*, or a blank and read/write head
  - The head can move back and forth along the tape scanning the contents of each cell
  - The head can exist in one of a finite set of internal "states" and contains a set of instructions (program(
  - Program specifies, given current state, how the state must change given the bit currently being read under the head
  - Which direction the head has to move



- Any algorithmic process can be simulated on a Turing machine – an idealized and rigorously defined mathematical model of a computing device
- Many different models of computation are equivalent to the Turing machine (TM)

Halting Problem

- Entscheidungsproblem corresponds to the halting problem
- Given a description of a program and a finite input, decide whether the program finishes running or will run forever, given that input

- Gödel showed that “Any sufficient strong” formal system of arithmetic is incomplete if it is consistent
- There are sentences *P* and *NOT(P)* such that neither *P* nor *NOT(P)* is provable using the rules of the formal system
- There must be true statements of a formal system which can never be proved
- **Truth and the provability are distinct concepts!**

The Church-Turing thesis

- Doesn´the definition of P depend upon the computational model used in the statement of the definition, namely, the Turing machine?
- Church-Turing thesis: Any algorithmic process can be simulated on a **Turing machine**

- Strong Church-Turing thesis:
  - Any physically reasonable algorithmic process can be simulated on a Turing machine, with at most a polynomial slowdown in the number of steps required to do the simulation

- Deutsch: Maybe computers based on quantum mechanics might violate the strong Church-Turing thesis?

Strong Church-Turing thesis

- New formulation:
- The strong Church-Turing thesis implies that the problems in P are precisely those for which a polynomial-time solution is the best possible, in any **physically reasonable** model of computation

- Any irreversible operation in a circuit is necessarily accompanied by the dissipation of heat
  - information is lost, entropy grows
- Can we compute without dissipating heat?
  - The trick is to compute using only reversible circuit elements!
  - No information loss!
- Importance to us: quantum gates are most naturally viewed as reversible gates

- In a quantum computer, each bit could be represented by the state of a simple 2-state quantum system such as the spin state of a 1/2 particle
- The spin of such a particle when measured is always found to exist in one of two possible states, represented as *spin-up* or *spin-down*

$$\left|+\frac{1}{2}\right\rangle (spin-up)$$

$$\left|-\frac{1}{2}\right\rangle (spin-down)$$

- This intrinsic "discreteness" is called quantization
- As the spin of a particle is quantized we can use one spin state to represent binary value *0*, and the other state to represent the binary value *1*
  - Any 2-state quantum system, such as the direction of the polarization of the photon, or the discrete levels in an excited atom, would work equally well
- Goal: make a complete register out of a chain of such systems

Simple 2-state system

- Can be defined to be in two possible states

$$|\Psi\rangle = \omega_0|\Psi_0\rangle + \omega_1|\Psi_1\rangle = \begin{bmatrix}\omega_0\\ \omega_1\end{bmatrix}$$

- ω_i are complex numbers
- Ψ_i eigenstates form a complete orthogonal basis for the state vector
- Complete, any state in the Hilbert space can be represented as a weighted sum of $|\Psi_i\rangle$

- Superposition represented of state $|\Psi\rangle$ is given by:

$$|\Psi\rangle = \omega_0|\Psi_0\rangle + \omega_1|\Psi_1\rangle = \omega_0\begin{bmatrix}1\\0\end{bmatrix} + \omega_1\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\omega_0\\\omega_1\end{bmatrix}$$

$$|\Psi^{(1)}\rangle = \omega_0^{(1)}|\Psi_0^{(1)}\rangle + \omega_1^{(1)}|\Psi_1^{(1)}\rangle = \begin{bmatrix}\omega_0^{(1)}\\\omega_1^{(1)}\end{bmatrix}$$

$$|\Psi^{(2)}\rangle = \omega_0^{(2)}|\Psi_0^{(2)}\rangle + \omega_1^{(2)}|\Psi_1^{(2)}\rangle = \begin{bmatrix}\omega_0^{(2)}\\\omega_1^{(2)}\end{bmatrix}$$

$$|\Psi_0^{(1)}\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |\Psi_1^{(1)}\rangle = \begin{pmatrix}0\\1\end{pmatrix}, |\Psi_0^{(2)}\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |\Psi_1^{(2)}\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

$$|\Psi^{(1)}\rangle \otimes |\Psi^{(2)}\rangle = \begin{pmatrix}\omega_0^{(1)}\\\omega_1^{(1)}\end{pmatrix} \otimes \begin{pmatrix}\omega_0^{(2)}\\\omega_1^{(2)}\end{pmatrix} = \begin{pmatrix}\omega_0^{(1)}\omega_0^{(2)}\\\omega_0^{(1)}\omega_1^{(2)}\\\omega_1^{(1)}\omega_0^{(2)}\\\omega_1^{(1)}\omega_1^{(2)}\end{pmatrix} = |\Psi^{(1,2)}\rangle = \begin{pmatrix}\omega_{00}\\\omega_{01}\\\omega_{10}\\\omega_{11}\end{pmatrix}$$

New Basis

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

- A general state of a 2-bit memory register is

$$\left|\Psi^{(1),2}\right\rangle = \omega_{00}|00\rangle + \omega_{01}|01\rangle + \omega_{10}|10\rangle + \omega_{11}|11\rangle$$

  - Generalization is straightforward

- The basis $|x_1\rangle, |x_2\rangle, \ldots, |x_n\rangle$
  - It refers to an observable that can have some system properties with the respect to the chosen basis
  - The probability that the system x_i is $|\omega_i|^2$
    - Quantum description of two state system 0 and 1 (quantum coin)

$$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- The wavefunction in quantum mechanics evolves according to the Schrödinger equation into a linear superposition of different states
  - It describes the probability of the presence of certain states
- The actual measurements always find the physical system in a definite state

Probabilistic System

- We do not know the states of the system
- We know the probability distribution of the system
- We know that system is in states $x_1,...,x_n$ with probabilities $p_1,....,p_n$ that sum up to 1
- $p_1[x_1]+ p_2[x_2]+... +p_n[x_n]$ called mixed state

