# Part I
# Quantum mechanics

## 1 State spaces and bra/ket notation

The state space of a quantum system, consisting of the positions, moments, polarizations, spins, etc. of the various particles is modeled by a Hilbert space of wave functions. For quantum computing we need only deal with finite quantum systems and it suffices to consider finite dimensional complex vector spaces with an inner product that are spanned by abstract wave functions such as the vector $|\rightarrow\rangle$.

Quantum state spaces and the transformations acting on them can be described in terms of vectors and matrices or in the more compact bra/ket notation invented by Dirac. $|x\rangle$ represents a column vector and $\langle x| := |x\rangle^*$ (the conjugate gradient). So $\langle x|\,|z\rangle$ equals the inner product and $|x\rangle\,\langle z|$ gives a matrix mapping $|z\rangle$ to $|x\rangle$ (for an orthonormal basis only?). A matrix transformation changing the basis is $|x\rangle\,\langle z| + |z\rangle\,\langle x|$.

## 2 Quantum bits

A quantum bit, or qubit, is a unit vector in a two dimensional complex vector space for which a particular basis denoted by $\{|0\rangle, |1\rangle\}$ has been fixed. They can correspond for example to polarizations of photons or to the spin up spin down state of an electron. Unlike classical bits however, qubits can be in a **superposition** $a\,|0\rangle + b\,|1\rangle$ where $a$ and $b$ are complex numbers such that $|a|^2 + |b|^2 = 1$.

The measurement postulate of quantum mechanics states that any device measuring a 2-d system has an associated orthonormal basis with respect to which the quantum measurement takes place. **Measurement of a state transforms the state into one of the measuring device's associated basis vectors**. It is important to note that a second measurement with respect to the *same* basis will return the previous result with probability 1.

If a state $a\,|0\rangle + b\,|1\rangle$ is measured with respect to the basis $\{|0\rangle, |1\rangle\}$ the probability that the measured value is $|0\rangle$ is $|a|^2$ and of $|1\rangle$ is $|b|^2$, where $|a|^2 + |b|^2 = 1$. After measuring the state we change the original unknown state into either the state $1\,|0\rangle + 0\,|1\rangle = |0\rangle$ or the state $0\,|0\rangle + 1\,|1\rangle = |1\rangle$.

### 2.1 Multiple Qubits

In classical physics, the possible states of a system of $n$ particles, whose individual states can be described by a vector in a 2 dimensional vector space, form a vector space of $2n$ dimensions. Whereas in classical physics, a complete description of the state of this system requires only $n$ bits, in quantum

physics, a complete description of the state of this system requires $2^n - 1$ complex numbers. In a quantum system the resulting state space of a system of $n$ qubits has $2^n$ dimensions. The dimension of the state in classical physics corresponds to the Cartesian product of the individual vector spaces for each particle: $\dim(X \times Y) = \dim(X) + \dim(Y)$, whereas in a quantum system it corresponds to the tensor product: $\dim(X \otimes Y) = \dim(X) \times \dim(Y)$. For example, the basis for a three qubit system is denoted as:

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

where e.g. $|001\rangle$ is shorthand for $|0\rangle \otimes |0\rangle \otimes |1\rangle$.

The state $|00\rangle + |11\rangle$ is an example of a quantum state that cannot be described in terms of the state of each of it components (qubits) separately. In other words, we cannot find $a_1, a_2, b_1, b_2$ such that $(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) = |00\rangle + |11\rangle$. States that cannot be decomposed in this way are called **entangled states**. These are the states that have no classical counterpart and that provide the exponential growth of the state spaces with the number of particles. Measurement gives another way of thinking about entangled particles. Particles are not entangled if the measurement of one has no effect on the other.

## 2.2 Quantum Parallelism

Any arbitrary classical function $f$ with $m$ inputs and $k$ output bits can be implemented on a quantum computer. We can also build a quantum gatearray $U_f$ defined as a linear (unitary) transformation of the states to compute $f(x)$ as $U_f |x, 0\rangle = |x, f(x)\rangle$. If $U_f$ is applied to a superposition, then, since $U_f$ is a linear transformation, it is applied to all basis vectors in the superposition simultaneously and will generate a superposition of the results. In this way it is possible to compute $f(x)$ for $n$ values of $x$ in a single application of $U_f$. This effect is called **quantum parallelism**.

