Lecture Notes on Quantum Computing
WS 2000/01

Werner Kluge
Department of Computer Science
University of Kiel
D–24105 Kiel, Germany
email: wk@informatik.uni-kiel.de

May 7, 2001

Contents

1 Introduction **1**

1.1 Computers as physical systems 1
1.2 Technological issues 1
1.3 Capabilities of Quantum Computers 2

2 The basics of Quantum Mechanics **3**

2.1 a simple experiment 4
2.2 the same experiment with electrons 4
2.3 the electron experiment repeated 6
2.4 some fundamental conclusions 6
2.5 Dirac Notation of Probabilities 8
2.6 scattering colliding particles 10
2.7 The Stern-Gerlach Experiment 11
2.8 Base states of quantum systems 15
2.9 Quantum mechanical machinery 17
2.10 Transforming a state to a different base 18
2.11 Base transformations in spin 1/2 systems 18
2.12 some formal properties of probability amplitudes 24
2.13 Choosing suitable base states 26
2.14 State changes with time 26
2.15 An example: the ammonia molecule 27

3 Hilbert Spaces **29**

3.1 basic definitions 29
3.2 linear operators 30
3.3 projections 30
3.4 observables of quantum systems 31

4 Elements of quantum computing **32**

4.1 the quantum bit (qubit) 32
4.2 Two-bit quantum register 34
4.3 n-qubit quantum registers 37

5 Quantum Gates **40**

5.1 classical reversible logic gates 40
5.2 Quantum gates 41
5.3 Composition of gates 43
5.4 the role of measurement gates 47
5.5 Universal quantum gates 48
5.6 Quantum arithmetic 51

6 Quantum States and Ensembles **52**

6.1 The 2-qubit quantum system revisited 52
6.2 Bipartite quantum systems 57
6.3 Quantum entanglement 60

7 Quantum Algorithms **60**
7.1 On the accuracy of unitary operations 61
7.2 Reversible algorithmic computations 61
7.3 The Deutsch problem 62
7.4 The Deutsch–Josza problem 63
7.5 Simon's problem 64
7.6 Quantum Searching $\rightarrow$ Grover's search algorithm 65
7.7 Searching through distributed data bases 67
7.8 Finding periodicities in functions 68
7.9 Implementation of Q_{FFT} 69
7.10 Factoring 71
7.11 The RSA cryptosystem 72
7.12 Breaking the RSA cryptosystem 73
7.12.1 The period finding quantum algorithm 73
7.12.2 Some remarks on the performance of factorization 74

8 Overview of quantum computing devices **75**
8.1 Photon beam splitting devices 76
8.2 Quantum dots 77
8.2.1 Logic operations 78
8.2.2 Measuring the state of an atom 79
8.2.3 Effecting superpositions 79
8.3 Ion traps 80
8.4 The cavity QED 81
8.5 NMR quantum computing 82
8.6 The outlook 82

9 Quantum teleportation **82**
9.1 Teleporting one qubit 83
9.2 The teleporting circuitry 84

10 Quantum error correction **86**
10.1 Decoherence and dissipation 86
10.2 Stabilizing quantum computations 86
10.3 Error models 88
10.4 Quantum error correcting codes 88
10.5 The basics of error correction 89

11 Quantum automata and Turing machines **89**
11.1 Classical finite automata 89
11.2 One-way quantum automata 90
11.3 Two-way quantum finite automata (2QFA) 92
11.4 Outline of a 2QFA that accepts $L = \{0^i1^i \mid i \geq 0\}$ 94
11.5 Quantum Turing machines (QTM) 95

1 Introduction

1.1 Computers as physical systems

Current computer systems are, in one way or another, based on the concept of (computational) states and state transformations by fixed sets of rules.

states $\rightarrow$ are mathmatical abstractions of physical states (states of physical systems).

basic level $\rightarrow$ binary states

$\rightsquigarrow$ current on | off

$\rightsquigarrow$ voltage high | low

$\rightsquigarrow$ magnetization left | right (up | down)

$\rightsquigarrow$ electical charges present | absent

first level of abstraction $\rightarrow$ binary digit 0|1

second level of abstraction $\rightarrow$ code representation of elementary | atomic objects (numbers | characters | operators | address) as n-tuples of binary digits.

third level of abstraction $\rightarrow$ representation of complex | compound objects as compositions of elementary objects (compound operators | operands)

fourth level of abstraction $\rightarrow$ representation of algorithms as (partially) ordered structures of observators and operands

...

The physics of the underlying system has little | no influence on the higher levels of abstraction | on the particular model of computation, other than on

$\rightarrow$ speed of computation

$\rightarrow$ size of the problem at hand

$\rightarrow$ energy consumption

(tractability of the problem in time and space). Otherwise $\rightarrow$ all systems are fully Turing compatible $\rightsquigarrow$ may realize all intuitively computable functions. However, steady pace of miniaturization of computer components at the current rate (of a factor of 1/2 per 18 month) leads to the size of individual atoms by 2020 with the consequence that

$\rightsquigarrow$ the classical Turing model becomes invalid, instead

$\rightsquigarrow$ quantum mechanical effects take over $\rightsquigarrow$ lead to a new model of computation based on an algebra | a calculus that describes quantum mechanical processes

Quantum computers

$\rightsquigarrow$ are inherently reversible, i.e. they can run computations forward and backward

$\rightsquigarrow$ may perform certain computations (np-hard search problems) exponentially faster than classical computers

$\rightsquigarrow$ teleport messages by novel mechanisms based on the entanglement of quantum states

$\rightsquigarrow$ betray eavesdropping while communicating messages

$\rightsquigarrow$ break supposedly unbreakable code

$\rightsquigarrow$ but otherwise are fully Turing compatible

1.2 Technological issues

Space | time | energy implications of making computers faster and of larger (memory) capacities.

$\rightsquigarrow$ reducing signal propagation delays | increasing capacities demand shorter distances among components $\rightarrow$ higher packaging density

$\rightsquigarrow$ higher packaging densities and higher clock rates demand reduced heat dissipation of individual components $\rightsquigarrow$ more energy efficiency

$\rightsquigarrow$ smaller component sizes $\rightsquigarrow$ reducing the number of atoms | elementary particles per unit information (bit)

An example: current memory technology

- $\rightsquigarrow$ 256 MBit per chip of $2cm^2$ real estate of which 75% are storage cells | the rest is wiring and (decoder) logic, resulting in
- $\rightsquigarrow$ $C = 30 \cdot 10^{-15}$ Farad electrical capacity per cell (1 Farad = 1 As/V, 10^{-15}F = 1pF)
- $\rightsquigarrow$ the electrical charge per cell is $q = C \cdot U$, U=5V $\rightsquigarrow$ $q = 1.5 \cdot 10^{-13}$ As
- $\rightsquigarrow$ with $e = 1.6 \cdot 10^{-19}$ As as electrical charge of a single electron we get 10^5 electrons per cell
- $\rightsquigarrow$ a linear reduction of cell size by a factor of 1/2 per 18 month, we have a reduction in 20 years by $2^{-240/18} = 2^{-15} \approx 10^{-5}$, leading to
- $\rightsquigarrow$ one electron per cell in 2020

$\rightarrow$ quantum mechanical effects take over with some 10...100 electrons per cell

1.3 Capabilities of Quantum Computers

Mathmatical models of computing (which were developed before computers came into existence) include

- $\rightsquigarrow$ Turing machines (Turing)
- $\rightsquigarrow$ λ-calculus (Church)
- $\rightsquigarrow$ recursive Functions (Kleen)
- $\rightsquigarrow$ Goedel numbers (Goedel)
- $\rightarrow$ the notion of intuitive computable functions is based on the equivalence of these models
- $\rightarrow$ Church-Turing thesis: intuitively computable functions $\Leftrightarrow$ Turing computable functions

The idea of the Turing machine was developed in response to one of the 23 mathematical problems posed by Hilbert in 1900 which required solutions: $\rightarrow$ is there a mechanical procedure to decide about truth or falsity of a mathematical | logical conjecture. The machine was based on four principal ingrediences thought essential for mathmatical reasoning:

- $\rightsquigarrow$ a set of rules for transforming mathematical statements
- $\rightsquigarrow$ a method to record each transformation step
- $\rightsquigarrow$ the ability to go back and forth over the steps executed sofar
- $\rightsquigarrow$ a mechanism to decide which rule to apply next

The TM uses a very basic representation of symblos $\rightarrow$ 0 | 1

The deterministic Turingmachine (DTM)

- $\rightarrow$ applies to each constellation (state) a unique rule (of a finite set of rules) to produce exactly one successor constellation $\rightsquigarrow$ made up from the contents of the tape to the left and right of the head and the state of the head.

The probabilistic Turing Machine (PTM)

- $\rightarrow$ given some constellation, there may be multiple rules to get into different successor constellations, of which one is chosen with some probability.
- $\rightarrow$ it is proven that the PTM can compute exactly the same as a DTM, but with greater efficiency $\rightarrow$ it may arrive at a solution much faster on average.

The quantum Turing Machine (QTM)

- $\rightarrow$ the constellation (the state) of the machine is highly non-classical $\rightarrow$ it is a superposition (linear combination) of classical constellations $\rightsquigarrow$ the computation is realised as a continuously evolving quantum constellation which results in | terminates with a superposition of all reachable classical constellations (state). $\rightsquigarrow$ however, inspecting | measuring the superimposed constellation results in its collapse and in returning just one of the classical constellations reached $\rightsquigarrow$ the one with the highest probability.

→ the classical PTM follows only one path | trace of computation → with some probability
→ the QTM follows all possible paths | traces concurrently but, when doing a mesurement, returns the constellation reached along only one of the traces

Computability as defined by classical TM relates to the halting problem
→ does there exist a mechanical procedure by which it can be decided whether or not any given Turing machine acting on any given input halts | terminates (wich is equivalent to deciding whether or not the truth or falsity on conjectures can be decided → Enscheidungsproblem)
→ by proof of contradiction (assuming that such a TM can be constructed) it has been shown that such a TM does not exist → the problem is not computable. ⇝ the proof is based on the construction of a TM named S which, when appliced to itself, cannot terminate (halt) and cannot not terminate.

this relates to two theorems by Goedel on formal systems:
→ any sufficiently strong formal system L (say, a set of axioms) is incomplete if it is consistent → there are statements P such that neither P nor its negation ¬P can be proved by the rules of L. ⇝ since P and ¬P are contradictory, one of them must be true → there must be true statements about L that cannot be proved ⇝ truth and theoremhood are different concepts.
→ consistency of L cannot be proved in L itself → there must be deep-seated contradictions in L

Quantum computing is based on a formal (mathematical) system → describes | models physics | the behavior of nature
→ features contradictions | undecidable problems
⇝ one can make precise predictions about the state of a quantum system but they cannot be verified | validated by experiments | measurements
⇝ given precisely specified initial states, almost all questions relating to the long-term dynamical behavior are undecidable
→ are the consequences of a self-referential theory → tries to describe its own means of verification → not a consequence of quantum theory itself

Quantum computability
→ one can always construct a QTM wich simulates a classical DTM | PTM
⇝ operates on base quantum states
⇝ takes the same number of steps to run a program
⇝ the class of functions (!) that can be computed remains the same for both QTM and DTM
→ QTMs can generate truly random numbers ⇝ cannot be generated as values of functions
→ quantum parallelism → functions are evaluated on a superposition of all possible inputs at once → all function values are computed in the same time it takes to compute one value ⇝ only one of the values may be obtained as output | may be measured.

2 The basics of Quantum Mechanics

quantum mechanics
→ describes the behavior of matter and light at atomic scale
→ is completely different from what is known from classical physics
→ the behavior is not directly observable ⇝ protons | neutrons | electrons | photons behave like waves or like particles ⇝ they behave like neither or as particle waves
→ the behavior is in many ways mysterious, cannot be understood even by experienced physicists
→ the workings of the mystery cannot be explained, it can only be told as it is ⇝ one can only answer to the how but not to the why.

2.1 a simple experiment

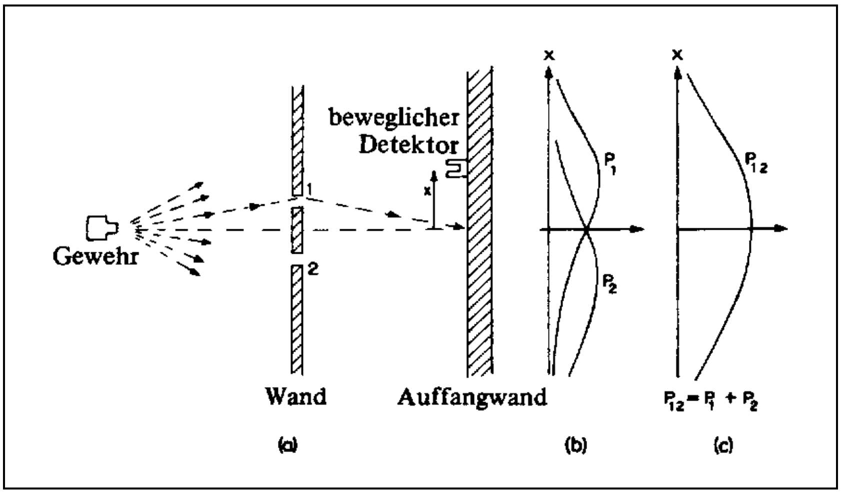


Figure 1: shooting tennisballs at 2 slits

→ shooting tabletennis balls at a wall with two wholes in it, and with a second wall behind it that has a detector moving up and down. the balls stray with a certain angulars spread at the source (the gun) and again at the wholes.
→ the probabilities of balls going through hole 1 while hole 2 is closed is P_1. (P_2 vice versa)
→ the probability of balls going through either hole and being detected at position z on the second wall is $P_{12} = P_1 + P_2$

2.2 the same experiment with electrons

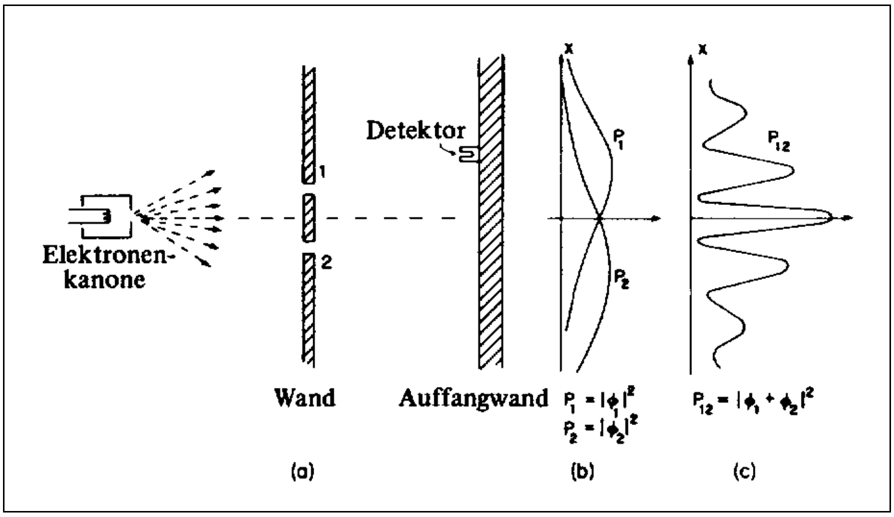


Figure 2: shooting electrons at 2 slits

→ the electron source emits electrons of the same momentum | same energy
→ the detector receives discrete clicks of the same intensity (energy) but ⇝ detects an interference pattern with the probability by which electrons arrive at the 2. wall along z.
→ proposition: electron goes either through hole 1 or hole 2; i.e. one should get $P_{12} = P_1 + P_2$ as the table tennis ball experiment

⇝ P_1 can be observed if only hole 1 is open
⇝ P_2 can be observed if only hole 2 is open

→ however, what seems to happen is $P_{12} \neq P_1 + P_2$ and P_{12} is a superposition of two wave functions of the general form

$$\phi = \phi_0 e^{j2\pi(\nu \cdot t + s/\lambda)}$$

with

$$\begin{aligned} \phi_0 &= \text{max. amplitude} \\ \nu &= \text{frequency of the wave} \\ \lambda &= \text{wave length} \\ t &= \text{time} \\ s &= \text{position in space} \end{aligned}$$

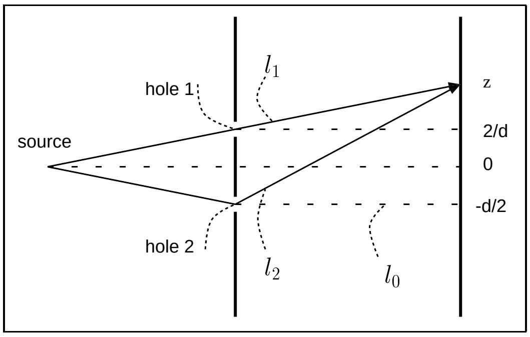


Figure 3: the interesting part of the geometry of the experiment

wave functions at z for
⇝ hole 1 : $\phi_1 = u_1 \cdot e^{j2\pi\nu t} \cdot e^{j2\pi l_1/\lambda}$
⇝ hole 2 : $\phi_2 = u_2 \cdot e^{j2\pi\nu t} \cdot e^{j2\pi l_2/\lambda}$

superposition yields:

$$\phi_1 + \phi_2 = e^{j2\pi\nu t}(u_1 \cdot e^{j2\pi l_1/\lambda} + u_2 \cdot e^{j2\pi l_2/\lambda})$$

with $z \ll l_0$ and $d \ll l_0$ one can approximate

$$\begin{aligned} l_1 &= l_0 - 1/2 \cdot d \cdot z/l_0 \\ l_2 &= l_0 + 1/2 \cdot d \cdot z/l_0 \end{aligned}$$

yielding

$$\phi = \phi_1 + \phi_2 = e^{j2\pi(\nu t + l_0/\lambda)} \cdot (u_1 \cdot e^{-j\pi \cdot dz/l_0} + u_2 \cdot e^{j\pi \cdot dz/l_0})$$

The intensity at z is given as

$$\begin{aligned} |\phi|^2 &= |\phi_1 + \phi_2|^2 \\ &= u_1^2 + u_2^2 + u_1 u_2 (e^{-j2\pi dz/l_0} + e^{j2\pi dz/l_0}) \\ &= u_1^2 + u_2^2 + 2u_1 u_2 \cdot cos\varphi \end{aligned}$$

with $\varphi = 2\pi dz/l_0$ the phase shift between the two waves traveling along l_1 and l_2

→ the electrons thus behave like waves and particles
⇝ they are particlewaves
⇝ the electrons arrive at the second wall as particles but their probability distribution is by wave interference

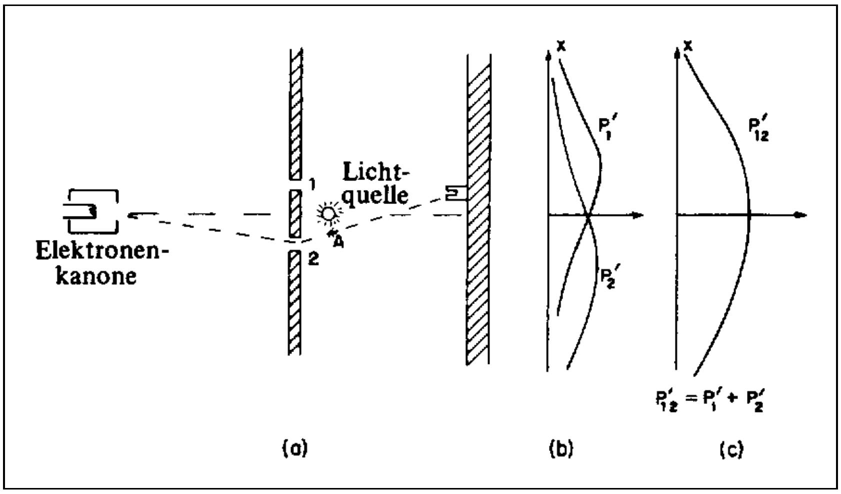


Figure 4: shooting electrons at 2 slits with light source behind

2.3 the electron experiment repeated

→ with a light source behind the first wall to detect which hole the electrons go through

⇝ flashes near hole 1 | 2 indicates that the electron went through hole 1 | 2

⇝ electrons are going with probability P_1 | P_2 through hole 1 | 2

⇝ the interference at the second wall disappears if there is a measurement (the light source) we find out where the electrons are actually going through; again we have $P_{12} = P_1 + P_2$

⇝ the measurement influences the system

⇝ there is some jolt | momentum given to the electrons by the photons of the light source

⇝ the jolt is $p = 1/\lambda$ ⇝ inversley proportional to wave length

⇝ if the frequency of the light is lowered | the wavelength λ increases,the jolt on the electrons is getting weaker ⇝ with the wavelength approaching the distance d of the slits,each electron produces a flash and one cannot anymore distinguish where it went through ⇝ the interference pattern reappears

⇝ if the light intensity is lowered, fewer electrons get hit by photons ⇝ the interference reappears too

⇝ these observations give rise to the uncertaincy principle of quantum mechanics

  → there is no way of designing an aparatus to detect which way an electron went through two separate holes without disturbing the electrons with the effect of destroying interference

  → this is a fundamental principle of quantum mechanics

2.4 some fundamental conclusions

consequences

→ it cannot exactly be determined in quantum mechanics what one particle is doing | in which state it is

→ quantum mechanics always works with

  ⇝ probability amplitudes ϕ

  ⇝ probabilities $|\phi|^2$

of events taking place | particles being in certain states

→ probability amplitudes for two or more events | states add up as

$$\phi = \phi_1 + \phi_2 + \ldots + \phi_n$$

and for probabilities holds

$$P = |\phi|^2 = |\phi_1 + \phi_2 + \ldots + \phi_n|^2$$

$\rightsquigarrow$ there is interference, if the events | states are indistinguishable !!!

$\rightarrow$ if experiments are being conducted | observations are being made to find out which of two or several alternatives are taken $\rightsquigarrow$ interference is lost and probabilities add up

$$P = P_1 + P_2 + \ldots + P_n$$

It is generally accepted in qm to be impossible to talk about anything but probability (amplitudes)

$\rightsquigarrow$ the odds of what might be happening | not what is actually going to happen

$\rightsquigarrow$ this is how nature behaves at the level of atoms

$\rightsquigarrow$ there are no natural mechnisms which we don't know anything of

$\rightarrow$ Heisenberg's uncertancy principle

$$\Delta p \cdot \Delta q = h = 6.63 \cdot 10^{-34} Js$$

$$\begin{aligned} \Delta p &\rightarrow \text{ variation in momentum} \\ \Delta q &\rightarrow \text{ variation in location} \end{aligned}$$

$\rightarrow$ the probability amplitude of finding a particle in a particular place at a particular time is in some special cases given as

$$\phi = \phi_0 e^{j(\omega t + \vec{k} \cdot \vec{r})}$$

$$\begin{aligned} \vec{k} = 2\pi/\lambda &\rightarrow \text{ wave number} \\ \vec{r} &\rightarrow \text{ location in space} \\ \omega = 2\pi\nu &\rightarrow \text{ periodic frequency} \end{aligned}$$

classical theory of particles has

$$\begin{aligned} E = \hbar \cdot \omega &\rightarrow \text{ (the energy)} \\ \vec{p} = \hbar \cdot \vec{k} &\rightarrow \text{ (the momentum)} \end{aligned}$$

$\rightsquigarrow$ if $|\phi|^2 = const$ than the probability of finding a particle in some place $\vec{r}$ is the same for all $\vec{r}$ $\rightsquigarrow$ it is completely unknown where it is.

$\rightsquigarrow$ if the position is fairly well known, then the probability of finding it in some place $\vec{r}$ is confined to some interval $\Delta\vec{r}$, outside of which the probability is zero, hence we have a waveform

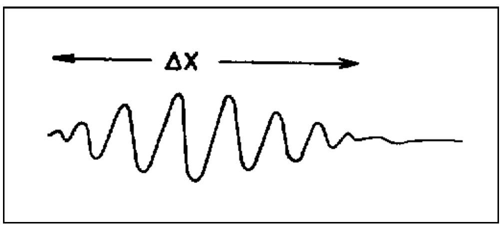


Figure 5: waveform

$\rightsquigarrow$ no unique frequency but a continuos spectrum of wavelength $\rightsquigarrow$ there is some variation Δp in the momentum | in the energy

example: for the application of the uncertainty relation $\rightarrow$ computing the size of an atom in a classical sense

$\rightsquigarrow$ an electron spiraling around a nucleus would zero in on the nucleus

$\rightarrow$ lose energy by reaction

$\rightarrow$ eventually fall into the nucleus

$\rightsquigarrow$ both location and momentum are wellknown

However: suppose the electron is some distance r away from the nucleus, the spread in distance is Δr, then we have $\Delta p = h/\Delta r$ as spread in momentum. The kinetic energy then is

$$E_{kin} = \frac{mv^2}{2} = \frac{\Delta p^2}{2m} = \frac{h^2}{2m\Delta r^2}$$

the potential energy is

$$E_{pot} = \frac{-e^2}{\Delta r}$$

and the total energy is

$$E = E_{kin} + E_{pot} = \frac{h^2}{2m\Delta r^2} - \frac{e^2}{\Delta r}$$

Minimizing E over Δr yields

$$\begin{aligned}
&\frac{dE}{d(\Delta r)} = \frac{-h^2}{m\Delta r^3} + \frac{e^2}{\Delta r^2} = 0 \\
&\hookrightarrow \Delta r = \frac{h^2}{me^2} \\
&\hookrightarrow \Delta r = 0.528 \cdot 10^{-18} m \quad (Bohr\ radius)
\end{aligned}$$

with this radius the potential energy computes as

$$E_0 = \frac{-e^2}{2\Delta r} = \frac{-e^4 \cdot m}{2h^2} = -13.6eV$$

(this is a very rough estimate which is however pretty accurate)

$\rightarrow$ energy levels of an atom

$$\begin{aligned}
\hbar \cdot \omega_{30} &= E_3 - E_0 \\
\hbar \cdot \omega_{32} &= E_3 - E_2 \\
\hbar \cdot \omega_{20} &= E_2 - E_0 \\
&\hookrightarrow \omega_{30} = \omega_{32} + \omega_{20}
\end{aligned}$$

2.5 Dirac Notation of Probabilities

example: the electron diffraction experiment

$< d|s > \equiv$ the probability amplitude for a particle departing from source s to arrive at detector (the destination) d $\rightsquigarrow$ it is a complex number (for technical reasons)

$< d|s >_p \equiv$ probability for electron going through hole p

$< d|s >_q \equiv$ probability for electron going through hole q

$$\begin{aligned}
< d|s >_p &= < d|p >< p|s > \\
< d|s >_q &= < d|q >< q|s >
\end{aligned}$$

(product of probability amplitudes) $\rightsquigarrow$ assuming that all electrons arriving at a hole also make it through

$$< d|s > = < d|s >_p + < d|s >_q$$

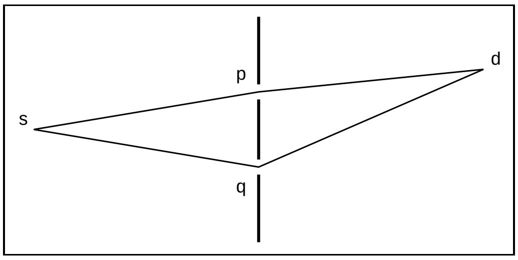


Figure 6: electron diffraction experiment

example: a more complicated apparatus here we have:

$$\begin{aligned} < d|s > &= < d|a >< a|p > < p|s > \\ &+ < d|b > < b|p > < p|s > \\ &+ < d|a >< a|q > < q|s > \\ &+ < d|b > < b|q > < q|s > \end{aligned}$$

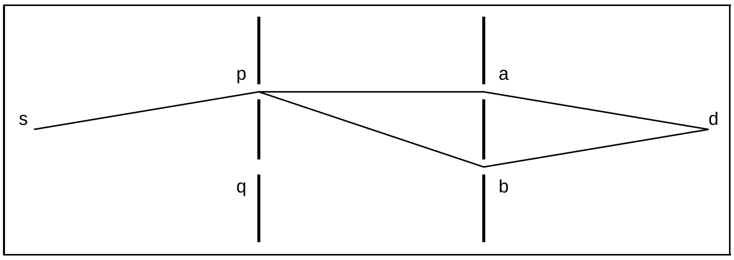


Figure 7: another electron diffraction experiment

example: the two-slit experiment with light source to detect where an electron went trough let (with the light l turned off):

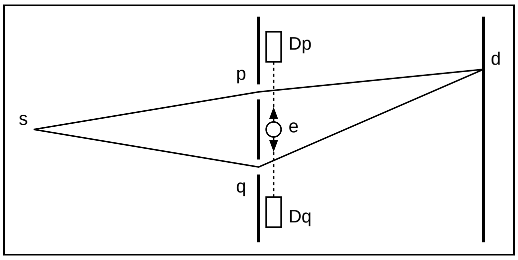


Figure 8: two-slit experiment

$$\begin{aligned} \phi_p &=< d|p >< p|s > \\ \phi_q &=< d|q >< q|s > \end{aligned}$$

amplitude of an electron passing through p | q <u>and</u> having scattered a photon into direction Dp | Dq (with light l turned on):

$$\begin{aligned} &< d|p > r_p < p|s > \\ &< d|q > r_q < q|s > \end{aligned}$$

$r_p \mid r_q$ are scattering amplitudes, $r_{pq} \mid r_{qp}$ amplitudes of a photon being scattered to Dp | Dq from electron passing through q | p

$$< d|p > r_{pq} < p|s >$$
$$< d|q > r_{qp} < q|s >$$

We thus get:

$$\left\langle \begin{array}{c} \text{electron at } d \\ \text{photon at } Dp \end{array} \middle| \begin{array}{c} \text{electron from } s \\ \text{photon from } l \end{array} \right\rangle = r_p\phi_p + r_{pq}\phi_q$$
$$\left\langle \begin{array}{c} \text{electron at } d \\ \text{photon at } Dq \end{array} \middle| \begin{array}{c} \text{electron from } s \\ \text{photon from } l \end{array} \right\rangle = r_q\phi_q + r_{qp}\phi_p$$

→ if an electron has been detected by either Dp or Dq, the route taken is determined ⇝ the electrons can be distinguished by their routes ⇝ distinguishable states ⇝ the posibilities for both alternatives are completely independent of each other ⇝ there is no interference ⇝ one must add posibilities, not amplitudes:

$$\left|\left\langle \begin{array}{c} \text{electron at } d \\ \text{photon at } Dp \end{array} \middle| \begin{array}{c} \text{electron from } s \\ \text{photon from } l \end{array} \right\rangle\right|^2 + \left|\left\langle \begin{array}{c} \text{electron at } d \\ \text{photon at } Dq \end{array} \middle| \begin{array}{c} \text{electron from } s \\ \text{photon from } l \end{array} \right\rangle\right|^2$$
$$= |r_p\phi_p + r_{pq}\phi_q|^2 + |r_q\phi_q + r_{qp}\phi_p|^2$$

→ whenever the events | states are distinguishable, one adds probabilities
→ whenever the events | states are inditinguishable, one adds amplitudes

2.6 scattering colliding particles

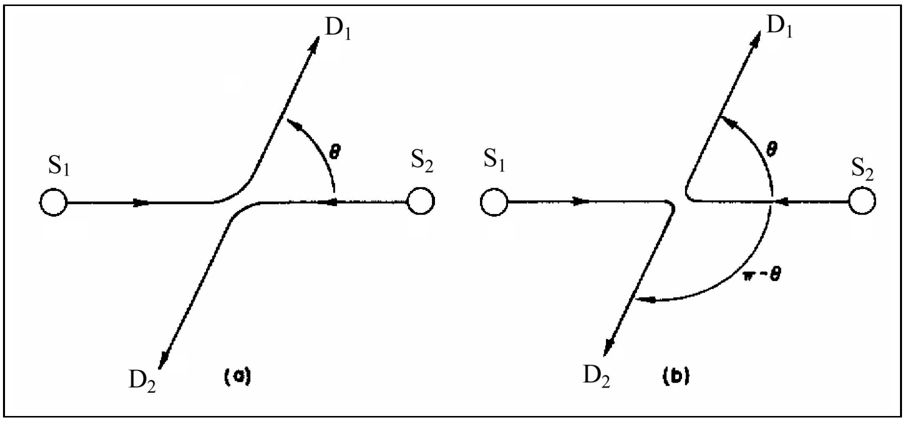


Figure 9: colliding particles

distinguishable particles emanating from s_1 and s_2 are deflected | scattered at angle θ into D_1, at angle $(\pi - \theta)$ into D_2

→ probability of particles ending up in D_1 is:

$$P_1 = | < D_1|s_1 > |^2 + | < D_1|s_2 > |^2 = |f(\theta)|^2 + |f(\pi - \theta)|^2$$

($f(\theta)$ is a function determining the number of particles going off at angle θ)

undistinguishable particle (α-particles with no spin) $\rightsquigarrow$ it cannot be detected whether a particle ending up in D_1 comes from s_1 or s_2, the probability of particles ending up in D_1 is:

$$P_1 = | < D_1|s_1 > + < D_1|s_2 > |^2 = |f(\theta) + f(\pi - \theta)|^2$$

→ with $\theta = \frac{\pi}{2}$, we have
  - $\rightsquigarrow$ for the distinguishable case: $P_1 = 2|f(\frac{\pi}{2})|^2$
  - $\rightsquigarrow$ for the indistinguishable case: $P_1 = |2f(\frac{\pi}{2})|^2 = 4|f(\frac{\pi}{2})|^2$

same experiment with electrons

→ indistinguishable electrons interfere with negative sign $\rightsquigarrow$ probability of an electron arriving from source s_1 or s_2 at detector D_1:

$$P_1 = | < D_1|s_1 > - < D_1|s_2 > |^2 = |f(\theta) - f(\pi - \theta)|^2 \qquad (*)$$

taking electron spins into consideration

→ if both spins are up or both spins are down, then the particles are indistinguishable $\rightsquigarrow$ there is interference as in (*)

→ if one of the spins is up (say from s_1) and the other is down (say from s_2) then at D_1 | D_2 it can be decided | distinguished where they came from $\rightsquigarrow$ the probabilities are

$$|f(\theta)|^2 \text{ or } |f(\pi - \theta)|^2$$

thus we have the following spin combinations:

$$\left.\begin{array}{lcl} \uparrow\uparrow & \rightarrow & \uparrow\uparrow \\ \downarrow\downarrow & \rightarrow & \downarrow\downarrow \end{array}\right\} \ \tfrac{1}{2} \text{ of all cases}$$
$$\begin{array}{lcll} \uparrow\downarrow & \rightarrow & \uparrow\downarrow \text{ or } \downarrow\uparrow \ \} & \tfrac{1}{4} \text{ of all cases} \\ \downarrow\uparrow & \rightarrow & \uparrow\downarrow \text{ or } \downarrow\uparrow \ \} & \tfrac{1}{4} \text{ of all cases} \end{array}$$

$\rightsquigarrow$ the total probability is therefore:

$$\frac{1}{2}|f(\theta) - f(\pi - \theta)|^2 + \frac{1}{2}|f(\theta)|^2 + \frac{1}{2}|f(\pi - \theta)|^2$$

2.7 The Stern-Gerlach Experiment

is based on the phenomenon that particles may have an angular momentum (a spin) that is quantized. This phenomenon can be used as the basis for describing all quantum mechanical behavior.

the Stern-Gerlach apparatus

→ splits a stream of particles with the spins up | down | no-spin into three different beams

→ the splitting is acomplished by the stream running through an inhomogeneous magnetic field perpendicular to the direction of the incoming beam which exercites magnetic force on the magnetic dipols | fields associated with the spins

→ the particles in the outgoing beams may be detected by appropriate devices
  - $\rightsquigarrow$ the spins within the beams are given by the angles at which the beams leave the apparatus
  - $\rightsquigarrow$ each beam contains particles of a specific spin only

→ the angle of the deflected beams is determinated by
  - $\rightsquigarrow$ the strength of the magnetic field
  - $\rightsquigarrow$ the length of the path through the field

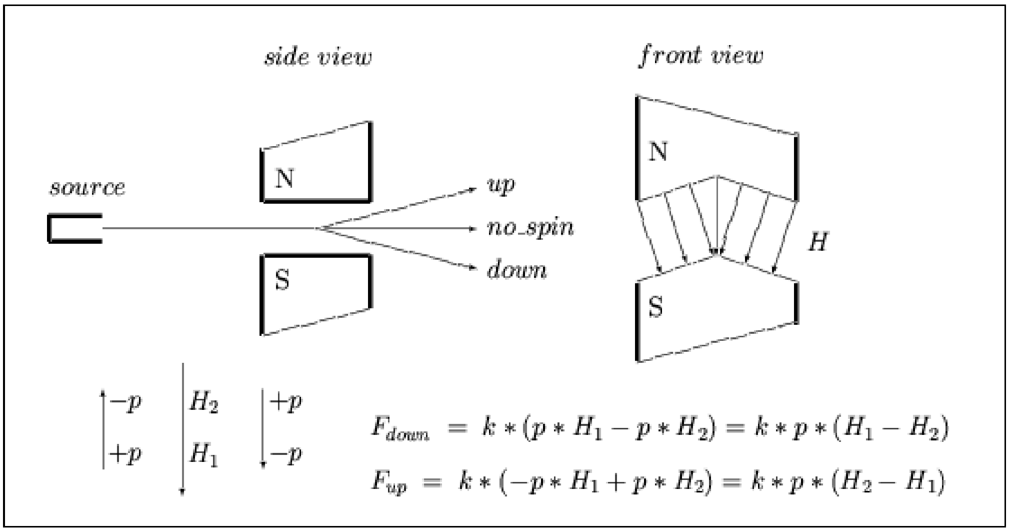


Figure 10: Stern-Gerlach apparatus

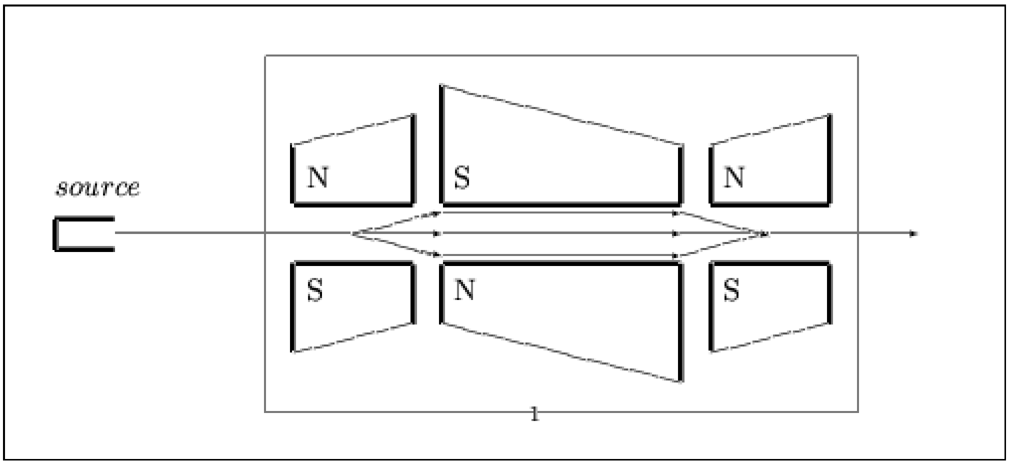


Figure 11: modified Stern-Gerlach apparatus

A thought experiment with a modified Stern-Gerlach apparatus

→ the beam passes through

  ⇝ a beam splitting downwards directed magnetic field of unit length, followed by

  ⇝ a beam-merging upwards directed magnetic field of twice the unit length followed by

  ⇝ a beam-joining downwards directed magnetic field of unit length which deflects the beams that come in at an angle into the horizontal direction

→ thus the beam is split up inside the apparatus but comes out again with all spin directions mixed, but

→ inside the apparatus one or two beams may be filtered out so that the outgoing beam contains particles of just two or one spins, respectively.