Quantum Mechanics

- Quantum mechanical description of a physical system looks very much like the probabilistic representation

$$|x_1\rangle, |x_2\rangle, \ldots, |x_n\rangle$$

- To describe a system we chose a basis of *n* dimensional Hilbert space H_n
- A state of n-level quantum system is described by a vector with complex numbers ω_i (amlitude of x_i)

$$\omega_1|x_1\rangle + \omega_1|x_1\rangle + \ldots + \omega_1|x_1\rangle$$

$$|\omega_1|^2 + |\omega_2|^2 + \ldots + |\omega_2|^2 = 1$$

Compound systems

- Suppose we have *n* and *m*-states

$$\{|x_1\rangle, |x_2\rangle, \ldots, |x_n\rangle\} \quad of \quad H_n$$

$$\{|y_1\rangle, |y_2\rangle, \ldots, |y_m\rangle\} \quad of \quad H_m$$

  - The compound system is described as a tensor product

$$H_n \otimes H_m \cong H_{nm}$$

  - With the basis states

$$|x_i\rangle \otimes |y_i\rangle = |x_i\rangle|y_i\rangle = |x_i, y_i\rangle \qquad i \in \{1,..,n\} \qquad j \in \{1,..,m\}$$

- A general state of a single quantum bit is a vector

$$\omega_0|0\rangle + \omega_1|1\rangle$$

$$|\omega_0|^2 + |\omega_1|^2 = 1$$

  - Having unit length
- Observation of a quantum bit in such a state will give 0 or 1 as an outcome with probabilities

$$|\omega_0|^2, |\omega_1|^2$$

- Let use the coordinate representation

$$|0\rangle = (1,0)^T \quad |1\rangle = (0,1)^T$$

- The unitary matrix defines an action

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- The unitary quantum gate defined by $M_\neg$ is called a quantum-not gate

$$M_\neg|0\rangle = |1\rangle, M_\neg|1\rangle = |0\rangle$$

- Another quantum gate

$$\sqrt{M_\neg} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \qquad \begin{aligned} \sqrt{M_\neg}|0\rangle &= \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \\ \sqrt{M_\neg}|1\rangle &= \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \end{aligned}$$

$$\left|\frac{1+i}{2}\right|^2 = \left|\frac{1-i}{2}\right|^2 = \frac{1}{2}$$

- 0 and 1 with a probability 1/2, because

$$\sqrt{M_\neg} \cdot \sqrt{M_\neg} = M_\neg$$

- Is called square root of the not-gate

Quantum Register

- A system of two quantm bits is a four-dimensional Hilbert space $H_4 = H_2 \otimes H_2$
- With the orthonormal basis $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$
- We write: $|0\rangle|0\rangle = |00\rangle, |0\rangle|1\rangle = |01\rangle, |1\rangle|0\rangle = |10\rangle, |1\rangle|1\rangle = |11\rangle$
- A state of a two-qubit system is a unit-length vector

$$\omega_0|00\rangle + \omega_1|01\rangle + \omega_2|10\rangle + \omega_3|11\rangle \qquad |\omega_0|^2 + |\omega_1|^2 + |\omega_2|^2 + |\omega_3|^2 = 1$$

- The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Is entangled, to prove it we assume the contrary $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a_0|0\rangle + a_1|1\rangle)(b_0|0\rangle + b_1|1\rangle) =$

$$= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle \rightarrow$$

$$a_0b_0 = \frac{1}{\sqrt{2}}$$

$$a_0b_1 = 0$$

$$a_1b_0 = 0$$

$$a_1b_1 = \frac{1}{\sqrt{2}} \qquad \textit{contradiction}$$

- Consider a quantum system having *n* **basis states** $|a_1\rangle, |a_2\rangle, \cdots, |a_n\rangle$
- We specify the state $|a_1\rangle$ in H_n to be a *"blanck sheet state"*
- A unitary mapping in $H_n \otimes H_n$ is called a quantum **copymachine**, for an state (vector) $|x\rangle \in H_n$

$$U(|x\rangle|a_1\rangle) = |x\rangle|x\rangle$$

No-cloning Theorem

- For *n > 1* there is no quantum copymachine

- *Proof*
- Assume that a quantum copymachine exists, even if n > 1…..
- Because n > 1, there are two orthogonal states $|a_1\rangle$ and $|a_2\rangle$

$$U\left(|a_1\rangle|a_1\rangle\right) = |a_1\rangle|a_1\rangle \quad U\left(|a_2\rangle|a_1\rangle\right) = |a_2\rangle|a_2\rangle$$

$$and \quad also$$

$$U\left(\frac{1}{\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)|a_1\rangle\right) = \left(\frac{1}{\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\right)\left(\frac{1}{\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\right)$$

$$= \frac{1}{2}\left(|a_1\rangle|a_1\rangle + |a_1\rangle|a_2\rangle + |a_2\rangle|a_1\rangle + |a_2\rangle|a_2\rangle\right)$$

$$U \quad linear$$

$$U\left(\frac{1}{\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)|a_1\rangle\right) = \frac{1}{\sqrt{2}}U(|a_1\rangle|a_1\rangle) + \frac{1}{\sqrt{2}}U(|a_2\rangle|a_1\rangle)$$

$$= \frac{1}{\sqrt{2}}|a_1\rangle|a_1\rangle + \frac{1}{\sqrt{2}}|a_2\rangle|a_2\rangle$$

$$U\left(\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)|a_1\rangle\right) = ?$$

$$\frac{1}{2}(|a_1\rangle|a_1\rangle + |a_1\rangle|a_2\rangle + |a_2\rangle|a_1\rangle + |a_2\rangle|a_2\rangle) \neq \frac{1}{\sqrt{2}}|a_1\rangle|a_1\rangle + \frac{1}{\sqrt{2}}|a_2\rangle|a_2\rangle$$

- Do not coincide by the very definition of tensor product

- There is no allowed operation that would **produce a copy of an arbitrary quantum state**
  - We can not make a copy of quantum state!
- Can we still build a quantum computer / develop an algorithm?