The power of quantum algorithms comes from taking advantage of quantum parallelism and entanglement. So most quantum algorithms begin by computing a function of interest on a superposition of all values as follows. Start with $n$-qubit state $|00\ldots0\rangle$. Apply the Walsh-Hammard transformation to the state to get a superposition

$$\frac{1}{\sqrt{2^n}} = \sum_{x=0}^{2^n-1} |x\rangle$$

which should be viewed as the superposition of all integers $0 \leq x < 2^n$. Add a $k$-bit register $|0\rangle$ then by linearity

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle\right) &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f |x, 0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle \end{aligned}$$

when you measure the state you get $|x_0, f(x_0)\rangle$ for some randomly chosen $x_0$. The heart of any quantum algorithm is the way in which it manipulates quantum parallelism so that desired results will be measured with high probability. One way is to amplify the output values of interest, i.e. to transform the state in such a way that values of interest have a larger amplitude and therefore have a higher probability of being measured. Another way is to find properties of all the values of $f(x)$. This idea is exploited in Shor's algorithm which uses a quantum Fourier transformation to obtain the period of $f$, i.e. after computing the superposition of all the values, he then computes the quantum Fourier transform of the function, which like classical Fourier transforms, puts all the amplitude of the function into multiples of the reciprocal of the period, which is then used to factor the integer $N$. The biggest complication is that the quantum Fourier transform is based on the fast Fourier transform and thus gives only approximate results in most cases.

# Part II
# Quantum computation

## 3 Introduction

The observation that several apparently different definitions of what it meant for a function to be computable yielded the same set of computable functions led to the proposal of **Church's thesis:** all computable devices can be simulated by a Turing machine. This thesis greatly simplifies the study of computation reducing the field of study from infinite potential computing devices to Turing machines.

It is generally accepted that efficient and inefficient computable functions is determined by whether the length of the computation scales polynomially or superpolynomially with the input size.

The class of problems that can be solved by algorithms having a number of steps polynomial in the input size is known as $\mathcal{P}$.

**Quantitative Church's Thesis**: Any physical (that can be built and made to work) computing device can be simulated by a Turing machine in a number of steps polynomial in the resources (space, time, precision, etc) used by the computing device.

-If we let the precision of a quantum computer grow polynomially in the input size (so the number of bits for precision grows logarithmically in the input size) we appear to obtain a more powerful computer. Allowing the same polynomial growth in precision does not appear to confer extra computing power to classical mechanics.-

Computer scientists have become convinced of the truth of the quantitative Church's thesis through the failure of all proposed counterexamples. Most of these proposed counterexamples have been based on the laws of classical

mechanics; however, the universe is in reality quantum mechanical. It seems plausible that the natural computing power of classical mechanics corresponds to that of Turing machines, while the natural computing power of quantum mechanics might be greater.

Benioff showed in 1980, 1982, that the reversible unitary evolution was sufficient to realize the computational power of a Turing machine, thus showing that quantum mechanics is computationally at least as powerful as classical computers. Feynman in 1982 and 1986 suggested that quantum mechanics might be computationally more powerful than Turing machines. In order to explore this, Deutsch defined in 1985 and 1989 the quantum Turing machines and quantum circuits.

Currently nobody knows how to build a quantum computer. The most difficult obstacles appear to be decoherence of quantum superpositions through the interaction of the computer with the environment (can be mitigated with quantum error correction), and the implementation of state transformations with enough precision. Both of these obstacles become more difficult as the size of the computer grows.

Even if no useful quantum computer is ever built, any general method for simulating quantum mechanics with at most a polynomial slowdown would lead to a polynomial-time algorithm for factoring.

# 4 Quantum computation

Computation is fundamentally a physical process, and that what can be computed efficiently may depend on subtle issues in physics.

A classical digital computer is a finite automaton, since any given computer has a fixed amount of memory, however, this representation is not particularly useful.

The complexity class BPP is viewed as the class of efficiently solvable problems, which require the aid of a random number generator and allowing a small probability of error.