+ → up-spin | 0 → no-spin | - → down-spin | S → name of the apparatus ⇝ the magnetic fields of the apparatus are assumed to point downwards and upwards exactly in the plane of the paper sheet

symbolic representation | notation is

$$\underset{S}{\begin{bmatrix} + \\ 0 \\ - \end{bmatrix}}$$

(will be used to describe phenomina of this apparatus, no quantum mechanical notation)

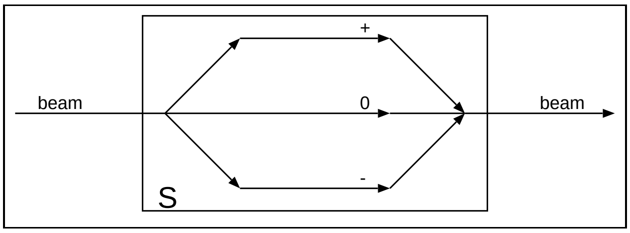


Figure 12: schematic representation of the modified Stern-Gerlach apparatus

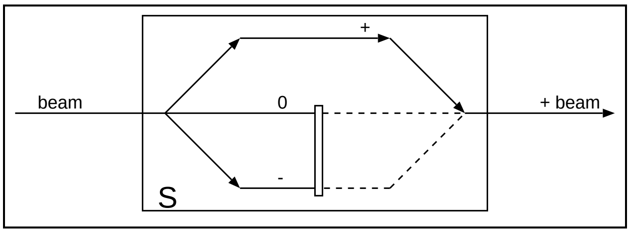


Figure 13: filtering spin directions out of the beam

→ the outgoing beam contains only particles with spin-up (+)
symbolic representation:

$$\left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S, \text{ other filters: } \left[\begin{smallmatrix} + & | \\ 0 & \\ - & | \end{smallmatrix}\right]_S, \left[\begin{smallmatrix} + & | \\ 0 & | \\ - & \end{smallmatrix}\right]_S$$

constructions of two Stern-Gerlach (SG) apparatuses with the same orientation (of magnetic field)

$$\left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S \left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S \Longleftrightarrow \left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]$$

$$\left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S \left[\begin{smallmatrix} + & | \\ 0 & | \\ - & \end{smallmatrix}\right]_{S'} \Longleftrightarrow \left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]$$

Shorthand notation for SG's with two beams blocked → a filter device

$$\left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right] \equiv \begin{smallmatrix} <+S| \\ |+S> \end{smallmatrix}, \left[\begin{smallmatrix} + & | \\ 0 & \\ - & | \end{smallmatrix}\right] \equiv \begin{smallmatrix} <0S| \\ |0S> \end{smallmatrix}, \left[\begin{smallmatrix} + & | \\ 0 & | \\ - & \end{smallmatrix}\right] \equiv \begin{smallmatrix} <-S| \\ |-S> \end{smallmatrix}$$

With $< b|a >$ meaning → a particle leaving a first SG in state a leaves a second GS in state b with the probability amplitude thus given
→ we have $< +S| + S >= 1$ | $< -S| - S >= 1$ | $< 0S|0S >= 1$,
but e.g. $< -S| + S >= 0$ | $< +S| - S >= 0$ | $\cdots$, or
→ in matix form:

	$+S$	$0S$	$-S$
$+S$	1	0	0
$0S$	0	1	0
$-S$	0	0	1

Combination of two SG apparatuses which have their magnetic fields oriented at an angle $\alpha \neq 0$ relate to each other, e.g.:

$$\left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S \left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_T \qquad \left[\begin{smallmatrix} + & \\ 0 & | \\ - & | \end{smallmatrix}\right]_S \left[\begin{smallmatrix} + & | \\ 0 & \\ - & | \end{smallmatrix}\right]_T$$

→ the state $|iS >$ is not the same as $|iT >$ for $i \in \{+, 0, -\}$

→ instead we have probability amplitudes

$$< iT|jS > \neq 0 \quad i,j \in \{+,0,-\}$$

and probabilities

$$< iT|jS >< iT|jS >^* = | < iT|jS > |^2$$

→ it is the probability that a particle in state $|jS >$ will also be in state $< iT|$

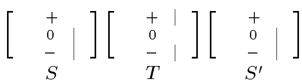
→ it also holds that

$$\begin{aligned} & < -T|jS >< -T|jS >^* \\ + & < +T|jS >< +T|jS >^* \\ + & < 0T|jS >< 0T|jS >^* \\ = & \sum_{i \in \{+,0,-\}} < iT|jS >< iT|jS >^* = 1 \end{aligned}$$

⇝ a particle being in state $|jS >$ must be in any of the states $< iT|$

experiment with three SG-filters

→ S and S' are oriented the same; T is at an angle $\alpha \neq 0$ oriented vs. S, S'



→ problem: do all particles that are coming from S and passing through T also pass through S' ?

→ the answer ⇝ no

⇝ particles filtered by T do not remember that they have been filtered by S ⇝ a quantum mechanical effect ⇝ (remember the mirror experiment)

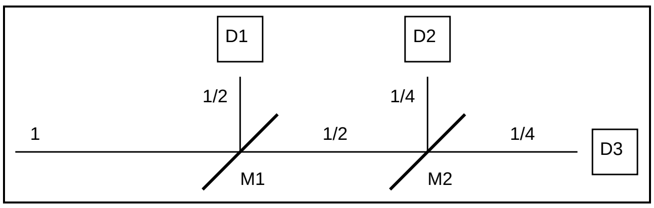


Figure 14: mirror experiment

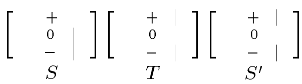
→ the probability amplitudes of a particle passing through all three SG filters is

$$< +S'|0T >< 0T| + S >$$

and the probability is

$$| < +S'|0T > |^2 | < 0T| + S > |^2$$

→ changing the experiment to $|0S' >$ as the last filter:



⇝ the probability of a particle getting through is $| < 0S'|0T > |^2 | < 0T| + S > |^2$

→ the probability ratio between both SG experiments is

$$\frac{| < +S'|0T > |^2}{| < 0S'|0T > |^2}$$

⇝ this ratio depends only on what is happening between T and S' ⇝ it is not sensitive against the previous history

2.8 Base states of quantum systems

$\rightsquigarrow$ come about due to a filtering process which cleanly separates particles into distinguishable sets
$\rightsquigarrow$ depend on the filter used
$\rightsquigarrow$ are, for instance $< +S|$,$< 0S|$,$< -S|$ or $< +T|$,$< 0T|$,$< -T|$ or any other convenient combination
$\rightarrow$ pure states $\rightsquigarrow$ are base states that can not be split up further by filters of the same kind
  $\rightsquigarrow$ particles in a pure state $| + T >$ will all pass through a filter $\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]$ but none will pass through a filter that blocks $| + T >$

Going from a base state w.r.t. one filter to a base state w.r.t. another filter

$$\underset{S}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \quad \underset{T}{\left[\begin{array}{cc} + & | \\ 0 & \\ - & | \end{array}\right]}$$

$\rightarrow$ the particles coming out of $|0T >$ have no knowledge that they came out of a state $| + S >$
$\rightarrow$ the information about preceding filters is not lost by separation into three beams (by filter S) but by the blocks that have been put into the filters
  $\rightsquigarrow$ verification by another thought experiment, S and S' are oriented the same, T is at a different angle:

$$\underset{S}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[N]{} \underset{T}{\left[\begin{array}{cc} + & | \\ 0 & \\ - & | \end{array}\right]} \xrightarrow[\alpha N]{} \underset{S'}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[\beta\alpha N]{}$$

$N \equiv$ number of particles coming out of $| + S >$
$\alpha N \equiv$ fraction of particles coming out of $|0T >$
$\beta\alpha N \equiv$ fraction of particles coming out of $| + S' >$
$\alpha = | < 0T| + S > |^2$, $\beta = | < +S'|0T > |^2$

  $\rightsquigarrow$ slightly modified experiment:

$$\underset{S}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[N]{} \underset{T}{\left[\begin{array}{cc} + & | \\ 0 & \\ - & | \end{array}\right]} \xrightarrow[\alpha N]{} \underset{S'}{\left[\begin{array}{cc} + & | \\ 0 & \\ - & | \end{array}\right]} \xrightarrow[\gamma\alpha N]{}$$

If both the previous experiments are changed so that T lets pass all particles (that are in any of the pure states), then we get
$\rightsquigarrow$ case A:

$$\underset{S}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[N]{} \underset{T}{\left[\begin{array}{c} + \\ 0 \\ - \end{array}\right]} \xrightarrow[N]{} \underset{S'}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[N]{}$$

$\rightsquigarrow$ all particles passing through T (the ones that come from S') also pass through S' $\rightsquigarrow$ the 'filter' T has no effect
$\rightsquigarrow$ case B:

$$\underset{S}{\left[\begin{array}{cc} + & \\ 0 & | \\ - & | \end{array}\right]} \xrightarrow[N]{} \underset{T}{\left[\begin{array}{c} + \\ 0 \\ - \end{array}\right]} \xrightarrow[N]{} \underset{S'}{\left[\begin{array}{cc} + & | \\ 0 & \\ - & | \end{array}\right]} \xrightarrow[0]{}$$

$\rightsquigarrow$ none of the particles passing through T passes through S'
$\rightsquigarrow$ the mystery is that T has open more channels than in the previouse example but nevertheless fewer (none) particles make it through
$\rightsquigarrow$ this is a purely quantum mechanical effect
$\rightsquigarrow$ it is the blocking in S', not the splitting of beams, that makes the difference
$\rightsquigarrow$ passing all or no particles in these experiments has to do with the interference of probability amplitudes $\rightsquigarrow$ resulting from indistinguishable particles

- $\rightsquigarrow$ thus we get
  - $\rightsquigarrow$ in case A:

$$\sum_{i\in\{+,0,-\}} <+S|iT><iT|+S>=1$$

or simply

$$\sum_{i\in\{+,0,-\}} <+S|i><i|+S>=1$$

  - $\rightsquigarrow$ in case B:

$$\sum_{i\in\{+,0,-\}} <0S|iT><iT|+S>=0$$

or simply

$$\sum_{i\in\{+,0,-\}} <0S|i><i|+S>=0$$

A similar law holds when replacing S' by an arbitrary filter R; than we have

$$\left[\ \underset{S}{\begin{smallmatrix}+\\0\\-\end{smallmatrix}}\ |\ \right]\left[\ \underset{T}{\begin{smallmatrix}+\\0\\-\end{smallmatrix}}\ \right]\left[\ \underset{R}{\begin{smallmatrix}+\\0\\-\end{smallmatrix}}\ |\ \right]$$

or

$$\sum_{i\in\{+,0,-\}} <+R|iT><iT|+S>=\sum_{i\in\{+,0,-\}} <+R|i><i|+S>=<+R|+S>$$

- $\rightsquigarrow$ the filter T is in fact not there as i enumerates all the base states of that filter | it lets all the base states pass

Generalization without reference to a particular base of S and R

- $\rightarrow$ let ϕ an ψ be states selected by the filters S and R, respectively, then we have

$$<\psi|\phi>=\sum_i <\psi|i><i|\phi> \qquad (*)$$

where i ranges over the base states of some particular filter
  - $\rightsquigarrow$ the above equation is invariant against the choice of the base states | the filter
  - $\rightsquigarrow$ the base states are orthogonal to each other, meaning that $\rightsquigarrow$ a particle in base state $|iS>$ cannot be in any of the base states $|jS>$ with $i \neq j$
- $\rightarrow$ if i and j denote base states (of any representation), then we have

$$\begin{aligned} <i|j> &= 0 \text{ if } i \neq j \\ <i|j> &= 1 \text{ if } i = j \\ or <i|j> &= \delta_{ij} \end{aligned} \qquad (**)$$

$$\text{the Kronecker symbol: } \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

If i,j refer to the same set of base states and assuming that in equation (*) we have $\phi = i$, we get

$$<\psi|i>=\sum_j <\psi|j><j|i>$$

- $\rightarrow$ since $<j|i>=\delta_{ji}$, and we thus get $<\psi|i>=<\psi|i>$ (identity), the laws (*) and (**) are not independent of each other.

Besides we have

- $\rightarrow$ $\sum_{i\in\{+,0,-\}} <iT|+S><iT|+S>^*=1$

$\rightsquigarrow$ a particle in state $|+S>$ must be with probability 1 in one of the states $|iT>$

$\rightarrow$ $\sum_{i\in\{+,0,-\}} <+S|iT><iT|+S>=1$

$\rightarrow$ These two equations are consistent only if $<+S|iT>=<iT|+S>^*$ for each $i \in \{+,0,-\}$

$\rightsquigarrow$ for any states $\psi \mid \phi$ follows

$$<\phi|\psi>=<\psi|\phi>^*$$

$\rightsquigarrow$ if this would not hold, probabilities wouldn't be preserved $\rightsquigarrow$ particles would be lost

$\rightarrow$ several laws about amplitudes:

1. $<\psi|\phi>=\sum_i <\psi|i><i|\phi>$
2. $<i,j>=\delta_{ij}$
3. $<\psi|\phi>=<\phi|\psi>^*$

2.9 Quantum mechanical machinery

the problem: given some quantum mechanical apparatus $\rightsquigarrow$ any configuration of SG filters $\rightsquigarrow$ what are the odds of some particle in state ϕ of going through an apparatus A and coming out in state ψ ?

example

$$\underset{S}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\ \big|\right]}\left[\ {\scriptstyle A}\ \right]\underset{R}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\ \big|\right]}$$

the notation for the probability amplitude: $<0R|A|+S>$
and the probability amplitude for the general case: $<\psi|A|\phi>$
extending the apparatus as

$$\underset{S}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\ \big|\right]}\underset{T}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\right]}\left[\ {\scriptstyle A}\ \right]\underset{T}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\right]}\underset{R}{\left[\begin{smallmatrix}+\\0\\-\end{smallmatrix}\ \big|\right]}$$

yields the amplitude

$$\sum_{ij} <0R|j><j|A|i><i|+S>$$

or, if $<0R|$ and $|+S>$ are replaced by ψ and ϕ, respectively

$$\sum_{ij} <\psi|j><j|A|i><i|\phi>$$

$\rightarrow$ with

$\rightsquigarrow$ $<i|\phi>$ being the amplitude of each base state i for the particle to be in state ϕ

$\rightsquigarrow$ $<\psi|i>$ being the amplitude of each base state to have a component ψ

$\rightarrow$ it follows that the apparatus A is completely defined by a matrix which describes what A is doing to the base states

$\rightsquigarrow$ A describes the changes of amplitudes in the base states when going from one state to another

$\rightarrow$ if the apparatus is constructed as $[C]=[A][B]$ then the matrix $<j|C|i>$ is the product of the matrices A and B

$\rightsquigarrow$ $<\chi|C|\phi>=\sum_k <\chi|B|k><k|A|\phi>$

$\rightsquigarrow$ $<i|C|j>=\sum_k <i|B|k><k|A|j>$

2.10 Transforming a state to a different base

Let $< iS|\phi >$ be the amplitude component of ϕ in base state $|iS >$, $< jT|\phi >$ be the amplitude component of ϕ in base state $|jT >$, then we can use formula (*) as

$$< jT|\phi >= \sum_i < jT|iS >< iS|\phi >$$

to relate the representation of ϕ in $|iS >$ to the representation in $|jT >$. $< jT|iS >$ is the transformation matrix.
With $C'_j =< jT|\phi >$, $C_i =< iS|\phi >$ and $R_{ji} =< jT|iS >$ transformation to a different base may be written as

$$C'_j = \sum_i R_{ji} C_i$$

$\rightsquigarrow$ which is similar to transforming vectors from one base to another
$\rightsquigarrow$ the coefficients of the matrix R_{ji} can be found by plain reasoning based on a few assumptions

2.11 Base transformations in spin 1/2 systems

→ are somewhat easier to deal with than spin 1 systems when trying to determine the coefficients R_{ji} of the transformation matrices
→ relate directly to the state transformations that quantum computing works with | is based upon.

In a spin 1/2 system the particles (e.g. electrons) can only be in one of two states
$\rightsquigarrow$ spin up (↑) | spin down (↓)
$\rightsquigarrow$ an SG apparatus splits a beam of such particles up into two beans, of which one may be filtered out

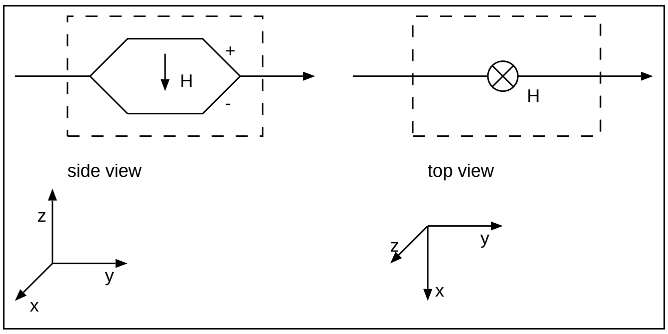


Figure 15: SG apparatus with spin 1/2 particles

$\rightsquigarrow$ a transformation matrix R_{ji} describing state transformations from one SG filter to another is a 2×2 matix

rotation about some axis Putting two SG filters with the field vector H oriented in the zy plane at an angle α after each other

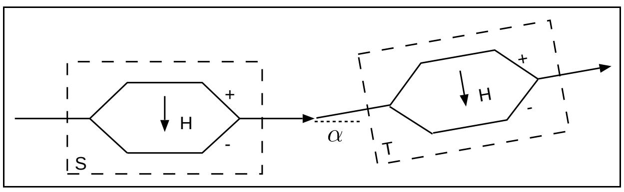


Figure 16: 3 GS apparatuses about x-axis

→ the questions to be raised w.r.t. this experiment are what are the probability amplitudes for particles

- ⇝ leaving apparatus S in state ↑ and passing through apparatus T in, say state ↓
- ⇝ and likewise for all other combinations of S and T states i.e. ⇝ what are the probability amplides $<\uparrow T|\uparrow S>$ | $<\downarrow T|\downarrow S>$ | $<\uparrow T|\downarrow S>$ |$<\downarrow T|\uparrow S>$?
- ⇝ the probability amplitudes are given by the matrix R_{ji} in equation

$$C'_j = \sum_{i\in\{\uparrow,\downarrow\}} R^{TS}_{ji} C_i$$

with $C'_j =< jT|\phi >$, $C_i =< iS|\phi >$

→ adding a third SG apparatus U yields:

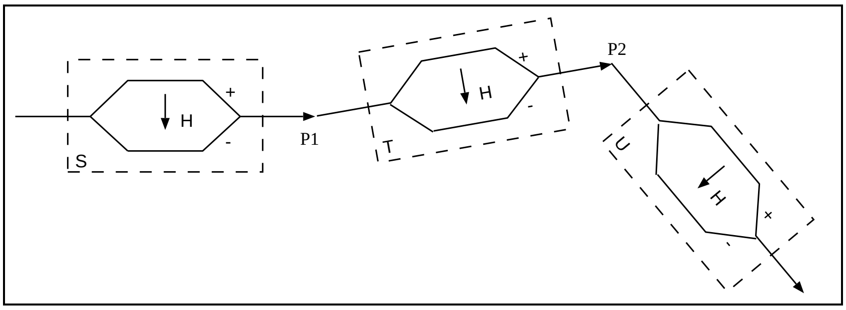


Figure 17: 3 GS apparatuses about x-axis

$$C''_k = \sum_{j\in\{\uparrow,\downarrow\}} R^{UT}_{kj} \cdot C'_j = \sum_{j\in\{\uparrow,\downarrow\}} R^{UT}_{kj} \sum_{j\in\{\uparrow,\downarrow\}} R^{TS}_{ji} \cdot C_i = \sum_j \sum_i R^{UT}_{kj} R^{TS}_{ji} \cdot C_i$$

⇝ since T lets pass both orientations ↑T and ↓T, we have in fact

$$C''_k = \sum_i R^{US}_{ki} \cdot C_i$$

with $R^{US}_{ki} = \sum_j R^{UT}_{kj} R^{TS}_{ji}$

rotation by ϕ about z-axis Rotation of two SG apparatuses about the z-axis relative to each other

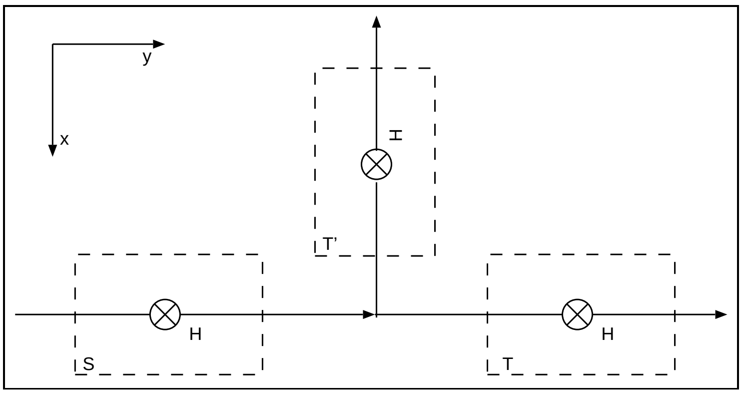


Figure 18: 3 GS apparatuses about z-axis

⇝ a particle in state ψ getting into and out of S would have, w.r.t.

- $\rightsquigarrow$ base states in S: $C_\uparrow = <\uparrow S|\psi>$, $C_\downarrow = <\downarrow S|\psi>$
- $\rightsquigarrow$ base states in T: $C'_\uparrow = <\uparrow T|\psi>$, $C'_\downarrow = <\downarrow T|\psi>$

$\rightsquigarrow$ the beam splits up in S into $|\uparrow S>$ and $|\downarrow S>$ and recombines

$\rightsquigarrow$ since the same happens in T, it should be safe to assume that $C'_\uparrow = C_\uparrow$ and $C'_\downarrow = C_\downarrow$

$\rightsquigarrow$ the story is different for T' $\rightsquigarrow$ what can safely be concluded is that $|C''_\uparrow| = |<\uparrow T'|\psi>| = |C_\uparrow|$ and $|C''_\downarrow| = |<\downarrow T'|\psi>| = |C_\downarrow|$ but the phases of the amplitudes may de different

Why should the phases be different? Consider two configurations of SG apparatuses

$\rightarrow$ S, T and U arranged in a straight line

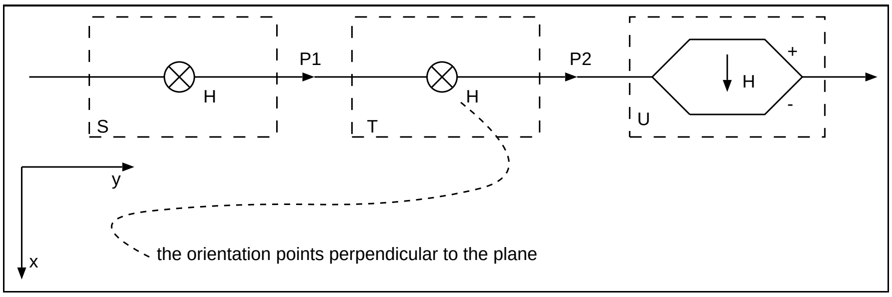


Figure 19: 3 GS apparatuses in a straight line

- $\rightsquigarrow$ suppose particles enter the S apparatus in a (+x) state $\rightsquigarrow$ S splits them up and recombines them
- $\rightsquigarrow$ the same happens in T $\rightsquigarrow$ at P_2 we have again all particles in a (+x) state
- $\rightsquigarrow$ but $\rightsquigarrow$ in apparatus U all particles go into the $\downarrow$beam $\rightsquigarrow$ and can be filtered out

$\rightarrow$ T and U are swung around by 90^0 against S

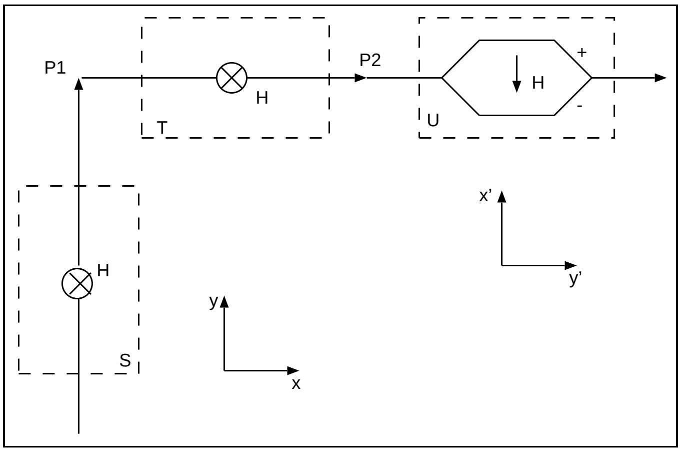


Figure 20: 3 GS apparatuses at 90^0

- $\rightsquigarrow$ the apparatus T puts out what it receives at the input $\rightsquigarrow$ particles that are in state (+x) w.r.t. the apparatus S
- $\rightsquigarrow$ apparatus U then receives particles that are in state (+x) w.r.t. S but it splits up | analyses particles that are in states (+y) or (-y) w.r.t. S
- $\rightsquigarrow$ this is in contradiction to conventional wisdom according to which nothing should have changed when turning the corner at P
- $\rightsquigarrow$ if there is a difference between the two arrangements w.r.t. probability amplitudes $\rightsquigarrow$ it should be phases, i.e. one should have $C'_\uparrow = e^{i\lambda} \cdot C_\uparrow \mid C'_\downarrow = e^{i\mu} \cdot C_\downarrow$, $\lambda \mid \mu$ are real numbers $\rightsquigarrow$ may be different

- $\rightsquigarrow$ since equal phase changes in <u>all</u> amplitudes have no consequences w.r.t. physics, one can add to $\lambda \mid \mu$ as follows:

$$\lambda' = \lambda - \frac{\lambda+\mu}{2} \quad | \quad \mu' = \mu - \frac{\lambda+\mu}{2}$$
$$\rightsquigarrow \lambda' = \frac{\lambda-\mu}{2} = -\mu'$$
$$\rightsquigarrow \lambda = -\mu$$
$$\rightsquigarrow C'_\uparrow = e^{i\lambda} \cdot C_\uparrow \quad | \quad C'_\downarrow = e^{-i\lambda} \cdot C_\downarrow$$

$\rightarrow$ relating λ to the angle ϕ between S and T

- $\rightsquigarrow$ from the first experiment it is known that $\lambda = 0$ if $\phi = 0$
- $\rightsquigarrow$ for arbitrary angles we may assume that $\lambda = q \cdot \phi$ (q = const) $\rightsquigarrow C'_\uparrow = e^{iq\phi} \cdot C_\uparrow \mid C'_\downarrow = e^{-iq\phi} \cdot C_\downarrow$

$\rightarrow$ determining q

- $\rightsquigarrow$ rotating T by 2π should give $C'_\uparrow = C_\uparrow \mid C'_\downarrow = C_\downarrow \rightsquigarrow e^{i2\pi \cdot q} = 1 \rightsquigarrow q = 1$
- $\rightsquigarrow$ however, if $q = 1$, we have for $\phi = \pi$: $C'_\uparrow = e^{i\pi} \cdot C_\uparrow = -C_\uparrow$, $C'_\downarrow = e^{i\pi} \cdot C_\downarrow = -C_\downarrow \rightsquigarrow$ this means that other than for a phase shift by π, $C'_\uparrow = C_\uparrow \mid C'_\downarrow = C_\downarrow$. i.e., the system would be indistinguishable from the system with $\phi = 0$
- $\rightsquigarrow$ this cannot be, since at $\phi = \pi$, the (+x) state of U must be the (-x) state of S and vice versa $\rightsquigarrow$ so $q = 1$ is wrong
- $\rightsquigarrow$ if only rotation by $\phi = 2\pi$ reproduces the same physical states, then we must have $q = \frac{1}{2}$, so that $C'_\uparrow = e^{i2\pi/2} \cdot C_\uparrow = e^{i\pi} \cdot C_\uparrow$, $C'_\downarrow = e^{-i2\pi/2} \cdot C_\downarrow = e^{-i\pi} \cdot C_\downarrow$ and for arbitrary angles ϕ we have

$$C'_\uparrow = e^{i\phi/2} \cdot C_\uparrow \quad | \quad C'_\downarrow = e^{-i\phi/2} \cdot C_\downarrow$$

$\rightarrow$ Transformation of spin 1/2 states about the z-axis may thus be described as:

$$\boxed{(C'_\uparrow, C'_\downarrow) = \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix} \times \begin{pmatrix} C_\uparrow \\ C_\downarrow \end{pmatrix}}$$

rotating about y-axis Rotating two SG apparatuses S, T relative to each other by $180^0 \mid 90^0$ about the y-axis

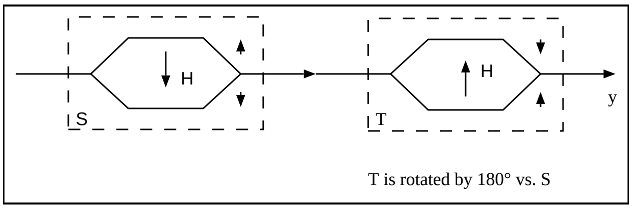


Figure 21: 2 GS apparatuses at 180^0 about the y-axis

$\rightarrow$ what went through the upper channel in S also goes through the upper channel in T since both the field and the field gradient have changed directions

$\rightarrow$ with respect to the probability amplitudes $C'_\uparrow$, $C'_\downarrow$ that come out of T and $C_\uparrow$, $C_\downarrow$ that come out of S, holds at least $|C'_\uparrow| = |C_\downarrow| \mid |C'_\downarrow| = |C_\uparrow|$

$\rightarrow$ assuming some phaseshift, as in the case of rotation about the z-axis gets:

$$C'_\uparrow = e^{i\beta} \cdot C_\downarrow \text{ , } C'_\downarrow = e^{i\gamma} \cdot C_\uparrow$$

$\rightarrow$ rotation by 360^0 about the y-axis should not change anything $\rightsquigarrow$ bring everything back to the non-rotated state $\rightsquigarrow$ since rotation about any axis by 360^0 should cause the same effect as with the z-axis, for two consecutive rotations by 180^0 should hold

$$C''_\uparrow = e^{i\beta} \cdot C'_\downarrow = e^{i\gamma} e^{i\beta} \cdot C_\uparrow \text{ , } C''_\downarrow = e^{i\gamma} \cdot C'_\uparrow = e^{i\beta} e^{i\gamma} \cdot C_\downarrow \text{ and } e^{i\gamma} \cdot e^{i\beta} = -1 \rightsquigarrow e^{i\gamma} = -e^{-i\beta}$$

(the - sign comes from the effect that rotation by 360^0 about the z-axis changes signs) $\rightsquigarrow$ thus we get

$$C''_\uparrow = e^{i\beta} \cdot C'_\downarrow \ , \ C''_\downarrow = -e^{i\beta} \cdot C'_\uparrow$$

for rotation about 180^0

→ the line of reasoning for obtaining $C''_\uparrow$ and $C''_\downarrow$ may be thought of as being the same for any rotation by 180^0 about an axis in the xy-plane, and the phase shift may depend on the angle of this axis relative to the y-axis, with $\beta = 0$ along the y-axis itself

→ determining the phase shift factor β for rotating about an axis $\overrightarrow{a}$ in the xy-plane with angle α relative to the y-axis
  - $\rightsquigarrow$ rotation about $\overrightarrow{a}$ is the same as
    - $\rightsquigarrow$ a rotation by 180^0 about the y-axis followed by
    - $\rightsquigarrow$ a rotation by -2α about the z′-axis

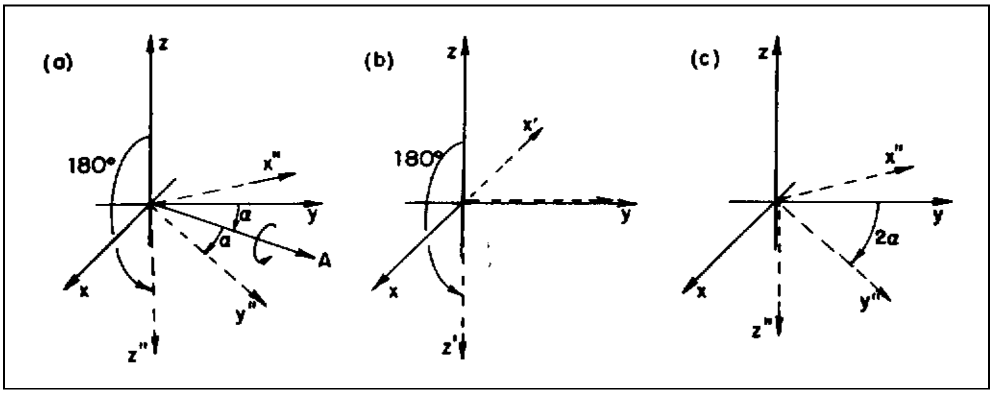


Figure 22: rotating about xy-plane

  - $\rightsquigarrow$ with respect to rotation about $\overrightarrow{a}$ it holds: $C''_\uparrow = e^{i\beta_a} \cdot C_\downarrow \mid C''_\downarrow = -e^{-i\beta_a} \cdot C_\uparrow$ (this by direct rotation)
  - $\rightsquigarrow$ rotating about y by 180^0 yields: $C'_\uparrow = e^{i\beta} \cdot C_\downarrow \mid C'_\downarrow = -e^{-i\beta} \cdot C_\uparrow$ (*)
  - $\rightsquigarrow$ rotating about z by -2α yields: $C''_\uparrow = e^{-i\alpha} \cdot C'_\uparrow \mid C''_\downarrow = e^{i\alpha} \cdot C'_\downarrow$ (**)
  - $\rightsquigarrow$ combining (*) and (**) yields: $C''_\uparrow = e^{i(\beta-\alpha)} \cdot C_\downarrow \mid C''_\downarrow = -e^{-i(\beta-\alpha)} \cdot C_\uparrow$ $\rightsquigarrow$ which means that there must be $\beta_a = \beta - \alpha$
  - $\rightsquigarrow$ choosing $\beta = \alpha$, we get: $C''_\uparrow = C_\downarrow \mid C''_\downarrow = -C_\uparrow$
  - $\rightsquigarrow$ if some axis in the xy-plane can be chosen to have $\beta = 0$, than it may well be the y-axis, which means that we have

$$\boxed{C'_\uparrow = C_\downarrow,\ C'_\downarrow = -C_\uparrow \text{ for rotation by } 180^0 \text{ about the y-axis}}$$

→ rotation by 90^0 about the y-axis may be deduced from two consecutive rotations by 90^0 which should result in a rotation by 180^0.
  - $\rightsquigarrow$ assuming $C'_\uparrow = \alpha_{\uparrow\uparrow}C_\uparrow + \alpha_{\uparrow\downarrow}C_\downarrow$, $C'_\downarrow = \alpha_{\downarrow\uparrow}C_\uparrow + \alpha_{\downarrow\downarrow}C_\downarrow$ for rotation by 90^0, we get for rotation by 180^0

$$\begin{aligned}
C''_\uparrow &= \alpha_{\uparrow\uparrow}C'_\uparrow + \alpha_{\uparrow\downarrow}C'_\downarrow \\
C''_\downarrow &= \alpha_{\downarrow\uparrow}C'_\uparrow + \alpha_{\downarrow\downarrow}C'_\downarrow \text{ or} \\
C''_\uparrow &= (\alpha_{\uparrow\uparrow} \cdot \alpha_{\uparrow\downarrow} + \alpha_{\uparrow\downarrow} \cdot \alpha_{\downarrow\downarrow}) \cdot C_\downarrow + (\alpha_{\uparrow\uparrow} \cdot \alpha_{\uparrow\uparrow} + \alpha_{\uparrow\downarrow} \cdot \alpha_{\downarrow\uparrow}) \cdot C_\uparrow \\
C''_\downarrow &= (\alpha_{\downarrow\uparrow} \cdot \alpha_{\uparrow\uparrow} + \alpha_{\downarrow\downarrow} \cdot \alpha_{\downarrow\uparrow}) \cdot C_\downarrow + (\alpha_{\downarrow\uparrow} \cdot \alpha_{\uparrow\downarrow} + \alpha_{\downarrow\downarrow} \cdot \alpha_{\downarrow\downarrow}) \cdot C_\downarrow
\end{aligned}$$

$\rightsquigarrow$ this yields the equations

$$(\alpha_{\uparrow\uparrow} \cdot \alpha_{\uparrow\downarrow} + \alpha_{\uparrow\downarrow} \cdot \alpha_{\downarrow\downarrow}) = 1 \qquad (a)$$
$$(\alpha_{\uparrow\uparrow} \cdot \alpha_{\uparrow\uparrow} + \alpha_{\uparrow\downarrow} \cdot \alpha_{\downarrow\uparrow}) = 0 \qquad (b)$$
$$(\alpha_{\downarrow\uparrow} \cdot \alpha_{\uparrow\uparrow} + \alpha_{\downarrow\downarrow} \cdot \alpha_{\downarrow\uparrow}) = -1 \qquad (c)$$
$$(\alpha_{\downarrow\uparrow} \cdot \alpha_{\uparrow\downarrow} + \alpha_{\downarrow\downarrow} \cdot \alpha_{\downarrow\downarrow}) = 0 \qquad (d)$$

$\rightsquigarrow$ combining (b) and (c) yields $\alpha_{\uparrow\uparrow}^2 = \alpha_{\downarrow\downarrow}^2 \rightsquigarrow \alpha_{\uparrow\uparrow} = \alpha_{\downarrow\downarrow}$ ($\alpha_{\uparrow\uparrow} = -\alpha_{\downarrow\downarrow}$ is out since that would conflict equations (a) and (c))

$\rightsquigarrow$ with $\alpha_{\uparrow\uparrow} = \alpha_{\downarrow\downarrow}$ we get from (a) and (c) $\alpha_{\uparrow\downarrow} = \frac{1}{2}\alpha_{\uparrow\uparrow} \mid \alpha_{\downarrow\uparrow} = -\frac{1}{2}\alpha{\downarrow\downarrow}$

$\rightsquigarrow$ from (b) follows that $\alpha_{\uparrow\uparrow}^2 - \frac{1}{4}\alpha_{\downarrow\downarrow}^2 = 0 \rightsquigarrow \alpha_{\uparrow\uparrow}^4 = \frac{1}{4} \rightsquigarrow \alpha_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}$ as the standard situation

$\rightarrow$ Transformation of spin 1/2 states about y-axis yields:

$$\boxed{\text{rotation by } +90^0 : \qquad (C'_\uparrow, C'_\downarrow) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} C_\uparrow \\ C_\downarrow \end{pmatrix}}$$

$$\boxed{\text{rotation by } -90^0 : \qquad (C'_\uparrow, C'_\downarrow) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} C_\uparrow \\ C_\downarrow \end{pmatrix}}$$

rotating by α about the x-axis Rotating the SG apparatuses S, T relativ to each other by α about the x-axis.