- In the proof , we did not make any use of unitary
- Only the linearity of time-evolution mapping was needed
- For **basis states**, there is a solution!

$$U(|a_i\rangle|a_j\rangle) = |a_{i'}\rangle|a_{j'}\rangle$$

- Is a permutation of **basis** vectors of $H_n \otimes H_n$
- And such **a permutation is unitary**

$$U(|a_i\rangle|a_1\rangle) = |a_i\rangle|a_i\rangle$$

- Is a copymachine on the **basis vectors!**

- Defines a reversible gate on three bits

$$T : F_2^3 \to F_2^3, T(x_1,x_2,x_3) = (x_1,x_2,x_1 \cdot x_2 - x_3)$$

$$T(x_1,x_2,x_3) = (x_1,x_2,(x_1 \wedge x_2) \oplus x_3)$$

permutation on F_2^m

$$(2^3)! = 8! = 40320$$

gates on 3bits

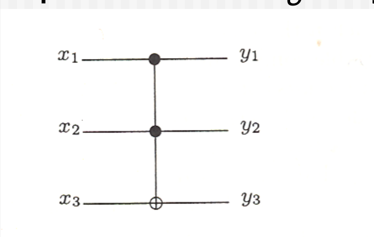
INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Toffoli gate

$$T : F_2^3 \to F_2^3, T(x_1,x_2,x_3) = (x_1,x_2,x_1 \cdot x_2 - x_3)$$

- This gate is called Toffoli gate
- Toffoli gate does not change bits x_1 and x_2
- It computes the not-operation on x_3 only if $x_1=1$ and $x_2=1$

- Symbol for Toffoli gate



- All Boolean circuits can be simulated by using only reversible gates
  - Not gates are reversible
  - And gate are simulated by Toffoli gate with $x_3=0$

$$T(x_1,x_2,x_3) = (x_1,x_2,x_1 \cdot x_2 - x_3)$$
$$T(x_1,x_2,0) = (x_1,x_2,x_1 \cdot x_2)$$

  - $x_1 \vee x_2 = \neg(\neg x_1 \wedge \neg x_2)$
  - Fanout (multiple wires leaving a gate) is simulated by the controlled not-gate with $x_2=0$

$$C(x_1,x_2) = (x_1,x_1 - x_2) \quad C(x_1,0) = (x_1,x_1)$$

- A quantum gate on m qubits is a unitary mapping in $H_2 \otimes H_2 \otimes \ldots\ldots \otimes H_2$ (*m* times), which operates on a fixed number qubits (independent of m)

- **Permutation matrix** is always unitary

$$M(f)^*_{ij} = 1 \Leftrightarrow f(e_i) = e_j$$

- *M(f)** represents the inverse permutation of *M(f)*

- H_2

$$W_2 = H_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad \begin{aligned} H_2|0\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ H_2|1\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

  - $W_{2,}$ H_2 is called Walsh matrix, Hadamard matrix or Hamarad-Walsh matrix

$$W_2\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}W_2|0\rangle + \frac{1}{\sqrt{2}}W_2|1\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |0\rangle$$

Hadamard matrix

- $H_n = H_2 \otimes H_2 \otimes \ldots. \otimes H_2$ n times

$$H_n|\mathbf{z}\rangle \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathrm{F}_2^n} (-1)^{\mathbf{z}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

$$\mathbf{z} \cdot \mathbf{x} = z_1 x_1 + \cdots + z_n x_n$$

- H_n is called Hadamard matrix

Matrix representation of serial and parallel operations

- Circuit for application of the phase gate, followed by Hadanard gate and then followed by Z gate

$$ZHP(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\theta} \\ -1 & e^{i\theta} \end{pmatrix}$$

- Computation in Parallel (of one qbit)

$$W_2 \otimes W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} W_2 & W_2 \\ W_2 & -W_2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Quantum Parallelism

- Functions *f(x)* on one bit:
  - *i)* identity function, *ii)+iii)* constant functions and *iv)* bit flip function

$$x \in \{0,1\}$$

$$i) \qquad f(x) = \begin{cases} 0 & if \quad x = 0 \\ 1 & if \quad x = 1 \end{cases}$$

$$ii) \qquad f(x) = 0$$

$$iii) \qquad f(x) = 1$$

$$iv) \qquad f(x) = \begin{cases} 0 & if \quad x = 1 \\ 1 & if \quad x = 0 \end{cases}$$

- Apply Hadamard Gates to the input state *|01>* to produce a state of two superpositions
- Apply U_f to that product state
- Apply a Hadamard gate to the first qubit leaving the second qubit alone

$$|\Psi_{out}\rangle = (W_2 \otimes I)U_f(W_2 \otimes W_2)|0\rangle|1\rangle$$
$$|\Psi_{out}\rangle = (W_2 \otimes I)U_f W_4|01\rangle$$

Deutsch-Jozsa Algorithm

- Generalization of the Deutsch's algorithm
  - In the Deutsch-Jozsa problem, we are given a black box quantum computer known as an oracle that implements the function
  - We are promised that the function is either **constant** (0 on all inputs or 1 on all inputs) or **balanced** (returns 1 for half of the input domain and 0 for the other half); the task then is to determine if *f* is constant or balanced by utilizing the oracle

- We start by

$$|\Psi'\rangle = \left(W_2^{\otimes n}\right)\left(|0\rangle^{\otimes n}\right) \otimes (W_2|1\rangle)$$

$$|\Psi'\rangle = (W_n)\left(|0\rangle^{\otimes n}\right) \otimes (W_2|1\rangle)$$

$$|\Psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in F_2^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Next we apply $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$
- The first *n* qubits are the value of *x*
- *y* is one qubit

- The output is

$$|\Psi''\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in F_2^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Applying a Hadamard gate to n qubits

$$W_n|x\rangle = \sum_{y\in F_2^n}(-1)^{x\cdot y}|y\rangle$$

$$|\Psi_{out}\rangle = \frac{1}{2^n}\sum_{y\in F_2^n}\sum_{x\in F_2^n}(-1)^{x\cdot y+f(x)}|y\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

  - Measurments on n qubits ly>
    - Returns 0's. In this case *f(x)* is constant
    - Otherwise, if at least one of the qubits is to be 1, *f(x)* is balanced

Discrete Fourier Transform

- Operates on discrete complex-valued function
  - Given a function *a* :

$$a:[0,1,...,N-1]\to C$$

  - The discrete Fourier transform produces a function *A* :

$$A:[0,1,...,N-1]\to C$$

$$A(x)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}a(k)\cdot e^{2\pi i\cdot\frac{kx}{N}}$$

- DFT can be seen as a linear transform talking the column vector ***a*** to a column vector ***A***