If they are allowed a small probability of error, quantum Turing machines and quantum gate arrays can compute the same functions in polynomial time. The class of functions computable in quantum polynomial time with a small probability of error is called, by analogy to the classical class BPP, as BQP (bounded error probability quantum polynomial time).

In order to use a physical system for computation, we must be able to change the state of the system. The laws of quantum mechanics permit only unitary transformations of state vectors. A unitary matrix is one whose conjugate transpose is equal to its inverse, and requiring state transformations to be represented by unitary matrices ensures that summing the probability over all possible outcomes yields 1.

# 5 Quantum cryptographic algorithms

Even if large-scale quantum computers become a reality, this would not affect information-theoretic schemes such as one time pad. Not even all public key crypto is threatened by quantum computing: it has been argued [1] that there could be strong one-way functions that can be computed efficiently with classical computers and difficult to invert even with quantum computers. This suffices to achieve computationally secure pseudorandom generation, bit commitment schemes and zero-knowledge protocols for all of $\mathcal{NP}$. Information theoretic secure (i.e. unconditionally) quantum bit commitment is impossible [2].

# 6 Prime factorization and discrete logarithms [3]

In 1994 Peter Shor gave the first practical computational problem that quantum computers could solve faster than classical computers. Before his results no one was sure how to use the quantum effects to speed up computation even though there was the speculation that computation could be done more efficiently. (Although there is no proof that factoring is not in $\mathcal{P}$ in the classical setting).

## 6.1 Factorization

The exponent factorization method assumes we have an exponent $r > 0$ and an integer $a$ such that $a^r = 1 mod N$ ($r$ is the order of $a$). With high probability the algorithm will succeed computing the factors $p, q$ of $N$ as $p = gcd(a^{r/2} + 1, N)$ and $q = gcd(a^{r/2} - 1, N)$.

Given $N$ we select a random $a \in \{2, 3 \ldots, N-1\}$ (if $a$ is 0 or 1, the exponent factorization algorithm fails) and consider the sequence $1, a, a^2, a^3, \ldots mod N$. If $a^r = 1 mod N$, then this sequence will repeat every $r$ terms, so by computing the period (or any multiple of the period) $r$ of the function $f_N(x) = a^x mod N$ we will have an $r$ such that $a^r = 1 mod N$. Classically calculating $r$ is as difficult as trying to factor $N$. Quantum computers can potentially find $r$ in time which grows only as a quadratic function of the number of digits in $N$.

### 6.1.1 Quantum Fourier Transform

The discrete Fourier transform (DFT) of a (sampled) function ($L$ samples) of period $r$ is a function concentrated near multiples of $\frac{L}{r}$. If the period $r$ divides $L$ evenly, the result is a function that has non-zero values only at multiples of $\frac{L}{r}$. Otherwise the result approximates this behavior and the "biggest" values of the DFT will occur in the integers close to multiples of $\frac{L}{r}$.

The Fast Fourier transform (FFT) is a version of the DFT where $L = 2^m$ for some $m$. The quantum Fourier transform (QFT) is essentially the standard

FFT adapted for a quantum computer. It is defined as

$$U_{QFT} : |x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{2\pi icx/2^m} |c\rangle$$

The QFT operates on the amplitude of the quantum state by sending

$$\sum_{x=0}^{2^m-1} g(x) |x\rangle \rightarrow \sum_{c=0}^{2^m-1} G(c) |c\rangle$$

where $G(c)$ represents the DFT of $g(x)$. So if the state is measured after the QFT is performed, the probability that the result is $|c\rangle$ would be $|G(c)|^2$. Shor shows that the QFT is efficiently computable by using only $\frac{m(m+1)}{2}$ gates.

### 6.1.2 Shor's Algorithm

The steps of the algorithm are illustrated with an example where we factor $M = 21$.