$\rightarrow$ can be realized by

$\rightsquigarrow$ rotating about the y-axis by $+90^0$ ($\frac{\pi}{2}$) to get the z′-axis down to x-axis to get (x′,y′,z′)

$\rightsquigarrow$ rotating about the z′-axis by α to get (x″,y″,z″)

$\rightsquigarrow$ rotate about the new y″-axis by -90^0

$\rightarrow$ the result is rotation by α about the x-axis

Assuming (x′,y′,z′) to be the new axes after rotation by 90^0 about the y-axis results in

$$C'_\uparrow = \frac{1}{\sqrt{2}}(C_\uparrow + C_\downarrow)$$
$$C'_\downarrow = \frac{1}{\sqrt{2}}(-C_\uparrow + C_\downarrow)$$

Another rotation by α about the z′-axis yields in (x″,y″,z″):

$$C''_\uparrow = e^{i\alpha/2} \cdot C'_\uparrow$$
$$C''_\downarrow = e^{-i\alpha/2} \cdot C'_\downarrow$$

Rotating back by -90^0 about the y″-axis completes the rotation by α about the x-axis, yielding in (x‴,y‴,z‴):

$$C'''_\uparrow = \frac{1}{\sqrt{2}}(C''_\uparrow - C''_\downarrow)$$
$$C'''_\downarrow = \frac{1}{\sqrt{2}}(C''_\uparrow + C''_\downarrow)$$

or, when substituting for $C''_\uparrow \mid C''_\downarrow$:

$$C'''_\uparrow = \frac{1}{\sqrt{2}}(e^{i\alpha/2} \cdot C'_\uparrow - e^{-i\alpha/2} \cdot C'_\downarrow)$$
$$C'''_\downarrow = \frac{1}{\sqrt{2}}(e^{i\alpha/2} \cdot C'_\uparrow + e^{-i\alpha/2} \cdot C'_\downarrow)$$

or, when substituting for $C'_\uparrow \mid C'_\downarrow$:

$$C'''_\uparrow = \frac{1}{2}(e^{i\alpha/2} \cdot (C_\uparrow + C_\downarrow) - e^{-i\alpha/2} \cdot (-C_\uparrow + C_\downarrow))$$
$$C'''_\downarrow = \frac{1}{2}(e^{i\alpha/2} \cdot (C_\uparrow + C_\downarrow) + e^{-i\alpha/2} \cdot (-C_\uparrow + C_\downarrow))$$
$$\rightsquigarrow \quad C'''_\uparrow = \frac{1}{2}((e^{i\alpha/2} + e^{-i\alpha/2}) \cdot C_\uparrow + (e^{i\alpha/2} - e^{-i\alpha/2}) \cdot C_\downarrow)$$
$$\rightsquigarrow \quad C'''_\downarrow = \frac{1}{2}((e^{i\alpha/2} - e^{-i\alpha/2}) \cdot C_\uparrow + (e^{i\alpha/2} + e^{-i\alpha/2}) \cdot C_\downarrow)$$

with $2\cos\phi = e^{i\phi} + e^{-i\phi} \mid 2i\sin\phi = e^{i\phi} - e^{-i\phi}$ we finaly get (for a rotation by α about x-axis):

$$C'''_\uparrow = \cos\alpha/2 \cdot C_\uparrow + i \cdot \sin\alpha/2 \cdot C_\downarrow$$
$$C'''_\downarrow = i \cdot \sin\alpha/2 \cdot C_\uparrow + \cos\alpha/2 \cdot C_\downarrow$$

or:

$$\boxed{(C'''_\uparrow, C'''_\downarrow) = \begin{pmatrix} \cos\alpha/2 & i \cdot \sin\alpha/2 \\ i\sin\alpha/2 & \cos\alpha/2 \end{pmatrix} \cdot \begin{pmatrix} C_\uparrow \\ C_\downarrow \end{pmatrix}}$$

arbitrary rotation rotation about any angles α, β, γ of a new coordinate system (x^r, y^r, z^r) w.r.t. an original system (x,y,z)

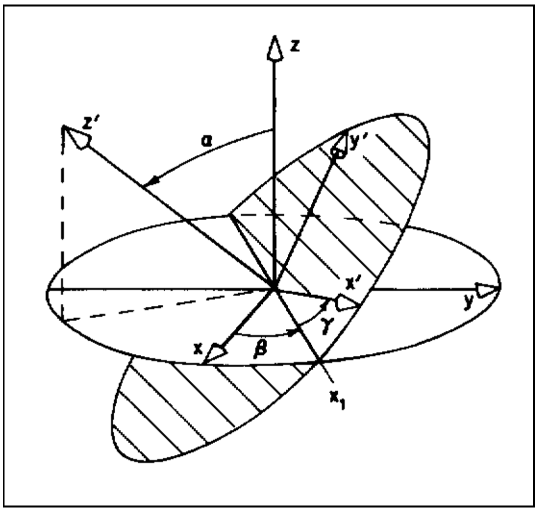


Figure 23: arbitrary rotation

→ starting at (x,y,z)
  ⇝ rotate by β about the z-axis bringing x to some new position x′, y to y′
  ⇝ rotate by α about the new axis x′ to bring z′ down to position x^r
  ⇝ rotate about z^r by γ brings x′ into x^r and y′ into y^r
→ results in

$$\boxed{\begin{aligned} C^r_\uparrow &= \cos\alpha/2 \cdot e^{i(\beta+\gamma)/2} \cdot C_\uparrow + i \cdot \sin\alpha/2 \cdot e^{-i(\beta-\gamma)/2} \cdot C_\downarrow \\ C^r_\downarrow &= i \cdot \sin\alpha/2 \cdot e^{i(\beta-\gamma)/2} \cdot c_\uparrow + \cos\alpha/2 \cdot e^{-i(\beta+\gamma)/2} \cdot C_\downarrow \end{aligned}}$$

defines the amplitudes of the spin 1/2 particles in state ψ, which come out of a SG apparatus in coordinates (x,y,z) as $<\uparrow S|\psi> \mid <\downarrow S|\psi>$, and out of a subsequent SG apparatus T rotated by α, β, γ in a coordinate system (x^r,y^r,z^r) as $<\uparrow T|\psi> \mid <\downarrow T|\psi>$

2.12 some formal properties of probability amplitudes

→ the equation $<\chi|\phi>=\sum_i <\chi|i><i|>\phi>$ describes the probability amplitudes of getting from ϕ to χ as the sum over the probability amplitudes of
  ⇝ going from ϕ to base state i followed by
  ⇝ going from base state i to ψ
→ this equation is similar to an inner vector product $\vec{x} \cdot \vec{y} = \sum_{i\in\{1,2,3\}}(\vec{x} \cdot \vec{e_i})(\vec{e_i} \cdot \vec{y})$ and

$$\vec{x} = x_1 \cdot \vec{e_1} + x_2 \cdot \vec{e_2} + x_3 \cdot \vec{e_3}$$
$$\vec{y} = y_1 \cdot \vec{e_1} + y_2 \cdot \vec{e_2} + y_3 \cdot \vec{e_3}$$

where $\vec{e_1}$, $\vec{e_2}$, $\vec{e_3}$ are unit vectors with the property $\vec{e_i} \cdot \vec{e_j} = \delta_{ij}$
→ ϕ and ψ may be considered amplitude vectors
→ $<i|\phi> \mid <\chi|i>=<i|\chi>^*$ may be considered vector components relative to the base vectors i
→ likewise

$$|\phi>=\sum_i |i><i|\phi> \qquad (*)$$

is equivalent to the vector equation

$$\vec{x} = \sum_i \vec{e_i} \cdot (\vec{e_i} \cdot \vec{x})$$

→ for a purely formal basis the $|\phi>$ may be abstracted from eqn. (*), yielding:

$$| = \sum_i |i><i|$$

which applies only to quantum mechanics ⇝ there is no equivalent law in vector analysis

→ the 'operator' | can be completed to it's left and right, yielding

$$<\psi| = \sum_i <\psi|i><i|$$

$$\text{or } |\phi> = \sum_i |i><i|\phi>$$

⇝ $<\psi|$ is called the bra-vector

⇝ $|\phi>$ is called the ket-vector of the inner vector product $<\psi|\phi>$

⇝ $<\psi|$ may be considered a row vector

⇝ $|\phi>$ may be considered a column vector

→ some more exercises:

we have

$$<i|\phi> = C_i \quad , \quad <i|\chi> = D_i$$

and thus

$$|\phi> = \sum_i |i> C_i \quad , \quad |\chi> = \sum_i |i> D_i$$

⇝ knowing that $<\chi| = \sum_i <\chi|i><i|$ and that $<\chi|i> = <i|\chi>^* = D_i^*$

we also get

$$<\chi| = \sum_i D_i^* <i|$$

and

$$<\chi|\phi> = \sum_{ji} D_j^* <j|i> C_i$$

and with $<j|i> = \delta_{ij}$ we get

$$<\chi|\phi> = \sum_i D_i^* \cdot C_i$$

which is equivalent to an inner vector product

$$\vec{x} \cdot \vec{y} = \sum_i x_i \cdot y_i$$

⇝ remainder: the quantum mechanical base states may be any number n, they are not confined to the three unit vectors of a three-dimensional vector space

⇝ the equation $<\psi|A|\phi> = \sum_{ij} <\psi|i><i|A|j><j|\phi>$ describes the probability amplitude of going from state ϕ to state ψ through the apparatus A. stripping $<\psi|$ of to the left and $|\phi>$ off to the right yields a specification of the apparatus

$$A = \sum_{ij} |i><i|A|j><j|$$

2.13 Choosing suitable base states

is more or less a matter of convenience or convention

- $\leadsto$ the spin of an electron may be oriented along the z-axis of a coordinate system $\leadsto$ but any other coordinate system will do as well
- $\leadsto$ suitable base states usually correspond to physical properties
  - $\leadsto$ in the case of electrons $\leadsto$
    - $\leadsto$ spin (two states $\leadsto$ up | down)
    - $\leadsto$ momentum (several states $\leadsto \ldots -1, 0, +1, \ldots$)
- $\leadsto$ amplitudes associated with base states tell the probability of an electron (a particle) to be in that state (or a combination of other states)
- $\leadsto$ with two electrons there are four spin states and nine momentum states
- $\leadsto$ with n electrons there are 2^n spin states and 3^n momentum states

The problem of describing the nature in general always breaks down, at quantum level, to finding a suitable set of base states. A linear combination of which in terms of probability amplitudes describes the probability amplitude of finding the system in a mixture of states.

2.14 State changes with time

The state of a quantum system, left to itself, will change in time, e.g., due to no effects of external inferences $\leadsto$ electric | magnetic fields etc.

- $\rightarrow$ can be described in terms of an apparatus acting on a state ϕ at time t_1, transforming it into a state ψ at time $t_2 > t_1$
- $\rightarrow$ the 'apparatus' may be described by an operator $U(t_2, t_1)$

$$< \psi|U(t_2,t_1)|\phi >= \sum_{ij} < \psi|i >< i|U(t_2,t_1)|j >< j|\phi >$$

- $\rightarrow$ the question is: how does $U(t_2, t_1)$ work like?

In a small interval of time Δt we have

$$|\phi(t+\Delta t) >= U(t+\Delta t)|\phi(t) >$$

or

$$< \psi|\phi(t+\Delta t) >=< \psi|U(t+\Delta t)|\phi(t) >$$

or

$$< i|\phi(t+\Delta t) >= \sum_j < i|U(t+\Delta t)|j >< j|\phi(t) >$$

or with $C_i(t) =< i|\phi(t) >$ we get

$$C_i(t+\Delta t) = \sum_j U_{ij}(t+\Delta t, t) \cdot C_j(t)$$

It is known at a time $\Delta t = 0 : U_{ij}(t,t) = \delta_{ij} \leadsto$ nothing happens in the intervall $\Delta t = 0$

- $\rightarrow$ for small non-zero intervals we may assume $U_{ij} = \delta_{ij} + K_{ij}\Delta t$ or $U_{ij} = \delta_{ij} - \frac{i}{\hbar} H_{ij}(t)\Delta t$ which means

$$C_i(t+\Delta t) = \sum_j (\delta_{ij} - \frac{i}{\hbar} H_{ij}(t) \cdot \Delta t) \cdot C_j(t) \text{ or } \frac{C_i(t+\Delta t) - C_i(t)}{\Delta t} = -\frac{i}{\hbar} \sum_j H_{ij}(t) \cdot C_j(t)$$

$\leadsto$

$$\frac{dC_i(t)}{dt} = -\frac{i}{\hbar} \sum_j H_{ij}(t) \cdot C_j(t)$$

or

$$i\hbar \frac{d < i|\phi(t) >}{dt} = \sum_j H_{ij}(t) \cdot < j|\phi(t) >$$

$\rightsquigarrow$ this is the quantum mechanical description of the physics of the world
$\rightsquigarrow$ the famous Schrödinger equation
$\rightarrow$ describing a quantum mechanical system requires
  $\rightsquigarrow$ a set of base states
  $\rightsquigarrow$ the coefficients of the so-called Hamiltonian Matrix H_{ij}
$\rightarrow$ from the criterion that a particle | a set of particles must be in some state it follows that

$$\sum_i |C_i(t)|^2 = 1$$

and for this to be true, we must have

$$H_{ij}^* = H_{ij}$$

$\rightarrow$ H_{ij} is more properly refered to as the energy matrix, which may be deduced from the following
  $\rightsquigarrow$ assuming a simple system of just one state and H_{11} being not time dependent, we have

$$i\hbar \frac{dC_1}{dt} = H_{11} C_1$$

and thus

$$C_1 = k \cdot e^{-(i/\hbar) \cdot H_{11} \cdot t}$$

Since $h = 6.63 \cdot 10^{-34}$ Js, we have $[H_{11}]$ = Joule $\rightsquigarrow$ measure of energy

2.15 An example: the ammonia molecule

Disgarding all other components (spins, momentums), the criteria instead can be considered to be in one of two states

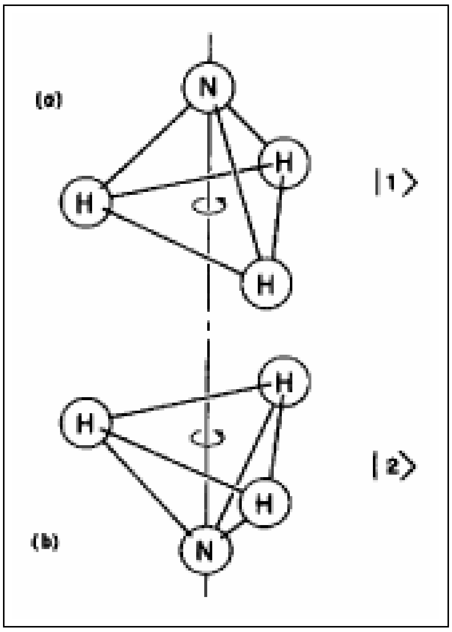


Figure 24: states $|1>$ and $|2>$

$\rightsquigarrow$ the nitrogen atom being above the plane of the hydrogen atoms (state $|1>$)

$\rightsquigarrow$ the nitrogen atom being below the plane of the hydrogen atom (state $|2>$)
the state vectors can then be written as:

$$|\phi> = |1><1|\phi> + |2><2|\phi>$$
$$= |1> C_1 + |2> C_2$$

changes in time of the amplitudes may be denoted as:

$$i\hbar \cdot \frac{dC_1}{dt} = H_{11}C_1 + H_{12}C_2$$
$$i\hbar \cdot \frac{dC_2}{dt} = H_{21}C_1 + H_{22}C_2$$

$\rightsquigarrow$ assuming H_{12} and H_{21} to be zero (if one decidable is in one state, it has no chance of getting into the other state), we get:

$$C_1 = k_1 \cdot e^{-(i/\hbar)H_{11} \cdot t} \qquad | \qquad C_2 = k_2 \cdot e^{-(i/\hbar)H_{22} \cdot t}$$

which are the amplitudes for the stationary state.

$\rightsquigarrow$ it is reasonable to assume that $k_1 = k_2$ and $H_{11} = H_{22}$ for reasons of symmetry of the two states

$\rightsquigarrow$ the same symmetry considerations apply to the energies H_{12} and H_{21}, which must be different from zero to allow transitions between the states $|1>$ and $|2>$.

$\rightsquigarrow$ with $H_{12} = H_{21} = -A$ and $H_{11} = H_{22} = E_0$, we get

$$i\hbar \cdot \frac{dC_1}{dt} = E_0C_1 - AC_2$$
$$i\hbar \cdot \frac{dC_2}{dt} = E_0C_2 - AC_1$$

$\rightsquigarrow$ adding the two equations yields

$$i\hbar \cdot (\frac{dC_1}{dt} + \frac{dC_2}{dt}) = (E_0 - A)(C_1 + C_2)$$

$\rightsquigarrow$ substracting them yields

$$i\hbar \cdot (\frac{dC_1}{dt} - \frac{dC_2}{dt}) = (E_0 + A)(C_1 - C_2)$$

$\rightsquigarrow$ with the solutions

$$C_1 + C_2 = a \cdot e^{-\frac{i}{\hbar}(E_0 - A) \cdot t}$$
$$C_1 - C_2 = b \cdot e^{-\frac{i}{\hbar}(E_0 + A) \cdot t}$$

$\rightsquigarrow$ adding and subtracting these equations, we obtain

$$C_1(t) = \frac{a}{2} \cdot e^{-(\frac{i}{\hbar})(E_0 - A) \cdot t} + \frac{b}{2} \cdot e^{-(\frac{i}{\hbar})(E_0 + A) \cdot t}$$
$$C_2(t) = \frac{a}{2} \cdot e^{-(\frac{i}{\hbar})(E_0 - A) \cdot t} - \frac{b}{2} \cdot e^{-(\frac{i}{\hbar})(E_0 + A) \cdot t}$$

$\rightsquigarrow$ considering the special cases

- $\rightsquigarrow$ b=0 yields
  $C_1(t) = C_2(t) = \frac{a}{2}e^{-(\frac{i}{\hbar})(E_0 - A) \cdot t}$ $\rightsquigarrow$ there is a stationary state of energy $(E_0 - A)$ at which both amplitudes $C_1(t)$ | $C_2(t)$ are the same
- $\rightsquigarrow$ a=0 yields
  $C_1(t) = -C_2(t) = \frac{b}{2}e^{-(\frac{i}{\hbar})(E_0 + A) \cdot t}$ $\rightsquigarrow$ there is another stationary state with energy $(E_0 + A)$

$\rightsquigarrow$ since the molecule can flip from one state to the other, the energy levels are not just E_0 but $(E_0 + A)$ and $(E_0 - A)$

$\rightsquigarrow$ this spliting applies to all states of the molecule that depend upon momentum | spin etc. $\rightsquigarrow$ doublet of energy levels

$\rightsquigarrow$ determining a and b can be done by means of the following consideration

$\rightsquigarrow$ Assuming that at time $t = 0$ the system is in state $|1>$ but not in state $|2>$, then we have

$\rightsquigarrow$ $C_1(0) = \frac{(a+b)}{2} = 1 \mid C_2(0) = \frac{(a-b)}{2} = 0$, which yields $a = b = 1$

$\rightsquigarrow$ we thus get:

$$
\begin{aligned}
C_1(t) &= e^{-\frac{i}{\hbar}\cdot E_0 t}\left(\frac{e^{\frac{i}{\hbar}At} + e^{-\frac{i}{\hbar}At}}{2}\right) \\
C_2(t) &= e^{-\frac{i}{\hbar}\cdot E_0 t}\left(\frac{e^{\frac{i}{\hbar}At} - e^{-\frac{i}{\hbar}At}}{2}\right) \\
\text{or}\quad C_1(t) &= e^{-\frac{i}{\hbar}E_0 t}\cdot \cos\frac{At}{\hbar} \\
C_2(t) &= e^{-\frac{i}{\hbar}E_0 t}\cdot i\sin\frac{At}{\hbar} \\
\text{or}\quad |C_1(t)|^2 &= \cos^2\frac{At}{\hbar} \\
|C_2(t)|^2 &= \sin^2\frac{At}{\hbar}
\end{aligned}
$$

$\rightarrow$ this means that the probability of the molecule being in states $|1>$ and $|2>$ periodically swaps between the two states $\rightsquigarrow$ behavior like coupled pendulums

3 Hilbert Spaces

3.1 basic definitions

Definition [Hilbert Space]
A Hilbert Space is a vector space H over complex numbers from the set $\mathbb{C}$. Vectors are denoted as $|\psi> \in \mathbb{C}^n = H$. There is an inner | scalar vector product $<.|.>: H \times H \to \mathbb{C}$ such that for every $\phi, \phi', \psi \in H$ and $c_1, c_2 \in \mathbb{C}$ we have

$\rightsquigarrow$ $<\psi|\phi> = <\phi|\psi>^*$

$\rightsquigarrow$ $<\psi|\psi> \geq 0$ and $<\psi|\psi> = 0$ iff $|\psi> = 0$

$\rightsquigarrow$ $<\psi|c_1\phi + c_2\phi'> = c_1 <\psi|\phi> + c_2 <\psi|\phi'>$

$\rightsquigarrow$ completeness of the norm: $|\psi| = \sqrt{<\psi|\psi>}$

The inner product of two vectors | states $\psi = (u_1, \ldots, u_n) \in \mathbb{C}^n$ and $\phi = (v_1, \ldots, v_n) \in \mathbb{C}^n$ is defined as

$$<\psi|\phi> = <(u_1, \ldots, u_n)|(v_1, \ldots, v_n)> = \sum_{i=1}^{n} u_i^* \cdot v_i$$

(u^* is the conjugate complex of u) $\diamond$

Definition [orthogonal, orthonormal]
Two vectors $\phi, \psi \in H$ are orthogonal if $<\phi|\psi> = 0$. A set $S \subset H$ is orthogonal if for all $\phi_i, \phi_j \in S$ with $\phi_i \neq \phi_j$ holds $<\phi_i|\phi_j> = 0$. S is orthonormal if S is orthogonal and all $\phi_i \in S$ have norm 1. $\diamond$

Definition [subspace]
A subspace G of H is a subset of H that is closed under addition and inner product. $\diamond$

For each closed subspace W of H there exists a unique subspace $W^{\perp}$ of H that for all $\phi \in W$ and $\psi \in W^{\perp}$ holds $< \phi|\psi >= 0$, and each $\phi \in H$ has a unique representation $\phi = \phi_1 + \phi_2$ with $\phi_1 \in W$ and $\phi_2 \in W^{\perp}$.
Definition [orthonormal basis]
An orthonormal set $B \subseteq H$ is an orthonormal basis of H if none of its supersets is orthonormal. ◇

Definition [representation of ϕ]
If $B = \{\phi_i | i \in \{0, 1, \ldots, n-1\}\}$ is an orthonormal basis of an n-dimensional Hilbert space H and for $\psi \in H$ holds $\psi = \sum_{i=0}^{n-1} \alpha_i \phi_i$ then $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is the representation of ϕ in B.

$< \psi|$ is the bra-vector corresponding to the ket-vector $|\psi >$
$< \psi|$ may be considered a row vector
$|\psi >$ may be considered a column vector
$< \phi|\psi >$ is a scalar product
$|\phi >< \psi|$ is a tensor product

e.g. if $|\phi >= \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \cdots \\ \alpha_n \end{pmatrix}$ and $< \psi| = (\beta_0 \ \beta_1 \ \cdots \ \beta_n)$

then $|\psi >< \phi| = \begin{pmatrix} \alpha_0\beta_0 & \cdots & \alpha_0\beta_n \\ \vdots & \ddots & \vdots \\ \alpha_n\alpha_0 & \cdots & \alpha_n\beta_n \end{pmatrix}$

◇

3.2 linear operators

Definition [linear operator]
A linear operator of H is a mapping $A : H \rightarrow H$
(linearity is defined as $A(\alpha\phi + \beta\psi) = \alpha A\phi + \beta A\psi$) ◇

The adjoint of A, called A^*, is defined as

$$< \psi|A|\phi >=< A^*\psi|\phi >$$

If $A = A^*$ then the operator is self-adjoint. An operator A is usually represented by a matrix M_A of degree n for an n-dimensional Hilbert space H_n. If A is self-adjoint in H_n, then there exist n eigenvalues λ such that there is a vector solution ϕ_λ with the property that $A \cdot \phi_\lambda = \lambda \cdot \phi_\lambda$. ϕ_λ is an eigenvector of A. The set of eigenvalues of A is called its spectrum. The set of eigenvalues is said to be non-degenerable if all pairs of eigenvalues from the set are different. For any Hilbert space H and any of its self-adjoint operators A there is an orthonormal basis consisting of eigenvalues of A.

3.3 projections

Projections are special operators that map vectors into subspaces.
Definition [projection]
Let H be a Hilbert space with subspaces W and $W^{\perp}$ such that $H = W + W^{\perp}$, then each $\phi \in H$ has a unique representation $\phi = \phi_W + \phi_{W^{\perp}}$ such that $\phi_W \in W$ and $\phi_{W^{\perp}} \in W^{\perp}$. The projections are then

$$P_W(\phi) = \phi_W \qquad | \qquad P_{W^{\perp}}(\phi) = \phi_{W^{\perp}}$$

◇

If W is a subspace spanned by a single vector ψ, then the projection ϕ onto ψ is denoted as $P_\psi(\phi)$.
Definition [projection]
If $\{|\phi_0>, |\phi_1>, \ldots, |\phi_{n-1}>\}$ is an orthogonal basis, and $|\psi>$ is given relative to this basis as

$$|\psi> = \sum_{i=0}^{n-1} <\phi_i|\psi> |\phi_i>$$

then the projection P_{ϕ_i} is defined as:

$$P_{\phi_i}|\psi> = <\phi_i|\psi> |\phi_i>$$

For any $\phi \in H$ with $|\phi| = 1$, the operator $P_\phi = |\phi><\phi|$ with

$$P_\phi|\psi> = |\phi><\phi|(|\psi>) = <\phi|\psi> |\phi>$$

is the projection of ψ onto the one-dimensional space $|\phi>$. ◇

If $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ are eigenvalues of an operator A in a Hilbert space H_n, then A has the spectral representation

$$A = \sum_{i=0}^{n-1} \lambda_i |\phi_i><\phi_i| = \sum_{i=0}^{n-1} \lambda_i P_{\phi_i}$$

where ϕ_i are the eigenvectors that are associated with λ_i

3.4 observables of quantum systems

→ measurements are the most controversal problem in quantum physics
  ⇝ in classical physics ⇝ a measurement always is an answer to the question: what is the value of a particular state | property of an object of real world ⇝ it relates to some pre-existing measurable reality
  ⇝ in quantum physics the question must be rephrased: is there an object whose property | state takes on a specific value?
  ⇝ only by being measured does the object assume such value, otherwise the state | property is completely undetermined
→ an observable is a self-adjoint operator A with

$$A = \sum_{i=0}^{n-1} a_i P_i$$

where a_i are the eigenvalues of A and the P_i are projections onto the eigenvectors | eigenstates associated with the eigenvalues a_i With ϕ_i being an eigenvector, we have

$$P_i = |\phi_i><\phi_i|$$

→ a measurement of an observable A has a numerical outcome which is an eigenvalue a_i of A ⇝ after the measurment, the quantum state collapses into

$$a_i|\phi_i>$$

(a_i is the eigenvalue measured, and ϕ_i is the eigenvector associated with it)

→ if the quantum state at the time of measurement was ψ, then the outcome a_i is obtained with probability

$$p(a_i) = ||P_i|\psi>||^2 = <\psi|P_i|\psi>$$

and the normalized quantum state becomes

$$\frac{P_i|\psi>}{<\psi|P_i|\psi>^2}$$

→ another measurment of the state results in the same state with probability $p(a_i) = 1$

→ since a non-degenerate operator A of degree n produces n eigenvalues, one gets one of n possible outcomes of a measurement ⇝ the state collapses into one of n possible states specified by the eigenvectors

→ the observable | the operator A (the choice of it) determinates what the eigenvectors (and the projections to them) are.

→ the operator A in fact specifies the apparatus which does the measurement

4 Elements of quantum computing

4.1 the quantum bit (qubit)

→ The quantum bit (qubit) is a quantum state in a 2-dim Hilbert space H_2, denoted as

$$|\psi>= \alpha|0> + \beta|1>$$

with $|0>$ and $|1>$ as base states and $\alpha, \beta \in \mathbb{C}$ and $\alpha^2 + \beta^2 = 1$ ⇝ the qubit is with probability 1 in either of the two base states

→ alternative representation

$$|\psi>= \cos\theta \cdot |0> + e^{j\varphi} \cdot \sin\theta \cdot |1>$$

$$\text{with } <\psi|\psi>= (\cos\theta, e^{-j\varphi} \cdot \sin\theta) \cdot \begin{pmatrix} \cos\theta \\ e^{j\varphi} \cdot \sin\theta \end{pmatrix} = \cos^2\theta + \sin^2\theta = 1$$

→ a qubit may take as value any linear combination | superposition of ground states $|0>$ and $|1>$

→ representation of qubits as vectors with $|0>= \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1>= \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\alpha|0> + \beta|1>= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

→ physical realization as electron in ground state | excited state || spin up (↑) | spin down (↓) ⇝ $|0>= |\uparrow>$, $|1>= \downarrow>$

measurements on qubits

→ are defined through an observable A (which is a self-adjoint operator)

$$A = \sum_{i=0}^{1} a_i P_i$$

with a_i as eigenvalues, $P_i = |\phi_i><\phi_i|$ as projections onto the eigenvectors associated with a_i

→ measurements w.r.t. eigenvectors $|0>$, $|1>$ yield the following observable:

$$P_0 = |0><0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot (1\ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$P_1 = |1><1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot (0\ 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{and } A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\rightarrow$ it is

$$A \cdot |0> = |0>$$
$$A \cdot |1> = |1>$$
$$A \cdot (\alpha|0> + \beta|1>)^T = \alpha|0> + \beta|1>^*$$

$\rightarrow$ the measurement yields the base state $|0>$ with probability

$$p(a_0) = <\psi|P_0|\psi> = \alpha^2$$

and collapses into state $|0>$, and yields the base state $|1>$ with probability

$$p(a_1) = <\psi|P_1|\psi> = \beta^2$$

and collapses into base state $|1>$

qubit measurements w.r.t. another base $\rightsquigarrow$ the so-called dual base
$\rightarrow$ transformation into this base by means of Hadamard matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot |0> = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot \begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |0'>$$
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot |1> = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot \begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = |1'>$$

$\rightsquigarrow$ this yields

$$|0'> = \frac{1}{\sqrt{2}}(|0> + |1>)$$
$$|1'> = \frac{1}{\sqrt{2}}(|0> - |1>)$$

(which could also be obtained by the inner product)

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot \begin{pmatrix}|0>\\ |1>\end{pmatrix} = \begin{pmatrix}|0'>\\ |1'>\end{pmatrix}$$

$\rightarrow$ rearranging the equations for $|0'>, |1'>$ yields

$$|0> = \frac{1}{\sqrt{2}}(|0'> + |1'>)$$
$$|1> = \frac{1}{\sqrt{2}}(|0'> - |1'>)$$

and

$$\begin{aligned}|\psi> &= \alpha|0> + \beta|1>\\ &= \frac{\alpha}{\sqrt{2}}(|0'> + |1'>) + \frac{\beta}{\sqrt{2}}(|0'> - |1'>)\\ &= \frac{(\alpha+\beta)}{\sqrt{2}} \cdot |0'> + \frac{(\alpha-\beta)}{\sqrt{2}} \cdot |1'>\end{aligned}$$

$\rightarrow$ w.r.t. the new base, we get again an observable $A = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

composed of projections $P_0 = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$; $P_1 = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$ and thus the base states

$$|0'> \text{ with probability } \frac{(\alpha+\beta)^2}{2}$$
$$|1'> \text{ with probability } \frac{(\alpha-\beta)^2}{2}$$

→ if the states $|0' >$ or $|1' >$ are measured w.r.t. the standard basis $|0>$ and $|1>$, then because of

$$|0' > = \frac{1}{\sqrt{2}}(|0 > +|1 >)$$
$$|1' > = \frac{1}{\sqrt{2}}(|0 > -|1 >)$$

we get both $|0>$ and $|1>$ with probability amplitude $\frac{1}{\sqrt{2}}$ and thus with probability $\frac{1}{2}$. ⇝ applying the Hadamard matrix H to the standard basis is similar to coin tossing → both base states occur with the same probability.

qubit evolution

→ is specified by an operator of the general form $A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ which does the transformation

$$A \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = (a_{00}\alpha + a_{01}\beta) \cdot |0 > +(a_{10}\alpha + a_{11}\beta) \cdot |1 >$$

on $|\psi >= \alpha|0 > +\beta|1 >$

→ important transformations are

⇝ Hadamard transformation

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

it does the transformations

$$H|0 > = |0' > \qquad H|0' > = |0 >$$
$$H|1 > = |1' > \qquad H|1' > = |1 >$$

from the standard base to the dual base and vice versa
(dual base ≡ Hadamard base ≡ Fourier base)

⇝ the NOT transformation

$$H_{NOT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

it does

$$\begin{aligned} H_{NOT}^2 \cdot |0 > = H_{NOT}^2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= H_{NOT} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= H_{NOT} \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} \\ &= -|1 > \end{aligned}$$

4.2 Two-bit quantum register

→ are represented as tensor products of two qubits ⇝ span a Hilbert space H_4 of dim 4.

→ a standard base has the following base states:

$$|0 > = |00 >= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |1 > = |01 >= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|2 > = |10 >= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |3 > = |11 >= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

→ the general state of a 2-qubit register is given as:

$$|\psi >= \alpha_{00}|00> +\alpha_{01}|01> +\alpha_{10}|10> +\alpha_{11}|11>$$

with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

→ other bases are

⇝ the dual base

$$|0'0'> \quad | \quad |0'1'> \quad | \quad |1'0'> \quad | \quad |1'1'>$$

⇝ the Bell base

$$\frac{1}{\sqrt{2}}(|00> +|11>) \quad | \quad \frac{1}{\sqrt{2}}(|00> -|11>) \quad | \quad \frac{1}{\sqrt{2}}(|01> +|10>) \quad | \quad \frac{1}{\sqrt{2}}(|01> -|10>)$$

⇝ the magic base

$$\frac{1}{\sqrt{2}}(|00> +|11>) \quad | \quad \frac{i}{\sqrt{2}}(|00> -|11>) \quad | \quad \frac{i}{\sqrt{2}}(|01> +|10>) \quad | \quad \frac{1}{\sqrt{2}}(|01> -|10>)$$

→ measurements of 2-qubit states w.r.t. the standard base are effected by an observable

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \sum_i P_i \quad , \qquad P_i = |i><i| \quad , \qquad i \in \{0,1,2,3\}$$

⇝ the outcome of the measurements is state $|pq>$, $p, q \in \{0, 1\}$ with probability α_{pq}^2.