$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{0\cdot 0}{N}} & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{0\cdot 1}{N}} & \cdots & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{0\cdot N-1}{N}} \\ \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{0\cdot 1}{N}} & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{1\cdot 1}{N}} & \cdots & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{(N-1)\cdot 1}{N}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{0\cdot(N-1)}{N}} & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{1\cdot(N-1)}{N}} & \cdots & \frac{1}{\sqrt{N}} \cdot e^{2\pi i \frac{(N-1)\cdot(N-1)}{N}} \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

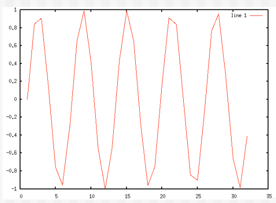
- Simplification

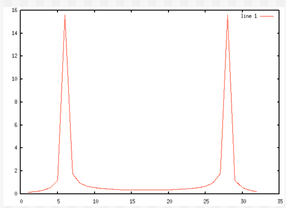
$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & e^{2\pi i \frac{1\cdot 1}{N}} & \cdots & e^{2\pi i \frac{(N-1)\cdot 1}{N}} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & e^{2\pi i \frac{1\cdot(N-1)}{N}} & \cdots & e^{2\pi i \frac{(N-1)\cdot(N-1)}{N}} \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

- Example, N=4

$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

- Any periodic complex-valued function a with *period* ***r*** and frequency ***u=N/r*** can be approximated using its Fourier series as the sum of exponential functions whose frequencies are multiples of ***u***.





- A complex root of unity is a complex number $\omega^N = 1$
- There are exactly nth roots of unity:

$$e^{2\pi i \frac{k}{N}} \quad for \quad k = 0,1,\ldots,N-1$$

- We define $\omega_N = e^{2\pi i \frac{1}{N}}$

$$e^{iu} = \cos(u) + i \cdot \sin(u)$$

$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & e^{2\pi i \frac{1\cdot 1}{N}} & \cdots & e^{2\pi i \frac{(N-1)\cdot 1}{N}} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & e^{2\pi i \frac{1\cdot(N-1)}{N}} & \cdots & e^{2\pi i \frac{(N-1)\cdot(N-1)}{N}} \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N^{1\cdot 1} & \cdots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{1(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

Remarks

$$\begin{pmatrix} A(0) \\ A(1) \\ \vdots \\ A(N-1) \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N^{1\cdot 1} & \cdots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{1(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \cdot \begin{pmatrix} a(0) \\ a(1) \\ \vdots \\ a(N-1) \end{pmatrix}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N^{1\cdot 1} & \cdots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{1(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

The Quantum Fourier Transform

- QFT is a variant of FFT with $N=2^n$

$$\sum_x a(x)|x\rangle \rightarrow \sum_x A(x)|x\rangle$$

- *A(x)* are the Fourier coefficients of the discrete Fourier transform *a(x)*
- After the Fourier transform the probability of the resulting state *|x>* would be *|A(x)|*^{2}

- Applying the quantum Fourier transform to a state whose amplitude are given by a periodic function *a(x)* with period *r*, where *r* is a power of *2*
- **would result in *A(x)* zero except where *x* is a multiple *N/r, for example j*N/r***

- Quantum Fourier transform (QTF) on orthonormal basis

$$U_{F^n} : |x\rangle \rightarrow \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} e^{2\pi i \cdot \frac{kx}{N}} |x\rangle = \sum_{x \in F_2^n} \frac{1}{\sqrt{N}} e^{2\pi i \cdot \frac{kx}{2^n}} |x\rangle$$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N^{1\cdot 1} & \cdots & \omega_N^{(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{1(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

$$\omega_N = e^{2\pi i \frac{1}{N}}$$

Shor's Algorithm

- Shor's quantum algorithm for factoring relies upon a result from number theory
- Relates the period of a particular periodic function to the factor of an integer
- Given an integer *n* (number to be factored) construct a function
- $f_n(a)=x^a \bmod n$
  - where *x* is an integer chosen at random that is a coprime to *n*
  - Coprime, means that the greatest common divisor of *x* and *n* is *1*, $gcd(x,n)=1$

- Why is this function interesting with respect to the problem of factoring *n*
  - It turns out that $f_n(a)$ is periodic
  - For $a=0,1,2,3,..$ the values of the function $f_n(0),f_n(1),f_n(2),f_n(3),..$ fall into repeating pattern eventually
  - Different values of *x* give rise to different patterns
  - The number of values in between the repeating pattern, for a particular value *x* is called *period of x modulo n* indicated by *r*
  - $x^r=1 \bmod n$

- *x^r=1 mod n*
  - If *r* is an even number, then

$$x^r = 1 \mod n$$
$$\left(x^{\frac{r}{2}}\right)^2 = 1 \mod n$$
$$\left(x^{\frac{r}{2}}\right)^2 - 1 = 0 \mod n$$
$$\left(x^{\frac{r}{2}}\right)^2 - 1^2 = 0 \mod n$$
$$\left(x^{\frac{r}{2}} - 1\right)\left(x^{\frac{r}{2}} + 1\right) = 0 \mod n$$

- The product *$(x^{r/2}-1)(x^{r/2}+1)$* is some integer multiple of *n*
- Dividing *$(x^{r/2}-1)(x^{r/2}+1)$* by *n* results in a reminder of zero
- One of the terms *$(x^{r/2}-1)(x^{r/2}+1)$* must have a nontrivial factor in common with n
  - *$gcd((x^{r/2}-1),n)$ and $gcd((x^{r/2}+1),n)$*

- Our goal it to find *r* of $f_{x,n}(a)=x^a \bmod n$
- To do it we create a quantum register with two parts called Register1 and Register2
- Although the complete register consists of a chain of qubits, we will use a more compact notation for representation
- Register1 is holding the number *a* (base 10) and Register2 is holding the number *b* (base 10)
- Complete register is $|a,b\rangle$

- Next we create in Register1 a superposition of the integer $a=0,1,2,3,\ldots,q-1$
- This values become the arguments of the function $f_{x,n}(a)$
- We evaluate in quantum parallel $f_{x,n}(a)$ on each *a* and place the results in Register2
  - Time corresponds to computation of one value on a classical computer
- In Register2 we have a superposition of the function evaluations

- In Register2 we have a superposition of the function evaluations
- We measure the Register2
  - Collapse the superposition stored in Register2 and we obtain some answer, say *k*
  - This means there was some value of such that x^a *mod n=k*
  - Act of measuring has a side-effect on Registe1
  - Measurements made on one part of a quantum register have the effect of projecting out the states of other parts of the register

- By observing the Register2 we actually change the content of Register1
- Register1 will represent now the superposition of just those values of a, such that x^a *mod n=k*
- The values in Register1 are

$$\{a, a+r, a+2r, a+3r, \ldots\}$$

$$\omega|a\rangle + \omega|a+2r\rangle + \omega|a+3r\rangle + + \cdots$$

- Note, the amplitudes are all equal
  - How to get *r*?

