Quantum Information Theory: MAT 4953 XLS 5983. Lesson 04 (Sep 20-22), Fall 2022.

José A. Morales E., UTSA Math and Physics & A. Depts.

Abstract

Operators in Quantum Mechanics. Classical cryptography.

1. Operators in Quantum Mechanics

Remember state vectors in QM belong to a Hilbert space $\mathbb{V}$, which is a vector space (either finite or infinite dimensional) with inner product and with the completeness property (see Quantum-Mechanics-Review PDF), taking as field the complex numbers. In general, an operator maps a (ket) vector to another (ket) vector, as in

$$\widehat{A}\,|\Psi\rangle = |\Phi\rangle \in \mathbb{V}$$

We will consider linear operators acting over our vectors, meaning that for $\widehat{A}$ linear,

$$\widehat{A}(b\,|\Psi_1\rangle + c\,|\Psi_2\rangle) = b\widehat{A}\,|\Psi_1\rangle + c\widehat{A}\,|\Psi_2\rangle\,, \quad b, c \in \mathbb{C}$$

This means that if we expand our vectors in terms of an orthonormal basis of the Hilbert space, by linearity it follows that

$$|\Psi\rangle = \sum_j \psi_j\,|v_j\rangle \implies \widehat{A}\,|\Psi\rangle = \sum_j \psi_j \widehat{A}\,|v_j\rangle$$

So, if we understand the action of an operator over the basis elements,

$$\widehat{A}\,|v_j\rangle = \sum_i A_{ij}\,|v_i\rangle$$

by linearity we know then what's the action over any vector in the Hilbert space. We have denoted by A_{ij} the matrix elements of the operator $\widehat{A}$ in the basis $|v_i\rangle$, since (remembering our basis is orthonormal)

$$\left\langle v_i|\widehat{A}|v_j\right\rangle = A_{ij}$$

Email address: jose.morales4@utsa.edu (José A. Morales E., UTSA Math and Physics & A. Depts.)

where the matrix is N^2 if $\mathbb{V}$ is of dimension N, or if $\mathbb{V}$ is infinite dimensional then the matrix is infinite. In either case, we have

$$\widehat{A}\,|\Psi\rangle = \begin{pmatrix} A_{11} & \cdots & A_{1i} & \cdots \\ \vdots & \ddots & \vdots & \vdots \\ A_{i1} & \cdots & A_{ii} & \cdots \\ \vdots & \cdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_j \\ \vdots \end{pmatrix} = \begin{pmatrix} \sum_j A_{1j}\psi_j \\ \vdots \\ \sum_i A_{ij}\psi_j \\ \vdots \end{pmatrix}$$

So our A_{ij} are literally the matrix coefficients of the operator in the chosen basis (where the matrix can be finite or infinite). We can also write this as an outer product

$$\widehat{A} = \sum_{ij} A_{ij}\,|v_i\rangle\,\langle v_j|$$

If we happen to choose as the orthonormal basis the actual eigenbasis of the operator $\widehat{A}$, then the matrix representation of $\widehat{A}$ in its own eigenbasis is diagonal (where the coefficients are possibly complex):

$$\widehat{A} = \sum_{i} a_i\,|a_i\rangle\,\langle a_i|$$

this is called the spectral decomposition, where the eigenbasis elements solve the eigenvalue problem as below,

$$\widehat{A}\,|a_i\rangle = a_i\,|a_i\rangle$$

1.1. Adjoint of an operator

We remember that in QM there are also "bra-vectors", which are simply functionals of our Hilbert space (conjugate transposes of ket-vectors, if you wish). We can also think of

$$\langle\Psi|\,\widehat{A} = \langle\chi|$$

meaning the action of a linear operator "to the left" (on bras), producing another bra (functional). However, in general we have that if

$$\widehat{A}\,|\Psi\rangle = |\Phi\rangle$$

then

$$\langle\Psi|\,\widehat{A} = \langle\chi| \neq \langle\Phi|$$

An operator $\widehat{A}^\dagger$ is called the adjoint to $\widehat{A}$ (its Hermitian conjugate) if for any ket-vector $|\Psi\rangle$ then

$$\langle\Psi|\,\widehat{A}^\dagger = (\widehat{A}\,|\Psi\rangle)^\dagger,$$

that is, meaning that if $\widehat{A}\,|\Psi\rangle = |\Phi\rangle$ then $\langle\Psi|\,\widehat{A}^\dagger = (|\Phi\rangle)^\dagger = \langle\Phi|$. It holds that, for any two states,

$$\left\langle \Psi|\widehat{A}^\dagger|\Omega \right\rangle = \langle\Phi|\Omega\rangle = \langle\Omega|\Phi\rangle^* = \left\langle \Omega|\widehat{A}|\Psi \right\rangle^*$$

Interpreting our linear operators as matrices, the Hermitian conjugate (its matrix representation) is obtained by transposing the operator matrix and then taking the complex conjugate of each element.