⇝ the state collapses into $|pq>$

measuring a qubit in a two-bit register w.r.t. the standard base:

⇝ taking $|00>$, $|01>$, $|10>$, $|11>$ as the eigenvectors that form the base, the observable again is $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

⇝ measuring the probability of bit 0 being in state 0, what is required is a projection into base states $|00>$, $|01>$; i.e. we have $P_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ thus we get

$$p(a_{01}) = (\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

and the state collapses into

$$|\psi_0^0 >= \frac{\alpha_{00}|00> +\alpha_{01}|01>}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

⇝ measuring the probability of bit 0 being in state 1, what is required is a projection into base states $|10>$, $|11>$; i.e. we have $P_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and get

$$p(a_{23}) = (\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = |\alpha_{10}|^2 + |\alpha_{11}|^2$$

and the state collapses into

$$|\psi_0^1 >= \frac{\alpha_{10}|10> + \alpha_{11}|11>}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

$\leadsto$ likewise for bit 1 to be on state 0 $\leadsto$ projection into $|00>$, $|10>$ yields

$$p(a_{02}) = |\alpha_{00}|^2 + |\alpha_{10}|^2$$

and

$$|\psi_1^0 >= \frac{\alpha_{00}|00> + \alpha_{10}|10>}{\sqrt{|\alpha_{00}|^2 + |\alpha_{10}|^2}}$$

$\leadsto$ for bit 1 to be in state 1 $\leadsto$ projection into $|01>$, $|11>$ yields

$$p(a_{12}) = |\alpha_{01}|^2 + |\alpha_{11}|^2$$

and

$$|\psi_1^1 >= \frac{\alpha_{01}|01> + \alpha_{11}|11>}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}$$

Remark: Renormalization of the resulting state by $\frac{1}{\sqrt{}}$ is necessary in order to bring the sum over probibilities up to 1 again.

2-qubit evolution

$\rightarrow$ is specified by a operator of the general form $A = \begin{pmatrix} a_{00} & \cdots & a_{03} \\ \vdots & & \vdots \\ a_{30} & \cdots & a_{33} \end{pmatrix}$ which does the transformation

$$A \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} a_{00}\alpha_{00} & + \cdots + & a_{03}\alpha_{11} \\ a_{10}\alpha_{00} & + \ldots + & a_{13}\alpha_{11} \\ \vdots & & \vdots \\ a_{30}\alpha_{00} & + \ldots + & a_{33}\alpha_{11} \end{pmatrix}$$
$$= (a_{00}\alpha_{00} + \ldots + a_{03}\alpha_{11}) \cdot |00>$$
$$+ (a_{10}\alpha_{00} + \ldots + a_{13}\alpha_{11}) \cdot |01>$$
$$+ (a_{20}\alpha_{00} + \ldots + a_{23}\alpha_{11}) \cdot |10>$$
$$+ (a_{30}\alpha_{00} + \ldots + a_{33}\alpha_{11}) \cdot |11>$$

example: an eor-gate performing the mapping $eor : |x, y> \rightarrow \; |x, x \oplus y>$ with

$$A_{eor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

follows:

$$A_{eor} \cdot \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \rightarrow \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad , \quad A_{eor} \cdot \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \rightarrow \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad , \quad A_{eor} \cdot \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \rightarrow \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \quad , \quad A_{eor} \cdot \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \rightarrow \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

4.3 n-qubit quantum registers

→ are described by states vectors in a 2^n-dimensional Hilbert space with the base vectors

$$B = \{|r> |r \in \{0,1\}^n\}$$

with $|r> = |b_0 b_1 \dots b_{n-1}>$, $b_i \in \{0,1\}$ forming the standard base.

⇝ alternative representation:

$$B = \{|r> |0 \leq r < 2^n\}$$

in which case we have $r = \sum_{i=0}^{n-1} b_i \cdot 2^{(n-1-i)}$

→ the state of the n-qubit register is given as

$$|\psi> = \sum_{r=0}^{2^n-1} \alpha_r \cdot |r>$$

with $\sum_{r=0}^{2^n-1} |\alpha_r|^2 = 1$

⇝ the number of base states grows exponentially with the number of qubits

⇝ there is a linear time transition between base states, requiring at most n NOT-operations

⇝ there is exponentially more information to be stored in an n-qubit register, however what can be retrieved by measurement is just n bits.

evolution of n-qubit registers

→ requires a unitary operator A represented by a $2^n \times 2^n$ matrix

→ in most cases such an operator is composed of rotation operators | Hadamard transformations on single qubits or unitary operations on two adjacent qubits

→ applying a single unitary operation U to the i-th position of a quantum register (and leaving all other positions unchanged) may be expressed by a unitary operator | matrix of the form

$$\otimes_{k=0}^{i-1} I \otimes U \otimes_{k=i+1}^{n-1} I$$

when I is the identity matrix, and ⊗ denotes the tensor product.

example applying I to qubits 0 and 2 and $H_H \cdot \frac{1}{\sqrt{2}} \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$ to qubit 1 of a 3-qubit register:

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix}1 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\0 & 1 & 0 & 1 & 0 & 0 & 0 & 0\\1 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\0 & 1 & 0 & -1 & 0 & 0 & 0 & 0\\0 & 0 & 0 & 0 & 1 & 0 & 1 & 0\\0 & 0 & 0 & 0 & 0 & 1 & 0 & 1\\0 & 0 & 0 & 0 & 1 & 0 & -1 & 0\\0 & 0 & 0 & 0 & 0 & 1 & 0 & -1\end{pmatrix}$$

→ the general case of applying unitary operators U_i to qubit positions $i \in \{0, \ldots, n-1\}$ yields a unitary operator

$$U_0 \otimes U_1 \otimes U_2 \otimes \cdots \otimes U_{n-1} = \otimes_{i=0}^{n-1} U_i$$

→ the problem of designing quantum algorithms | quantum networks is to decompose a given problem specification into a sequence of one- or two-qubit-operations from a small set of available standard operations ⇝ or to construct a unitary operator of some complexity (that realizes a given algorithm) from elementary operations

measurements of n-qubit registers

→ w.r.t. the standard base can be done by means of an observable

$$A = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \sum_r P_r \quad , \qquad P_r = |r><r|$$

⇝ the outcome of the measurement is base state $|r>$ with probability $<\psi|P_r|\psi> = |\alpha_r|^2$ and the state subsequently colapses into $|r>$.

→ measuring the j-th qubit out of an n-qubit register

⇝ requires projection into a subspace spawned by all base vectors $|r>_{b_j=0}$, i.e. having qubit $|r>_{b_j=0}$, or

⇝ projection into a subspace spawned by all base vectors $|r>_{b_j=1}$

⇝ this gives $b_j = 0$ with probability $\sum_{r/|r>_{b_j=0}} |\alpha_r|^2$ and the state collapses into

$$|\psi'> = \frac{\sum_{r/|r>_{b_j=0}} \alpha_r \cdot |r>}{\sqrt{\sum |\alpha_{|r>_{b_j=0}}|^2}}$$

and likewise for $b_j = 1$.

→ measuring the first m of n qubits representing the state as

$$|\psi> = \sum_{r=0}^{2^{m-1}-1} \sum_{s=0}^{2^{n-m-1}-1} C_{rs}|r, s>$$

⇝ we get every $|r>$ with $r \in \{0,1\}^m$ with probability

$$p(|r>) = \sum_{s=0}^{2^{n-m-1}-1} |C_{rs}|^2$$

and the state collapses into

$$|\psi'> = \frac{1}{\sqrt{p(|r>)}} \sum_{s=0}^{2^{n-m-1}-1} C_{rs}|r, s>$$

Transformation to the dual | Hadamard base of an n-qubit state

→ using H_H as $H_H^{(n)} = \otimes_{i=0}^{n-1} H_H$ yields

⇝

$$H_H^{(n)}|0^{(n)}> = \otimes_{i=0}^{n-1} H_H|0> = \otimes_{i=0}^{n-1}|0'> = |0'^{(n)}> = \frac{1}{\sqrt{2^n}} \sum_{r=0}^{2^n-1} |r>$$

$\leadsto$ in general, for $r \in \{0,1\}^n$, we have

$$H_H^{(n)}|r>= \frac{1}{\sqrt{2^n}} \sum_{s \in \{0,1\}^n} (-1)^{r \cdot s} |s>$$

(with $r \cdot s = \oplus_{i=0}^{n-1} r_i \cdot s_i$)

$\rightarrow$ of importance is the first case $\leadsto$ it gets an empty register $|0^{(n)}>$ into a state which is the superposition of all base states with the same probability amplitude $\leadsto$ coin tossing

$\rightarrow$ validation of the first case

$\leadsto$ with

$$H_H^{(3)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \oplus \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \oplus \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \oplus \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad = \frac{1}{\sqrt{2^3}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

$\leadsto$ we get

$$H_H^{(3)} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2^3}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

i.e.

$$H_H^{(3)}|0^{(3)}>= \frac{1}{\sqrt{2^3}} \sum_{r=0}^{2^n-1} |r>$$

$$H_H^{(3)} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2^3}} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \\ 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

i.e.

$$\begin{aligned} H_H^{(3)}|011> = \frac{1}{\sqrt{2^3}}(&|000> - |001> - |010> + |011> \\ &+ |100> - |101> - |110> + |111>) \end{aligned}$$

⇝ validation of the signs (r=3)

$$\begin{aligned} r \cdot s &= 011 \cdot 000 = 0 \rightsquigarrow \ + \\ &= 011 \cdot 001 = 1 \rightsquigarrow \ - \\ &= 011 \cdot 010 = 1 \rightsquigarrow \ - \\ &= 011 \cdot 011 = 0 \rightsquigarrow \ + \\ &= 011 \cdot 100 = 0 \rightsquigarrow \ + \\ &= 011 \cdot 101 = 1 \rightsquigarrow \ - \\ &= 011 \cdot 110 = 1 \rightsquigarrow \ - \\ &= 011 \cdot 111 = 0 \rightsquigarrow \ + \end{aligned}$$

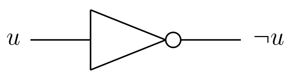
5 Quantum Gates

→ are to realize logic functions on basic and superimposed quantum states
- ⇝ they are inherently reversible as they must maintain the invariance of probability sums over base states w.r.t. operations ⇝ if $\phi = \alpha_r|r>$, $\psi = \alpha'_r|r>$ and $<\psi|A|\phi>$ then it must hold $\sum_r |\alpha_r|^2 = \sum_r |\alpha'_r|^2 = 1$
- ⇝ reversibility in the classical sense requires information preservation of logic operations ⇝ nothing must get lost | nothing must be gained

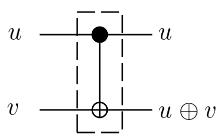
5.1 classical reversible logic gates

→ the not-gate

$$f(u) = \neg u \quad , \qquad u \in \{0,1\}$$

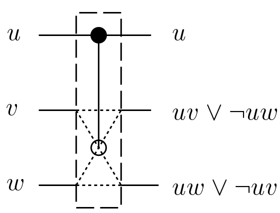


→ the eor-gate



$$f(u,v) = (u, u \oplus v) \quad , \qquad u,v \in \{0,1\}$$

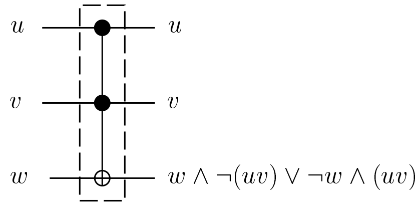
→ the Quinetransfer (Fredkin) gate



$$f(u,v,w) = (u, u \wedge v \vee \neg u \wedge w, \neg u \wedge v \vee u \wedge w) \quad , \qquad u,v,w \in \{0,1\}$$

→ the Toffoli gate

$$f(u,v,w) = (u, v, w \wedge \neg(u \wedge v) \vee \neg w \wedge (u \wedge v)) \quad , \qquad u,v,w \in \{0,1\}$$



→ logical completeness requires that there be means to realize the not-function and the (n)and-function

⇝ Quinetransfer:

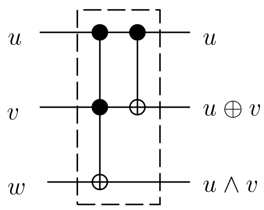
$$\begin{aligned} f(u,v,0) &= (0, u \wedge v, u \neg v) \rightsquigarrow \; and - function \\ f(u,0,1) &= (u, \neg u, u) \qquad\quad \rightsquigarrow \; not - function \end{aligned}$$

⇝ Toffoli gate:

$$\begin{aligned} f(u,v,0) &= (u, v, u \wedge v) \rightsquigarrow \; and - function \\ f(1,1,w) &= (1,1,\neg w) \quad\; \rightsquigarrow \; not - function \end{aligned}$$

⇝ the eor-gate (in combination with a not gate) is not logically complete as it does not allow realization of a nand-function

→ a two-bit adder (reversible):



$$f(u,v,0) = (u, u \oplus v, u \wedge v)$$

5.2 Quantum gates

→ are specified by unitary operatores $U : H^{(2^n)} \rightarrow \; H^{(2^n)}$ that map Hilbert spaces of dimension 2^n into Hilbert spaces of dimension 2^n, with n being the number of 'inputs' and 'outputs'. The operators are realized by unitary matrices of dimension 2^n.

→ the not-gate is realized by a matrix $A_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (which may be obtained from

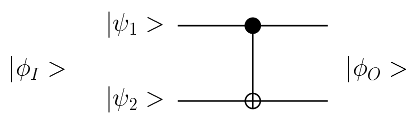
$$H_{NOT} \cdot H_{NOT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

by ignoring the - sign of the first element in the second row)

$$A_{not} | (\alpha|0> + \beta|1>) >= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

⇝ $|\phi' >= \beta|0> + \alpha|1>$ with

$$\begin{aligned} \beta = 0 &\rightsquigarrow \; |\phi >= |0> \rightarrow \; |\phi' >= |1> \\ \alpha = 0 &\rightsquigarrow \; |\phi >= |1> \rightarrow \; |\phi' >= |0> \end{aligned}$$



→ the eor-gate is realized by a matrix

$$A_{eor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

with

$$|\psi_1> = \alpha_1|0> + \beta_1|1>$$
$$|\psi_2> = \alpha_2|0> + \beta_2|1>$$

we get

$$\begin{aligned} |\phi_I> &= |\psi_1> \otimes |\psi_2> \\ &= \alpha_1\alpha_2|00> + \alpha_1\beta_2|01> + \beta_1\alpha_2|10> + \beta_1\beta_2|11> \end{aligned}$$

and thus $A_{eor}|\phi_I> = |\phi_O>$ as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\beta_2 \\ \beta_1\alpha_2 \end{pmatrix}$$

$\rightsquigarrow$ $|\phi_O> = \alpha_1\alpha_2|00> + \alpha_1\beta_2|01> + \beta_1\beta_2|10> + \beta_1\alpha_2|11>$
with $\alpha_2 = 1$, $\beta_2 = 0 \rightsquigarrow \psi_2| = |0>$ we get

$$|\phi_O> = \alpha_1|00> + \beta_1|11>$$

- $\rightsquigarrow$ this produces an entangled state $\rightsquigarrow$ if the value of a qubit 0 is known, then the value of qubit 1 is also known (and vice versa)
- $\rightsquigarrow$ if $\alpha_1 = 1$, $\beta_1 = 0$ then $|\phi_0> = |00>$ if $\alpha_1 = 0$, $\beta_1 = 1$ then $|\phi_0> = |11> \rightsquigarrow$ the qubits $|0>$ and $|1>$ on the control input $|\psi_1>$ are copied into both outputs if $|\psi_2> = |0>$.
- $\rightsquigarrow$ if just the second output (the target qubit) is considered, then we have a so-called mixed state $\rightsquigarrow$ we get
  - $|0>$ with probability $|\alpha_1|^2$
  - $|1>$ with probability $|\beta_1|^2$

→ the Quinetransfer (Fredkin) gate must realize the function

$$f(u, v, w) = (u, u \wedge v \vee \neg u \wedge w, \neg u \wedge v \vee u \wedge w)$$

or the truth table

$$\begin{array}{lcl}
|uvw> \to & & |u'v'w'> \\
|000> & \to & |000> \\
|001> & \to & |010> \\
|010> & \to & |001> \\
|011> & \to & |011> \\
|100> & \to & |100> \\
|101> & \to & |101> \\
|110> & \to & |110> \\
|111> & \to & |111>
\end{array}$$

which can be realized by a matrix $A_F = \begin{pmatrix} 1 & & & & & & & \\ & 0 & 1 & & & & 0 & \\ & 1 & 0 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & 0 & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}$

→ the Toffoli gate must realize the function

$$f(u,v,w) = (u, v, w \wedge \neg(u \wedge v) \vee \neg w \wedge (u \wedge v))$$

or the truth table

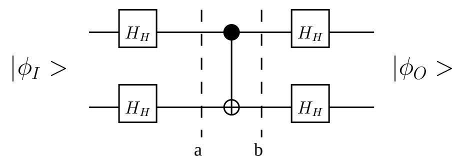
$$\begin{array}{lcl}
|uvw> \to & & |u'v'w'> \\
|000> & \to & |000> \\
|001> & \to & |001> \\
|010> & \to & |010> \\
|011> & \to & |011> \\
|100> & \to & |100> \\
|101> & \to & |101> \\
|110> & \to & |111> \\
|111> & \to & |110>
\end{array}$$

which can be realized by a matrix $A_F = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & 0 & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$

5.3 Composition of gates

→ let G_1 and G_2 be two gates in parallel, and A_1, A_2 the transformation matrices specifying these gates, then the composite gate realizes the tensor product $A_1 \otimes A_2$

→ let G_1 and G_2 be two (composite) gates in series, A_1 and A_2 the respective transformation matrices, then the composite gate realizes the matrix product $A_1 \cdot A_2$



example:

⇝ at (a) we have:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix} = H_H^{(2)}$$

thus, with input:

$$|\phi >= \alpha_0|00> +\alpha_1|01> +\alpha_2|10> +\alpha_3|11>$$

we get as output:

$$\begin{aligned} H_H^{(2)}|\phi >= |\phi_a >= \frac{1}{2}((&\alpha_0+\alpha_1+\alpha_2+\alpha_3)|00>+\\ (&\alpha_0-\alpha_1+\alpha_2-\alpha_3)|01>+\\ (&\alpha_0+\alpha_1-\alpha_2-\alpha_3)|10>+\\ (&\alpha_0-\alpha_1-\alpha_2+\alpha_3)|11>) \end{aligned}$$

⇝ at (b) we have:

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix}\alpha_0+\alpha_1+\alpha_2+\alpha_3\\ \alpha_0-\alpha_1+\alpha_2-\alpha_3\\ \alpha_0+\alpha_1-\alpha_2-\alpha_3\\ \alpha_0-\alpha_1-\alpha_2+\alpha_3\end{pmatrix} = \frac{1}{2}\begin{pmatrix}\alpha_0+\alpha_1+\alpha_2+\alpha_3\\ \alpha_0-\alpha_1+\alpha_2-\alpha_3\\ \alpha_0-\alpha_1-\alpha_2+\alpha_3\\ \alpha_0+\alpha_1-\alpha_2-\alpha_3\end{pmatrix}$$

⇝

$$\begin{aligned} |\phi_b >= \frac{1}{2}((&\alpha_0+\alpha_1+\alpha_2+\alpha_3)|00>+\\ (&\alpha_0-\alpha_1+\alpha_2-\alpha_3)|01>+\\ (&\alpha_0-\alpha_1-\alpha_2+\alpha_3)|10>+\\ (&\alpha_0+\alpha_1-\alpha_2-\alpha_3)|11>) \end{aligned}$$

⇝ another transformation by $H_H^{(2)}$ yields

$$\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix}\alpha_0+\alpha_1+\alpha_2+\alpha_3\\ \alpha_0-\alpha_1+\alpha_2-\alpha_3\\ \alpha_0+\alpha_1-\alpha_2-\alpha_3\\ \alpha_0-\alpha_1-\alpha_2+\alpha_3\end{pmatrix} = \begin{pmatrix}\alpha_0\\ \alpha_3\\ \alpha_2\\ \alpha_1\end{pmatrix}$$

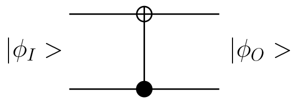
or

$$|\psi >= \alpha_0|00> +\alpha_3|01> +\alpha_2|10> +\alpha_1|11>$$

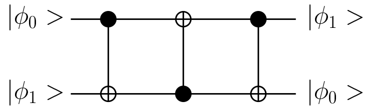
$\rightsquigarrow$ we thus get for

$$
\begin{aligned}
\alpha_0 = 1,\, \alpha_1 = \alpha_2 = \alpha_3 = 0 &\rightsquigarrow\ |00> \to\ |00> \\
\alpha_1 = 1,\, \alpha_0 = \alpha_2 = \alpha_3 = 0 &\rightsquigarrow\ |01> \to\ |11> \\
\alpha_2 = 1,\, \alpha_0 = \alpha_1 = \alpha_3 = 0 &\rightsquigarrow\ |10> \to\ |10> \\
\alpha_3 = 1,\, \alpha_0 = \alpha_1 = \alpha_2 = 0 &\rightsquigarrow\ |11> \to\ |01>
\end{aligned}
$$

which is equivalent to an turned-around eor-gate



example: the flipping gate



$\rightsquigarrow$ on the input side we have

$$|\phi_0>= \alpha_0|0> + \beta_0|1> \qquad , \qquad |\phi_1>= \alpha_1|0> + \beta_1|1>$$

and $|\phi_0> \otimes |\phi_1>= \alpha_0\alpha_1|00> + \alpha_0\beta_1|01> + \beta_0\alpha_1|10> + \beta_0\beta_1|11>$
$\rightsquigarrow$ on the output side we should obtain

$$|\phi_1> \otimes |\phi_0>= \alpha_1\alpha_0|00> + \alpha_1\beta_0|01> + \beta_1\alpha_0|10> + \beta_1\beta_0|11>$$

$\rightsquigarrow$ the eor-gate is given by the matrix

$$A_{eor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$\rightsquigarrow$ the turned-around eor-gate must transform

$$|x, y>\to\ |x \oplus y, y>$$

or

$$|00>\to\ |00> \qquad |01>\to\ |11> \qquad |10>\to\ |10> \qquad |11>\to\ |01>$$

i.e.

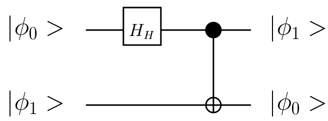
$$A_{\overline{eor}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$\rightsquigarrow$

$$A_{eor} \cdot A_{\overline{eor}} \cdot A_{eor} \cdot \begin{pmatrix} \alpha_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\alpha_1 \\ \beta_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\beta_1 \end{pmatrix}$$

$\rightsquigarrow$

$$|\phi_1> \otimes |\phi_0>= \alpha_1\alpha_0|00> + \alpha_1\beta_0|01> + \beta_1\alpha_0|10> + \beta_1\beta_0|11>$$



example: generating Bell states, which have the form

$$\left\{ \frac{1}{\sqrt{2}}(|00> + |11>), \quad \frac{1}{\sqrt{2}}(|00> - |11>), \quad \frac{1}{\sqrt{2}}(|01> + |10>), \quad \frac{1}{\sqrt{2}}(|01> - |10>) \right\}$$

$\leadsto$ first stage $A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$

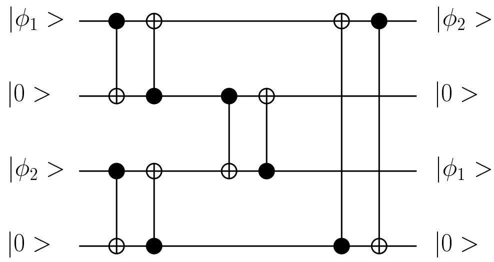
$\leadsto$ second stage $A_2 = A_{eor}$

$\leadsto$ $A = A_2 \cdot A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$

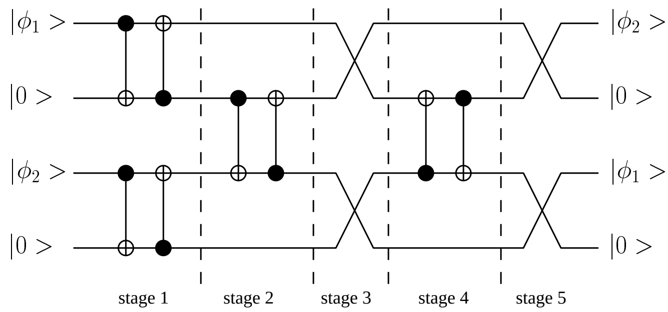
$\leadsto$ $A \cdot (|\phi_0 > \otimes |\phi_1 >) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0\alpha_1 + \beta_0\alpha_1 \\ \alpha_0\beta_1 + \beta_0\beta_1 \\ \alpha_0\beta_1 - \beta_0\beta_1 \\ \alpha_0\alpha_1 - \beta_0\alpha_1 \end{pmatrix}$

$$|\psi >= \frac{1}{\sqrt{2}}((\alpha_0\alpha_1(|00> + |11>) + \alpha_0\beta_1(|01> + |10>) + \beta_0\alpha_1(|00> - |11>) + \beta_0\beta_1(|01> - |10>))$$

example: a permutation network (circulating round robin all inputs by one position)
$\leadsto$ for two inputs



$\leadsto$ to bring the lines of the third stage in adjacent positions $\leadsto$ cross over switch: flipping gate



$\rightsquigarrow$ to describe the full state transformation effected by this cicuit, we need the unitary matrices

$$A = A_{\overline{eor}} \cdot A_{eor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad , \quad B = A_{eor} \cdot A_{\overline{eor}} \cdot A_{eor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\rightsquigarrow$ thus we get

for stage 1: $A \otimes A$
for stage 2: $I \otimes A \otimes I$
for stage 3: $B \otimes B$
for stage 4: $I \otimes (A_{eor} \cdot A_{\overline{eor}}) \otimes I$
for stage 5: $B \otimes B$

and for the entire circuit

$$C = (B \otimes B) \cdot (I \otimes (A_{eor} \otimes A_{\overline{eor}}) \otimes I) \cdot \cdot (B \otimes B) \cdot (I \otimes A \otimes I) \cdot (A \otimes A)$$

which is supposed to transform

$$|\phi_2 > \otimes |0 > \otimes |\phi_1 \otimes |0 >= C \cdot (|\phi_1 > \otimes |0 > \otimes |\phi_2 > \otimes |0 >)$$

5.4 the role of measurement gates

$\rightarrow$ measurements involve an observable of the form

$$A_0 = \sum_{i=0}^{2^n-1} a_i |P_i > \quad \text{with } P_i = |\phi_i >< \phi_i|$$

where P_i is the projection onto eigenvectors $|\phi_i >$ associated with eigenvalues a_i

$\rightarrow$ measurements on n-qubits w.r.t. standard base require an observable

$$A_0 = I^{(n)} = \begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & 1 \end{pmatrix} = \sum_i P_i$$

$\rightarrow$ the outcome of the measurement is some base state $|\phi_i >$ with probability $< \psi|P_i|\psi >= \alpha_i^2$ (with $|\psi >= \sum_i \alpha_i |\phi_i >$)

$\rightarrow$ measurement gates (realizing an observable) may be used to control quantum computations in some particular way:

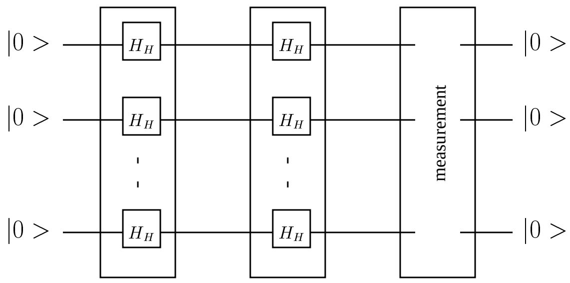
example:

$\rightsquigarrow$ the first gate $H_H^{(n)}$ produces

$$H_H^{(n)} |0^{(n)} >= \frac{1}{\sqrt{2}} \sum_{r=0}^{2^n-1} |r >= |0^{'(n)>}$$

$\rightsquigarrow$ applying $H_H^{(n)}$ again yields

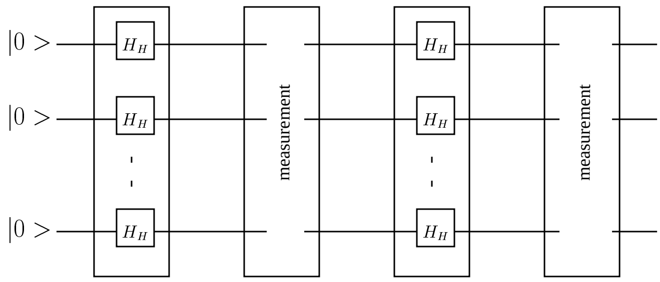
$$H_H^{(n)} 0^{'(n)} >= I^{(n)}$$



⤳ applying

$$H_H^{(n)} \cdot H_H^{(n)} \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \rightsquigarrow |0^n>$$

i.e. the subsequent measurement gate measures base state $|\underbrace{00\dots0}_{n}>$ with probability 1.



example:

⤳ the first gate $H_H^{(n)}$ again produces

$$H_H^{(n)}|0^{(n)}> = |0^{'(n)}> = \frac{1}{\sqrt{2}} \sum_{r=0}^{2^n-1} |r>$$

⤳ the first measurement gate $I^{(n)}$ produces with probability $\frac{1}{2^n}$ some random qubit $|r>$

⤳ the second gate $H_H^{(n)}$ then produces

$$H_H^{(n)}|r> = \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{r\cdot s}|s>$$

⤳ the second gate $I^{(n)}$ then again produces as value some random qubit string $|c>$ with probability $\frac{1}{2^n}$

5.5 Universal quantum gates

→ since operations on quantum states are generally continuous with respect to probability amplitudes, the concept of universality of quantum computations | quantum gates is more complicated, involving operations on probability amplitudes that change then by arbitrary complex amounts

→ a set of quantum operators | gates is said to be *universal* if any unitary transformation U can be performed on a quantum state represented by an n-qubit register

→ a quantum gate is universal by itself if it forms a universal set (including constant inputs $|0>$ and $|1>$)

→ quantum operations are operators on vectors in Hilbert spaces of dimension n
- ⇝ they are composed of elementary operations on two-state (one qubit) (spin-up | spin-down) systems
- ⇝ generally describe notations of base states about the axis of a three dimensional space (compare section 2 on rotating SG-apparatuses against each other)

→ it is known that arbitrary rotations of a base system can be described as follows:
- ⇝ it is

$$R_Z(\phi) = \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix}$$
$$R_X(\theta) = \begin{pmatrix} \cos\theta/2 & i\sin\theta/2 \\ i\sin\theta/2 & \cos\theta/2 \end{pmatrix}$$

- ⇝ the complete rotation about all three angles is

$$\begin{aligned} U_1 &= R_Z(\gamma) \cdot R_X(\alpha) \cdot R_Z(\beta) \\ &= \begin{pmatrix} e^{i(\beta+\gamma)/2} \cdot \cos\alpha/2 & i \cdot e^{i(\gamma-\beta)} \sin\alpha/2 \\ i \cdot e^{i(\beta-\gamma)/2} \sin\alpha/2 & e^{-i(\beta+\gamma)} \cdot \cos\alpha/2 \end{pmatrix} \end{aligned}$$

→ spezialization of U_1 by setting $\beta = -\gamma$ and by multiplication with a phase factor $e^{i\phi}$ yields

$$U_2 = e^{i\phi} \cdot U_1|_{\gamma=-\beta} = \begin{pmatrix} \cos\alpha/2 \cdot e^{i\phi} & i\sin\alpha/2 \cdot e^{i(\phi-\beta)} \\ i\sin\alpha/2 \cdot e^{i(\phi+\beta)} & \cos\alpha/2 \cdot e^{i\phi} \end{pmatrix}$$

→ U_1 is universal in the following sense: by specialization of the angles $\alpha,\ \beta,\ \gamma$ one can obtain
- ⇝ the set of Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

by means of which any unitary operator on a two-state system can be specified as

$$U = I + c_x \cdot \sigma_x + c_y \cdot \sigma_y + c_z \cdot \sigma_z$$

(where c_x, c_y, c_z are complex numbers)

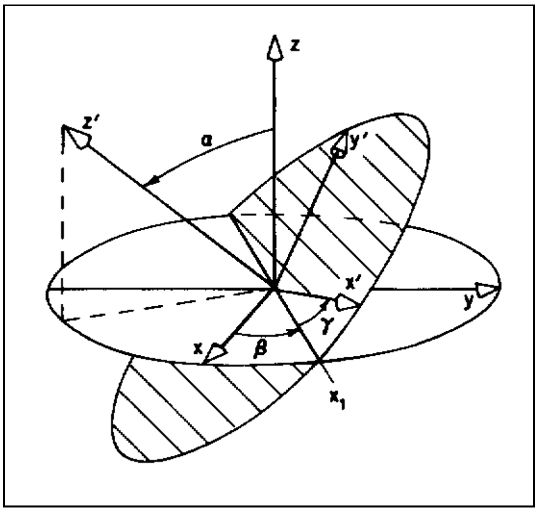


Figure 25: arbitrary rotation

$\rightsquigarrow$ one gets

$$\begin{aligned}
\sigma_x &= i \cdot U_1|_{\alpha=\pi,\,\beta=\gamma} && (= i \cdot U_2|_{\alpha=\pi,\,\beta=\phi=0}) \\
\sigma_y &= i \cdot U_1|_{\alpha=\pi,\,\beta-\gamma=\pi} && (= i \cdot U_2|_{\alpha=\pi,\,\phi=0,\,\beta=\pi/2}) \\
\sigma_z &= -i \cdot U_1|_{\alpha=0,\,\beta+\gamma=\pi} && (\text{does not work with } U_2)
\end{aligned}$$

$\rightsquigarrow$ the set of matrices

$$R_x(\theta) = \begin{pmatrix} \cos\theta/2 & i\sin\theta/2 \\ i\sin\theta/2 & \cos\theta/2 \end{pmatrix}$$

as $R_x(\theta) = U_1|_{\alpha=\theta,\,\beta=\gamma=0} (= U_2|_{\alpha=\theta,\,\phi=0})$

$$R_y(\theta) = \begin{pmatrix} i\cos\theta/2 & \sin\theta/2 \\ \sin\theta/2 & i\cos\theta/2 \end{pmatrix}$$

as $R_y(\theta) = U_2|_{\alpha=\theta,\,\phi=\beta=0}$

$$R_z(\theta) = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

as $R_z(\theta) = U_1|_{\alpha=0,\,\beta+\gamma=\theta} (= U_2|_{\alpha=\theta,\,\phi=\theta})$

$\rightarrow$ universal gates based upon specializations of U_1 include

$\rightsquigarrow$ the Deutsch gate (as generalization of the Toffoli gate)

$$D(\theta) = \begin{pmatrix} I^{(4)} & 0^{(4)} \\ 0^{(4)} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{$R_y(\theta)$}} \\ 0 & 0 & & \end{matrix} \end{pmatrix}$$

($I^{(4)}$ is the identity matrix of degree 4, $0^{(4)}$ is a 0-matrix of degree 4)

$\rightsquigarrow$ the selector | Weinfurter gate

$$S(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\pi/4}\cos\pi i/2 & e^{-i\pi/4}\sin\pi i/2 \\ 0 & 0 & e^{-i\pi/4}\sin\pi i/2 & e^{i\pi/4}\cos\pi i/2 \end{pmatrix}$$

with the property $S^2(\tau/2) = D(\pi\tau/2)$

$\rightsquigarrow$ the Barenco gate

$$A(\phi,\alpha,\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

(which uses U_2 as a submatrix)

$\rightsquigarrow$ the U gate (as an extension of the Barenco gate, another universal variant of the Toffoli gate)

$$V(\phi,\alpha,\theta) = \begin{pmatrix} 1^{(4)} & 0^{(4)} \\ 0^{(4)} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{U_2}} \\ 0 & 0 & & \end{matrix} \end{pmatrix}$$

with

$$V(\phi - \frac{\pi}{2}, 0, \beta) = \begin{pmatrix} I^{(4)} & 0^{(4)} \\ 0^{(4)} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\beta & e^{-i\phi}\sin\beta \\ 0 & 0 & e^{i\phi}\sin\beta & \cos\beta \end{matrix} \end{pmatrix}$$

and

$$R'_z(\beta) = \begin{pmatrix} I^{(4)} & 0^{(4)} \\ 0^{(4)} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{$R_z(2\beta)$}} \\ 0 & 0 & & \end{matrix} \end{pmatrix}$$

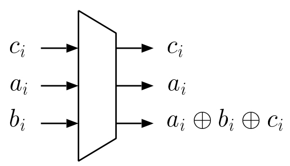
we also get $D(\theta) = R'_z(\phi/2) \cdot V(\phi, \pi/2, \phi) \cdot R'_z(-\phi/2)$

5.6 Quantum arithmetic

→ is based on two quantum gates to

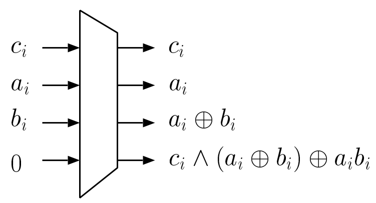
⇝ compute a qubit result from two qubits a_i, b_i and from a carry qubit c_i by means of a summation gate

$$sum(c_i, a_i, b_i) = (c_i, a_i, a_i \oplus b_i \oplus c_i)$$

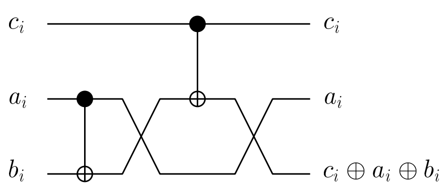


⇝ compute a qubit carry from a_i, b_i, c_i by means of a carry gate

$$carry(c_i, a_i, b_i, 0) = c_i, a_i, a_i \oplus b_i, c_i \wedge (a_i \oplus b_i) \vee a_i b_i)$$



→ realization of the sum gate ⇝ with two eor-gates (as usual) the unitary operator realized by this



gate is

$$(I \otimes B) \cdot (A_{eor} \otimes I) \cdot (I \otimes B) \cdot (I \otimes A_{eor}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

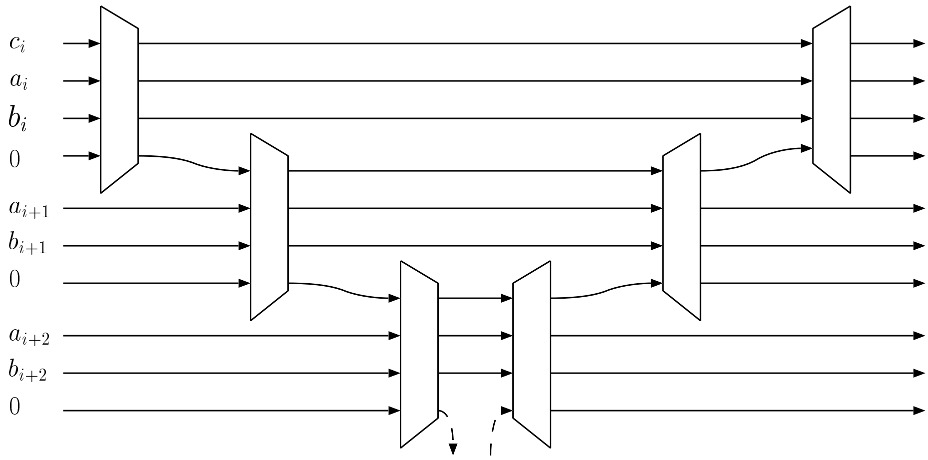


Figure 26: the complete adder (two stages)

6 Quantum States and Ensembles

The basic axioms of quantum physics as outlined in chapter 3 and formalized in chapter 2 hold for closed quantum systems that are not subject to external influences (which for all practical purposes is the universe). When considering only a small part of the universe which somehow interacts with an environment, we have to deal with the problems that

- quantum states are not pure states (cannot be represented as vectors in finite-dimensional Hilbert spaces)
- measurements are not orthogonal projections on base states
- evolution of quantum states cannot be represented by unitary operations | state transformations

6.1 The 2-qubit quantum system revisited

Let A and B be two qubits, and let $\{| \, 0 >_A, \; | \, 1 >_A\}$ and $\{| \, 0 >_B, \; | \, 1 >_B\}$ be the respective base states, and let the quantum state of both be

$$| \, \Psi >_{AB} = \alpha_{00} | \, 0 >_A | \, 0 >_B \; + \alpha_{11} | \, 1 >_A | \, 1 >_B$$

or simpler

$$| \, \Psi > = \; \alpha_{00} |00 > \; + \alpha_{11} |11 >$$

(which is an entangled state $\rightarrow$ when measuring qubit A, the state of qubit B is known (to be the same) and vice versa)

$\Rightarrow$
remember $\rightarrow$ an observable wrt standard base has the form $A = \sum_i a_i \, P_i$ where a_i is eigenvalue of

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and $P_i = \mid i >< i \mid \mid i \in \{0, 1, 2, 3\}$ is a projection onto base state i.