- We compute the discrete Fourier transform of the content of the Register1 and put the results back in Register1, (the amplitude corresponds to the frequency intensity)
  - Register1 contains a periodic function
  - Its Fourier transform will be peaked (high values) at the multiples of the inverse period *1/r*
    - Map the functions of time to the frequency domain
    - The frequency is the inverse of the period
- Now the amplitudes with which various states appear are no longer equal

- States corresponding to integer multiples of the inverse period, and these close to them, appear with a greater amplitudes
- Those that do not correspond to integer multiples of the inverse period have a lower amplitude
- If we measure the state of Register1 we obtain highly likely a result which is close to some multiple of the inverse period
  - After repeating the whole process several times, we obtain enough samples of integer multiples of the inverse period to be able to determine the period *r*

Quantum blackbox

- In order to model the quantum search we have to fix the notation of a quantum blackbox function *f(x)* on a quantum computer
- We will use a source **register** */x>* (n bits) and a target **bit** */b>*
- A query operator Q_f is a linear mapping

$$Q_f |\mathbf{x}\rangle |b\rangle = |\mathbf{x}\rangle |b \oplus f(\mathbf{x})\rangle$$

- $\oplus$ means addition modulo 2, exclusive or operation

- If we flip the target bit to one and apply to it H_2 we get

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathrm{F}_2^n} |\mathbf{x}\rangle H_2 |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathrm{F}_2^n} |\mathbf{x}\rangle \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right)$$

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathrm{F}_2^n} |\mathbf{x}\rangle \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right) = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{\mathbf{x} \in \mathrm{F}_2^n} |\mathbf{x}\rangle |0\rangle - \sum_{\mathbf{x} \in \mathrm{F}_2^n} |\mathbf{x}\rangle |1\rangle \right)$$

- After applying the query Q_{fy}

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\in\mathrm{F}_2^n}|\mathbf{x}\rangle|0\rangle - \sum_{\mathbf{x}\in\mathrm{F}_2^n}|\mathbf{x}\rangle|1\rangle\right) = \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle|0\rangle + |\mathbf{y}\rangle|\mathbf{1}\rangle - \sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle|1\rangle - |\mathbf{y}\rangle|\mathbf{0}\rangle\right)$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle|0\rangle + |\mathbf{y}\rangle|\mathbf{1}\rangle - \sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle|1\rangle - |\mathbf{y}\rangle|\mathbf{0}\rangle\right) = \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle\left(|0\rangle - |1\rangle\right) + |\mathbf{y}\rangle\left(|1\rangle - |0\rangle\right)\right)$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle\left(|0\rangle - |1\rangle\right) + |\mathbf{y}\rangle\left(|1\rangle - |0\rangle\right)\right) = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{f_y(\mathbf{x})}|\mathbf{x}\rangle\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

target bit

target

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{\mathbf{x}\neq y}|\mathbf{x}\rangle\left(|0\rangle - |1\rangle\right) + |\mathbf{y}\rangle\left(|1\rangle - |0\rangle\right)\right) = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{f_y(\mathbf{x})}|\mathbf{x}\rangle\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

- Notice that the target bit in superposition before applying the query operator is used to encode the value $f_y(\boldsymbol{x})$ by value $(-1)^{f_y(\mathbf{x})}$
- We do not need the target bit anymore!

$$\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{f_y(\mathbf{x})}|\mathbf{x}\rangle$$

$$\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{f_y(\mathbf{x})}|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{\mathbf{x}\in\mathbf{F}_2^n}|\mathbf{x}\rangle - 2|\mathbf{y}\rangle\right)$$

Think about the probabilistic coin, we get ***0*** because of **+**

- If ***x=y*** then it is subtracted in the sum
- After applying Hadamard W_n we get

$$W_n\left(\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\mathbf{F}_2^n}|\mathbf{x}\rangle - \frac{2}{\sqrt{2^n}}|\mathbf{y}\rangle\right) = |\mathbf{0}\rangle - \frac{2}{2^n}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{\mathbf{x}\cdot\mathbf{y}}|\mathbf{x}\rangle$$

$$|\mathbf{0}\rangle - \frac{2}{2^n}\sum_{\mathbf{x}\in\mathbf{F}_2^n}(-1)^{\mathbf{x}\cdot\mathbf{y}}|\mathbf{x}\rangle = \left(1-\frac{2}{2^n}\right)|\mathbf{0}\rangle - \frac{2}{2^n}\sum_{\mathbf{x}\neq\mathbf{0}}(-1)^{\mathbf{x}\cdot\mathbf{y}}|\mathbf{x}\rangle$$

We separate |***0***> from sum. How?

Grover's Amplification

- Operators which we will use:
  - We need a query operator which calls for value f_y uses n qubits for the source register and one target bit $\mathbf{y}\in F_2^n$

$$V_f|\mathbf{x}\rangle = (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle \qquad f_y(\mathbf{x}) = \begin{cases} 1, if & \mathbf{x}=\mathbf{y} \\ 0, & otherwise \end{cases}$$

  - We need a quantum operator R_n defined on n qubits and operating as

$$R_n|\mathbf{0}\rangle = -|\mathbf{0}\rangle \quad and \quad R_n|\mathbf{x}\rangle = |\mathbf{x}\rangle, \mathbf{x}\neq\mathbf{0}$$

Amplitude Amplification

- Finding ***y*** by the quantum operator
  - $G_n = -H_n R_n H_n V_f$
  - Working on *n* qubits representing elements ***x***
  - $H_n R_n H_n$ can be written as a $2^n x 2^n$ matrix

$$H_n R_n H_n = \begin{pmatrix} 1-\frac{2}{2^n} & -\frac{2}{2^n} & -\frac{2}{2^n} & \cdots & -\frac{2}{2^n} \\ -\frac{2}{2^n} & 1-\frac{2}{2^n} & -\frac{2}{2^n} & \cdots & -\frac{2}{2^n} \\ -\frac{2}{2^n} & -\frac{2}{2^n} & 1-\frac{2}{2^n} & \cdots & -\frac{2}{2^n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{2}{2^n} & -\frac{2}{2^n} & -\frac{2}{2^n} & \cdots & 1-\frac{2}{2^n} \end{pmatrix}$$