Definition 1. A self-adjoint operator (also called Hermitian) is one for which

$$\widehat{A}^\dagger = \widehat{A}$$

meaning that the conjugate transpose of the matrix gives the same matrix again.

Theorem 2. *Self-adjoint (Hermitian) operators have real eigenvalues and orthogonal eigenvectors.*

Proof. The solutions of the eigenvalue equation for $\widehat{A}$ satisfy (using "Sturm-Liouville" notation)

$$\widehat{A}\,|\lambda_n\rangle = \lambda_n\,|\lambda_n\rangle$$

and taking inner product with another eigenvector, we have that

$$\left\langle \lambda_m|\widehat{A}|\lambda_n \right\rangle = \lambda_n \langle \lambda_m|\lambda_n\rangle$$

But on the other hand, if we use the adjoint properties we have that

$$\left\langle \lambda_m|\widehat{A}|\lambda_n \right\rangle = \left\langle \lambda_n|\widehat{A}^\dagger|\lambda_m \right\rangle^* = \left\langle \lambda_n|\widehat{A}|\lambda_m \right\rangle^* = (\lambda_m \langle \lambda_n|\lambda_m\rangle)^* = \lambda_m^* \langle \lambda_m|\lambda_n\rangle$$

therefore

$$\lambda_m^* \langle \lambda_m|\lambda_n\rangle = \left\langle \lambda_m|\widehat{A}|\lambda_n \right\rangle = \lambda_n \langle \lambda_m|\lambda_n\rangle$$

$$(\lambda_m^* - \lambda_n)\langle \lambda_m|\lambda_n\rangle = 0$$

If $m = n$, then that implies that $\lambda_n^* = \lambda_n$ so the eigenvalues must be real: $\lambda_n \in \mathbb{R}$ for all indices n. If $\lambda_m = \lambda_m^* \neq \lambda_n$, then we have that $\langle \lambda_m|\lambda_n\rangle = 0$, so the eigenvectors are orthogonal, and under normalization of our eigenbasis we can make it an orthonormal one:

$$\langle \lambda_m|\lambda_n\rangle = \delta_{mn}$$

The only case left is when $\lambda_m = \lambda_n$ for $m \neq n$, which is when there is a degeneracy for the eigenvalue $\lambda_m = \lambda_n = \lambda$. In that case, you simply generate an orthonormal basis for the degenerate eigenspace of dimension greater than one. □

1.2. Measurement in Quantum Mechanics

In Quantum Mechanics, the process of measuring a physical observable (measureable quantity) is represented by applying a linear operator, which is taken as self-adjoint in order to guarantee that the eigenvalues (representing the only possible measured values for the observable) are real numbers. Quantum Mechanics is a deterministic theory with respect to the wavefunction evolution, but it is probabilistic with respect to the experimental outcomes. This means

that we can only predict the probabilities of obtaining as measurement of an observable the eigenvalue j , where these probabilities are given by the Born rule:

$$P_j = |\langle v_j|\Psi_{\text{before}}\rangle|^2$$

with $|v_j\rangle$ the $j-$th eigenvector of the operator representing our observable.

As you might know, in QM the process of measuring perturbs the wave vector representing the state. Then, measuring collapses (projects) the state vector along the eigendirection associated to the measured eigen-value, so

$$|\Psi_{\text{before}}\rangle = \sum_i c_i |v_i\rangle \rightarrow |\Psi_{\text{after}}\rangle = |v_j\rangle$$

with a probability $P_j = |\langle v_j|\Psi_{\text{before}}\rangle|^2 = |c_j|^2$. In the particular case where $|c_i| = \delta_{ik}$, then $P_j = \delta_{jk}$, then since the system was already in the k-th eigenstate of the operator, it will stay in the k-th eigenstate with probability 1. So that implies that if you measure the same quantity twice consecutively (the second measurement immediately after the first one), after the first measurement you project the state vector in one of the operator eigendirections, and in the second measurement, since it was already in an eigendirection, it will stay in that eigendirection.