A measurement of qubit A only is defined by a projection

$$P_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

onto the base states 0 and 1 (or $\mid 0 >_A \mid 0 >_B$ and $\mid 0 >_A \mid 1 >_B$, respectively), resulting in an expectation value of

$$_{AB} < \Psi \mid P_{01} \mid \Psi >_{AB} = \begin{pmatrix} \alpha_{00}^* & 0 & 0 & \alpha_{11}^* \end{pmatrix} * P_{01} * \begin{pmatrix} \alpha_{00} \\ 0 \\ 0 \\ \alpha_{11} \end{pmatrix} = \alpha_{00}^2$$

(likewise, for a measurement on qubit B we get $_{AB} < \Psi \mid P_{23} \mid \Psi >_{AB} = \alpha_{11}^2$)

$\rightarrow$ An observable operating on qubit A wrt any base may be expressed as $A_A = M_A \otimes I_B$ where

- M_A is the matrix of a self-adjoint operator on qubit A
- I_B is the identity matrix acting on qubit B

The expectation value | probability of some outcome | of the observable acting on $\mid \Psi >_{AB}$ is:

$$\begin{aligned} _{AB} < \Psi | M_A \otimes I_B | \Psi >_{AB} = \quad & (\alpha_{00}^* |0 >_A \, |0 >_B \, + \alpha_{11}^* |1 >_A \, |1 >_B) * (M_A \otimes I_B) \\ & *(\alpha_{00} |0 >_A \, |0 >_B \, + \alpha_{11} |1 >_A \, |1 >_B)^T \end{aligned}$$

where

$$M_A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}; \quad I_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

respectively are matrix representations of the observable on qubit A and of the identity operation on qubit B (which is not affected by the measurement). With

$$M_A \otimes I_B = \begin{pmatrix} a_{00} & 0 & a_{01} & 0 \\ 0 & a_{00} & 0 & a_{01} \\ a_{10} & 0 & a_{11} & 0 \\ 0 & a_{10} & 0 & a_{11} \end{pmatrix}$$

as the tensor product of both matrices we get for the above expectation value

$$
{}_{AB} < \Psi \mid M_A \otimes I_B \mid \Psi >_{AB} \;=\; \begin{pmatrix} \alpha_{00}^* & 0 & 0 & \alpha_{11}^* \end{pmatrix} * \begin{pmatrix} a_{00}\alpha_{00} \\ a_{01}\alpha_{11} \\ a_{10}\alpha_{00} \\ a_{11}\alpha_{11} \end{pmatrix}
$$

$$
= |\alpha_{00}|^2 * a_{00} \;+\; |\alpha_{11}|^2 * a_{11}
$$

Using the equalities

$$
a_{00} \;=\; {}_A < 0 \mid M_A \mid 0 >_A = \begin{pmatrix} 1 & 0 \end{pmatrix} * \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} * \begin{pmatrix} 1 \\ 0 \end{pmatrix}
$$

and

$$
a_{11} \;=\; {}_A < 1 \mid M_A \mid 1 >_A = \begin{pmatrix} 0 & 1 \end{pmatrix} * \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} * \begin{pmatrix} 0 \\ 1 \end{pmatrix}
$$

this expectation value can also be denoted as

$$
{}_{AB} < \Psi | M_A \otimes I_B | \Psi >_{AB} = \alpha_{00}^2 \; {}_A < 0 | M_A | 0 >_A + \alpha_{11}^2 \; {}_A < 1 | M_A | 1 >_A
$$

a little excercise in between regarding matrix algebra: Let

$$
\mid \Phi > = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix}; \quad B \;=\; \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}
$$

then we get, on the one hand, as expectation value

$$
\begin{aligned}
< \Phi \mid B \mid \Phi > \;&=\; \begin{pmatrix} u_0^* & u_1^* \end{pmatrix} * \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} * \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \\
&=\; \begin{pmatrix} u_0^* & u_1^* \end{pmatrix} * \begin{pmatrix} b_{00} * u_0 + b_{01} * u_1 \\ b_{10} * u_0 + b_{11} * u_1 \end{pmatrix} \\
&=\; b_{00} * u_0^2 + b_{01} * u_0^* u_1 + b_{10} * u_1^* u_0 + b_{11} * u_1^2
\end{aligned}
$$

on the other hand we have

$$
\begin{aligned}
B(\mid \Phi >< \Phi \mid) \;&=\; \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} * \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \otimes \begin{pmatrix} u_0^* & u_1^* \end{pmatrix} \\
&=\; \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} * \begin{pmatrix} u_0^2 & u_0 u_1^* \\ u_1 u_0^* & u_1^2 \end{pmatrix} \\
&=\; \begin{pmatrix} b_{00}u_0^2 + b_{01}u_1u_0^* & b_{00}u_0u_1^* + b_{01}u_1^2 \\ b_{10}u_0^2 + b_{11}u_1u_0^* & b_{10}u_0u_1^* + b_{11}u_1^2 \end{pmatrix}
\end{aligned}
$$

and thus get as expectation value the trace over this matrix:

$$
< \Phi \mid B \mid \Phi > = \; trace\ (B \mid \Phi >< \Phi \mid)
$$

$\Leftarrow$

With the result of this little excercise in mind, we can now rewrite our expectation value as:

$$
\begin{aligned}
{}_{AB} < \Psi|M_A \otimes I_B|\Psi >_{AB} &= \alpha_{00}^2 \; {}_A < 0|M_A|0 >_A + \alpha_{11}^2 \; {}_A < 1|M_A|1 >_A \\
&= trace\ (M_A * (\alpha_{00}^2|0 >_A \; {}_A < 0| + \alpha_{11}^2|1 >_A \; {}_A < 1|)) \\
&= trace\ (M_A\ \rho_A)
\end{aligned}
$$

where

$$\rho_A \ = \ \alpha_{00}^2 \mid 0 >_A \; {}_A < 0 \mid \ + \ \alpha_{11}^2 \mid 1 >_A \; {}_A < 1 \mid \ = \ \begin{pmatrix} \alpha_{00}^2 & 0 \\ 0 & \alpha_{11}^2 \end{pmatrix}$$

denotes a so-called *density operator* (or *density matrix*)
Since ${}_{AB} < \Psi \mid M_A \otimes I_B \mid \Psi >_{AB} = \ trace\ (M_A\ \rho_A)$ holds for any observable M_A operating on qubit A, ρ_A may be interpreted as representing an ensemble of possible quantum states, each occuring with some specific probability:

- it is in quantum state $\mid 0 >_A$ with probability $|\alpha_{00}|^2$ or in quantum state $\mid 1 >_A$ with probability $|\alpha_{11}|^2$

M_A may be considered the projection P_A onto the relevant eigenspace of a particular observable:

$$Prob\ (a) \ = \ |\alpha_{00}|^2 \; {}_A < 0 \mid P_A \mid 0 >_A \ + |\alpha_{11}|^2 \; {}_A < 1 \mid P_A \mid 1 >_A$$

is the probability of outcome a summed over the ensemble, and weighted over the probability of each state in the ensemble.

We now extend the notion of a density operator to a pure quantum state

$$
\begin{aligned}
\mid \Phi >_{AB} \quad = \quad & \alpha_{00}\mid 0 >_A \mid 0 >_B \ + \alpha_{01}\mid 0 >_A \mid 1 >_B \\
& + \ \alpha_{10}\mid 1 >_A \mid 0 >_B \ + \alpha_{11}\mid 1 >_A \mid 1 >_B
\end{aligned}
$$

Computing the expectation value ${}_{AB} < \Phi \mid M_A \otimes I_B \mid \Phi >_{AB}$ now yields

$$
\begin{pmatrix} \alpha_{00}^* & \alpha_{01}^* & \alpha_{10}^* & \alpha_{11}^* \end{pmatrix} * \begin{pmatrix} a_{00}\alpha_{00} + a_{01}\alpha_{10} \\ a_{00}\alpha_{01} + a_{01}\alpha_{11} \\ a_{10}\alpha_{00} + a_{11}\alpha_{10} \\ a_{10}\alpha_{01} + a_{11}\alpha_{11} \end{pmatrix} = \begin{matrix} a_{00}\alpha_{00}^2 + a_{01}\alpha_{00}^*\alpha_{10} \\ +a_{00}\alpha_{01}^2 + a_{01}\alpha_{01}^*\alpha_{11} \\ +a_{10}\alpha_{00}\alpha_{10}^* + a_{11}\alpha_{10}^2 \\ +a_{10}\alpha_{01}\alpha_{11}^* + a_{11}\alpha_{11}^2 \end{matrix}
$$

The expression on the right hand side may be a little re-arranged so that

$${}_{AB} < \Phi \mid M_A \otimes I_B \mid \Phi >_{AB} = \ trace\ (M_A\ \rho'_A)$$

With $\rho'_A \ = \ trace_B\ (\mid \Phi >_{AB} \; {}_{AB} < \Phi \mid)$ and

$$
\mid \Phi >_{AB} \; {}_{AB} < \Phi \mid \quad = \quad \begin{pmatrix} \alpha_{00}^*\alpha_{00} & \alpha_{00}^*\alpha_{01} & \alpha_{00}^*\alpha_{10} & \alpha_{00}^*\alpha_{11} \\ \alpha_{01}^*\alpha_{00} & \alpha_{01}^*\alpha_{01} & \alpha_{01}^*\alpha_{10} & \alpha_{01}^*\alpha_{11} \\ \alpha_{10}^*\alpha_{00} & \alpha_{10}^*\alpha_{01} & \alpha_{10}^*\alpha_{10} & \alpha_{10}^*\alpha_{11} \\ \alpha_{11}^*\alpha_{00} & \alpha_{11}^*\alpha_{01} & \alpha_{11}^*\alpha_{10} & \alpha_{11}^*\alpha_{11} \end{pmatrix}
$$

we get

$$\rho'_A \ = \ trace_B\ (\mid \Phi >_{AB} \; {}_{AB} < \Phi \mid) = \begin{pmatrix} \alpha_{00}^*\alpha_{00} + \alpha_{01}^*\alpha_{01} & \alpha_{00}^*\alpha_{10} + \alpha_{01}^*\alpha_{11} \\ \alpha_{10}^*\alpha_{00} + \alpha_{11}^*\alpha_{01} & \alpha_{10}^*\alpha_{10} + \alpha_{11}^*\alpha_{11} \end{pmatrix}$$

where $trace_B$ denotes the partial trace over the subsystem B of the density matrix of the combined system AB

$$\begin{aligned} \textit{trace}\ (M_A\ \rho'_A) \quad = \quad & a_{00}(\alpha_{00}^2 + \alpha_{01}^2)\ +\ a_{01}(\alpha_{10}^* + \alpha_{11}^*\alpha_{01}) \\ & + a_{10}(\alpha_{10}^*\alpha_{00} + \alpha_{11}^*\alpha_{01})\ +\ a_{11}(\alpha_{10}^* + \alpha_{11}^*\alpha_{11}) \end{aligned}$$

which is as above,i.e., we have indeed

$$_{AB} < \Phi \mid M_A \otimes I_B \mid \Phi >_{AB} = \textit{trace}\ (M_A\ \rho'_A)$$

$\rightarrow$ ρ'_A operates on the subsystem made up by the qubit A

Example for the interpretation of the density matrix ρ_A of an entangled quantum state:
Suppose we have the quantum states

$$\mid 0' >= \frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >) \text{ and } \mid 1' >= \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >)$$

(which in fact is the dual (or Hadamard) base), then measurements relative to the standard base $\mid 0 >, \mid 1 >$ yield

$$< 0' \mid P_0 \mid 0' > = \frac{1}{2} \ \mid \ < 1' \mid P_1 \mid 1' > = \frac{1}{2},$$

with the projections

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad .$$

Measurements of the states

$$\frac{1}{\sqrt{2}}(\mid 0' > + \mid 1' >) \ \mid \ \frac{1}{\sqrt{2}}(\mid 0' > - \mid 1' >)$$

relative to the base $\mid 0 >, \mid 1 >$ yield

$$\frac{1}{\sqrt{2}}(\mid 0' > + \mid 1' >) \ = \ \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >) \ + \ \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >)) \ = \ \mid 0 >$$

and $< 0 \mid P_0 \mid 0 > = 1$, and likewise $< 1 \mid P_1 \mid 1 > = 1$.

The ensemble in which $\mid 0 >$ and $\mid 1 >$ occur with probability $\frac{1}{2}$ is given by

$$\rho \ = \ \frac{1}{2}(\mid 0 >< 0 \mid \ + \ \mid 1 >< 1 \mid) \ = \ \frac{1}{2} * I$$

and the projection onto $\mid 0' >$ is given as

$$\textit{trace}\ (\mid 0' >< 0' \mid \rho) \ = \ \frac{1}{2}$$

$\Leftarrow$
Interpretation of density matrices
Comparing ρ_A and ρ'_A, it may be noted that

- in ρ_A there are only diagonal elements different from zero, and that ρ_A represents an entangled state

  $$\mid \Psi >_{AB} = \alpha_{00} \mid 00 > \ + \alpha_{11} \mid 11 >$$

  which cannot be expressed as the tensor product of two component parts (or matrices of lesser dimensionalities).

- in ρ'_A all elements are non-zero, representing an unentangled (or pure) state

$$\mid \Phi >_{AB} = \alpha_{00} \mid 00 > + \alpha_{01} \mid 01 > + \alpha_{10} \mid 10 > + \alpha_{11} \mid 11 >$$

which may be expressed as the tensor product of two component parts $\mid \Phi >_{AB} = \mid \phi >_A \otimes \mid \phi >_B$ with $\mid \phi >_A = \alpha_0 \mid 0 > + \alpha_1 \mid 1 >$ and $\mid \phi >_B = \beta \mid 0 > + \beta \mid 1 >$

$\rightarrow \mid \Phi >_{AB}$ is called a pure state
$\rightarrow \mid \Psi >_{AB}$ is called a mixed (or entangled) state

Density matrices provide a more compact description of mixed states versus pure states. Pure states are also called coherent (wrt superposition of probability amplitudes), mixed states are decohering $\rightarrow$ the non-diagonal elements of the density matrix are gradually disappearing over time.

6.2 Bipartite quantum systems

We will now generalize the notion of a density operator | density matrix to quantum systems of some $(n + m)$ qubits, of which the first n qubits that make up the subsystem A are observable (or subject to measurements), whereas the remaining m qubits if the subsystem B are somehow hidden (or inaccessible to measurements).

The Hilbert space H of such a bipartite quantum system partitions into two subspaces H_A with base $\{\mid i >_A\}$ and H_B with base $\{\mid j >_B\}$ so that $H = H_A \otimes H_B$ with an orthonormal base $\{\mid i >_A \otimes \mid j >_B\}$.

A pure quantum state in H may be denoted as

$$\mid \Psi >_{AB} = \sum_{i,j} \alpha_{ij} \mid i >_A \mid j >_B$$

with $\sum_{i,j} \mid \alpha_{ij} \mid^2 = 1$.

For the expectation value of an observable $M_A \otimes I_B$ acting on the subsystem A we get, very similar to the 2 qubit system,

$${}_{AB} < \Psi \mid M_A \otimes I_B \mid \Psi >_{AB} = \sum_{i,j,k} \alpha^*_{ik} \alpha_{jk} \; {}_A < i \mid M_A \mid j >_A = trace\,(M_A\, \rho_A)$$

with

$$\rho_A = trace_B(\mid \Psi >_{AB} \; {}_{AB} < \Psi \mid) = \sum_{i,j,k} \alpha^*_{ik} \alpha_{jk} \mid i >_A \; {}_A < j \mid$$

From this definition it follows immediately that

- ρ_A is self-adjoint $\rightarrow \rho_A = \rho^*_A$
- ρ_A is positive $\rightarrow {}_A < \Psi \mid \rho_A \mid \Psi >_A \geq 0$ for any state $\mid \Psi >_A$
- $trace\,(\rho_A) = 1$

which means that ρ_A may be diagonalized, all eigenvalues are real and non-negative, and the sum over all eigenvalues is one.

We consider now a quantum system as being composed of an accessible subsystem A that is embedded in a larger system $A \otimes B$. Then we may have

- a state $\mid \Psi >_{AB}$ that is pure in $H_A \otimes H_B$ but not necessarily pure in H_A alone;

- a state $\mid \Psi >_A$ that is pure in H_A, in which case the density matrix becomes $\rho_A \; = \; \mid \Psi >_A \; {}_A < \Psi \mid$, and ρ_A is a projection on the one-dimensional space made up by $\mid \Psi >_A$;
- a density matrix ρ_A of a pure state that has the property $\rho_A * \rho_A \; = \; \rho_A$ since we have

$$\mid \Psi >_A \; {}_A < \Psi \mid \Psi >_A \; {}_A < \Psi \mid \; = \; \mid \Psi >_A \; {}_A < \Psi \mid$$

and $\mid \Psi >_A \; {}_A < \Psi \mid \; = \; 1$.

A density matrix represented in the basis $\{\mid \Psi >_i\}$ in which it is diagonal has the form

$$\rho_A \; = \; \sum_i p_i \mid \Psi_i >< \Psi_i \mid$$

with $0 \leq p_i \leq 1$ and $\sum_i p_i \; = \; 1$. A pure state has just one term in this sum; the state is not pure if there is more than one term in the sum and

$$\rho_A^2 \; = \; \sum_i p_i^2 < \sum_i p_i \; = \; 1 \quad (\text{or} \quad \rho_A^2 \; \neq \; \rho_A)$$

The expectation value of any observable M operating on some subsystem can be written as

$$< M > = \; trace \, (M \; \rho) \; = \; \sum_i p_i < \Psi_i \mid M \mid \Psi_i >$$

and ρ may be considered an ensemble of pure quantum states, in which each state $\mid \Psi_i >$ occurs with probability p_i.

Example: Let A be a single qubit (or a two-state subsystem), and let $\mid \Psi >_{AB}$ be a pure state of the entire quantum system, then we have (as above)

$$\rho_A' \; = \; trace_B \, (\mid \Phi >_{AB} \; {}_{AB} < \Phi \mid) \; = \; \begin{pmatrix} \alpha_{00}^* \alpha_{00} + \alpha_{01}^* \alpha_{01} & \alpha_{00}^* \alpha_{10} + \alpha_{01}^* \alpha_{11} \\ \alpha_{10}^* \alpha_{00} + \alpha_{11}^* \alpha_{01} & \alpha_{10}^* \alpha_{10} + \alpha_{11}^* \alpha_{11} \end{pmatrix}$$

Assuming, for reasons of simplicity, that

$$|\alpha_{00}|^2 \; + \; |\alpha_{01}|^2 \; = \; |\alpha_{10}|^2 \; + \; |\alpha_{11}|^2 \; = \; \frac{1}{2}$$

and

$$\alpha_{10}^* \alpha_{00} \; + \; \alpha_{11}^* \alpha_{01} \; = \; \alpha_{00}^* \alpha_{10} \; + \; \alpha_{01}^* \alpha_{11} \; = \; -\frac{1}{2}$$

we take as values for the probability amplitudes

$$\alpha_{00} \; = \; \alpha_{11} \; = \; \frac{1}{2} \; || \; \alpha_{01} \; = \; \alpha_{10} \; = \; -\frac{1}{2}$$

This, in turn, results in a density matrix ρ_A with the property

$$\rho_A * \rho_A \; = \; \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} * \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \; = \; \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \; = \; \rho_A$$

i.e., we have a pure quantum system. Diagonalization of this matrix (which is possible since it is symmetric wrt the diagonal axis) requires first computing its eigenvalues as

$$det \, (\rho_A \; - \; \lambda \, I) \; = \; 0$$

i.e., we have

$$det \begin{pmatrix} \frac{1}{2}-\lambda & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2}-\lambda \end{pmatrix} = ((\frac{1}{2})^2 - \lambda + \lambda^2) - (-\frac{1}{2})^2 = 0$$

for which we get as a non-trivial solution $\lambda_0 = 1$ and as a trivial solution $\lambda_1 = 0$. Both solutions are required to form a diagonalization matrix C with the property

$$C^T * \rho_A * C = \rho_D$$

The column vectors of C happen to be the eigenvectors of ρ_A associated with the eigenvalues λ_0 and λ_1. These eigenvectors may be obtained as solutions of the equation

$$(\rho_A - \lambda I) \mid \phi_0\, \phi_1 >= 0$$

For $\lambda_0 = 1$ we get

$$\begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix} * \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix} = 0 \rightarrow \begin{pmatrix} -1 \\ 1 \end{pmatrix} \mid \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

and for $\lambda_1 = 0$ we get

$$\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} * \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix} = 0 \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

From these two column vectors we obtain a diagonalization matrix as $C = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, and from $C^T * \rho_A * C = \rho_D$ we get

$$\rho_D = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} * \frac{1}{2} \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} * \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

which results in the diagonalized density matrix $\rho_D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.
Computing the eigenvalues for ρ_D from the equation

$$det \begin{pmatrix} 1-\lambda & 0 \\ 0 & 1-\lambda \end{pmatrix} = \lambda^2 - \lambda = 0$$

again yields the non-trivial solution $\lambda_0 = 1$ and the trivial solution $\lambda_1 = 0$.

From this density matrix (which has the general form

$$\rho_D = \sum_i p_i \mid \Psi_i >< \Psi_i \mid$$

and just one non-zero diagonal element) we can immediately conclude that $\mid \Psi_1 > = \mid 0 >$ and $p_1 = 1$, i.e., we have indeed a pure state.
This contrasts withy the entangled state $\mid \Psi >_{AB} = \alpha_{00} \mid 00 > + \alpha_{11} \mid 11 >$ which features a density matrix $\rho_A = \begin{pmatrix} |\alpha_{00}|^2 & 0 \\ 0 & |\alpha_{11}|^2 \end{pmatrix} = \rho_D$ which is already diagonal. However, it has more than one diagonal element different from zero, and can therefore composed as $\rho_D = \sum_{i=0,1} p_i \mid \Psi_i > < \Psi_i \mid$ with $p_0 = |\alpha_{00}|^2$ — $\mid \Psi_0 >= \mid 0 >$ and $p_1 = |\alpha_{11}|^2$ — $\mid \Psi_1 >= \mid 1 >$

$\Leftarrow$

6.3 Quantum entanglement

As we have seen in the preceding subsection,

- a state in $H = H_A \otimes H_B$ is entangled (or non-separable) if its density matrix has more than one non-zero eigenvalue (or its diagonalized density matrix has more than one non-zero diagonal element), otherwise the state is unentangled (or pure);

- a separable bipartite pure state $| \Psi >_{AB}$ is a tensor product of pure states $| \phi >_A$ and $| \phi >_B$ in H_A and H_B, respectively $\rightarrow$ $| \Phi >_{AB} = | \phi >_A \otimes | \phi >_B$; the reduced density matrices $\rho_A = | \phi >_A \ {}_A < \phi |$ and $\rho_B = | \phi >_B \ {}_B < \phi |$ are then pure as well;

- any state that cannot be expressed in this form is entangled $\rightarrow$ the density matrices ρ_A and ρ_B are in a mixed state.

Entanglement between the subsystems A and B comes about by close interaction; local transformations of the form $U_A \otimes U_B$ cannot increase the number of eigenvalues of the state $| \Psi >_{AB}$. Entanglement requires a global operation that cannot be represented as a tensor product of two operations on the partitions A and B (or on the Hilbert spaces H_A and H_B).

7 Quantum Algorithms

are to solve computational problems by networks composed of elementary quantum operations | circuits. The design of quantum algorithms consists in de-composing a complex unitary transformation | operation into tensor or matrix products of simple | elementary operations which perform local changes on quantum states.

Let $| \Phi >$ and $| \Psi >$ be initial and final states of a quantum computation U_T, then the art of designing a quantum algorithm that realizes U_T is to construct some sequence of elementary unitary operations | transformations $U_1, U_2, \ldots, U_s$ such that

$$| \Psi > = U_T | \Phi > = U_s U_{s-1} \ldots U_2 U_1 | \Phi >$$

If $| \Phi >$ is a pure state defined as $| \Phi >= \sum_{i=1}^{2^n-1} \alpha_i | i >$ and for all $i \in \{0, \ldots, 2^n - 1\}$ we have $\alpha_i = \frac{1}{\sqrt{2^n}}$, then U_T operates on the superposition of all base states in $| \Phi >$ simultaneously $\rightarrow$ which is also referred to as quantum parallelism. It trades exponential complexity in time of classical algorithms for exponentiality in quantum states, which may lead to considerable speed-ups of classical over quantum computations. In particular, we may have

- non-exponential speed-ups which can be achieved with some class of algorithms that merely separates the world of classical from quantum computable problems $\rightarrow$ an example being the quantum search through an unsorted data base;

- relative exponential speed-ups which apply to the class of so-called oracles $\rightarrow$ finding out what quantum black boxes (circuits) are doing (which function they realize) by feeding them with some well prepared superimposed quantum state $\rightarrow$ an example being finding out the periodicity of a two-to-one mapping;

- truly exponential speed-ups for computationally hard (in a classical sense intractable) problems $\rightarrow$ exponential complexity in time can be reduced to polynomial time $\rightarrow$ an example is Shor's factoring algorithm for very large numbers.

7.1 On the accuracy of unitary operations

There is some degree of inaccuracy in all unitary quantum operations which is bound to introduce compounding errors into computations. Instead of a purely unitary operation on a pure state we get

$$|\ \overline{\Psi_T} > = \ |\ \Psi_T > \ + |\ \Delta_T > = \ \overline{U_T}|\ \Phi >$$

or, on a stepwise basis

$$|\ \overline{\Psi_s} > = \ |\ \Psi_s > \ + |\ \Delta_s > = \ \overline{U_s}|\ \Psi_{s-1} >$$

with $|\ \Delta_s > = \ (\overline{U_s} - U_s)|\ \Psi_{s-1} >$ as the deviation of state $|\ \overline{\Psi_s} >$ from the correct state $|\ \Psi_s >$. The errors effect slight changes in the angle between $|\ \Psi_s >$ and $|\ \overline{\Psi_s} >$. If all errors add up in the same direction, we get

$$||\ |\ \overline{\Psi_s} > -|\ \Psi_s >||\ \leq\ \sum_{i=1}^{s} ||\ |\ \Delta_i >||$$

If the deviation is bounded as $||\overline{U_s} - U_s|| \leq \epsilon$, then we have, after some s operations in sequence,

$$||\ |\ \overline{\Psi_s} > \ - |\ \Psi_s >||\ \leq\ s * \epsilon$$

i.e., the angular distance between $|\ \overline{\Psi_s} >$ and $|\ \Psi_s >$ increases at most by order of ϵ.

7.2 Reversible algorithmic computations

Classical computations on the contents of some n-bit register have the form:

$$f : \{\ 0,\ 1\}^n\ \rightarrow\ \{\ 0,\ 1\}^m$$

with f mapping the contents of an n-bit register into an m-bit register. Such computations may not be reversible as information contained in the domain value may get lost when transforming it into the result value $\rightarrow$ the mapping is injective.

The general scheme for making such computations reversible, which is what quantum computations inherently do, is to apply to the contents of an $(n+m)$-register a function F as follows:

$$F : (\ x,\ 0^{(m)}\ )\ \rightarrow\ (\ x,\ f(\ x\ )\ )$$

where $x \in \{\ 0,\ 1\ \}^n$, and $0^{(m)}\ =\ \overline{0}$ is the m-fold Cartesian product of 0. The function F realizes a one-to-one (bijective) mapping of inputs to outputs, as the input x uniquely distinguishes all outputs even if $f(\ x\ )$ is injective.

Example: Computing $f(\ f(\ f(\ \ldots\ f(\ x\ )\ \ldots\ )\ )\ )$, i.e., a k-fold nesting of applications of f to x, can be done quantum mechanically with a one-to-one recursive function

$$\begin{array}{rcl} F(\ x,\ \overline{0}^k\ ) & \rightarrow & (\ x,\ F(\ f(\ x\ ), \overline{0}^{k-1}\ )\ ) \\ F(\ x,\ \overline{0}\ ) & \rightarrow & (\ x,\ x\ ) \end{array}$$

The garbage produced by the recursive application of F in terms of intermediate function values may be removed | collected by application of the reverse function F^{-1}:

$$\begin{array}{rcl} F^{-1}(\ f(\ x\ ),\ \overline{0}^{k-1}\ ) & \rightarrow & (\ x, \overline{0}^k\ ) \\ F(\ x,\ x\ ) & \rightarrow & (\ x,\ x\ ) \end{array}$$

The full computation, including garbage collection, may thus be specified as:

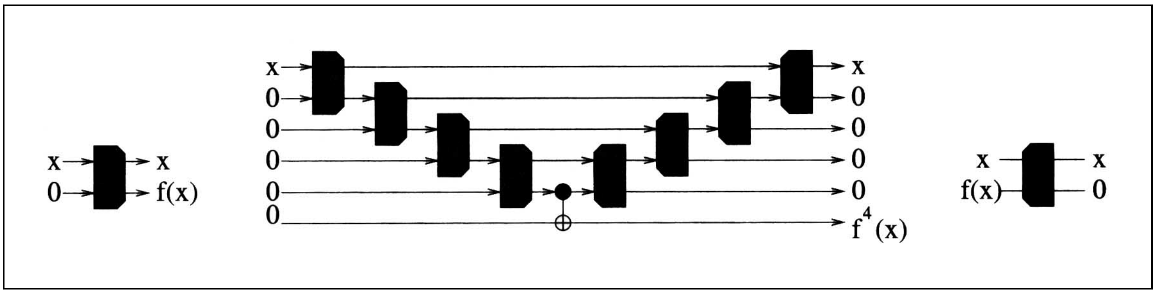


Figure 27: reversible computation with garbage removal

$$F(\ x,\ \overline{0}^k\ )\quad\rightarrow\quad F^{-1}(\ x,\ F(\ f(\ x\ ),\overline{0}^{k-1}\ )\ )$$

(the application $F(\ x,\ x\ )$ that terminates the recursive expansion is not reversed as its function value must be forwarded as the output value of the entire computation).

A quantum circuit implementing this computation for $k = 3$ is shown in fig. 27.

A more general one-to-one function which duplicates a function call and also takes care of garbage has the following form:

- $F(\ x,\ \overline{0},\ \overline{0})\ \rightarrow\ (\ x,\ g(\ x\ ),\ f(\ x\ )\ )$
  (with $g(\ x\ )$ being the function that produces the garbage);
- $D(\ x,\ g(\ x\ ),\ f(\ x\ ),\overline{0}\ )\ \rightarrow\ (\ x,\ g(\ x\ ),\ f(\ x\ ),\ f(\ x\ )\ )$
  (the function that transports the garbage and duplicates $f(\ x\ )$);
- and the respective reverse functions
  $F^{-1}(\ x,\ g(\ x\ ),\ f(\ x\ )\ )\ \rightarrow\ (\ x,\overline{0},\ \overline{0}\ )$
  $D^{-1}(\ x,\ g(\ x\ ),\ f(\ x\ ),\ f(\ x\ )\ )\ \rightarrow\ (\ x,\ g(\ x\ ),\ f(\ x\ ),\ \overline{0}\ )$

(an example of applying such function is the adder circuit given in figure 26).

7.3 The Deutsch problem

is a very simple problem to get acquainted with the intricacies of constructing quantum algorithms. Given a black box that realizes a binary function $f : \{\ 0,\ 1\ \} \rightarrow \{\ 0,\ 1\ \}$, the problem is to find out whether f is

- a constant function with the property $f(\ 0\ ) \oplus f(\ 1\ ) = 0$ (i.e., it returns 0 for all argument values), or
- a balanced function with the property $f(\ 0\ ) \oplus f(\ 1\ ) = 1$ (i.e., it returns 0 for one half of the argument values and 1 for the other half).

In a classical system, it would take two tests (with input values 0 and 1) in succession to find the answer; in a quantum system the answer may be found by means of just one superimposed input, using the following steps:

1. apply the Hadamard transformation to the input $|0 > |1 >$, yielding the quantum state
   $$H_H|\ 0 > \otimes H_H|\ 1 > = \frac{1}{2}(\ (\ |\ 0 >\ +|\ 1 >) \otimes (\ |\ 0 >\ -|\ 1 >\ )$$
2. apply to this state the unitary operator
   $$U_f : |\ x > \otimes |\ y > \rightarrow\ |\ x >\ \otimes |\ y \oplus f(\ x\ ) >$$
   (which realizes the function F of the preceding section for all inputs $x, y \in \{0,1\}$) to obtain:

$$
\begin{aligned}
U_f(\tfrac{1}{2} (| 0 > + | 1 >) \otimes (| 0 > - | 1 >)) & \\
= \tfrac{1}{2} ((| 0 > \otimes (| 0 \oplus f(0) > - | 1 \oplus f(0) >)) & \\
+ (| 1 > \otimes (| 0 \oplus f(1) > - | 1 \oplus f(1) >))) &
\end{aligned}
$$

This quantum state allows for the following interpretation wrt to the values of the function f:

if $f(0) = f(1) = 0$ then
$\rightarrow \frac{1}{2}(| 0 > (| 0 > - | 1 >) + | 1 > (| 0 > - | 1 >))$
$= \frac{1}{2}(| 0 > + | 1 >) \otimes (| 0 > - | 1 >) = | 0'1' >$

if $f(0) = f(1) = 1$ then
$\rightarrow \frac{1}{2}(| 0 > + | 1 >) \otimes (| 1 > - | 0 >) = -| 0'1' >$

if $f(0) = 0$; $f(1) = 1$ then
$\rightarrow \frac{1}{2}(| 0 > - | 1 >) \otimes (| 0 > - | 1 >) = | 1'1' >$

if $f(0) = 1$; $f(1) = 0$ then
$\rightarrow \frac{1}{2}(| 0 > - | 1 >) \otimes (| 1 > - | 0 >) = -| 1'1' >$

i.e., we obtain in all cases base states wrt the dual basis.