- $H_n R_n H_n$ can be also expressed as
  - $H_n R_n H_n = I - 2P$
- Where I is a $2^n x 2^n$ identity matrix and P is a $2^n x 2^n$ projection matrix whose every entry is $1/2^n$

- In this example we consider function

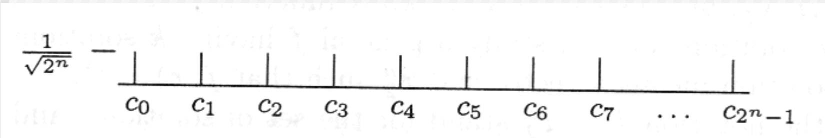
$$\mathbf{y} \in F_2^n$$

$$f_5(\mathbf{x}) = \begin{cases} 1, if & \mathbf{x} = \mathbf{y} \\ 0, & otherwise \end{cases}$$

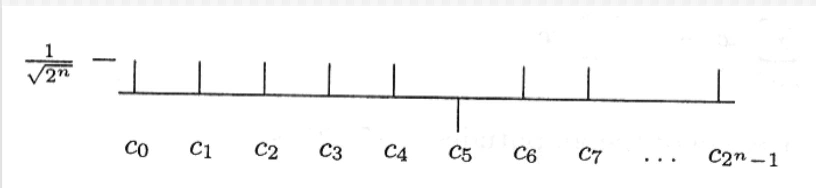
  - The search begins with superposition

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in F_2^n} |\mathbf{x}\rangle$$

$$c_0 = c_1 = c_2 = \cdots c_{2^n - 1} = \frac{1}{\sqrt{2^n}}$$



- V_{f5} is applied o change the sign of ***x=y***
- Those amplitudes that are coefficients of a vector *|**x**>* satisfying $f_5(\mathbf{x})=1$ become negative, c_5 becomes negative



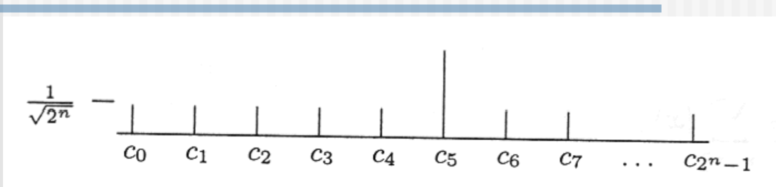
- The average of the amplitude is now

$$A = \frac{1}{2^n}\left(\left(2^n - 1\right)\frac{1}{\sqrt{2^n}} - \frac{1}{\sqrt{2^n}}\right) = \frac{1}{\sqrt{2^n}}\left(1 - \frac{2}{2^n}\right)$$

- Inversion about the average-operator $-H_nR_nH_n$ will perform a transformation

$$\frac{1}{\sqrt{2^n}} \mapsto 2A - \frac{1}{\sqrt{2^n}} \approx \frac{1}{\sqrt{2^n}}$$

$$-\frac{1}{\sqrt{2^n}} \mapsto 2A + \frac{1}{\sqrt{2^n}} \approx 3 \cdot \frac{1}{\sqrt{2^n}}$$



$$\frac{1}{\sqrt{2^n}} \mapsto 2A - \frac{1}{\sqrt{2^n}} \approx \frac{1}{\sqrt{2^n}}$$

$$-\frac{1}{\sqrt{2^n}} \mapsto 2A + \frac{1}{\sqrt{2^n}} \approx 3 \cdot \frac{1}{\sqrt{2^n}}$$

- The probability to find the answer is *$9/2^n$* by a single query, *4.5* times better than a classical randomized search can do

- Iterative use of the mapping
  - $G_n = -H_n R_n H_n V_f$

- Instead of a blackbox function that assumes only one solution, we will study a general function *f* having *k* solutions

- By using a quantum circuit, any problem in **NP** can be solved with a nonvanishing correctness probability in time

$$O\left(\sqrt{2^n}\, p(n)\right)$$

- Where p is polynomial depending on the particular problem

Optimality of the search algorithm

- To search N items, we need to consult the oracle (black box function) $O(\sqrt{N})$ times
- No quantum algorithm can perform this task using fewer than $\Omega(\sqrt{N})$ access to the search oracle
- Grover's algorithm is optimal!

- Suppose the algorithm starts with state $|\psi\rangle$
- For simplicity, the search problem has just one solution y
- To determine y we are allowed to apply the oracle O_y which gives a phase shift *-1* to the solution $|y\rangle$

- Algorithm starts with $|\psi\rangle$ and applies O_y k times within some unitary operations $U_1, U_2, \ldots, U_k$

$$|\psi_k^y\rangle = U_k O_y U_{k-1} O_y \ldots U_1 O_y |\psi\rangle$$

$$|\psi_k\rangle = U_k U_{k-1} \ldots U_1 |\psi\rangle$$

- $|\psi_k\rangle$ without the oracle

- We define D_k as the deviation after k steps caused by the oracle from the evaluation without the oracle cal with $|\psi_0\rangle = |\psi\rangle$ as

$$D_k = \sum_y \left\| |\psi_k^y\rangle - |\psi_k\rangle \right\|^2$$

- Proof will be as:

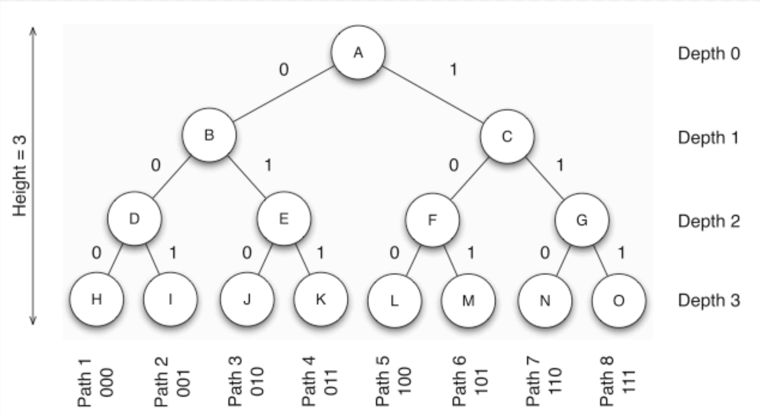
1. A bound on D^k that shows it can not grow faster than $O(k^2)$
2. D_k must be $\Omega(\sqrt{N})$ if it is possible to distinguish N alternatives (to see where the solution is)