1.3. Expectation (mean) value of an observable.

Let's assume our physical observable is associated in Quantum Mechanics with an operator $\widehat{V}$,where

$$\widehat{V} = \sum_i v_i |v_i\rangle \langle v_i|$$

to be applied to the state vector $|\Psi\rangle$. We know we will obtain the result v_j with probability $P_j = |\langle v_j|\Psi\rangle|^2$. If we repeat our measurement many times (as for a stat mech ensemble of the same wave vector), we obtain the expectation value (mean)

$$\langle V\rangle = \sum_i P_i v_i = \sum_i |\langle v_i|\Psi\rangle|^2 v_i$$

which is also given by

$$\left\langle \Psi|\widehat{V}|\Psi\right\rangle = \left\langle \Psi|\sum_i v_i |v_i\rangle \langle v_i| |\Psi\right\rangle = \sum_i v_i \langle \Psi |v_i\rangle \langle v_i| \Psi\rangle = \sum_i v_i |\langle v_i|\Psi\rangle|^2$$

Therefore

$$\langle V\rangle = \left\langle \Psi|\widehat{V}|\Psi\right\rangle$$

In general, $\left\langle \widehat{V}\right\rangle \neq v_i$ for any i . However, the equality holds for a normalized $|\Psi\rangle \propto |v_i\rangle$.

1.4. Uncertainty of an observable

Since we have mentioned that QM is a physical theory probabilistic regarding the measurement outcomes, it's not surprising that we will talk about the variance on it. The variance of the value of V is

$$\Delta V^2 = \left\langle \Psi | (\widehat{V} - \langle V \rangle)^2 | \Psi \right\rangle$$

which we can prove is also given by

$$\Delta V^2 = \left\langle \Psi | \widehat{V}^2 - 2 \langle V \rangle \widehat{V} + \langle V \rangle^2 | \Psi \right\rangle = \left\langle \Psi | \widehat{V}^2 | \Psi \right\rangle - 2 \langle V \rangle \left\langle \Psi | \widehat{V} | \Psi \right\rangle + \langle V \rangle^2 \langle \Psi | \Psi \rangle =$$

$$= \left\langle \Psi | \widehat{V}^2 | \Psi \right\rangle - 2 \langle V \rangle^2 + \langle V \rangle^2 = \left\langle \Psi | V^2 | \Psi \right\rangle - \langle V \rangle^2 = \left\langle V^2 \right\rangle - \langle V \rangle^2$$

a relation you might recall from statistics. The uncertainty in QM is taken as the square root of the variance:

$$\Delta V = \sqrt{\Delta V^2}$$

1.5. Compatible and incompatible observables

We say two observables A, B are compatible when their operators have the same eigenvectors, since in that case they can be known simultaneously (to arbitrary accuracy).

When they have different eigenvectors, they are called incompatible, since then both cannot be known simultaneously to arbitrary accuracy.

The compatibility condition is that their operators commute:

$$\widehat{0} = \widehat{A}\widehat{B} - \widehat{B}\widehat{A} =: [\widehat{A}, \widehat{B}]$$

where along the way we have defined the commutator for QM.

Proof. Let's assume both operators have common eigenvectors. Therefore,

$$\widehat{A} |\psi_n\rangle = \lambda_n |\psi_n\rangle, \quad \widehat{B} |\psi_n\rangle = \mu_n |\psi_n\rangle$$

$$\widehat{A}\widehat{B} |\psi_n\rangle = \lambda_n \mu_n |\psi_n\rangle, \quad \widehat{B}\widehat{A} |\psi_n\rangle = \lambda_n \mu_n |\psi_n\rangle$$

$$(\widehat{A}\widehat{B} - \widehat{B}\widehat{A}) |\psi_n\rangle = 0 |\psi_n\rangle \, \forall n$$

therefore the action of the commutator over the common eigenbasis is equivalent to applying the zero operator. That means,

$$\widehat{A}\widehat{B} - \widehat{B}\widehat{A} = \widehat{0}$$

□

Fact 3. *We can define a complete set of commuting observables for every quantum system.*

1.5.1. Commutator and Anticommutator.

We have defined along the way the commutator in QM. Just some remarks. You might have noticed that so far QM has involved the use of linear operators, which can be represented as matrices of finite or infinite dimension. From Linear Algebra, we know that in general we cannot expect matrices to commute. So we shouldn't expect in QM that operators will commute. In general,

$$\widehat{A}\widehat{B} \neq \widehat{B}\widehat{A}$$

A way to quantify the degree to which two operators don't commute is by using their commutator:

$$[\widehat{A}, \widehat{B}] := \widehat{A}\widehat{B} - \widehat{B}\widehat{A}$$