3. following this interpretation, all it takes to find out what the black box is doing is to measure the first of the quantum bits wrt the dual basis. We thus otain
$\rightarrow$ $| 0' >$ with probability 1 if $f(0) \oplus f(1) = 0$, i.e., the function f is constant;
$\rightarrow$ $| 1' >$ with probability 1 if $f(0) \oplus f(1) = 1$, i.e., the function f is balanced.

7.4 The Deutsch–Josza problem

is a generalization of the Deutsch problem $\rightarrow$ finding out whether a black box function

$$f : \{ 0, 1\}^n \rightarrow \{ 0, 1\}$$

is constant (all outputs are zero) or balanced (the outputs of half the inputs are zero, the outputs of the other half are one).

To get a crack at this problem, we need another operation

$$V_f \, | x > \rightarrow (-1)^{f(x)} | x >$$

which changes the sign of $| x >$ if $f(x) = 1$ and leaves it unchanged if $f(x) = 0$. This operation may be realized by means of the operator U_f as

$$
\begin{aligned}
U_f | x, \tfrac{1}{\sqrt{2}}(| 0 > - | 1 >) > &= \tfrac{1}{\sqrt{2}}(| x, 0 \oplus f(x) > - | x, 1 \oplus f(x) >) \\
&= (- 1)^{f(x)} | x, \tfrac{1}{\sqrt{2}}(| 0 > - | 1 >) >
\end{aligned}
$$

using $| \frac{1}{\sqrt{2}}(| 0 > - | 1 >) >$ as an additional qubit which is just being passed through.

With classical circuitry, the solution to this problem would require applying all 2^n input patterns $x \in \{ 0, 1 \}^n$ in succession.

The quantum solution consists in the following unitary transformations:

1. apply the Hadamard transformation $H_H^{(n)}$ to the input $\mid 0^{(n)} >$ to obtain the randomized quantum state
$$\mid \Phi > = H_H^{(n)} \mid 0^{(n)} > = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \mid i >$$
2. apply to this state the unitary transformation V_f;
$$V_f \mid \Phi > = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(\,i\,)} \mid i > = \mid \Phi' >$$
which transfers the values of $f(\,i\,)$ to the amplitudes of $\mid \Phi' >$.
3. measure $\mid \Phi' >$ relative to the one-dimensional subspace spanned by
$$\mid \Psi_a > = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \mid i >$$
and relative to a subspace orthogonal to $\mid \Psi_a >$, in which we have a vector $\mid \Psi_b >$. The projection of $\mid \Phi' >$ onto $\mid \Psi_a >$ and $\mid \Psi_b >$ clearly has the form
$$\mid \Phi' > = \alpha \mid \Psi_a > + \beta \mid \Psi_b > \quad \text{with } \mid \alpha \mid^2 + \mid \beta \mid^2 = 1$$
4. determine α by a projection
$$\alpha = < \Psi_a \mid \Phi' > = \left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} < i \mid \right) \left(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{f(\,j\,)} \mid j > \right)$$
or
$$\alpha = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} (-1)^{f(\,j\,)} < i \mid j >$$
Since we have $< i \mid j > = I$, this term can be further simplified to
$$\alpha = \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{f(\,i\,)}$$
Following this formula, we conclude that
$\rightarrow$ if $f(\,x\,)$ is balanced, then we have the same number of 1's and (-1)'s, i.e., $\alpha = 0$, and the measurement returns the outcome b with probability $\mid \beta \mid^2 = 1$;
$\rightarrow$ if $f(\,x\,)$ is constant, then $\alpha = 1$ or $\alpha = -1$ (depending on whether $f(\,x\,) = 0$ or $f(\,x\,) = 1$, respectively), i.e., the measurement returns the outcome a with probability $\mid \alpha \mid^2 = 1$.

7.5 Simon's problem

We consider now a black box that computes some function
$$f : \{\,0,\;1\}^n \rightarrow \{\,0,\;1\}^n$$
of which two things are known:

- it is a two-to-one function, meaning that exactly two different input values are mapped into one output value;
- the function has a period $a \in \{\,0,\;1\}^n$ such that for all $x \in \{0,1\}^n : f(x) = f(x \oplus a)$.

The problem consists in finding the period a.

The classical solution to this problem is hard. We need to find pairs of elements $x,\ y \in \{\ 0,\ 1\}^n$ so that $f(\ x\ ) = f(\ y\ )$ and $x \oplus a = y$. If we were to choose $2^{n/4}$ input patterns | queries, then the number of pairs to be formed with these patterns | queries would be $(2^{n/4})^2\ =\ 2^{n/2}$. For each pair of patterns the probability that $x \oplus a = y$ would be 2^{-n}, i.e., the probability of finding such a pair among those $2^{n/2}$ pairs would be $2^{-n/2}$ → the chances of finding such a pair even with exponential searches would be pretty small.

In contrast, the quantum mechanical solution to this problem takes just some polynomial number of queries; the steps to do so are the following:

1. prepare two quantum registers of n qubits each with the state $|\ 0^{(n)} > |\ 0^{(n)} >$
2. apply the Hadamard transformation to the first register to obtain
$$H_H^{(n)}\ |\ 0^{(n)} > \otimes I\ |\ 0^{(n)} > = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\ x > |\ 0^{(n)} >$$
3. applying the operator U_f to the resulting state yields
$$U_f\ (\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\ x > |\ 0^{(n)} >\ )\ =\ (\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\ x > |\ f(\ x\ ) >)$$
Suppose we would now measure the second register, then we would obtain some function value, say $f(\ x_0\ )$, with probability 2^{-n}. However, with a two-to-one mapping realized by f, $f(\ x_0\ )$ would be the result of mapping both $f(\ x_0\ )$ and $f(\ x_0\ \oplus a\ )$, i.e., the first register must necessarily be in the state $\frac{1}{\sqrt{2}}(|\ x_0 >\ + |\ x_0\ +\ a >)$ after the measurement → measuring the first register in this state would yield either $|\ x_0 >$ or $|\ x_0\ +\ a >$ with probability $1/2$, neither of which would help to determine the value of a.
However →
4. when applying once more, before measurement, the Hadamard transformation $H_H^{(n)}$ to the first register, we obtain
$$H_H^{(n)}\ |\ \frac{1}{\sqrt{2}}(|\ x_0 >\ + |\ x_0\ +\ a >) > = \frac{1}{\sqrt{2^{(n-1)}}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 * y} + (-1)^{(x_0+a)*y})\ |\ y >$$
with $x * y\ =\ x_0 * y_0\ \oplus x_1 * y_1\ \oplus\ \ldots\ \oplus x_{n-1} * y_{n-1}$.
Now,
→ if $a * y\ =\ 1$ we have $(-1)^{x_0 * y} + (-1)^{(x_0 \oplus 1)*y}\ =\ 0$
→ if $a * y\ =\ 0$ we have $(-1)^{x_0 * y} + (-1)^{x_0 * y}\ = \begin{cases} -1 & \text{if } x_0 * y = 1 \\ 1 & \text{if } x_0 * y = 0 \end{cases}$
In the latter case, the outcome of the measurement is then selected randomly from all possible values for y such that $y * a = 0$, of which each has probability $\frac{1}{2^{(n-1)}}$.
We may hope to find different values for y when running the algorithm repeatedly; once we have n equations of the form $y_i * a = 0$, a can be uniquely determined → the algorithm thus has complexity $O(\ n\ )$.

7.6 Quantum Searching → Grover's search algorithm

The problem to be solved here consists in finding in some unsorted list | data base of some N items a single item that meets some specific property → an example being the search for a string $\omega \in \{\ 0,\ 1\}^n$ within a set of 2^n possible strings.

The search function may be defined as

$$f_\omega(x) = \begin{cases} 1 \; if \; x = \omega \\ 0 \; if \; x \neq \omega \end{cases}$$

which is a typical oracle function → when submitting some value x to the oracle, it decides whether or not $x = \omega$.

A classical search would take $N/2$ steps on average; a quantum search may be performed as follows: Applying the operator V_{f_ω} to $\mid x >$ yields

$V_{f_\omega} \mid x >= (-1)^{f_\omega(x)} \mid x >$ or $V_{f_\omega} = I - 2 * \mid \omega > \mid \omega >$

Now, if $\mid x >= \mid \omega >$ then

$V_{f_\omega} \mid \omega >= I \mid \omega > -2 * \mid \omega >< \omega \mid \omega >= I \mid \omega > -2 * \mid \omega > = - \mid \omega >$

but if $\mid x > \neq \mid \omega >$ then we have $V_{f_\omega} \mid x >= I \mid x > -2 * \mid \omega >< \omega \mid x >= I \mid x >= \mid x >$
since ω and x are orthogonal to each other if different.

Thus the oracle V_{f_ω} flips the sign of $\mid x >$ if $\mid x >= \mid \omega >$ but operates trivially on all $\mid x > \neq \mid \omega >$, with the following interpretation:

When operating on some vector $\mid x >$ in H^{2^n}, V_{f_ω} reflects it about the hyperplane orthogonal to $\mid \omega >$. We know that the reflection is performed for some base state $\mid \omega >$, but nothing is known about the string ω itself. The problem is to determine ω by pushing up its probability by consulting the oracle several times.
Here are the steps of this so-called Grover iteration:

1. create a perfect random state
$$\mid \Phi > = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \mid x >$$
by application of the Hadamard transformation to the state $\mid 0^{(n)} >$. We know about $\mid \omega >$ at least that it is a base state, which means that $\mid < \omega \mid \Phi > \mid = \frac{1}{\sqrt{2^n}}$ irrespective of what $\mid \omega >$ actually is.

   Measuring the state $\mid \Phi >$ by projection onto its base $\{ \mid x > \}$ would return the state $\mid \omega >$ only with probability $1/N$ (as all other base states).

2. combine the unknown reflection V_{f_ω} with some known reflection $V_\Phi = 2 * \mid \Phi >< \Phi \mid - I$ and apply it as
$$V_\Phi \mid x > = 2 * \mid \Phi >< \Phi \mid x > - I \mid x > = - \mid x >$$
It flips the sign of $\mid x >$ if it is orthogonal to $\mid \Phi >$ (since then $< \Phi \mid x > = 0$), and preserves the sign of $\mid x >$ if $\mid x > = \mid \Phi >$ (since then we have $< \Phi \mid \Phi > = I$).

   → Acting on some arbitrary vector, V_Φ preserves the component along $\mid \Phi >$ but flips all components in the hyperplane orthogonal to $\mid \Phi >$.

3. apply the operator $R_{grov} = V_\Phi * V_{f_\omega}$ to some vector $\mid x >$ with the following effect:
→ the vectors $\mid \Phi >$ and $\mid \omega >$ span a plane in H^{2^n}, with a vector $\mid \omega^\perp >$ that is orthogonal to $\mid \omega >$ in that plane;
→ any vector $\mid x >$ in that plane is by V_{f_ω} flipped about $\mid \omega^\perp >$ and by V_Φ flipped about $\mid \Phi >$

   To understand what this means, consider the geometry in a two-dimensional Hilbert space shown in fig. 28. Here we have the following angular relationships:

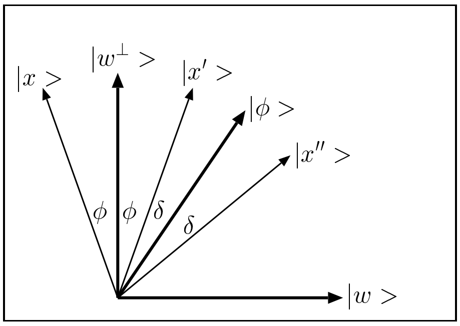


Figure 28: 2D visualisation of a grover iteration

$\rightarrow$ the angle between $| \Phi >$ and $| \omega >$ is given as $< \Phi | \omega > = 1/\sqrt{2^n} = \cos(\pi/2 - \theta) = \sin\theta$
$\rightarrow$ a vector $| x >$ is by V_{f_ω} flipped about $| \omega^{\perp} >$ and thereby changes its angle by $2 * \phi$ (with ϕ being the angle between $| x >$ and $| \omega^{\perp} >$);
$\rightarrow$ the vector $V_{f_\omega} | x >$ is by V_Φ flipped about $| \Phi >$, thus changing its angle by $2 * \delta$;
$\rightarrow$ the total change of angle effected by $V_\Phi * V_{f_\omega}$ is thus $2 * \phi + 2 * \delta = 2 * \theta$, which is the effect of one Grover iteration.

4. repeat the Grover iteration until the probability of finding the input item in the data base approaches the value 1.

Example: Assuming that the data base contains just 4 items, a classical sequential search would require 2 steps on average to find a particular item. A quantum-mechanical search for an item $| x > = | s >$ would set out with $| < s | \omega > | = 1/\sqrt{4} = \sin(\theta) = 1/2$, which means that $\theta = 30^o$. A rotation by $2 * \theta = 60^o$ brings $| s >$ into a 90^o angle with $| \omega^{\perp} >$, or in line with $| \omega >$. Measuring at this point $V_\Phi * V_{f_\omega} | s >$ wrt the standard basis yields $| \omega >$ with probability 1.

$\Leftarrow$

For the general case of finding one item in a set of 2^n items we simply assume that we need some r iterations to bring $| \Phi >$ close to $| \omega >$ (or to turn it away from $| \omega^{\perp} >$ by an angle of $\pi/2$). After r iterations we thus get a rotation by $\theta + 2r * \theta = \pi/2a$, or $2 * r + 1 = \pi/2 * \theta$. Since $\sin\theta = \theta = 1/2^n$, we may choose $r = (\pi/4) * \sqrt{2^n} * (1 + O(N^{-1/2}))$ to obtain as the result of a measurement $| \omega >$ with probability

$$Prob(\omega) = \sin^2((2 * r + 1) * \theta) = 1 - O(2^{-n})$$

i.e., only some $(\pi/4) * \sqrt{2^n}$ queries | iterations are required to find $| \omega >$ with high probability.

7.7 Searching through distributed data bases

The problem here is the following: there are two people, Alice and Bob, with separate calendars A and B, respectively, in which are marked, say as 1's, the days at which these people are available for meetings (all other days are marked 0). Each calendar has some $N = 2^n$ entries (for as many days).

The problem is to find a day for both to meet, and to do so with the least number of bits exchanged between the calendars. The classical solution requires exchanging $O(N)$ calendar entries to find such a date, whereas the quantum mechanical solution gets the job done by exchanging just $O(\sqrt{N}\ log(N))$ qubits.

To do so, both A and B have access to an oracle each that computes a function $f_A(x)$ and $f_B(x)$, respectively. Both functions combined realize an oracle $f_{AB}(x) = f_A(x) f_B(x)$.

Either one of the oracles can compute the reflection U_s in order to perform a full Grover iteration in search for a day x for which $f_{AB}(x) = 1$, i.e., both Alice and Bob can meet.

Here is how the interaction between A and B works:

- A performs a transformation

$$U_{f_A} \mid x >\mid 0 > \rightarrow \mid x > \mid f_A(x) >$$

  on one of the base states $\mid x >$, and sends the result $\mid x > \mid f_A(x) >$ (of $n+1$ qubits) to B.

- B performs some unitary transformation

$$U'_{f_A} \mid x > \mid f_A(x) > \rightarrow (-1)^{f_A(x) f_B(x)} \mid x > \mid f_A(x) >$$

  on the input received. The phase factor preceding $\mid x >$ now contains the full oracle $f_{AB}(x) = f_A(x) f_B(x)$.

- B now sends the $n+1$ qubits of the resulting state back to A, and A performs once more its oracle U_{f_A} to transform

$$U_{f_A}(-1)^{f_{AB}(x)} \mid x > \mid f_A(x) > \rightarrow (-1)^{f_{AB}(x)} \mid x > \mid 0 >$$

- thus, after having exchanged $2*(n+1)$ qubits, A can now perform one Grover iteration (after having accomplished one query).

- after some $\frac{\pi}{4} * \sqrt{2^n}$ Grover iterations which require a total of $\frac{\pi}{4} * \sqrt{2^n} * 2 * (n+1)$ qubit exchanges, A may measure its quantum state to obtain an agreeable meeting date with probability close to 1.

7.8 Finding periodicities in functions

This is a generalization of Simon's problem solved in section 7.5. Given a function $f : \{ 0,\ 1\}^n \rightarrow \{ 0,\ 1\}^m$ which has some unknown periodicity $r \in \{ 1,\ \ldots\ ,\ 2^n - 1\}$ such that $f(\ x\ ) = f(\ x + m * r\ )$ with $m,\ x,\ x + m * r \in \{ 1,\ \ldots\ ,\ 2^n\}$, what is to be determined is the value of r.

For this purpose we assume some unitary transformation

$$Q_{FFT} \mid x > \rightarrow 1/\sqrt{N} * \sum_{y=0}^{N-1} e^{2\pi j * xy/N} \mid y >$$

which is the quantum version of the Fast Fourier Transform (FFT).

In order to compute some period r using Q_{FFT} we first prepare a fully randomized quantum state by means of the Hadamard transformation

$$H_H^{(n)} \mid 0^{(n)} > \rightarrow 1/\sqrt{N} * \sum_{x=0}^{N-1} \mid x >$$

and then apply the operator U_f to obtain

$$U_f\ (1/\sqrt{N} * \sum_{x=0}^{N-1} \mid x >) \mid 0^{(n)} > \rightarrow 1/\sqrt{N} * \sum_{x=0}^{N-1} \mid x > \mid f(\ x\ ) >$$

When we now measure the output register $\mid f(\ x\ ) >$, its state collapses to some function value $\mid f(\ x_0\ ) >$ (with $0 \leq x_0 < r$), and in the input register we get a coherent superposition of some k values x which map into the same function value $f(\ x_0\ )$, i.e., we have

$$1/\sqrt{k} * \sum_{i=0}^{k-1} \mid x_0 + i * r\ >$$

with $N - r \leq x_0 + (k-1) * r < N$.

Applying now the Fast Fourier Transform Q_{FFT} to this first register yields the state

$$1/\sqrt{kN} * \sum_{y=0}^{N-1} \left(e^{2\pi j * x_0 y/N} \sum_{i=0}^{k-1} e^{2\pi j * iry/N} \right) \mid y >$$

If we measure this state wrt standard base, the probability of obtaining as an outcome the base state y is

$$Prob(y) \ = \ k/N \mid 1/k * \sum_{i=0}^{N-1} e^{2\pi j * iry/N} \mid^2$$

which strongly favors values for y such that yr/N becomes an integer value since then the exponent of e becomes a multiple of $2\pi j$ and the value of $e^{2\pi j * iry/N}$ becomes 1 (which is the highest it can get). For instance, if N/r is integer and hence must inevitably be equal to k, we get

$$Prob(y) \ = \ 1/r \mid 1/k * \sum_{j=0}^{k-1} e^{2\pi j * iy/k} \mid^2 \ = \begin{cases} \frac{1}{r} & \text{if } y = k * l \\ 0 & \text{otherwise} \end{cases}$$

from which after some lengthy paper-and-pencil excercise the value of r can be derived.

7.9 Implementation of Q_{FFT}

Our aim is now to find a suitable decomposition of Q_{FFT} into operations on one or two qubits so that it can be implemented as a quantum circuit composed of elementary quantum gates. To do so, we set out with the following observations:

$\rightarrow$ when applying Q_{FFT} to $\mid 0^{(n)} >$, we obtain

$$Q_{FFT} \mid 0^{(n)} > \rightarrow \ 1/\sqrt{N} * \sum_{y=0}^{N-1} \mid y >$$

since with $\mid x > = \ \mid 0^{(n)} >$ we get $e^{2\pi j * xy/N} \ = \ 1$, i.e., Q_{FFT} is a generalization of the Hadamard transformation $H_H^{(n)}$.

$\rightarrow$ some state $\mid y >$ can be written as $\mid y > = \ \mid y_{n-1} > \mid y_{n-2} > \ \ldots \mid y_0 >$ with $y_l \ \in \ \{ \ 0, \ 1 \}$, and summation over all $y \ \in \ \{ \ 0, \ \ldots \ , \ N-1 \}$ is nothing but a tensor product of the form

$$\sum_{y=0}^{N-1} \mid y > = \ (\mid 0 > + \mid 1 >) \otimes (\mid 0 > + \mid 1 >) \otimes \ldots \otimes (\mid 0 > + \mid 1 >)$$

As for computing the terms $e^{2\pi j * xy/N}$, we can represent the numbers x and y as polynoms

$$\begin{aligned} x \ &= \ x_{n-1} * 2^{n-1} + \ \ldots \ + \ x_1 * 2^1 \ + \ x_0 \\ y \ &= \ y_{n-1} * 2^{n-1} + \ \ldots \ + \ y_1 * 2^1 \ + \ y_0 \end{aligned}$$

the product of which may be simplified by the following consideration: if the product of the pth component of x and of the qth component of y is $x_p * 2^p * y_q * 2^q \ = \ x_p * y_q * 2^{(p+q)}$ and $(p+q) \geq n$, then the factor $2^{(p+q)}/N \ = \ 2^{(p+q)-n}$ changes the phase represented by $2\pi j * 2^{(p+q)-n}$ just by multiples of 2π and thus does not contribute anything to the total phase shift. Hence all terms with $(p+q) \geq n$ may simply be dropped, i.e., we can write $x * y/2^n$ as

$$y_{n-1} \ (.x_0) \ + \ y_{n-2} \ (.x_1 x_0) \ + \ \ldots \ y_1 \ (.x_{n-2} x_{n-3} \ldots x_0) \ + \ y_0 \ (.x_{n-1} x_{n-2} \ldots x_0)$$

where

$$.x_p x_{p-1} \dots x_0 \;=\; x_p/2^1 \;+\; x_{p-1}/2^2 \;+\; \dots \;+\; x_0/2^{p+1}$$

Looking at the full state produced by $Q_{FFT} \mid x >$, we can therefore write

$$\frac{1}{\sqrt{2^n}} \left(e^{2\pi j * y_{n-1}(.x_0)}(\mid 0 > + \mid 1 >) \otimes e^{2\pi j * y_{n-2}(.x_1 x_0)}(\mid 0 > + \mid 1 >) \otimes \dots \otimes e^{2\pi j * y_0(.x_{n-1} \dots x_0)}(\mid 0 > + \mid 1 >) \right.$$

Since

$$e^{2\pi j * y_q\,(\dots)} \;=\; \begin{cases} 1 \text{ if } y_q = 0 \\ e^{2\pi j\,(\dots)} \text{ if } y_q = 1 \end{cases}$$

we can re-arrange the state description a little so that it becomes

$$1/\sqrt{2^n}\;(\mid 0 > + e^{2\pi j\,(.x_0)} \mid 1 >)\;(\mid 0 > + e^{2\pi j\,(.x_1 x_0)} \mid 1 >)\;\dots\;(\mid 0 > + e^{2\pi j\,(.x_{n-1} \dots x_0)} \mid 1 >)$$

i.e., the factors $e^{2\pi j\,(.x_p \dots x_0)}$ produce phase shifts between the qubit base states $\mid 0 >$ and $\mid 1 >$.

With this in mind, we can now break down the implementation of Q_{FFT} into a quantum network composed of just two operators | quantum gates, of which

→ one realizes a modified Hadamard transformation

$$H'_H \mid x_k > \to\; 1/\sqrt{2}(\mid 0 > + e^{2\pi j\,(.x_k)} \mid 1 >)$$

which produces some first phase shift between the base states $\mid 0 >$ and $\mid 1 >$ which depends on the particular (kth) qubit itself;

→ the other realizes a conditional rotate transformation

$$R_d \;=\; \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi j/2^d} \end{pmatrix}$$

with $d \;=\; k - i$ as the distance between the kth qubit under consideration and the ith qubit that effects a phase shift on the kth qubit. The additional phase shift is given as

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi j/2^d} \end{pmatrix} * \begin{pmatrix} 1 \\ e^{2\pi j\,(.x_k)} \end{pmatrix} \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{2\pi j\,(.x_k) + 2\pi j/2^{d+1}} \end{pmatrix}$$

Such phase shifts are performed based on the condition that qubit $i < k$ is set to one.

Example: for Q_{FFT} on three qubits we get the quantum network shown in fig. 29.

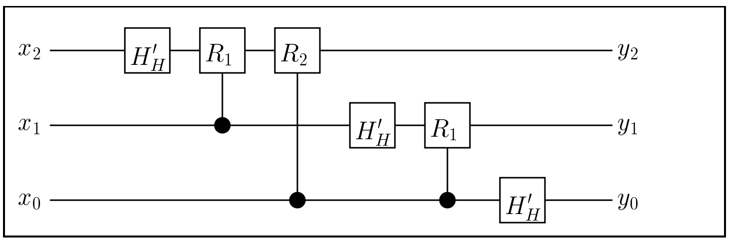


Figure 29: Q_{FFT} circuit with $k = 3$

⇐

For the general case of an n-qubit quantum FFT operator Q_{FFT} we need

→ n H'_H gates | operators ;

→ $\begin{pmatrix} n \\ 2 \end{pmatrix} \;=\; 1/2 * n * (n-1)$ R_d gates | operators.

Thus the quantum network is roughly of complexity $(log\ N)^2$, where N is the problem size.

7.10 Factoring

concerns finding prime factors for very large integer numbers. This problem plays a key role in securely encoding and decoding messages. It relates to finding periods in functions and can therefore be solved using quantum algorithms (see preceding section).
Given some large integer number $N \in \{1, \ldots, 2^n - 1\}$ of n bits, we need to find some prime factor $x < N$, which may be done as follows:

- select some integer $x < N$ randomly and compute the greatest common denominator of x and N, using the well known recursive function $gcd(\ x,\ N)$, which does it in $O(log\ N)$ steps;
- if $gcd(\ x,\ N) > 1$ then x is a non-trivial factor of N which is also prime, i.e., we are done $\rightarrow$ x is a prime factor;
- if $gcd(\ x,\ N) = 1$ then x is coprime to N (both have no non-trivial divisor in common) $\rightarrow$ this case requires further treatment.

The numbers $x < N$ that are coprime to N form a group under multiplication $(mod\ N)$ with the property that
$\rightarrow$ each element of the group has some finite order r, which is the smallest integer value such that

$$(\ x^r\ mod\ N\ ) = 1 \quad (\text{ or equivalently }) \quad x^r \equiv 1\ (\ mod\ N\ )$$

which means that $x^r - 1$ divides without remainder by N.
$\rightarrow$ the order r of $(\ x\ mod\ N\ )$ is the period of the function

$$f_{N,x}(\ y\ )\ =\ x^y\ mod\ N \quad (=\ f_{N,x}(\ y + r\ )\ )$$

As we know, there is a fast quantum algorithm (based on Q_{FFT}) to find such a period. What is needed is a fast way of computing $f_{N,x}$ for fairly large values of y, which can be done thus:
for $y < 2^m$ we can write y in binary representation as

$$y\ =\ y_{m-1} * 2^{m-1} +\ \ldots\ +\ y_1 * 2^1\ +\ y_0$$

and, using this representation, the function $(\ x^y\ mod\ N\ )$ as

$$(x^{2^{m-1}})^{y_{m-1}} * (x^{2^{m-2}})^{y_{m-2}} * \ \ldots\ * (x^{2^1})^{y^1} * (x^1)^{y^0}\ (\ mod\ N\ )$$

Since

$$x^{2^j}\ (\ mod\ N\ )\ =\ (x^{2^{j-1}})^2\ (\ mod\ N\ )$$

it takes just $m - 1$ steps to compute y, using the algorithm

```
y = 1; j = 0;
while ( j < m )
  { if ( y_j = 1 ) then y = y * x**2**j;
    j++
  }
```

Assume now that some period r has been found for $(\ x\ mod\ N\ )$, then the following cases need to be distinguished:

- r is even, then from

  $$x^r \equiv 1\ (\ mod\ N\ )\ \rightarrow\ ((\ x^r - 1\ )\ mod\ N\ )\ =\ 0$$

  we can conclude that N divides

  $$(\ x^{r/2}\ -\ 1\ )\ (\ x^{r/2}\ +\ 1\ )\ =\ (\ x^r\ -\ 1\ )$$

  without remainder.

- Having found an even r, N does certainly not divide $x^{r/2} - 1$ since this would mean that we have $x^{r/2} \equiv 1$ ($mod\ N$), which in turn, means that the order of x would be $\leq r/2$, but then the original value of r wouldn't have been the smallest.

- if N also does not divide $x^{r/2} + 1$, which means that $x^{r/2} \not\equiv -1$ ($mod\ N$), then N must have a non–trivial factor with both $x^{r/2} + 1$ and $x^{r/2} - 1$, and this factor can be found by computing $gcd(\ N,\ x^{r/2} + 1\ )$ (or $gcd(\ N,\ x^{r/2} - 1\ )$) by classical methods, and by taking the larger of the two values as the factor that we are looking for.

Thus, the algorithm for finding a factor of N consists of the following steps:

1. choose randomly some value $x \in \{\ 2, \ldots,\ N\ \}$;

2. compute $z = gcd(\ N,\ x\ )$; if $z \neq 1$ a factor has been found and the algorithm terminates; otherwise continue with the next step;

3. find a period r for the function $f_{N,x}(\ y\ ) = (\ x^y\ mod\ N\ )$; it holds that: $x^r \mod N = 1$

4. if r is odd or $x^{r/2} = \pm 1(\ mod\ N\ )$, then go back to step 1 and repeat; otherwise $x^{r/2}$ is a non-trivial solution with which to continue;

5. compute $z = gcd(\ N,\ x^{r/2} \pm 1\ )$; if $z \neq 1$, then return z as output and terminate, otherwise resume at step 1.

7.11 The RSA cryptosystem

The idea of RSA[1] is to communicate messages between two parties A and B based on the exchange of public rather than private keys for secure encoding and decoding, but nevertheless render deciphering an intractable problem for conventional computers.
The encoding | decoding protocol works as follows:
Upon agreeing that A wishes to send a message to B

- B chooses two large prime numbers p and q and computes $N = p * q$ and the value of the Euler function
$$\phi(\ N\ ) = N - p - q + 1 = (\ p - 1\ )\ (\ q - 1\ )$$
The factorization of $\phi(\ N\ )$ is hard to figure out if only N is known.

- B then randomly selects some number $e < \phi(\ N\ )$ that is coprime to $\phi(\ N\ )$, and then sends both N and e to A.

- A converts the message to be sent to some agreed upon number $a < N$ coprime to N, encodes it as
$$b = f(\ a\ ) = a^e\ (\ mod\ N\ )$$
and sends it of to B.

- B deciphers the encoded message b as follows:
$\rightarrow$ B knows that $a^{\phi(\ N\ )} = 1$ ($mod\ N$), provided that a is coprime to N (which had to be ensured by A), which is a consequence of all $a < N$ and coprime to N forming a group of order $\phi(\ N\ )$ under multiplication ($mod\ N$).
$\rightarrow$ Since $gcd(e, \phi(\ N\ )) = 1$, we also have an inverse to e which is $d = e^{-1} *\ mod(\phi(\ N\ ))$ or

[1] named after its inventors Rivest, Shamir, Adleman

$ed \equiv 1 \ (\ mod \ \phi(\ N \ ))$; the value of d is only known to B.
$\rightarrow$ B now computes

$$f^{-1}(b) = b^d (mod \ N) \ = \ a^{ed}(mod \ N) \ = \ a * (a^{\phi(N)})^s (mod \ N) = a (mod \ N)$$

to obtain the value of a in unencoded | deciphered form. (with an integer s)

The RSA scheme is secure for large numbers of N (say, of more than 2048 binary digits) relative to conventional computers, but the codes may be cracked by extremely fast computing machines by
$\rightarrow$ factoring N, which leads to $\phi(N)$ and thus to d (since e is known);
$\rightarrow$ and, with b and d known, by computing $f^{-1}(b)$.

7.12 Breaking the RSA cryptosystem

As pointed out in the preceding section, RSA code may be broken by intercepting the exchange of the public keys N, e and by factoring N. However, factorization can even be avoided by some clever method which requires only computing the order of the encrypted text.
Given some encrypted message $b = a^e \ (\ mod N \ )$, it is known that the order of b equals the order of a since e is coprime to $\phi(\ N \ )$ by definition. With some value d such that $ed = 1 \ (\ mod \ order\_of \ (\ b \ ))$ or $ed = k * order\_of(\ b \ ) + 1$ for some integer k we have

$$b^d = a^{ed} = a^{k*order\_of(\ b \ )+1} = a \ (\ mod \ N \ )$$

Thus, all we need to find is the order of b and we are done.

7.12.1 The period finding quantum algorithm

sets out with an initial quantum state composed of five quantum registers

$$| \ N, \ x, \ q, \ 0^{(n)}, \ 0^{(n)} >$$

where
$\rightarrow$ N denotes a register of n qubits that holds the value N;
$\rightarrow$ x denotes a register of n qubits that holds some randomly choosen value $x < N$;
$\rightarrow$ q denotes a register of some n qubits that holds some value $q \in O(N^2)$ [2];
$\rightarrow$ two more registers are initialized with all qubits set to zero.

The next steps of the algorithm are as follows:

- apply the Hadamard transformation $H_H^{(n)}$ to the fourth register to compute the random state

$$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} | \ N, \ x, \ q, \ y, \ o^{(n)} >$$

- compute in the fifth register the function $f_{N,x}(\ y \ ) \ = \ x^y \ (\ mod \ N \ )$, using the operator $U_{f_{N,x}}$, which computes function values for all y simultaneously (in one conceptual step), yielding

$$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} | \ N, \ x, \ q, \ y, \ x^y \ (\ mod \ N \ ) >$$

[2] It should be noted here that it is not quite clear how this value (which has been taken over from the literature) comes about and what exactly it means that a value is of the order of N^2, if the register obviously accommodates n qubits.

- take then a measurement on the fifth register only, which returns a value $z = x^l \ (\ mod\ N\ )$.
  → if r is the period of $f_{N,x}$, then we have $x^l = x^{p*r+l} \ (\ mod\ N\ )$ for all indices p, assuming that l has property $l < r$.
  → in the fourth register we therefore get a linear combination | superposition of p values from the set $\{\ l + p * r \mid 0 \leq p \leq s\}$ where s is the largest integer so that $l + s * r \leq q$;
  since $l \leq r < N$ and $q \in O(N^2)$, we get roughly $s \approx q/r$ (when neglecting the relatively small offset value of l);
  → when disregarding from now on the registers N, x, q and $z = x^{p*r+l} \ (\ mod\ N\ )$, the state after the measurement becomes

$$\mid \Phi_l >= \frac{1}{\sqrt{s+1}} \sum_{p=0}^{s} \mid p * r + l > \ ;$$

  → when considering the special case $p = q/r - 1$ only, we have

$$\mid \Phi_l > = \sqrt{\frac{1}{q}} \sum_{p=0}^{q/r-1} \mid p * r + l > \ ;$$

- apply now the fast Fourier transform operator Q_{FFT} to this state in order to extract its periodicity; we get

$$\frac{1}{\sqrt{q}} \sum_{w=0}^{q-1} \sqrt{\frac{1}{q}} \sum_{p=0}^{q/r-1} e^{2\pi j w(p*r+l)/q} \mid w >$$

  which can be re-written as

$$\sqrt{\frac{1}{q}} \sum_{w=0}^{q-1} e^{2\pi jl*w/q} * \sum_{p=0}^{q/r-1} e^{2\pi j*wpr/q} \mid w >$$

  Interpretation of this state leads us to conclude that with w being a multiple of q/r we have $e^{2\pi j*wpr/q} = 1$ because the exponent becomes a multiple of $2\pi j$. In all other cases we get $\sum_{p=0}^{q/r-1} \ e2\pi jwpr/q = 0$ because the summation goes over a set of q/r values arranged at equal angular distances around a circle, i.e., they cancel each other out. Thus, the state is in fact given as

$$\mid \Phi >= Q_{FFT} \mid \Phi_l >= \frac{1}{\sqrt{r}} \sum_{p=0}^{r-1} e^{2\pi jlw/q} \mid p * (q/r) >$$

  This state has the nice property that the annoying offset value l has been moved into a phase shift factor and thus has no influence on the probabilities with which the base states occur in the superposition.

- measuring the state $\mid \Phi >$ yields one of the states $w = \lambda * (q/r)$ with probability $1/r$, where λ is randomly chosen and q is also known as part of the initial state.
  Now,
  → if $gcd(\ \lambda,\ r) = 1$, then we have $r = q/gcd(\ w,\ q)$, and
  → the probability that $gcd(\ \lambda,\ r) = 1$ is $O(\ 1/lg\ lg\ r\ )$, i.e., when repeating the entire computation $O(\ lg\ lg\ r\ )$ times some order r can be found with probability close to 1.

7.12.2 Some remarks on the performance of factorization

The perspectives of factorization on classical and quantum computers are summarized in the following tables.

Estimated factoring times for large numbers (measured in binary digits) on state-of-the-art networks of 1000 conventional workstations are

no of bits	1024	2048	4096
time in 2006	10^5 years	$5 * 10^{15}$ years	$3 * 10^{29}$ years
time in 2024	38 years	10^{12} years	$7 * 10^{25}$ years
time in 2042	3 days	$3 * 10^8$ years	$2 * 10^{22}$ years

i.e., factorizing even relatively modest 1024 digit numbers with current technology becomes an intractable problem, and even in more than 20 years from now remains intractable for all practical purposes since nobody will be interested in code breaking that takes 38 years.

The situation drastically changes with quantum computing, where estimated factoring times for quantum computers with minimal clock speed of 100 MHz are several orders of magnitude lower.

number of bits	1024	2048	4096
number of qubits	5124	10244	20484
number of quantum gates	$3 * 10^9$	$2 * 10^{11}$	$2 * 10^{12}$
factoring time	4.5 min	36 min	4.8 hours

Here we have the situation that even codes of 4096 bits length can be cracked in acceptable time, which means that the RSA cryptosystem for all practical purposes becomes useless.