- Why?
- van Neumann probabilities!
  - Amplitude ➔ Probabilities
  - <u>Oracle: solution indicated by **minus** (*phase shift)*</u>
  - Probability of measuring solution:

$$solution: O_y|\psi_k\rangle - |\psi_k\rangle = -2 \cdot amplitude|y\rangle = -2 \cdot \langle y|\psi_k\rangle |y\rangle$$

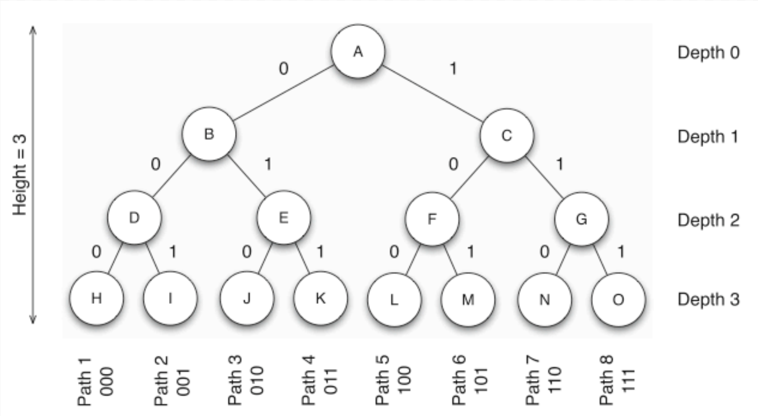
$$\left|\langle y|\psi_k^y\rangle\right|^2 \geq \frac{1}{2} = 0.5 \quad \left|\langle y|\psi_k\rangle\right|^2 \geq \frac{1}{N}$$

- For b=2 and d=3



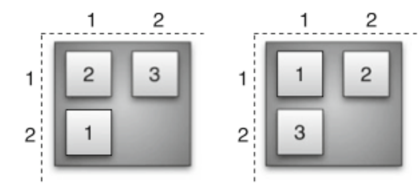
- The binary tree presented depicts the nodes reached from a root node A by applying one of two possible actions, respectively, 0 or 1
- The actions applied during the search are the production system equivalent of applying rules
- The set of actions leading to a leaf node is the **path** taken during the tree-search

- For b=2 and d=3



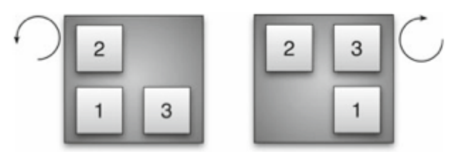
- Develop possible problem-solving strategies from a quantum computation perspective in order to produce a hybrid quantum production system
- A mechanism incorporating classical tree-search concepts capable of being applied alongside Grover's algorithm

- A a reversible production system capable of solving instances of the 3-puzzle

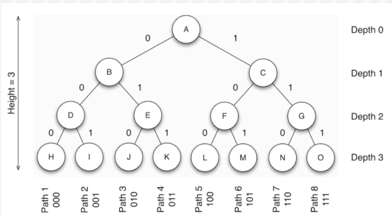


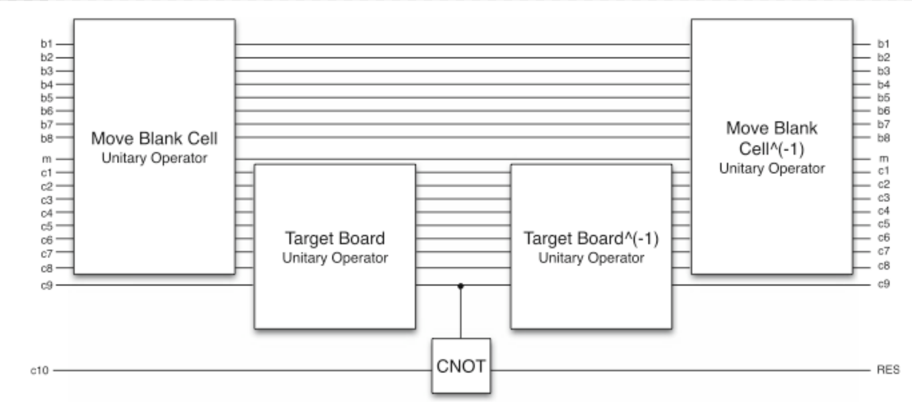
(a) Initial board configuration. **(b)** Target board configuration.

Simplification: 3-Puzzle



(a) Blank-cell counter-clockwise movement. **(b)** Blank-cell clockwise movement.





$$b_{avg} > 2^{\left\lceil \frac{\log_2 b_{\max}}{2} \right\rceil}$$

- our hybrid system will yield a speedup over classical search algorithms

Speed up

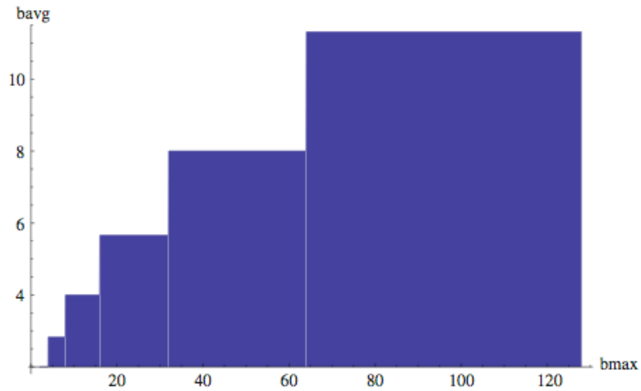
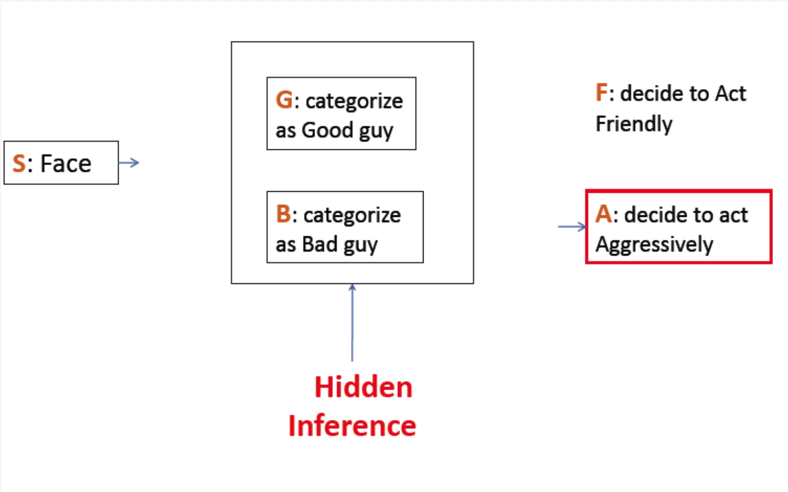