If you have taken a QM course before, you might know that when the variables are canonically conjugated (as for x_i, p_i a cartesian position coordinate and its respective momentum coordinate), they are incompatible and their canonical commutator is given by

$$[\widehat{x}_i, \widehat{p}_i] = i\hbar$$

The canonical commutator was discovered by Max Born in 1925 (look at his gravestone on Wikipedia). On the other hand, we define the anticommutator as

$$\{\widehat{A}, \widehat{B}\} = \widehat{A}\widehat{B} + \widehat{B}\widehat{A}$$

1.6. Heisenberg's uncertainty principle

One could summarize this famous result by indicating it's a natural relation, that actually appears in Fourier transforms. We will sketch its proof below.

Theorem 4. *Heisenberg's uncertainty principle: For two observables represented by the operators $\widehat{A}$, $\widehat{B}$,we have that*

$$\Delta A \Delta B \geq \frac{|\left\langle \Psi|[\widehat{A}, \widehat{B}]|\Psi \right\rangle|}{2}$$

Proof. We define the operators (also self-adjoint)

$$\widehat{A}' = \widehat{A} - \langle A \rangle, \quad \widehat{B}' = \widehat{B} - \langle B \rangle$$

and we name

$$|\Phi_1\rangle = \widehat{A}'|\Psi\rangle, \quad |\Phi_2\rangle = \widehat{B}'|\Psi\rangle.$$

From Linear Algebra you might recall the Cauchy-Schwarz inequality (we also mentioned it in a lecture), where

$$\langle\Phi_1|\Phi_1\rangle \langle\Phi_2|\Phi_2\rangle \geq |\langle\Phi_1|\Phi_2\rangle|^2$$

So we have

$$\Delta A^2 \Delta B^2 = \left\langle \Psi|(\widehat{A} - \langle A\rangle)^2|\Psi \right\rangle \left\langle \Psi|(\widehat{B} - \langle B\rangle)^2|\Psi \right\rangle = \left\langle \Psi|(\widehat{A}')^2|\Psi \right\rangle \left\langle \Psi|(\widehat{B}')^2|\Psi \right\rangle = \left\langle \widehat{A}'\Psi|\widehat{A}'|\Psi \right\rangle \left\langle \widehat{B}'\Psi|\widehat{B}'|\Psi \right\rangle$$

$$\geq |\left\langle \widehat{A}'\Psi|\widehat{B}'\Psi\right\rangle|^2 = |\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle|^2 = |\Re\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle + i\Im\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle|^2$$

observing

$$[\widehat{A}', \widehat{B}'] = [\widehat{A}-\langle A\rangle, \widehat{B}-\langle B\rangle] = [\widehat{A}, \widehat{B}-\langle B\rangle]-[\langle A\rangle, \widehat{B}-\langle B\rangle] = [\widehat{A}, \widehat{B}-\langle B\rangle] = [\widehat{A}, \widehat{B}]$$

and

$$\left\langle \Psi|[\widehat{A}, \widehat{B}]|\Psi\right\rangle = \left\langle \Psi|\widehat{A}\widehat{B}|\Psi\right\rangle - \left\langle \Psi|\widehat{B}\widehat{A}|\Psi\right\rangle = \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle - \left\langle \widehat{B}\Psi|\widehat{A}\Psi\right\rangle = \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle - \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle^*$$

$$= 2i\Im\left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle = 2i\Im\left\langle \Psi|\widehat{A}\widehat{B}|\Psi\right\rangle$$

so

$$\left\langle \Psi|[\widehat{A}', \widehat{B}']|\Psi\right\rangle = 2i\Im\left\langle \Psi|\widehat{A}'\widehat{B}'|\Psi\right\rangle$$

and since

$$\left\langle \Psi|\{\widehat{A}, \widehat{B}\}|\Psi\right\rangle = \left\langle \Psi|\widehat{A}\widehat{B}|\Psi\right\rangle + \left\langle \Psi|\widehat{B}\widehat{A}|\Psi\right\rangle = \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle + \left\langle \widehat{B}\Psi|\widehat{A}\Psi\right\rangle = \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle + \left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle^*$$