1. Quantum parallelism: Choose an arbitrary integer $a$. Assume $\gcd(a, n) = 1$; otherwise we have a factor of n. Let $m$ be the solution to $N^2 \leq 2^m \leq 2N^2$. [This choice is made so that the approximation for functions whose period is not a power of 2 will be good enough for the rest of the algorithm to work.] Use the quantum parallelism to compute $f_N(x)$ for all integers from 0 to $2^m - 1$. The function is thus encoded in the quantum state

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x, f_N(x)\rangle$$

   If $a = 11$ then $m = 9$. If we measure the second part, the probability to obtain a measurement of 1 would be $43/2^9 \approx 1/6$ as $f_N(x)$ repeats every 6 terms, and the approximation comes from the fact that 6 does not divide $2^9$ for the FFT. I guess that for larger primes the period of $f_N(x)$ is much larger and the probability of measuring 1 immediately would decrease exponentially.

2. A step whose amplitude has the same period as $f_N(x)$: Measure the bits of the state encoding $f_N(x)$ (the last $\lceil \log_2 M \rceil$ qubits) obtaining a random value $u$. The value $u$ is not of interest in itself; only the effect the measurement has on our set of superpositions is of interest. This measurement projects the state space onto the subspace compatible with the measured value, so the state after measurement is

$$C \sum_{x=0}^{2^m-1} g(x) |x, u\rangle$$

where

$$g(x) = \begin{cases} 1 \text{ if } f_N(x) = u \\ 0 \text{ otherwise} \end{cases}$$

Notice that the x's appearing in the sum differ by multiples of the period, so $g(x)$ is the function we are looking for, in fact, $g(x)/C$ is the probability mass function of measuring $x$ after measuring $u$. In the above example with $a = 11$, if we measure the value 2, we would reduce our state to

$$\frac{1}{\sqrt{85}}(|5,2\rangle + |11,2\rangle + |17,2\rangle + \ldots + |503,2\rangle + |509,2\rangle)$$

if we could measure two elements $x$ and $y$ in the above sum we would have the period (or a multiple of it) since $11^x = 11^y mod 21$, and thus $r = y - x$. However the laws of quantum physics tells us that the second measurement would give the same answer as the first.

3. Applying a quantum Fourier transform: The $|u\rangle$ part of the state will not be used, so we will no longer write it. Apply the QFT to the state obtained above:

$$U_{QFT} : \sum_{x=0}^{2^m-1} g(x)\,|x\rangle \rightarrow \sum_{c=0}^{2^m-1} G(c)\,|c\rangle$$

where most of the amplitude of $G(c)$ will be close to $j\frac{2^m}{r}$ for some integer $j$.

4. Extracting the period: Making an observation of the state will give a result $v$. Shor showed that with high probability (of at least $1/3r^2$), $v$ is within $\frac{1}{2}$ of some $j\frac{2^m}{r}$, i.e.

$$\left| v - j\frac{2^m}{r} \right| < \frac{1}{2}$$

Since $2^m > N$ then with high probability $\frac{j}{r}$ is within $\frac{1}{2N^2}$ from $\frac{v}{2^m}$, i.e.

$$\left| \frac{v}{2^m} - \frac{j}{r} \right| < \frac{1}{2N^2}$$

Furthermore, two distinct rational numbers $\frac{j}{r}$ and $\frac{j'}{r'}$ with $0 < r < N$ and $0 < r' < N$ are separated more than $\frac{1}{N^2}$, i.e.

$$\left| \frac{j}{r} - \frac{j'}{r'} \right| > \frac{1}{N^2}$$

so we can use the (efficient) continued fractions algorithm to find a rational number $\frac{p}{q}$ s.t. $0 < q < N$ (within $\frac{1}{2N^2}$ of $\frac{v}{2^m}$, hopefully) and with high probability the rational number obtained will be $\frac{j}{r}$. We take the denominator $q$ of the obtained fraction as our guess for the period, which

will work when $j$ and $r$ are relatively prime ( so $q$ would be a factor of the period, and not the period itself). Shor shows that at least with probability $\phi(r)/3r$ (where $\phi$ is the Euler toitent function) we obtain $r$. It is known that $\phi(r)/r > \delta/\log\log r$ for some constant $\delta$, thus repeating the experiment $O(\log\log r)$ we are assured a high probability of success. We can also try nearby $v$'s or test for multiples of $q$ as heuristics, to avoid repetitions of the quantum evaluations.