8 Overview of quantum computing devices

Sofar we have only seen how the formal apparatus of quantum mechanics (essentially unitary operations on vectors in Hilbert spaces) may be used to specify and perform elementary and compound operations | algorithms. The interesting aspects that make the difference between quantum and conventional computing are that
→ due to the unitary of operations all computations are reversible (though this is not of too much practical value since inspecting the results of forward computations destroys the quantum states that need to be 'rolled' backward);
→ there are classes of algorithms which are intractable by classical computing machinery but tractable with quantum computing.

The problems that remains to be addressed include
→ the construction of physical machinery from elementary devices that exploit quantum effects for computing;
→ the interfacing | interaction of such highly sensitive machinery with the robust environment of conventional computing.

The physical devices needed for quantum computing must be capable of representing and manipulating qubits as prescribed by the formal apparatus, with the following essentials in mind:
→ qubits must be stored and held long enough in some reasonably stable state to perform some well-defined operations on them;
→ qubits must be well enough separated | isolated from the environment to reduce the effects of unintended entanglements | decoherence;
→ there must be reliable and easy-to-implement means to set up and measure | read the states of qubits and to effect controlled interactions among them in order to realize elementary quantum gate

operations;

The physical phenomena to do so as of now appear to be quite exotic and pretty hard to control in a reliable manner, contrary to what is required to perform useful computations. Moreover, the devices to implement them appear to be rather clumsy, still in their infancy, and the technology is not yet there to produce them large scale.

8.1 Photon beam splitting devices

are merely to demonstrate, in a clean and easy-to-understand setting, how quantum effects may be utilized to perform some very elementary operations. They are not of much practical value since they are optical devices which take up too much space to be used in large quantities and extremely sensitive wrt to alignments. The basic idea is illustrated in fig. 30:

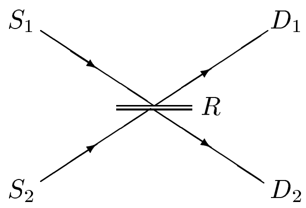


Figure 30: A simple beam splitter

→ A beam of photons emitted from a source $S1$ (i.e., a beam of coherent light) is under a certain angle directed at a half-reflecting | half-transmitting surface R;
→ the beam is split up by R into two beams, one directed upwards (annotated u), the other is directed downwards (annotated d);
→ photon detectors $D1$ and $D2$ placed into the beams count the same number of photons per unit time, exactly half as many as are sent out by $S1$;
→ when using $S2$ as the photon source, the same photon counts may be measured at $D1$ and $D2$ (provided that $S2$ emits photons at the same rate as $S1$);

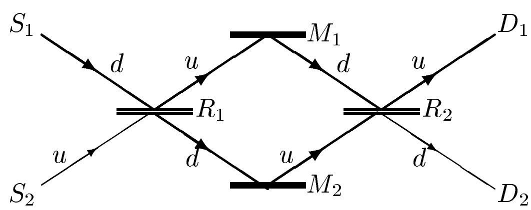


Figure 31: Realizing the NOT gate with beam splitters

We now extend this elementary beam splitter by two fully reflecting mirrors $M1$ and $M2$ an by another beam splitter, as shown in fig. 31. This apparatus works as follows:
→ the beam sent out by source $S1$ is split up by $R1$ into two beams of half the number of photons, one reflected by $M1$, the other by $M2$, so that both meet again at the same spot on the beam splitter $R2$;
→ when readjusting the vertical positions of the mirrors $M1$ and $M2$ a tiny little bit, we may produce constellations where
⇝ all photons end up in the detector $D1$ and none in $D2$ (or vice versa);

⇝ $D1$ and $D2$ each receive half the number of photons
⇝ anything in between may also be possible as londg as $r(S1) = r(D1) + r(D2)$ where $r(S1)$ is the number photons emitted by $S1$; $r(D1)$ and $r(D2)$ are the number of photongs received by $D1$ and $D2$, respectively;
→ with$S1$ turned off and $S2$ turned on, the complementary effects may be observed.

These phenomena have the following interpretation:
→ the second beam splitter obviously distinguishes between beams coming from $S1$ or $S2$;
→ since $R1$ and $R2$ are not different from each other, the distinction between two different directions is obviously effected by a superposition of probability amplitudes (which cancel each other out in one direction but reinforce each other in the other direction), not by superposition of probabilities (of photons traveling along either of the beams), as this would mean equal distribution of photons over $D1$ and $D2$ under all circumstances;
→ the probability amplitudes for photons moving upwards (u-photons) are obviously not the same as those for photons moving downwards (d-photons):
⇝ a d-photon is split up by R into amplitudes $\frac{1}{\sqrt{2}}(1,1)$;
⇝ a u-photon is split up by R into amplitudes $\frac{1}{\sqrt{2}}(1,-1)$;
(the first component stands for photons transmitted, the second component stands for photons reflected at R);
→ interpreting the quantum state of a d-photon as $\mid 1 >$ and of a u-photon as $\mid 0 >$, the beam splitter obviously performs the Hadamard transformation $H_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ which transforms the standard bases $\mid 0 >$ and $\mid 1 >$ into the dual bases $\frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >)$ and $\frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >)$, respectively;
→ the double beam splitter arrangement which transmits all photons from $S1$ to $D1$ (or from $S2$ to $D2$) performs two Hadamard transformations in succession:

$$H_H * H_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} * \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

which realizes negation (as shown in the figure);

A controlled NOT (or an XOR-gate) can be realized using photon polarization as an additional carrier of a qubit in conjunction with the u-photon | d-photon concept of a beam splitter. Photon polarization may be manipulated by some crystal (e.g., sugar) so as to rotate from horizontal to vertical (or vice versa).
→ associating, say,
⇝ horizontal polarization with $\mid 0 >$
⇝ vertical polarization with $\mid 1 >$
we may realize a controlled NOT simply as a crystal (with rotation by 90^0) in the path of d-photons of a simple beam splitter, as shown in fig. 32, whereas the polarization of the u-photons remains unchanged.

Thus, using the direction as the controlling bit and the polarization as the target bit of the controlled NOT, we get what we want. However, the problem with this device is that we need detectors for both direction and polarization and means to convert polarization into direction, and vice versa, which does not look like an elegant solution.

8.2 Quantum dots

are electrons captured in small regions that are sustained by means of fences erected by electro(magnetic) fields, e.g., of other atoms in the neighborhood or by standing waves of electromagnetic radiation

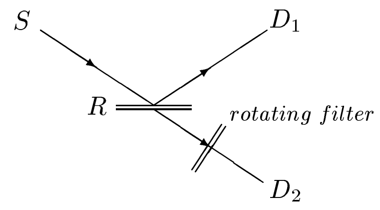


Figure 32: Realizing a controlled NOT with a polarizing beam splitter

(photons). Heteropolymers are usually used as substrates for arrays of atoms that act as qubits. As illustrated in fig. 33, these atoms may assume
$\rightsquigarrow$ a stable ground state of energy E_0 representing $\mid 0>$
$\rightsquigarrow$ a fairly unstable excited state of energy $E_2 > E_0$ representing $\mid 2>$ (which is to be taken just as short hand for E_2 but not as a legitimate quantum state)
$\rightsquigarrow$ a metastable excited state of energy E_1 (with $E_2 > E_1 > E_0$) representing $\mid 1>$.

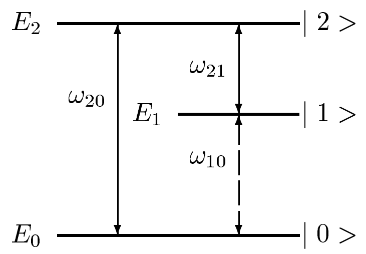


Figure 33: Essential energy levels of an isolated atom

Transitions between E_0 and E_2 (up and down) may be effected by laser pulses of frequency $\omega_{20} = (E_2 - E_0)/h$
$\rightsquigarrow$ each laser pulse emits showers of photons that trigger electrons to move up (by absorption of photons) or down (by emitting photons) several times;
$\rightsquigarrow$ a fairly long lasting pulse may effect some atoms to fall back from E_2 to the metastable state E_1 (or $\mid 1>$) where they remain for some time long enough to perform several steps of a useful computation.

8.2.1 Logic operations

come about by some form of interaction between two adjacent atoms which split energy levels up into two that are close by each other, with the splitting in one atom depending on the energy level(s) assumed by the other atom(s). The splitting of energy levels is shown in fig. 34 for two adjacent atoms A and B (the annotations $B0$ and $B1$ on the energy levels of atom A are to indicate that these levels are assumed by electrons in A if in atom B electrons occupy the levels $\mid 0>$ and $\mid 1>$, respectively, and vice versa).
$\Rightarrow$

Example: Copying the actual state of atom B to atom A:
there are four different constellations to be distinguished, namely [3]

[3]Notations such as ω_{A12}^{B1} are to be read as: the frequency of getting atom A from state $\mid 1>$ up to $\mid 2$. (or from energy level E_1 to E_2) while atom B is in state $\mid 1>$

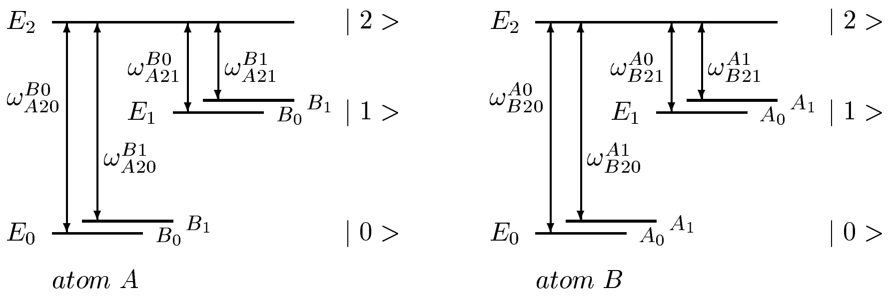


Figure 34: Split energy levels of two interacting atoms

$\rightarrow$ $B = \mid 0 >$ $\mid A = \mid 1 >$ which means that B is in state B_0^{A1} and A is in state $A_1^{B0} \leadsto$ sending out laser pulses with frequency ω_{A12}^{BO} to atom A lifts it to state $\mid 2 >$ which immediately collapses into A_0^{B0};
$\rightarrow$ $B = \mid 0 >$ $\mid A = \mid 0 > \leadsto$ nothing needs to be done, but laser pulses with frequency ω_{A12}^{BO} have no effect either since the actual state of atom A does not resonate with this frequency;
$\rightarrow$ $B = \mid 1 >$ $\mid A = \mid 0 >$ which means that B is in state B_1^{A0} and A is in state $A_0^{B1} \leadsto$ laser pulses with frequency ω_{A02}^{B1} excite atom A to state $\mid 2 >$ which (hopefully) collapses into state A_1^{B1} (or $\mid 1 >$); likewise, if A is in state $\mid 1 >$, then laser pulses ω_{A02}^{B1} have no effect since they are not in resonance with the actual state;
Thus, applying laser pulses with frequencies $[\omega_{A12}^{BO}, \omega_{A02}^{B1}]$ simulltaneously obviously does the job of copying the state of B to A.
$\Leftarrow$

Other logical operations on two qubits (represented as atoms with states as depicted in fig. 34 may in a similar way be performed by (sequences of) laser pulses with frequencies that effect the appropriate state changes. The table of fig. 8.2.1 shows these pulses for some typical operations on atoms A and B, with the result being encoded in the final state of atom A.

8.2.2 Measuring the state of an atom

(or reading the qubit represented by the state) may be accomplished by using yet another energy level E_3 with $E_2 > E_3 > E_1$, as depicted in fig. 36, and with a decay rate into ground state E_0 decidedly faster than into the excited state E_1.

Bombarding the atom with photons of frequency $\omega_{03} = \delta E_{03}/h$ has the effect that
$\leadsto$ the atom emits a fluorescending light flash if it was in state $\mid 0 >$ because the state $\mid 3 >$ rapidly collapses once excited from $\mid 0 >$;
$\leadsto$ the atom emits nothing if in state $\mid 1 >$ because the frequency ω_{03} because it cannot excite the electron, and this state decays considerably slower than state $\mid 3 >$.

8.2.3 Effecting superpositions

of base states may be accomplished by some carefully tuned interaction between the laser pulses (phase, polarization, magnitude of the electric field over the time of the pulse duration) and the dipole momentum of the atoms. It creates some superimposed state $\alpha \mid 0 > + e^{j\omega t} \mid 1 >$ where ω denotes the frequency with which the atom oscillates between ground and the metastable excited state.

operation	laser pulses
0	$[\,\omega_{A21}^{B0},\ \omega_{A21}^{B1}\,]$
$a \wedge b$	ω_{A21}^{B0}
$a \wedge \neg b$	ω_{A21}^{B1}
a	no pulses
$\neg a \wedge b$	$\omega_{A20}^{B0} + [\,\omega_{B20}^{A1},\ \omega_{A21}^{B0}\,] + [\,\omega_{A20}^{B0},\ \omega_{A20}^{B0}\,]$
b	$[\,\omega_{A20}^{B1},\ \omega_{A21}^{B0}\,]$
$a \oplus b$	not possible
$a \vee b$	ω_{A20}^{B1}
...	...
1	$[\,\omega_{A20}^{B0},\ \omega_{A20}^{B1}\,]$

Figure 35: Laser pulse frequencies for typical logical operations

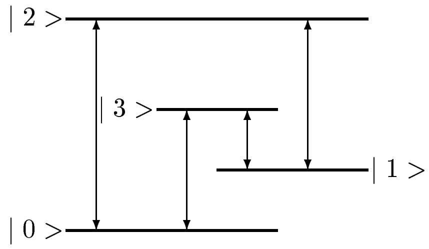


Figure 36: The fluorescending energy level for measuring the | 0 > state

8.3 Ion traps

are linear arrays of, for instance, Be^+ ions whose positions in space are fixed (trapped) by appropriate electrical fields. Each ion may be operated, as in the quantum dot approach, as a two-state system having a ground state $\mid 0 >$ and a metastable excited state $\mid 1 >$. The ions are held at equal distances to each other by electrical repulsion of the positive charges. Manipulation of the individual ion states is by laser pulses of appropriate frequencies, phases, duration etc. $\rightsquigarrow$ the entire array acts as a qubit register.

Another mode of excitation is realized through the horizontal motion of the mass centers of the ions $\rightsquigarrow$ it is in fact an oscillation that propagates through the chain of ions by repulsive electrostatic forces that act like springs between mechanical pendulums. These horizontal vibrations have energy levels different from those of the electrons in the individual ions. They can therefore be triggered | excited without affecting the ion energy levels.
$\rightarrow$ entanglement among the ions can be effected by transferring energy from the internal states of the ions to vibrational energy (and vice versa);
$\rightarrow$ the vibrational level acts as some kind of a bus to transfer information among the qubits represented by the ions.

Let $\mid g_i >$ and $\mid e_i >$ be ground and excited states of the i-th ion in the array, $\mid O_V >$ and $\mid 1_V >$ be the ground and first excited states of the chain vibrations, and
$\leadsto$ let ω_I be the frequency that effects transitions $\mid g_i > \rightarrow \mid e_i >$;
$\leadsto$ let ω_V be the frequency that effects transitions $\mid O_V > \rightarrow \mid 1_V >$;
Suppose now that the i-th qubit is flashed upon with laser pulses of frequency $\omega_I - \omega_V$ (with $\omega_I >> \omega_V$) while the actual vibrational state is $\mid O_V >$, then we have transitions

$$\mid g_i > \mid O_V > \rightarrow \mid g_i > \mid O_V > \quad \text{and} \quad \mid e_i > \mid O_V > \rightarrow \mid g_i > \mid 1_V >$$

i.e.,
$\rightarrow$ if the ion is in ground state, then nothing happens since the frequency $\omega_I - \omega_V$ is not in resonance with any of the possible state transitions;
$\rightarrow$ if the ion is in the excited state, then the laser pulse will effect a transition that collapses the excited into the ground state of the ion but at the same time lifts the vibrational state from ground to excited;
$\rightarrow$ the $\mid e_i >$ state of the ion is thus converted into a $\mid 1_V >$ state of the 'bus', from where it may be picked up by another ion trap pulsed with the frequency $\omega_I - \omega_V$ which converts $\mid g_i > \mid 1_V > \rightarrow$ $\mid e_j > \mid O_V >$.

The problem with ion traps is that they are inherently slow devices since changing the vibrational states requires laser pulses several times longer than $T = \omega / 2\pi$. The vibrational frequency, however, is in the order of 100 kHz, meaning that the frequency with which the array may be pulsed is several times slower.

8.4 The cavity QED

(QED standing for quantum electro dynamics)
This device centers around a photon trap made of two concave mirrors facing each other (the cavity) so that a photon may bounce several times back and forth between the mirrors and, while doing so, also interact with an atom that is either captured inside the cavity too, or it is just flying through $\leadsto$ the flying qubit.
$\rightarrow$ the interaction consisting in the atom emitting and absorbing the photon several times, provided that the cavity is not leaking;
$\rightarrow$ there are only two energy states of the atom participating in the photon interaction, just as in the case of the quantum dot or ion trap;
$\rightarrow$ the atom itself represents the (carrier of) the qubit captured or flying through.

The flying qubits may be excited by laser pulses before entering, while inside, and after leaving the cavity.

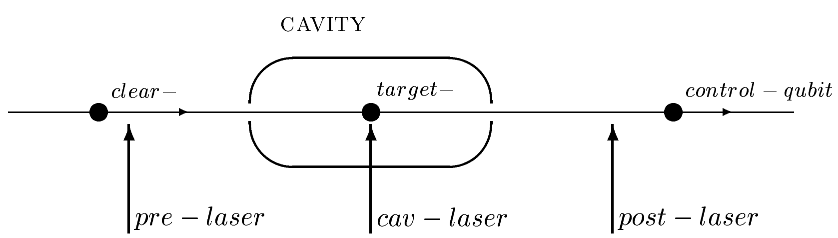


Figure 37: CNOT realized by means of a cavity device

Fig. 37 shows how a controlled NOT (or an XOR) is realized by means of a cavity device. It requires three atoms (qubits) passing through the cavity $\rightsquigarrow$ control | target | clear.
$\rightsquigarrow$ first the control qubit | atom (prepared by the pre-laser) passes through the cavity, leaving a photon there that represents the superimposed state carried by the atom;
$\rightsquigarrow$ next the target qubit | atom (also prepared by the pre-laser) follows which, stimulated by the cav-laser, inverts its state by interaction with the photon caught inside the cavity (with nothing happening if there is no photon);
$\rightsquigarrow$ finally the clear qubit | atom resets the cavity to its original no photon | empty state.

The time spent by the atoms inside the cavity must be large enough to enable interactions between atoms passing through and photons captured inside. Interaction times between successive atoms passing through is much shorter than with ion traps; the problem is highly controlled movement of atoms through cavities just about $1/100\,mm$ wide.

8.5 NMR quantum computing

(NMR standing for nuclear magnetic resonanz) is based on the representation of qubits as spins of individual atoms in large (organic) molecules $\rightsquigarrow$ preferably H atoms. Quantization is achieved by orientation of spins (up $\uparrow$ or down $\downarrow$) relative to some external magnetic field. These spins are very stable, there is almost no decoherence. Each individual molecule is its own quantum computer with some $10\ldots100$ atoms to carry spin information $\rightsquigarrow$ each individual qc may be in its own state.

The molecules are held by thousands in some test tube; at room temperature spin orientations appear to be randomly distributed over the sea of all molecules in the tube. However, there is some structure in the molecules that gives preference to certain orientations that stand out. Nevertheless, selecting some preferred set of molecular spins out of considerable background noise is a difficult problem as signal to noise ratios drop considerably with increasing numbers of molecules.

Operations require rotating | flipping spins relative to the external field by carefully tuned radio frequencies. The spins are not equal in large molecules, there are small deviations due to minor differences in the magnetic field at individual atoms within the molecules caused by adjacent atoms $\rightsquigarrow$ they require slightly different frequencies for flipping spins, which may in turn be used to address different spins.

8.6 The outlook

What has been accomplished so far are systems of some three to five qubits, e.g., entanglements over three bits in NMR. None of the technologies is mature enough yet to seriously consider them as candidates for large scale quantum computing. What is needed are devices scaled up by several orders of magnitude to perform reasonably complex computations.

The best looking technology right now are quantum dots, which is suitable for mass production, but fast decoherence is a severe problem. Hope essentially rests on some as yet undiscovered physical phenomena | technology.

9 Quantum teleportation

Teleportation refers to a process which transfers an object O from a location A to a location B by
$\rightsquigarrow$ disassembling O at location A;
$\rightsquigarrow$ transmitting information about the construction of O to location B;
$\rightsquigarrow$ re-constructing the object O at location B from material available at B;
the net effect being that the object O is being destroyed at A and a complete replica comes into being at B.

What sofar has been science fiction becomes reality in the form of teleporting quantum states, based on quantum entanglements and on non-local interactions that do not require transmission of real signals (not quite though).

Quantum teleportation uses a pair of entangled particles as a quantum communication channel, one of the particles being retained at the sending site, the other at the receiving site. Teleporting the state of a simple two-state quantum system requires

$\rightsquigarrow$ a classical component that transmits the outcome of a measurement on two correlated (not entangled !) states through a classical channel;

$\rightsquigarrow$ a quantum component that needs to be transmitted through a quantum communication channel.

Both transmissions are re-combined at the destination site to re-construct the original state on another (local) particle.

It is important to note that quantum teleportation teleports quantum states of objects, not the objects themselves $\rightsquigarrow$ one cannot teleport an electron but its spin, which may be absorbed by another electron at the receiving site to become a clone of the electron at the sending site (which loses this spin). Teleporting quantum states means teleporting qubits $\rightsquigarrow$ e.g. between locations within a quantum computer or across quantum computers.

9.1 Teleporting one qubit

The scheme is based on the participation of three particles, of which one carries the quantum state to be teleported from some location A to location B, the other two particles are entangled; one of them belongs to location A, the other to location B.

$\rightarrow$ Let

$$\mid \Phi >= \alpha\mid 0>_1 + \beta\mid 1>_1$$

be the state (of particle 1) to be teleported, and

$$\mid \Psi >= (1/\sqrt{2})(\mid 0>_2 \mid 1>_3 - \mid 1>_2 \mid 0>_3)$$

be the entangled states (of particles 2 and 3);

$\rightarrow$ the tensor product of the two states then is

$$\begin{aligned} \mid \Phi > \otimes \mid \Psi > \quad = \quad & (\alpha/\sqrt{2})(\mid 0>_1 \mid 0>_2 \mid 1>_3 - \mid 0>_1 \mid 1>_2 \mid 0>_3) \\ & + (\beta/\sqrt{2})(\mid 1>_1 \mid 0>_2 \mid 1>_3 - \mid 1>_1 \mid 1>_2 \mid 0>_3) \end{aligned}$$

(the state of particle 1 at this point is as yet not correlated with the entangled state of particles 2 and 3).

$\rightarrow$ the next step now is to somehow couple in location A the states of particles 1 and 2, and to teleport the state of particle 3 to B. To accomplish this, a measurement must be made of the states of particles 1 and 2 to obtain as a side effect a defined state of particle 3. The observable | the complete orthonormal basis for the measurement must be chosen so that it properly represents the quantum system made up from particles 1 and 2, this being, for instance, the so-called Bell basis with

$$\begin{aligned} \mid \Psi >_a &= (1/\sqrt{2})(\mid 0>_1 \mid 1>_2 - \mid 1>_1 \mid 0>_2 \\ \mid \Psi >_b &= (1/\sqrt{2})(\mid 0>_1 \mid 1>_2 + \mid 1>_1 \mid 0>_2 \\ \mid \Psi >_c &= (1/\sqrt{2})(\mid 0>_1 \mid 0>_2 - \mid 1>_1 \mid 1>_2 \\ \mid \Psi >_d &= (1/\sqrt{2})(\mid 0>_1 \mid 0>_2 + \mid 1>_1 \mid 1>_2 \end{aligned}$$

$\rightarrow$ Relative to this basis, the combined quantum state $|\Phi > \otimes |\Psi >$ can be written as

$$|\Phi > |\Psi >= (1/2)(\mid \Psi >_a \otimes \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix} + \mid \Psi >_b \otimes \begin{pmatrix} -\alpha \\ \beta \end{pmatrix} + \mid \Psi >_c \otimes \begin{pmatrix} \beta \\ \alpha \end{pmatrix} + \mid \Psi >_d \otimes \begin{pmatrix} -\beta \\ \alpha \end{pmatrix})$$

$\rightarrow$ Measuring in A now the qubits 1 and 2 the state $|\Psi>$ with respect to the basis

$$\{|\Psi>_a, |\Psi>_b, |\Psi>_c, |\Psi>_d\}$$

yields for particle | qubit 3 one of the quantum states

$$-\alpha|0>_3 -\beta|1>_3 \;,\; -\alpha|0>_3 +\beta|1>_3 \;,\; \beta|0>_3 +\alpha|1>_3 \;,\; -\beta|0>_3 +\alpha|1>_3$$

each with probability 1/4.
$\rightarrow$ A now sends to B by classical transmission the outcome of the measurement (either one of the base states $|\Psi>_a$, $|\Psi>_b$, $|\Psi>_c$, $|\Psi>_d$, whereupon B may compute | re-construct from the state of its particle 3 what the message was.
$\rightarrow$ Interpretation | re-construction from the state of particle | qubit 3 requires the following rotations:

outcome	$\vert\Psi>_a$	$\vert\Psi>_b$	$\vert\Psi>_c$	$\vert\Psi>_d$
rotation	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

9.2 The teleporting circuitry

requires four rotating operators to get the job done:
$\rightsquigarrow$ $L = (1/\sqrt{2}) \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$
which transforms $L|0>\rightarrow (1/\sqrt{2})(|0>+|1>)$ and $L|1>\rightarrow (1/\sqrt{2})(-|0>+|1>)$
$\rightsquigarrow$ $R = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$
which transforms $R|0>\rightarrow (1/\sqrt{2})(|0>-|1>)$ and $R|1>\rightarrow (1/\sqrt{2})(|0>+|1>)$
$\rightsquigarrow$ $S = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$
which transforms $S|0>\rightarrow i|0>$ | $S|1>\rightarrow |1>$ (rotation by $+90^o$);
$\rightsquigarrow$ $T = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$
which transforms $T|0>\rightarrow -|0>$ | $T|1>\rightarrow -i|1>$ (rotation by 180^o on $|0>$ and by -90^o on $|1>$).

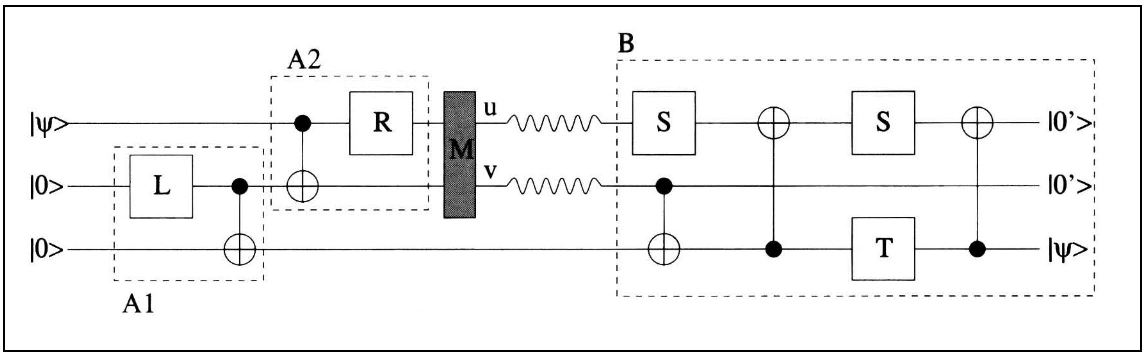


Figure 38: one-qubit teleport circuit

The circuitry to do this one-qubit teleportation is shown in fig.38. The actions taken by the sending site A are the following:
$\rightsquigarrow$ the message $|\Psi>= \alpha|0>_1 +\beta|1>_1$ to be transmitted enters on line 1 from the left;
$\rightsquigarrow$ the gate L followed by the XOR creates on lines 2 and 3 an entangled state $(1/\sqrt{2})(|0>_2|0>_3$

$+| 1 >_2 | 1 >_3)$
$\leadsto$ line 3 teleports the part of qubit 3 of the entangled state to the receiving site B;
$\leadsto$ the upper part comprising lines 1 and 2 of A produces an entanglement (through the XOR gate between these lines) between $\alpha| 0 >_1 +\beta| 1 >_1$ and $(1/\sqrt{2})(| 0 >_2 +| 1 >_2)$

The full transformation performed by the circuitry of A is specified by an $8 * 8$ matrix

$$M_a = (R \otimes I \otimes I) * (XOR \otimes I) * (I \otimes XOR) * (I \otimes L \otimes I)$$

applied to the state

$$| \Phi >= | \Psi >_1 \otimes| 0 >_2 \otimes| 0 >_3= (\alpha| 0 >_1 +\beta| 1 >_1) \otimes | 0 >_2 \otimes| 0 >_3= \alpha| 0_1 0_2 0_3 > +\beta| 1_1 0_2 0_3 >$$

$\to$ the matrix vector product $M_a * | \Phi >$ is thus given as:

$$\frac{1}{2} * \begin{bmatrix} \alpha \\ \beta \\ \beta \\ \alpha \\ -\alpha \\ \beta \\ \beta \\ -\alpha \end{bmatrix} = \frac{1}{2} * \begin{bmatrix} 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 & 1 & 0 & -1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{bmatrix} * \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ \beta \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

which produces at the outputs of the circuit A the state

$$\begin{array}{l} \frac{1}{2} * (\ \alpha| 0_1 0_2 0_3 > +\beta| 0_1 0_2 1_3 > +\beta| 0_1 1_2 0_3 > +\alpha| 0_1 1_2 1_3 > \\ -\alpha| 1_1 0_2 0_3 > +\beta| 1_1 0_2 1_3 > +\beta| 1_1 1_2 0_3 > -\alpha| 1_1 1_2 1_3 >\ ) \end{array}$$

A measurement of the combined state of qubits 1 and 2 yields the following constellations with respect to qubit 3:

$$\begin{array}{lcl} | 0_1 0_2 > & \leadsto & \alpha| 0 >_3 +\beta| 1 >_3 \\ | 0_1 1_2 > & \leadsto & \beta| 0 >_3 +\alpha| 1 >_3 \\ | 1_1 0_2 > & \leadsto & -\alpha| 0 >_3 +\beta| 1 >_3 \\ | 1_1 1_2 > & \leadsto & \beta| 0 >_3 -\alpha| 1 >_3 \end{array}$$

Transmitting by conventional means the measurement result on qubits 1 and 2 to location B requires as

$\to$ actions taken by the receiving site B the following transformations on qubit 3 as transmitted by entanglement:

$\leadsto$ $| 0_1 0_2 > \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; (no change)

$\leadsto$ $| 0_1 1_2 > \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; (flipping $| 0 >$ and $| 1 >$)

$\leadsto$ $| 1_1 0_2 > \to \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$; (phase shift of $| 0 >$ by 180^o)

$\leadsto$ $| 1_1 1_2 > \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; (flipping $| 0 >$, $| 1 >$ and phase shifting $| 0 >$)

These transformations are carried out by the circuit B, which returns the input $| \Psi >$ on line 3 and some garbage $| \Phi >$ on lines 1 and 2.

10 Quantum error correction

Errors in quantum computing are due to various physical phenomena that destabilize the states of qubits | qubit-registers, the major causes being dissipation and decoherence, caused by cosmic radiation, entanglement with environments, and spontaneous emission of radiation. It is also fairly difficult to sustain desired entanglements of quantum states until needed for operations.

10.1 Decoherence and dissipation

$\rightarrow$ Dissipation is a process whereby qubits lose energy to their environments $\rightsquigarrow$ by emitting photons while going from an excited state representing $\mid 1>$ to a ground state representing $\mid 0>$;
$\rightarrow$ Decoherence is due to a coupling between two (or more) initially isolated qubits | quantum states that randomizes the relative phases of register states $\rightsquigarrow$ the qubits become entangled with their environments $\rightsquigarrow$ this effect may best be described in terms of density matrices.

We remember that the density matrix of a quantum state $\mid \Psi >$ is defined as $\rho = \mid \Psi >< \Psi \mid$. If $\mid \Psi >= \alpha \mid 0 > + \beta \mid 1 >$for a single qubit, then the density matrix is given as

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

The effect of decoherence consists in a degradation of the off-diagonal elements over time, which may be expressed as:

$$\rho = \begin{pmatrix} |\alpha|^2 & e^{-t/\tau} * \alpha\beta^* \\ e^{-t/\tau} * \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

where τ is the decoherence time, which is a measure of how long it takes for the off-diagonal elements to degrade half-way down to 0 (at which point we have complete entanglement).

Decoherence times are much shorter than dissipation times, typical values for τ (in seconds) are:

	time per operation	coherence time	no of steps
GaAs electrons	10^{-13}	10^{-10}	10^3
In ion traps	10^{-14}	10^{-1}	10^{13}
electron spin	10^{-7}	10^{-3}	10^4
electron quantum dot	10^{-6}	10^{-3}	10^3
nuclear spin	10^{-3}	10^4	10^7

10.2 Stabilizing quantum computations

The basic idea behind stabilization is to replicate a computation on some quantum state $\mid \phi > \in H$ r times and to correct small deviations over time in each of these computations by projection into a so-called symmetric subspace which may contain the correct state.

Suppose we have a quantum computer whose correct state at time t is given as $\mid \phi(t) > \in H$ (where H is an n-dimensional Hilbert space), then r identical replicas would produce a correct state at time t that has the form:

$$\mid \Psi(t) >= \underbrace{\mid \phi(t) > \otimes \mid \phi(t) > \otimes \ldots \otimes \mid \phi(t)}_{r} >$$

This quantum state is symmetric against permutations of the components of the tensor product and thus element of a symmetric subspace $S^{(r)}$, i.e., we have $\mid \Psi(t) > \in S^{(r)} \subseteq H^{(r)}$. $S^{(r)}$ is assumed to be the smallest subspace of $H^{(r)} = \underbrace{H \otimes H \otimes \ldots \otimes H}_{r}$ that contains all the states $\underbrace{\mid \Phi > \otimes \mid \Phi > \otimes \ldots \otimes \mid \Phi >}_{r}$ with $\mid \Phi > \in H$.

However, with small deviations over time due to errors, the quantum state of the r computations would look like this:

$$|\,\overline{\Psi(t)}>=|\,\phi^{(0)}(t)>\otimes|\,\phi^{(1)}(t)>\otimes\ldots|\,\phi^{(r)}(t)>\notin S^{(r)}$$

i.e., the incorrect state is not anymore symmetric against permutations if there are pairs of states $|\,\phi^{(i)}(t)>\neq|\,\phi^{(j)}(t)>$ of the individual computers.

The idea of correction now is to project the erroneous state $|\,\overline{\Psi(t)}>$ back into $S^{(r)}$ which removes the erroneous components and leaves the correct components intact. However, it is important to note that this projection does not correct all deviations since the subspace $S^{(r)}$ also contains non-symmetric quantum states.

Realizing this correction requires a quantum register composed of $r*n$ qubits to accommodate the r replicas of $|\,\phi(t)>$ and some smallest integer greater than $log\,r$ of so-called ancilla qubits, initially set to 0, to specify a set of $r!$ permutations $\{\sigma_i \mid 0\leq i\leq r!\}$ of the r replicas, i.e., the register looks like this:

$$|\,0^{|log\,r|},\ \phi^{(0)}(t),\ \phi^{(1)}(t),\ldots\ \phi^{(r-1)}(t)>$$

.

The projection algorithm now works as follows:

- apply to the ancilla qubits of the register a transformation $\hat{U}$ which generates an equally weighted linear combination of vectors $i\in\{\,0,\ldots,\ r!-1\}$ representing permutations of the r state components $|\,\phi^{(j)}(t)>\ \mid j\in\{\,0,\ldots,\ r-1\,\}$:

$$\hat{U}|\,00\ldots0>=(1/r!)*\sum_{i=0}^{r!-1}|\,i>$$

(which, other than for the range of i is similar to Hadamard transformation).

- apply now to the full register | state

$$|\,\Psi(t)>=(1/r!)*\sum_{i=0}^{r!-1}|\,i,\ \phi^{(0)}(t),\ldots,\ \phi^{(r-1)}(t)>$$

a unitary transformation P (for permutation) which effects

$$P|\,i,\ \phi^{(0)}(t),\ldots,\ \phi^{(r-1)}(t)>=|\,i,\ \phi^{\sigma_i(0)}(t),\ldots,\ \phi^{\sigma_i(r-1)}(t)>$$

on each individual state, resulting in a superimposed state

$$|\,\Theta(t)>=(1/r!)*\sum_{i=0}^{r!-1}|\,i,\ \phi^{\sigma_i(0)}(t),\ldots,\ \phi^{\sigma_i(r-1)}(t)>$$

where $\sigma_i(j)$ denotes the original index of $\phi(t)$ that has been permuted into the position j by σ_i.

- applying now the reverse $\hat{U}^{-1}$ of $\hat{U}$ to the ancilla qubits should return the quantum state

$$|\,\overline{\Theta}>=|\,00\ldots0>(1/r!)*\sum_{i=0}^{r!-1}|\,\phi^{\sigma_i(0)}(t),\ldots,\ \phi^{\sigma_i(r-1)}(t)>$$

i.e., we should get a summation with equal probability amplitudes over all permutations of $\phi^{(0)}(t),\ldots,\ \phi^{(r-1)}(t)$, meaning that in each partition of the quantum register we should have a sum

$$\overline{\phi(t)}=\sum_{i=0}^{r!-1}\phi^{(i)}(t)$$

$\rightsquigarrow$ all partitions contain the same quantum state and we are back in $S^{(r)}$.