$$= 2\Re\left\langle \widehat{A}\Psi|\widehat{B}\Psi\right\rangle = 2\Re\left\langle \Psi|\widehat{A}\widehat{B}|\Psi\right\rangle$$

then

$$\left\langle \Psi|\{\widehat{A}', \widehat{B}'\}|\Psi\right\rangle = 2\Re\left\langle \Psi|\widehat{A}'\widehat{B}'|\Psi\right\rangle$$

and using these results, we have that

$$\Delta A^2\Delta B^2 \geq |\Re\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle + i\Im\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle|^2 = |\Re\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle|^2 + |\Im\left\langle \Psi|\widehat{A}'\widehat{B}'\Psi\right\rangle|^2 =$$

$$= |\frac{\left\langle \Psi|\{\widehat{A}', \widehat{B}'\}|\Psi\right\rangle}{2}|^2 + |\frac{\left\langle \Psi|[\widehat{A}', \widehat{B}']|\Psi\right\rangle}{2}|^2 \geq |\frac{\left\langle \Psi|[\widehat{A}', \widehat{B}']|\Psi\right\rangle}{2}|^2 = |\frac{\left\langle \Psi|[\widehat{A}, \widehat{B}]|\Psi\right\rangle}{2}|^2$$

therefore this implies

$$\Delta A\Delta B \geq \frac{1}{2}|\left\langle \Psi|[\widehat{A}, \widehat{B}]|\Psi\right\rangle|$$

□

Example 5. For the canonical commutator

$$[\widehat{x}, \widehat{p}] = i\hbar$$

this implies that

$$\Delta x\Delta p \geq \frac{1}{2}|\left\langle \Psi|[\widehat{x}, \widehat{p}]|\Psi\right\rangle| = \frac{1}{2}|\left\langle \Psi|i\hbar|\Psi\right\rangle| = \frac{\hbar}{2}$$

2. Qubits, the Bloch sphere, and related operators

Let's assume the state vector is given by the following linear combination,

$$|\Psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

In principle both a_i's can be complex, however, regarding observables, the wave functions are defined up to a phase. This implies that we can assume $a_0 \in \mathbb{R}$ and $a_1 \in \mathbb{C}$. Then, our state vector looks like

$$|\Psi\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2)e^{i\phi} \end{pmatrix} = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$$

which satisfies the normalization condition for $|\Psi\rangle$. We can graphically represent state vectors as points in a unit sphere (called the Bloch sphere), with θ, ϕ as spherical coordinates representing the polar and azimuthal angle. Below we present some examples of state vectors represented as points over the Bloch sphere.

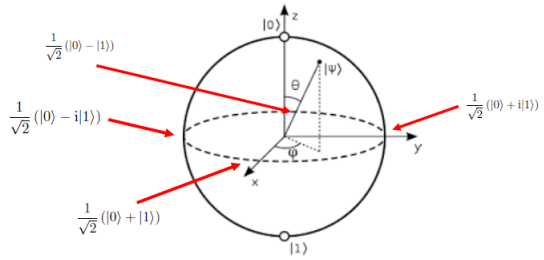

Fig. From "Operators", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

Remark 6. On the Bloch sphere, antipodal points correspond to orthogonal states.

2.1. Pauli spin operators

We define the Pauli spin operators as the matrices given by linear combinations of the following tensor products below:

$$\widehat{\sigma}_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1) + \begin{pmatrix} 0 \\ 1 \end{pmatrix}(1,0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\widehat{\sigma}_y = i(|1\rangle\langle 0| - |0\rangle\langle 1|) = i[\begin{pmatrix} 0 \\ 1 \end{pmatrix}(1,0) - \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1)] = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\widehat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1,0) - \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0,1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\widehat{I} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1,0) + \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0,1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where the last one is naturally the identity matrix. These operators will act over qubits defined as state vectors

$$|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

The Pauli operators can be proven to be Hermitian. Therefore, they have real eigenvalues, and an orthonormal eigenbasis.