5. Finding a factor of $N$: Since $(a^{r/2}-1)(a^{r/2}+1) = a^r - 1 = 0 mod N$, the numbers $\gcd(x^{r/2}-1, N)$ and $\gcd(x^{r/2}+1, N)$ will be factors of $N$. This procedure fails only if $r$ is odd, or if $x^{r/2} = -1 mod N$, in which case the procedure yields the trivial factors 1 and $N$. The algorithmic form is called the exponent factorization method: write $r$ as $2^k m$ with $m$ odd for some $k$. Let $b_0 = a^m mod N$. Square successively $b_0$ to get $b_1, b_2, \ldots$, until we reach $1 mod N$. If $b_u$ is the last $b_i \neq 1 mod N$, compute $\gcd(b_u - 1, N)$ to get a factor of $N$.

6. Repeat the algorithm if necessary: Various things could have gone wrong so that this process does not yield a factor of M: the value of $v$ is not within $\frac{1}{2}$ of $\frac{2^m}{r}$. The period $r$ and the multiplier $j$ could have had a common factor, or the exponent factorization method fails. However it is very likely that, in a few attempts, a factorization of $N$ will be found.

## 6.2 Discrete logarithms

For simplicity we will present the case assuming we can compute a DFT (to avoid the approximations made due to the FFT). Let $a$ be a generator of a group $G$ of order $q$. Given $b$, the discrete logarithm problem is to find a $0 < d < q-1$ such that $b = a^d$. Now consider the function $f(x,y) = a^x b^y$. Note that it has two independent periods

$$\begin{aligned} f(x+q, y) &= a^q a^x b^y = f(x,y) \\ f(x+d, y-1) &= a^d a^x b^y b^{-1} = f(x,y) \end{aligned}$$

so we can compute with quantum parallelism the above function to obtain

$$\frac{1}{q}\sum_{y=0}^{q-1}\sum_{x=0}^{q-1} |x, y, a^x b^y\rangle$$

so measuring the last register we obtain a value $a^{x_0}$ which implies that $x = x_0 - dy \bmod q$. the state is then

$$\frac{1}{q}\sum_{y=0}^{q} |x_0 - dy, y\rangle$$

Taking the DFT we obtain after simplification

$$\frac{1}{\sqrt{q}}\sum_{x'=0}^{q-1} e^{2\pi i x_0 x'/q} |x', y' = dx' mod\, q\rangle$$

So from a measurement of the states we can deduce $d = y'(x')^{-1} \, mod \, q$ if $\gcd(x', q) = 1$.

# 7 Quantum Key Distribution

The goal is to establish secret keys over unauthenticated channels without the need of public key cryptography. Most of the algorithms use an encoding based on two non-commuting observable (i.e. an eavesdropper cannot acquire sharp values of the two observables), e.g. rectilinear $\{|\rightarrow\rangle, |\uparrow\rangle\}$ and diagonal $\{|\nearrow\rangle, |\nwarrow\rangle\}$ polarizations of photons. If a photon is polarized as $|\rightarrow\rangle$, the probability of being read in the basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$is $1/2$ for each base.

The transmitter sends photons with one of the four polarizations (0 or 1 in rectilinear or diagonal form), with basis chosen at random. The receiver chooses at random the type of measurement but keeps it secret. Subsequently the receiver announces the type of measurement and the sender tells the receiver which measurements were of the correct type. An eavesdropper introduces error to this transmission because he does not know in advance the type of polarization of each photon. The two legitimate users of the quantum channel test for eavesdropping by revealing a random subset of the key bits and check in public the error rate.

## 7.1 Experimental Quantum Cryptography [4]

to be added

## 7.2 Free-space quantum key distribution

to be added

# 8 Other Quantum Cryptographic Protocols

Secure quantum multi-party computation [5].

# References


[1] C.H Bennet, E. Bernstein, G. Brassard, and U. Vazirani. Strenghths and weaknesses of quantum computing. *SIAM journal on Computing*, 1997.

[2] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17), April 1997.

[3] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[4] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Lecture Notes in Computer Science*, 473:253–??, 1991.

[5] C. Crepeau, D. Gottesman, and A. Smith. Secure multi-party quantum computation, 2002.