Fig. 3 The area plot of $b_{avg} \leq 2^{\frac{\lceil \log_2 b_{max} \rceil}{2}}$ for $b_{max} \in [2, 128]$. The shaded area indicates those values of b_{avg} that will produce better performance results over our hybrid quantum search system

- The states **exist** in the superposition as long as **not observed**
- They are described by the amplitudes
- Amplitudes *turn* into probabilities during measurement

No categorization, only decision



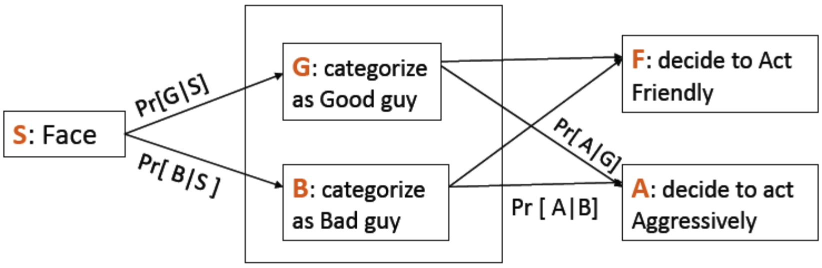
Theorem of total probability

If events $A_1, \ldots, A_n$ are mutually

exclusive with $\sum_{i=1}^{n} P(A_i) = 1$ then

$$P(B) = \sum_{i=1}^{n} P(B|A_i)P(A_i)$$

$$P(B) = \sum_{i=1}^{n} P(B, A_i)$$



$$\Pr[A \mid S] = \Pr[G|S] \cdot \Pr[A|G] + \Pr[B|S] \cdot \Pr[A|B]$$

Results

- Condition 1 (**without** categorization)
  $\Pr[A \mid S] = .69$
- Condition 2 (**after** categorization)
  $\Pr[G \mid S] = .17$; $\Pr[A \mid G] = .42$
  $\Pr[B \mid S] = .83$; $\Pr[A \mid B] = .63$

  Law of total probability:
  $\Pr[A \mid S] = (.17)(.42) + (.83)(.63) = .59$

Something is wrong!

ebit

- The entangled bits or qubits of a state are called an ebit
- An ebit is a shared resource
- An ebit is allways disrtributed between two particles (qubits) $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
- An ebit provides a channel for communication
- Once either particle comprising the ebit is measured, the states of both particles become definite

---

- Let´s denote the state that Alice wants to teleport to Bob

$$|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Alice and Bob Share an Entangled Pair of Particles

$$|\phi^+\rangle = \frac{|0_{Alice}\rangle|0_{Bob}\rangle + |1_{Alice}\rangle|1_{Bob}\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Alice and Bob are physically separate
- She can teleport a particle by interacting it with her member of the EPR pair

$$|\psi\rangle = |\chi\rangle \otimes |\phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

$$|\psi\rangle = \frac{\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)}{\sqrt{2}}$$

- The first two qubits belong to Alice the third to Bob

$$|\psi\rangle = \frac{\alpha\left(|0_{Alice}0_{Alice}0_{Bob}\rangle + |0_{Alice}1_{Alice}1_{Bob}\rangle\right) + \beta\left(|1_{Alice}0_{Alice}0_{Bob}\rangle + |1_{Alice}1_{Alice}1_{Bob}\rangle\right)}{\sqrt{2}}$$

- Alice applies a *CNOT* gate Bob doesn't do anything

$$U_{CNOT}|00\rangle = |00\rangle, U_{CNOT}|01\rangle = |01\rangle, U_{CNOT}|10\rangle = |11\rangle, U_{CNOT}|11\rangle = |10\rangle$$

$$|\psi'\rangle = U_{CNOT} \otimes I|\psi\rangle$$

$$|\psi'\rangle = \frac{\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)}{\sqrt{2}}$$

- Alice Applies a Hadarmad-Walsh gate

$$|\psi'\rangle = \frac{\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)}{\sqrt{2}}$$

$$|\psi'\rangle = \frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}}$$

$$|\psi''\rangle = \frac{\alpha W_2|0\rangle(|00\rangle + |11\rangle) + \beta W_2|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}}$$

$$|\psi''\rangle = \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$|\psi''\rangle = \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$|\psi''\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

- Alice measures her pair
  - If Alice measures

    $|00\rangle$
  - Then the state collapses and Bob has

    $\alpha|0\rangle + \beta|1\rangle$
  - Bob has

    $\chi = \alpha|0\rangle + \beta|1\rangle$

- Alice measures her pair
  - If Alice measures

    $|01\rangle$
  - Then the state collapses and Bob has

    $\alpha|1\rangle + \beta|0\rangle$
  - Bob has

    $\chi = \alpha U_{NOT}|1\rangle + \beta U_{NOT}|0\rangle = \alpha|0\rangle + \beta|1\rangle$

- Given the density matrix *p*, von Neumann defined the entropy as

$$S(p) = -Tr(p \ln p)$$

- It is a proper extension of the Gibbs entropy (and the Shannon entropy) to the quantum case
- We note that the entropy *S(p)* times the Boltzmann constant equals the thermodynamical or physical entropy

- If the system is finite (finite dimensional matrix representation) the entropy describes the departure of our system from a pure state
- In other words, it measures the degree of mixture of our state describing a given finite system

Conjugate pairs

- Another unexpected property of the nature:
- Physical variables come in „conjugate“ pairs
  - Position and momentum
  - Energy and time
- Both of which cannot be simultaneously measured with accuracy