Clearly, because the dimension of the vector space of 2×2 matrices is 4, and the 4 Pauli operators are linearly independent, they can generate any 2×2 matrix by linear combinations of those 4. So any operator in a 2D Hilbert space (over the complex) can be expanded in terms of Pauli operators. If we have particularly a Hermitian matrix (self-adjoint)

$$\widehat{H} = \begin{pmatrix} a & c - id \\ c + id & b \end{pmatrix}$$

we can decompose it in terms of Pauli operators as follows:

$$\widehat{H} = \begin{pmatrix} a & c - id \\ c + id & b \end{pmatrix} = \begin{pmatrix} \frac{a+b}{2} & 0 \\ 0 & \frac{a+b}{2} \end{pmatrix} + \begin{pmatrix} \frac{a-b}{2} & 0 \\ 0 & \frac{b-a}{2} \end{pmatrix} + \begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & -id \\ id & 0 \end{pmatrix}$$

therefore

$$\widehat{H} = \frac{a+b}{2}\widehat{I} + \frac{a-b}{2}\widehat{\sigma}_z + c\widehat{\sigma}_x + d\widehat{\sigma}_y$$

2.1.1. Eigensolutions of Pauli matrices

Since

$$\widehat{\sigma}_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\widehat{\sigma}_y = i(|1\rangle\langle 0| - |0\rangle\langle 1|) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\widehat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\widehat{I} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

one can prove that all these matrices have eigenvalues ± 1. The respective eigenvectors for each operator can be proven to be

$$\widehat{\sigma}_x |\Psi\rangle = \lambda |\Psi\rangle \implies |\Psi\rangle \in \{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\}$$

$$\widehat{\sigma}_y |\Psi\rangle = \lambda |\Psi\rangle \implies |\Psi\rangle \in \{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\}$$

$$\widehat{\sigma}_z |\Psi\rangle = \lambda |\Psi\rangle \implies |\Psi\rangle \in \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$$

As you can see from above, the two eigenvectors of each Pauli matrix are orthogonal. These sets of qubit eigenvectors can be identified with Jones vectors, since

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

are related to diagonal up/down polarization,

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}$$

relate to left/right circular polarization, and

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle\,, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

are related to HV polarization.

2.1.2. Commutation relations for the Pauli operators

One can prove that the following commutation relations hold for the Pauli matrices:

$$[\widehat{\sigma}_x, \widehat{\sigma}_y] = 2i\widehat{\sigma}_z$$

$$[\widehat{\sigma}_y, \widehat{\sigma}_z] = 2i\widehat{\sigma}_x$$
$$[\widehat{\sigma}_z, \widehat{\sigma}_x] = 2i\widehat{\sigma}_y$$

which can be summarized, if you know some tensor notation, as

$$[\widehat{\sigma}_a, \widehat{\sigma}_b] = 2i\epsilon_{abc}\widehat{\sigma}_c$$

where ϵ_{abc} is the so-called Levi-Civita symbol (± 1 depending on the permutation abc of xyz being even or odd). On the other hand, the following relations regarding anti-commutators hold,

$$\{\widehat{\sigma}_x, \widehat{\sigma}_y\} = \{\widehat{\sigma}_y, \widehat{\sigma}_z\} = \{\widehat{\sigma}_z, \widehat{\sigma}_x\} = 0$$

2.1.3. Pauli operator for an arbitrary direction

We define the Pauli operator for the direction $\vec{n}$ as

$$\vec{n} \cdot \vec{\widehat{\sigma}} = n_x\widehat{\sigma}_x + n_y\widehat{\sigma}_y + n_z\widehat{\sigma}_z$$

where $\vec{n}$ is a unit vector, so

$$n_x^2 + n_y^2 + n_z^2 = 1$$

therefore we can write it as

$$\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

which means that its polar angle is θ and its azimuthal is ϕ.

2.1.4. Operators representing single qubit logic gates: Examples

Example 7. Pauli x-gate: We remember that

$$\widehat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The matrix above clearly is flipping the coordinate directions, so this gate causes a bit-flip by mapping $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. This flip, BTW, viewed over the Bloch sphere, is a rotation on the Bloch sphere by π radians about the axis $\widehat{e}_x$.

Example 8. Hadamard gate: is represented by the following operator,

$$\widehat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\widehat{\sigma}_x + \widehat{\sigma}_z)$$

This is where Linear Algebra is helpful. The columns of a matrix represent how the operator transforms along a given coordinate direction. So that means that

$$\widehat{H}\,|0\rangle = \widehat{H}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\widehat{H}\,|1\rangle = \widehat{H}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

This means that the Hadamard gate creates a superposition when acting over $|0\rangle$ and $|1\rangle$. BTW, this operator can be viewed as a rotation on the Bloch sphere by π radians about the axis $(\widehat{e}_x + \widehat{e}_z)/\sqrt{2}$.

2.2. Unitary operators

It should be mentioned that not all operators are related to physical observables, so not all need to be Hermitian. Having said that, we define the following.