- if a measurement of the ancilla bits at this point indeed returns the state $\mid 00\ldots0>$ we have a quantum state over the entire register (minus the ancilla qubits) of

$$\mid \phi(t),\ \phi(t), \ldots,\ \phi(t) >\in S^{(r)}$$

otherwise symmetrization fails. However, again, symmetrization must not necessarily restore a correct quantum state $\leadsto$ there are other than symmetric states in $S^{(r)}$, into which the erroneous state may be projected.

10.3 Error models

The effects of errors on single qubits may be described by means of the Pauli operators

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

a linear combination of which is known to describe any transformation on a qubit. When applied to a quantum state $\alpha\mid 0> +\beta\mid 1>$,
$\leadsto$ σ_x causes a bit flip $\alpha\mid 0> +\beta\mid 1>\to \beta\mid 0> +\alpha\mid 1>$;
$\leadsto$ σ_z causes a phase shift $\alpha\mid 0> +\beta\mid 1>\to \alpha\mid 0> -\beta\mid 1>$;
$\leadsto$ σ_y causes both a bit flip and a phase shift $\alpha\mid 0> +\beta\mid 1>\to -i\beta\mid 0> +i\alpha\mid 1>$;
$\leadsto$ I describes the no-error state, i.e., it leaves the state as it is.

Any error on single qubits may be described by a linear combination of $\sigma_x,\ \sigma_y,\ \sigma_z,\ I$, and errors on the qubits of an n qubit register may be described by tensor products of the form $m = \otimes_{i=0}^{n-1}\ m_i$, with m_i being the error of the i-th qubit.

Classical error correction requires detecting an error by measurement of the state of a register. This is not possible in a quantum system as measurements collapse superimposed into base states, which rules out error correction, say, by (triple) modular redundancy and majority voting. Three independent quantum computers may perform the same computations and arrive at the same superimposed state, but measurement may collapse them into different base states, i.e., majority voting makes no sense at all.

10.4 Quantum error correcting codes

The basic idea here is to encode the state of a single logical qubit into a correlation among several physical qubits, hoping that in case of an error in one of these physical qubits there is enough information left in the correlation of the remaining qubits to correct the deviation.

An example of an encoding using entangled states of five qubits is due to Divicenzo and Shor:

$$\begin{aligned} \mid 0_L > \quad = \quad & (1/2\sqrt{2}) * (\mid 00000 > +\mid 00110 > +\mid 01001 > \\ & -\mid 01111 > +\mid 10011 > +\mid 10101 > \\ & +\mid 11010 > -\mid 11100 >) \end{aligned}$$

The encoding for $\mid 1_L >$ has all qubits in the code pattern of $\mid 0_L >$ flipped.

This encoding may be generated by means of the rotating operators

$$L = (1/\sqrt{2}) * \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad R = (1/\sqrt{2}) * \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

using the circuitry shown in fig. ??. Mirroring this circuit produces outputs $\mid \phi_0 > \ldots \mid \phi_4 >$ on the output lines $0\ldots4$. If no errors occur, the outputs will be $\mid \phi_0 >= \mid \Psi > \ \mid\mid \phi_1\ \ldots\ \phi_4 >= \mid 0000 >$, otherwise the outputs $1\ldots4$ carry error syndromes which identify the corrective actions that need to be taken.

Correction involves rotating one of the qubits as shown for a few typical errors in the following table:

error type	syndrome	correction
$P4$	1110	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$BP4$	1100	$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$
$B5$	1010	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$P2$	1101	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$BP2$	0100	$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$
$BP1$	0100	$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$

(with Pi, Bi, BPi respectively denoting a phase shift error, a bit flip error, and a combination of both in qubit i).

Other codes may be obtained by changing the base, e.g., by applying a Hadamard transformation so that

$$| 0'_L >= (1/\sqrt{2})(| 0_L > +| 1_L >) \quad | 1'_L >= (1/\sqrt{2})(| 0_L > -| 1_L >)$$

10.5 The basics of error correction

Error correction begins with an encoding of some k qubits into $n > k$ qubits, using a unitary transformation

$$E(| \Phi > \ | 0^{(n-k)} >) \to | \Phi_E >$$

where $| \Phi >$ is the unencoded k qubit quantum state, and $| \Phi_E >$ is the n qubit encoded state. Occurrences of errors transform $| \Phi_E >$ by some (not necessarily unitary) operator as $| \Phi_E > \to |\epsilon \ \Phi_E >$. Error correction first entangles the erroneous state $|\epsilon \ \Phi_E >$ with some auxiliary state $| A >$ and then applies some error correcting measure that transforms the entangled state into a tensor product of the original state and a new ancilla state $| A_\epsilon >$ that identifies the corrective action

$$| \epsilon\Phi_E > | A > \to | \Phi_E.| A_\epsilon >$$

to be taken on $| \epsilon\Phi_E >$:

11 Quantum automata and Turing machines

are to study some fundamental questions concerning quantum computability, its power and limitations in comparison to the respective classical models.

11.1 Classical finite automata

include

$\to$ deterministic finite automata (DFA) defined as n-tuples $A = (\ Q,\ \Sigma,\ q_0,\ Q_a,\ \delta\ )$ where

$\rightsquigarrow$ Q is a finite set of states;
$\rightsquigarrow$ Σ is the input alphabet;
$\rightsquigarrow$ $q_0 \in Q$ is the initial state;
$\rightsquigarrow$ $Q_a \subseteq Q$ is the subset of accepting states;
$\rightsquigarrow$ $\delta : Q \times \Sigma \rightarrow Q$ is the state transforming function.

DFAs come in two versions, based on the notion that the input is a tape from which a control unit with internal state $q \in Q$ reads input symbols
$\rightarrow$ the one-way finite automaton 1DFA reads symbols from the tape from left to right, working like the standard model of an automaton;
$\rightarrow$ the two-way automaton 2DFA moves a read head left and right across the input tape, and may also stay in particular tape position for more than one read action, i.e., the state transition function is defined as

$$\delta : Q \times \Sigma \rightarrow Q \times \{\leftarrow, \downarrow, \rightarrow\}$$

$\rightarrow$ the non-deterministic finite automaton (NFA) makes a non-deterministic choice of a next state, which may be described by a transition function

$$\delta : Q \times \Sigma \times Q \rightarrow \{0, 1\}$$

(or by a transition relation $\delta \subseteq Q \times \Sigma \times Q$).

$\rightarrow$ the probabilistic finite automaton (PFA) makes a probabilistic choice of next states, with a transition function

$$\delta : Q \times \Sigma \times Q \rightarrow [0, 1]$$

so that for each $q \in Q$ and $\sigma \in \Sigma$ we have a local probability criterion $\sum_{q' \in Q} \delta(q, \sigma, q') = 1$.

It is known from classical automata theory that both deterministic models and the non-deterministic model accept the same set of languages $\rightarrow$ regular languages; the same applies to probabilistic automata, if required to work in linear time wrt the size of the input. In some special cases, a PFA may also accept other than regular languages.

11.2 One-way quantum automata

are to model very simple quantum processors at work. They are defined as:

$$A = (\ Q,\ \Sigma,\ q_0,\ Q_a,\ Q_r,\ \delta\ )$$

with Q, Σ, q_0 as in the case of a classical FA, and with
$\rightsquigarrow$ $Q_a \subseteq Q$ as set of accepting states;
$\rightsquigarrow$ $Q_r \subseteq Q$ as set of rejecting states;
$\rightsquigarrow$ $Q_a \cap Q_r = \emptyset$
$\rightsquigarrow$ a transition function $\delta : Q \times \Gamma \times Q \rightarrow C_{[0,1]}$, where $\Gamma = \Sigma \cup \{\$, \#\}$ is the tape alphabet, and #,$ are unique start and end markers not belonging to Σ.

Evolution of A takes place in the inner product space with base

$$E_p = \{ | \, q > \ | \, q \in Q \}$$

which is operated on by the set of unitary operators $\{V_\sigma \mid \sigma \in \Sigma\}$ selected by the input symbols so that

$$V_\sigma | \, q >= \sum_{q' \in Q} \delta(q, \sigma, q') | \, q' >$$

There is an orthogonal decomposition of E_p into $E_p = E_n \uplus E_a \uplus E_r$ with $E_a = \{| q > \mid q \in Q_a\}$, $E_r = \{| q > \mid q \in Q_r\}$ and E_n being orthogonal to both E_a and E_r.

A measurement of the evolving quantum state would have to map it into the subspaces E_n (where the computation continues), E_a (where the computation terminates with acceptance of the input sequence), and E_r (where the input sequence is rejected as not belonging to the particular language). An observable O_p corresponding to this decomposition of E_p uses the projection operators P_u ($u \in \{a, r, n\}$).

A computation performed by the automaton on an input sequence $\#\sigma_1\sigma_2\ldots\sigma_n\$$ goes through the following steps:

- it applies the operator $V_{\sigma' \in \Gamma}$ selected by the actual input symbol to the actual state, yielding $| \Psi >= V_{\sigma'} | q >$
- next the observable O_p is applied to $| \Psi >$ to project it into a vector $| \Psi' >$ of one of the subspaces $E_a,\ E_r,\ E_n$: $| \Psi' >= P_u \mid \Psi >$;
- if
  $\rightsquigarrow$ $| \Psi' > \in E_r$, then the input is rejected;
  $\rightsquigarrow$ $| \Psi' > \in E_a$, then the input is accepted;
  $\rightsquigarrow$ $| \Psi' > \in E_n$, then after normalization, the next operator is applied to the resulting state.

The computation may thus be defined as

$$V'_\$ \, V'_{\sigma_n} \, V'_{\sigma_{n-1}} \ldots V'_{\sigma_1} \, V'_{\sigma_1} \, V'_\# \mid q_0 >$$

with applications of $V'_{\sigma_i} = P_u V_{\sigma_i}$ continuing as long as there are projections into E_n.

To define the probability of having some input sequence $\#\sigma_1\sigma_2\ldots\sigma_n\$$ accepted or rejected, we define the set of total states $S_a = E_p \times C \times C$ of the automaton. Then we have $(| \Psi >,\ p_a,\ p_r) \in S_a$ for some actual state, meaning that the input sequence processed sofar has probability p_a of being accepted, p_r of being rejected, and $1 - p_a - p_r$ =—Ψ—^{2} of being neither rejected nor accepted.We can now define an operator T_σ acting on the current total state upon input symbol σ:

$$T_\sigma(| \Psi >,\ p_a,\ p_r) = (P_n V_\sigma | \Psi >, p_a + ||P_a V_\sigma | \Psi > ||^2,\ p_r + ||P_r V_\sigma | \Psi > ||^2)$$

so that we get

$$T_{\#\sigma_1\sigma_2\ldots\sigma_n\$}(| q_0 >,\ 0,\ 0) = (| \Psi >,\ p_a,\ p_r)$$

The automaton A is said to accept some language L with probability $1/2 + \epsilon \mid \epsilon > 0$ if every input sequence belonging to L is accepted with probability $1/2 + \epsilon$, and every input sequence not belonging to L is rejected with probability $1/2 + \epsilon$.

$\Rightarrow$

Example: Construction of a 1QFA that recognizes | accepts the language $L = \{0^i 1^j \mid i, j \geq 0\}$. The base states of such an automaton are chosen as $Q = \{q_0,\ q_1,\ q_2,\ q_a,\ q_r\}$ with q_0 as initial state, and $Q_a = \{q_a\}$, $Q_r = \{q_r\}$. The operator V_σ is defined thus:

$$\begin{aligned}
V_\# | q_0 > &= \sqrt{1-p} \mid q_1 > + \sqrt{p} \mid q_2 > \\
V_0 | q_1 > &= (1-p) \mid q_1 > + \sqrt{p(p-1)} \mid q_2 > + \sqrt{p} \mid q_r > \\
V_0 | q_2 > &= \sqrt{p(1-p)} \mid q_1 > + p \mid q_2 > + \sqrt{1-p} \mid q_r > \\
V_1 | q_1 > &= | q_r > \quad V_1 | q_2 > \ = \ | q_2 > \\
V_\$ | q_1 > &= | q_r > \quad V_\$ | q_2 > \ = \ | q_a >
\end{aligned}$$

$\rightarrow$ consider now the case that the input is $x = \#0^i\$$, then we have the following steps

$$
\begin{aligned}
V_{\#} \mid q_0 > \quad &= \quad \sqrt{1-p} \mid q_1 > + \sqrt{p} \mid q_2 > \\
V_0(\sqrt{1-p} \mid q_1 > + \sqrt{p} \mid q_2 >) \quad &= \quad \sqrt{1-p} \mid q_1 > + \sqrt{p} \mid q_2 >
\end{aligned}
$$

i.e., V_0 reproduces the initial state while reading inputs 0. Finally, we have

$$V_{\$}(\sqrt{1-p} \mid q_1 > + \sqrt{p} \mid q_2 >) = \sqrt{1-p} \mid q_r > + \sqrt{p} \mid q_a >$$

$\leadsto$ When assuming a value $p = 1 - p^3$ (or $p \approx 0.68$) we find that $p > \sqrt{1-p}$, i.e., the sequence 0^i is accepted by the automaton.
$\rightarrow$ if the input is of the form $x = \#0^i1^j\$$, the automaton behaves the same as in the preceding case until it reads the first 1; then it transforms

$$V_1(\sqrt{1-p} \mid q_1 > + p \mid q_2 >) = \sqrt{1-p} \mid q_r > + p \mid q_2 > \quad .$$

This state is reproduced by all subsequent applications of V_1 until the \$ symbol is encountered. Then we get

$$V_{\$}(\sqrt{1-p} \mid q_r > + p \mid q_2 >) = \sqrt{1-p} \mid q_r > + p \mid q_a >$$

i.e., 0^i1^j is accepted since again we have $p > \sqrt{1-p}$.
$\rightarrow$ in all other cases we will have probabilities for outcome $\mid q_r >$ greater than probabilities for outcome $\mid q_a >$.

$\Leftarrow$

11.3 Two-way quantum finite automata (2QFA)

are the quantum counterparts of the classical 2FA, but are more powerful insofar as, beyond regular languages, they can also be made to accept special cases of non-regular languages.

A 2QFA is defined as

$$A = (Q,\ \Sigma,\ q_0,\ Q_a,\ Q_r,\ D,\ \delta)$$

with $D = \{\leftarrow, \downarrow, \rightarrow\}$ as the set of directions in which the read head may be moved over the tape, and $\delta : Q \times \Gamma \times Q \times D \rightarrow C_{[0,1]}$ as the transition function (all other symbols are the same as in the 1QFA).

The definition of the transition function δ has to satisfy the following criteria in order for the transformations on the respective quantum states to be unitary.

- local probability and orthogonality:
  $\sum_{q',d} \delta^*(q_1, \sigma, q', d)\ \delta(q_2, \sigma, q', d) = \begin{cases} 1 & \text{if } q_1 = q_2 \\ 0 & \text{otherwise} \end{cases}$
  (with $d \in D$)

- separability:
  $\rightarrow\ \sum_{q'} \delta^*(q_1, \sigma_1, q', \rightarrow)\ \delta(q_2, \sigma_2, q', \downarrow) = 0;$

  $\rightarrow\ \sum_{q'} \delta^*(q_1, \sigma_1, q', \downarrow)\ \delta(q_2, \sigma_2, q', \leftarrow) = 0;$

  $\rightarrow\ \sum_{q'} \delta^*(q_1, \sigma_1, q', \leftarrow)\ \delta(q_2, \sigma_2, q', \rightarrow) = 0;$

For some integer n, let K_n be the set of configurations of the automaton (which has cardinality $(n+2)*|Q|$), n being the length of the input $x \in \Sigma^n$, then a particular configuration is uniquely defined by a pair $(q,k) \in K_n$, where k is the actual position of the read head on the tape (with $0 \leq k \leq |x|+2$).

Let $E_K = \{| \, p, \, k > \; | \, (p.k) \in K_n\}$ denote the base of a configuration space, then we have for each state $\sum_{c \in K_n} \alpha_c | \, c >$ with $\sum_{c \in K_n} |\alpha_c|^2 = 1$.

For any input $x \in \Sigma^n$, the automaton A applies an operator U_x^δ to a configuration $| \, q, k >$ such that

$$U_x^\delta | \, q, k > = \sum_{q',d} \delta(q, x(k), q', d) | \, q', (k + \nu(d)) mod(n+2) >$$

where $x(k)$ denotes the symbol in the k-th position of x and $\nu(d) \in \{-1, 0, +1\}$ defines the movement of the head position (with -1, 0, $+1$ corresponding to $\leftarrow$, $\downarrow$, $\rightarrow$, respectively). U_x^δ being a linear operator, it also maps superpositions of base states.

Since proofs of the above criteria for unitarity of the operators U_x^δ are generally very difficult, it is more convenient to consider simpler forms of 2QFAs, which make the next move of the head dependent only on the next state reached.

$\rightarrow$ Automaton A is said to be simple (or unidirectional) if for each $\sigma \in \Sigma$ there is a linear operator V_σ on vectors in E_K and a function $\Delta : Q \rightarrow D$ such that for each $q \in Q$, $\sigma \in \Sigma$ we have

$$\delta(q, \sigma, q', d) = \begin{cases} < q' \, |V_\sigma| \, q > & \text{if } \Delta(q') = d \\ 0 & \text{otherwise} \end{cases}$$

i.e., we get

$$V_\sigma | \, q > = < q' \, |V_\sigma| \, q > | \, q' > \quad \text{for} \quad \delta(q, \sigma, q', d) | \, q' >$$

For such simple 2QFA the unitary criteria are satisfied iff for V_σ holds :

$$\sum_{q'} < q' \, |V_\sigma| \, q_1 >^* < q' \, |V_\sigma| \, q_2 > = \begin{cases} 1 & \text{if } q_1 = q_2 \\ 0 & \text{otherwise} \end{cases}$$

$\Rightarrow$

Example: of a 2QFA that accepts $L = \{0^i 1^j \mid i, j \geq 0\}\}$

with $Q = \{q_0, \, q_1, \, q_2, \, q_r, \, q_a\}$ and $Q_a = \{q_a\} \mid Q_r = \{q_r\}$
and with V_σ defined as in the following table (the direction arrows in the rightmost column derive from applying the function Δ to the states in the leftmost column):

	$V_\#$	V_0	V_1	$V_\$$	Δ
$\| q_0 >$	$\| q_0 >$	$\| q_0 >$	$\| q_1 >$	$\| q_1 >$	$\rightarrow$
$\| q_1 >$	$\| q_2 >$	$\| q_2 >$	$\| q_0 >$	$\| q_0 >$	$\leftarrow$
$\| q_2 >$	$\| q_r >$	$\| q_r >$	$\| q_2 >$	$\| q_a >$	$\rightarrow$
$\| q_a >$	$\| q_a >$	$\| q_a >$	$\| q_a >$	$\| q_2 >$	$\downarrow$
$\| q_r >$	$\| q_1 >$	$\| q_1 >$	$\| q_r >$	$\| q_r >$	$\downarrow$

$\rightarrow$ all operators V_σ of this automaton are obviously unitary (the can be applied forward and backward), and the automaton will accept all words of the language $\{0^i 1^j \mid i, j \geq 0\}$ with probability 1 and reject all words not belonging to this language with probability 1.
$\rightarrow$ consider as an example the input $\#0^3 1^2 \$$ which is processed as follows:

$$\begin{aligned}&| q_0, 0 > \rightarrow_{\#} | q_0, 1 > \rightarrow_0 | q_0, 2 > \rightarrow_0 | q_0, 3 > \rightarrow_0 | q_0, 4 > \\ &\qquad\qquad \rightarrow_1 | q_1, 3 > \rightarrow_0 | q_2, 4 > \rightarrow_1 | q_2, 5 > \rightarrow_1 | q_2, 6 > \rightarrow_{\$} | q_a, 6 >\end{aligned}$$

i.e., it terminates with the accepting state q_a. This contrasts with the sequence #0010$ which ends up in the rejecting state q_r:

$$\begin{aligned}&| q_0, 0 > \rightarrow_{\#} | q_0, 1 > \rightarrow_0 | q_0, 2 > \rightarrow_0 | q_0, 3 > \rightarrow_1 \\ &\qquad\qquad \rightarrow_1 | q_1, 2 > \rightarrow_0 | q_2, 3 > \rightarrow_1 | q_2, 4 > \rightarrow_0 | q_r, 4 >\end{aligned}$$

11.4 Outline of a 2QFA that accepts $L = \{0^i1^i \mid i \geq 0\}$

this is an example of a finite automaton that accepts a non-regular language, and thus is more powerful than its classical counterpart. It is defined as

$$A^{(n)} = (Q^{(n)},\ \{0,1\},\ q_0,\ Q_a^{(n)},\ Q_r^{(n)},\ D^{(n)},\ \delta^{(n)})$$

where n denotes some integer value to be chosen as explained later, and

$\rightsquigarrow$ $Q^{(n)} = \{q_0,\ q_1,\ q_2,\ q_3\}$
$\quad \cup \{r_{l,k} \mid 1 \leq l \leq n,\ 0 \leq k \leq max(l, n-l+1)\} \cup \{s_l \mid 1 \leq l \leq n\}$

$\rightsquigarrow$ $Q_a^{(n)} = \{s_n\};\ \ Q_r^{(n)} = \{q_3,\ s_1 \ldots s_{n-1}\}$

$\rightsquigarrow$ the transition function is defined as in the preceding subsection,and the operators V_σ are defined thus:

$$\begin{aligned}
&V_{\#}| q_0 >= | q_0 > \\
&V_{\#}| q_0 >= | q_0 > \\
&V_{\#}| r_{l,0} >= \tfrac{1}{\sqrt{n}} \textstyle\sum_{h=1}^{n} e^{(2\pi j/n)lh} | s_h >, (1 \leq l \leq n) \\
&V_{\$}| q_0 >= | q_3 > \\
&V_{\$}| q_2 >= \tfrac{1}{\sqrt{n}} \textstyle\sum_{l=1}^{n} | r_{l,0} > \\
&V_0| q_0 >= | q_0 > \\
&V_0| q_1 >= | q_1 > \\
&V_0| q_2 >= | q_3 > \\
&V_1| q_0 >= | q_2 > \\
&V_1| q_2 >= | q_2 > \\
&V_0| r_{l,0} >= | r_{l,l} >, (1 \leq l \leq n) \\
&V_0| r_{l,k} >= | r_{l,k-1} >, (1 \leq k \leq l,\ 1 \leq l \leq n) \\
&V_1| r_{l,0} >= | r_{l,n-l+1} >, (1 \leq l \leq n) \\
&V_1| r_{l,k} >= | r_{l,k-1} >, (1 \leq k \leq l \leq n)
\end{aligned}$$

the direction function $\Delta : Q \rightarrow D$ is:

$\Delta(q_0) = \rightarrow\ ||\ \Delta(q_1) = \leftarrow\ ||\ \Delta(q_2) = \rightarrow\ ||\ \Delta(q_3) = \downarrow$

$\Delta(r_{l,0}) = \leftarrow\ ||\ \Delta(r_{l,k}) = \downarrow\ ||\ \Delta(s_l) = \downarrow\ |\ 1 \leq l \leq n$

The computation of $A^{(n)}$ is organized in three phases:

- phase 1 traverses the input from left to right, involving only the states $q_0,\ q_1,\ q_2,\ q_3$, to accept inputs of the form 0^i1^j by ending up in state $| q_2 >$, with the head pointing at the end marker $, and to reject all other inputs (by ending up in state $| q_3 >$),

- phase 2 computes, after successful completion of phase 1, first $V_\$ \mid q_2 >$ to split the computation up into a superposition of n states $\mid r_{l,0} > \mid 1 \leq l \leq n$, each with amplitude $1/\sqrt{n}$, and then proceeds as follows:
  $\leadsto$ in the l-th path the head stays on each position with a $0 \mid 1$ in it for $l \mid n-l+1$ steps, respectively, and then moves one position to the left;
  $\leadsto$ an input sequence of the form 0^p1^q therefore requires $(l+1)*p+(n-l+2)*q+1$ steps to reach the left marker # in branch l. If for any pair of path indices l, l' we have

$$(l+1)*p+(n-l+2)*q+1 = (l'+1)*p+(n-l'+2)*q+1$$

  then and only then is $p = q$ (which then holds for all pairs $l \neq l'$), i.e., the sequence is from L, and all n heads (of the n superimposed paths) reach the left end marker # with the same number of steps.

- phase 3 applies the fast Fourier transform operator Q_{FFT} to the resulting state
  $\leadsto$ if $p = q$, then we obtain

$$\frac{1}{n}\sum_{h=1}^{n}\sum_{l=1}^{n} e^{(2\pi j/n)*h*l} \mid s_h >$$

  $\leadsto$ a measurement on this state returns $\mid s_n >$ with probability 1 (as only in this case we have $e^{(2\pi j/n)*l*n} = e^{2\pi j*l} = 1$ and a summation over n such 1s).
  $\leadsto$ if $p \neq q$, no two paths arrive at the left end marker with the same number of steps $\leadsto$ we get $\mid s_n >$ with probability $1/n$ accepted and with probability $1-1/n$ rejected. Thus, the larger n is chosen, the closer approaches the probability of acceptance 0 (and of rejection 1).

11.5 Quantum Turing machines (QTM)

have several things in common with two-way quantum finite automata, the basic difference being that the tape holds qubits which can be read and written (modified). QTMs are defined as

$$M = (\ \Sigma,\ Q,\ q_0,\ q_f,\ D,\ \delta\ )\ \mid D = \{\leftarrow, \downarrow, \rightarrow\}$$

where $q_0,\ q_f \in Q$ are initial and final states of the machine, Σ is the tape alphabet, and

$$\delta:\ Q \times \Sigma \times \Sigma \times Q \times D \rightarrow C_{[0,1]}$$

is the transition function which specifies probability amplitudes for going from one machine constellation to another. This function must specify unitary quantum state transformations, otherwise the machine is called a quasi-QTM, or qQTM for short.
$\rightarrow$ a constellation of M is described by a tuple $(\ q,\ \tau,\ i\ ) \in Q \times \Sigma^Z \times Z$ where
$\leadsto$ q denotes the actual state of the head;
$\leadsto$ τ denotes the actual contents of the tape;
$\leadsto$ i specifies the actual position on the tape of the head.
Let K_M denote the set of constellations of M, then computations of M are performed in the constellation space H_M with basis $\{\mid c > \mid c \in K_M\}$, with $\mid c >= \mid q > \mid \tau > \mid i >$.
$\rightarrow$ the transition function δ uniquely defines a mapping $h:\ K_M \times K_M \rightarrow C_{[0,1]}$ such that for constellations $c_1, c_2 \in K_m$ we have $h(c_1, c_2)$ as the probability amplitude of transforming base state $\mid c_1 >$ into base state $\mid c_2 >$.
$\rightarrow$ the evolution of M over time is then defined as

$$U_M:\ H_M \rightarrow H_M \quad \text{with} \quad U_M \mid c >= \sum_{c' \in K_M} h(c, c') \mid c' >$$

and if $| \Phi >= \sum_{c \in K_M} \alpha_c | c >$ is a superposition of configurations, then

$$U_M | \Phi >= \sum_{c \in K_M} \alpha_c U_M | c >$$

For the machine to perform unitary operations, i.e., to be truly a QTM, similar criteria as for a 2QFA need to be satisfied:

- local probability condition:
  for any $(q_1, \sigma_1) \in Q \times \Sigma \;:\; \sum_{(\sigma,q,d) \in \Sigma \times Q \times D} | \delta(q, \sigma_1, \sigma, q, d) |^2 = 1$
- separability conditions:
  $\rightsquigarrow$ for any two pairs $(q_1, \sigma_1),\ (q_2, \sigma_2) \in Q \times \Sigma :$
  $\sum_{(q,\sigma,d) \in Q \times \Sigma \times D} \delta^*(q_1, \sigma_1, \sigma, q, d) \delta(q_2, \sigma_2, \sigma, q, d) = 0;$

  $\rightsquigarrow$ for any $(q, \sigma, d), (q', \sigma', d') \in Q \times \Sigma \times D$ and $(q, \sigma, d) \neq (q', \sigma', d') :$
  $\sum_{(q_1,\sigma_1) \in Q \times \Sigma} \delta^*(q_1, \sigma_1, \sigma, q, d) \delta(q_1, \sigma_1, \sigma', q', d') = 0;$

  $\rightsquigarrow$ for any $(q_1, \sigma_1, \sigma_1'),\ (q_2, \sigma_2, \sigma_2') \in Q \times \Sigma \times \Sigma \ | \ d_1,\ d_2 \in D$ and $d_1 \neq d_2 :$
  $\sum_{q \in Q} \delta^*(q_1, \sigma_1, \sigma_1', q, d_1) \delta(q_2, \sigma_2, \sigma_2', q, d_2) = 0;$

$\rightarrow$ a computation of M then is a sequence of configurations $| c_0 >,\ | c_1 >,\ | c_2 >,\ \ldots,\ | c_{n-1} >,\ | c_n >$, where $| c_0 >$ is the initial configuration and for each $i \in \{0 \ldots, n-1\}$ we have
$\rightsquigarrow$ either $| c_i >= U_M | c_{i-1} >$
$\rightsquigarrow$ or $| c_i >$ is obtained from $| c_{i-1} >$ by an observation | a measurement.

Since it is generally very difficult to prove that a transition function δ satisfies the unitarity conditions listed above, the same restrictions on the movement of the head as in the case of the 2QFA have led to more manageable QTM models. A unidirectional quantum Turing machine M (or a uQTM) has the property that for any pair $(q_1, \sigma_1, \sigma_1'),\ (q_2, \sigma_2, \sigma_2') \in Q \times \Sigma \times \Sigma$ holds $d_1 = d_2$ whenever $\delta(q_1, \sigma_1, \sigma_1', q, d)$ and $\delta(q_2, \sigma_2, \sigma_2', q, d)$, i.e., the direction in which the head moves next solely depends on the state $q \in Q$ reached, irrespective of the preceding state and the symbol found (and modified) on the tape.

It has been shown that a uQTM can simulate a QTM with a slowdown of at most a factor of 5.

Constructing a QTM faces several problems:
$\rightarrow$ evolutions | operations must be unitary (or reversible), making it difficult to realize such basic functions as composition (of functions), branching and looping, which are essential for non-trivial computations;
$\rightarrow$ computational paths created by superpositions must, as in the case of the 2QFA described in the preceding subsection, be carefully synchronized to perform the same number of steps, as otherwise no interference between the paths would be possible $\rightsquigarrow$ synchronization requires configurations with the same tape contents, head positions and states.

Overcoming these constructive problems necessitates some standardizations of QTMs:
$\rightarrow$ A QTM is said to be well-behaved if for all inputs (initial tape contents) it halts with all configurations in a specific final state and has the head in the same tape position;
$\rightsquigarrow$ if the halting is also the starting position, then the QTM is called stationary.
$\rightsquigarrow$ the QTM is said to be in normal form if each transition from the final state is into the initial state.

$\Rightarrow$

Example: of a stationary, normal form QTM which maps a state $\mid \Psi >$ into a Hadamard transformed state.
We have in this machine an alphabet $\Sigma = \{0, 1, \#\}$ (# being a blank on the tape), a set of states $Q = \{q_0,\ q_a,\ q_b,\ q_c,\ q_f\}$, and the following transition function:

	#	0	1
q_0		$\mid q_a, 0, \leftarrow>$	$\mid q_a, 1, \leftarrow>$
q_a	$\mid q_b, \#, \rightarrow>$		
q_b	$\mid q_c, \#, \leftarrow>$	$\frac{1}{\sqrt{2}}(\mid q_b, 0, \rightarrow> + \mid q_b, 1, \rightarrow>)$	$\frac{1}{\sqrt{2}}(\mid q_b, 0, \rightarrow> - \mid q_b, 1, \rightarrow>)$
q_c	$\mid q_f, \#, \rightarrow>$	$\mid q_c, 0, \leftarrow>$	$\mid q_c, 1, \leftarrow>$
q_f	$\mid q_0, \#, \rightarrow>$	$\mid q_0, 0, \rightarrow>$	$\mid q_0, 1, \rightarrow>$

This machine processes a string $x \in \{0, 1\}^*$ by
$\rightsquigarrow$ starting at state q_0 and moving left and right to enter state q_b;
$\rightsquigarrow$ moving in state q_b to the right while applying the Hadamard transformation to each qubit on the tape;
$\rightsquigarrow$ switching to state q_c upon hitting a blank # on the tape, and thereupon moving left in state q_c until reaching a blank on the left;
$\rightsquigarrow$ having this blank move the machine back to the first non-blank tape position, from where it goes into the final state q_f.
$\Leftarrow$

To implement some essential operations such as composition, branching and looping, we need to introduce, beyond stationary normal form QTMs, two more extensions.
$\rightarrow$ QTMs that have multiple tracks on the tape (or have tape alphabets that are Cartesian products of tape alphabets)
$\rightsquigarrow$ $M_{dt} = (\Sigma_1 \times \Sigma_2,\ Q,\ q_0,\ q_f,\ D,\ \delta)$.
Clearly, such a machine acts as a machine with a single track if the other track is left unchanged by all operations;
$\rightarrow$ QTMs that are composed of two QTMs with disjoint sets of states and transition functions but share the same alphabet
$\rightsquigarrow$ if $M_1 = (\Sigma,\ Q_1, \ldots,\ \delta_1)$, $M_2 = (\Sigma,\ Q_2, \ldots,\ \delta_2)$ are well formed QTMs, $Q_1 \cap Q_2 = \emptyset$, then the union of both machines, $M = (\Sigma,\ Q_1 \cup Q_2, \ldots, \delta_1 \cup \delta_2)$, is also a well formed QTM.

$\rightarrow$ Composition of two QTMs can now be achieved by the union M of two machines M_1 and M_2 with initial and final states $q_0^{(1)}$, $q_f^{(1)}$ and $q_0^{(2)}$, $q_f^{(2)}$, respectively.
$\rightsquigarrow$ since both M_1 and M_2 are in normal form, there is only one transition from $q_f^{(1)}$ to $q_0^{(1)}$ (or from $q_f^{(2)}$ to $q_0^{(2)}$).
$\rightsquigarrow$ all it takes to have M execute the machine M_1 followed by machine M_2 is to change the transition from $q_f^{(1)}$ to $q_0^{(1)}$ into $q_f^{(1)}$ to $q_0^{(2)}$.

$\rightarrow$ Branching requires, at the core, a stationary normal form QTM B with
$\rightsquigarrow$ the alphabet $\{\#, 1\}$;
$\rightsquigarrow$ the states $\{q_o,\ q_1,\ q_1',\ q_2,\ q_2',\ q_3,\ q_f\}$ and
$\rightsquigarrow$ the transition function

$$\begin{array}{ll}
(q_0,\ \#,\ \#,\ q_2',\ \leftarrow) & (q_0,\ 1,\ \#,\ q_1',\ \leftarrow) \\
(q_1,\ \#,\ 1,\ q_3,\ \leftarrow) & (q_1',\ \#,\ \#,\ q_1,\ \rightarrow) \\
(q_2,\ \#,\ \#,\ q_3,\ \leftarrow) & (q_2',\ \#,\ \#,\ q_2,\ \rightarrow) \\
(q_3,\ \#,\ \#,\ q_f,\ \rightarrow) & \\
(q_f,\ \#,\ \#,\ q_0,\ \rightarrow) & (q_f,\ 1,\ 1,\ q_0,\ \rightarrow)
\end{array}$$

This machine always does four transition steps. If the tape has in its starting position
$\leadsto$ a 1, and blanks # elsewhere, then it moves into state q_1, leaves a blank in the starting position, and eventually returns, through state q_3, to q_f and then to q_0, leaving a 1 in the starting position.
$\leadsto$ a blank # (and also blanks elsewhere), then it goes through essentially the same motions, except that it passes through state q_2 instead of q_1, leaving the blank in the starting position unchanged after having returned through q_f to q_0.

The full branching QTM can now be constructed as a two-track well behaved normal form machine which executes on its first track
$\leadsto$ a QTM M_1 if the second track contains all blanks (including the start position);
$\leadsto$ a QTM M_2 if the second track contains a 1 in the starting position and blanks otherwise.
To do so

- the single track machines M_1 and M_2 need to be extended to include a second track with alphabet $\Sigma_B = \{1, \#\}$;
- the machine B needs to be extended to have a first track with alphabet $\Sigma_{M_1} \cup \Sigma_{M_2}$;
- M_1 and M_2 need to be inserted for the states q_1 and q_2, respectively, of the machine B.

The full machine thus executes either n_1 steps of M_1 or n_2 steps of M_2, plus four steps of the machine B, which performs the basic branching mechanism.

$\rightarrow$ Looping can be accomplished by a normal form QTM which, given some binary coded value $k \in \{\ 1,\ 2,\ \ldots\}$ on its tape, performs some $O(k)$ steps without changing the tape, thereby moving through a special state q^s exactly k times, with its head on the starting position $\leadsto$ inserting for q^s the another QTM that realizes the loop body does the job.

At this point it should be noted that the constructs for composition, branching and looping can be done with a classical Turing machine; they do not involve any quantum mechanical states and operations. This is to say that Turing compatibilty of quantum computations can only be had when falling back on non-quantum mechanisms for the very basic operations of replication | repetition and of selection among alternatives which are essential for implementing terminating recursions $\leadsto$ only then can QTMs be constructed that realize any intuitively computable function.