Definition 9. Unitary operators are the ones that satisfy both conditions below:

$$\widehat{U}\widehat{U}^\dagger = \widehat{I} = \widehat{U}^\dagger\widehat{U}$$

We emphasize both conditions in the definition because satisfaction of one doesn't guarantee the operator being actually unitary (as for the raising and lowering operators in the harmonic oscillator).

If a operator $\widehat{U}$ is unitary, then $\widehat{U}^\dagger = \widehat{U}^{-1}$ clearly from the definition.

Example 10. The rotation matrix is a unitary operator. Since

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

one can show that

$$R^\dagger(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & \sin(-\theta) \\ -\sin(-\theta) & \cos(-\theta) \end{pmatrix} = R(-\theta) = R^{-1}(\theta)$$

Example 11. The Pauli operators. They are unitary (in addition to being Hermitian).

2.2.1. Properties of unitary operators

Theorem 12. *The following conditions are equivalent for an operator $\widehat{U}$:*

- The operator $\widehat{U}$ satisfies $\widehat{U}\widehat{U}^\dagger = \widehat{I} = \widehat{U}^\dagger\widehat{U}$
- It preserves the norm of the vector
- It preserves the scalar product
- It maps any orthonormal basis into another orthonormal basis
- In the operator eigenbasis (where $\widehat{U}$ is diagonal), the matrix elements have absolute value 1.

Theorem 13. *We won't present the complete proof. We'll only sketch the proof of why the original definition implies the third condition. If*

$$|\psi'\rangle = \widehat{U}\,|\psi\rangle\,, \quad |\phi'\rangle = \widehat{U}\,|\phi\rangle \implies \langle\phi'|\psi'\rangle = \left\langle \phi|\widehat{U}^\dagger\widehat{U}|\psi\right\rangle = \langle\phi|\psi\rangle\,.$$

Fact 14. *Any unitary operator can be expressed in the form*

$$\widehat{U} = \exp(i\widehat{C})$$

where $\widehat{C}$ is Hermitian.

We have above an exponential matrix operator. If you haven't seen its definition, it's presented below.

Definition 15. The exponential of an operator as above is given by the following Taylor series:

$$\exp(i\widehat{C}) = \lim_{N\to\infty}\sum_{n=0}^{N}\frac{(i\widehat{C})^n}{n!} = \widehat{I} + i\widehat{C} - \frac{\widehat{C}^2}{2} - i\frac{\widehat{C}^3}{6} + \cdots\frac{(i\widehat{C})^n}{n!} + \cdots$$

provided the limit above exists.

2.3. Rotation Operator

The rotation operator for a particle with angular momentum $\vec{\widehat{J}}$ (taking units such that $\hbar = 1$) is

$$\widehat{R}(\vec{n},\theta) = \exp(-i\theta\vec{n}\cdot\vec{\widehat{J}}),$$

where $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ is a unit vector.

If we have a spin-1/2 particle, then $\vec{\widehat{J}} = \vec{\widehat{\sigma}}/2$. In that case, one can prove (by Taylor expanding and using $(\vec{n}\cdot\vec{\widehat{\sigma}})^2 = 1$) that

$$\widehat{R}(\vec{n},\theta) = \exp(-i\theta\vec{n}\cdot\vec{\widehat{\sigma}}/2) = \cos(\theta/2)\widehat{I} - i\sin(\theta/2)\vec{n}\cdot\vec{\widehat{\sigma}}$$

with

$$\vec{n}\cdot\vec{\widehat{\sigma}} = n_x\widehat{\sigma}_x + n_y\widehat{\sigma}_y + n_z\widehat{\sigma}_z$$

Remark 16. The most general 2×2 unitary matrix with determinant equal to 1 can be expressed in the form above. We can think then of a qubit as a spin-1/2 object; the rotation operator performs ANY unitary operation we wish to implement over a qubit.

Example 17. Let's construct a state pointing along the direction $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ (this direction has coordinates (θ, ϕ) on the Bloch sphere). We start in the state corresponding to the north pole $(1,0)^T$,and then we rotate it anti-clockwise by an angle θ about the axis $\vec{n}' = (-\sin\phi, \cos\phi, 0)$ over the equator, as in the figure below:

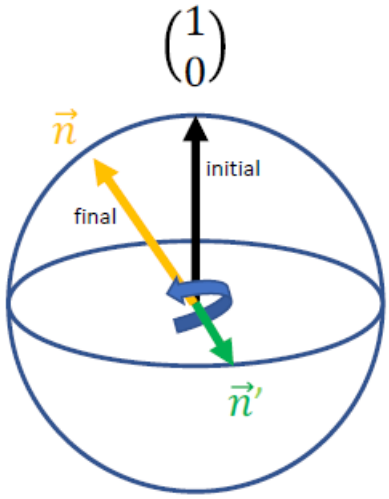

Fig. From "Operators", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

We compute first

$$\vec{n}' \cdot \vec{\hat{\sigma}} = (-\sin\phi, \cos\phi, 0) \cdot (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z) = -\sin\phi\hat{\sigma}_x + \cos\phi\hat{\sigma}_y$$

$$= -\sin\phi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \cos\phi \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sin\phi - i\cos\phi \\ -\sin\phi + i\cos\phi & 0 \end{pmatrix} = \begin{pmatrix} 0 & -ie^{-i\phi} \\ ie^{i\phi} & 0 \end{pmatrix}$$

and so the first step in the operation is represented by

$$\exp(-i\theta\vec{\hat{n}}' \cdot \vec{\hat{\sigma}}/2) = \exp[\theta \begin{pmatrix} 0 & -e^{-i\phi} \\ e^{i\phi} & 0 \end{pmatrix}/2] = \exp\begin{pmatrix} 0 & -e^{i\phi}\theta/2 \\ e^{i\phi}\theta/2 & 0 \end{pmatrix}$$

which one can prove is equal to

$$\exp(-i\theta\vec{\hat{n}}' \cdot \vec{\hat{\sigma}}/2) = \begin{pmatrix} \cos(\theta/2) & -e^{i\phi}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

So we just need to apply this operator to $(1,0)^T$ to get the desired state (which is clearly seen from the first column of the matrix above)

$$\exp(-i\theta\vec{\hat{n}}' \cdot \vec{\hat{\sigma}}/2) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) & -e^{i\phi}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}$$

so we get a point in the Bloch sphere represented by the polar-azimuthal coordinates (θ, ϕ). Up to a global phase (if we want to present the state more symmetric) we have that

$$|\vec{n}(\theta,\phi)\rangle = e^{-i\phi/2}\begin{pmatrix}\cos(\theta/2)\\ e^{i\phi}\sin(\theta/2)\end{pmatrix} = \begin{pmatrix}e^{-i\phi/2}\cos(\theta/2)\\ e^{i\phi/2}\sin(\theta/2)\end{pmatrix}$$

Global phases are unobservable. Moreover, the Bloch sphere is blind to global phases as it treats the states $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ as the same. The phase ϕ would only be observable in an interference experiment between two paths.

2.3.1. Bloch sphere double-covering by spin-1/2 rotations

Assuming we have a spin-$1/2$ particle, we have as discussed

$$\widehat{R}(\vec{n},\theta) = \exp(-i\theta\vec{n}\cdot\vec{\widehat{\sigma}}/2) = \cos(\theta/2)\widehat{I} - i\sin(\theta/2)\vec{n}\cdot\vec{\widehat{\sigma}}$$

Problem 18. Let's start on the $|0\rangle$ state, if we rotate it by $\theta = 2\pi$ around the $y-$axis, then we'll come back to the north pole; however, since

$$\widehat{R}(\widehat{e}_y, 2\pi) = \cos(\pi)\widehat{I} - i\sin(\pi)\vec{\widehat{\sigma}}_y = -\widehat{I}$$

our state will be

$$|0\rangle \to -|0\rangle = e^{\pm i\pi}|0\rangle$$

the negative of the original!

This implies that under a rotation of 2π, the state has been changed by a global phase of π. Since all points in the Bloch sphere are defined up to a global phase (which justifies our assumption of the coefficient of the state $|0\rangle$ being real, $\alpha \in \mathbb{R}$), its related geometric description is still fine.

Remark 19. We actually need a 4π rotation to bring back the state to the north pole with $+|0\rangle$. More information can be found in "Quantum Information, Chapter 2 of lecture notes by J. Preskill" (freely available).

2.3.2. Rotation operators for photons

Photons are spin-1 objects. Their state vectors then are not spinors and there's no double covering. Under units such that $\hbar = 1$, we have that $\vec{\widehat{J}} = \vec{\widehat{\sigma}}$,

$$\widehat{R}(\vec{n},\theta) = \exp(-i\theta\vec{n}\cdot\vec{\widehat{J}})$$

and we have the following examples.

Example 20. Rotation around $x-$axis:

$$\widehat{R}(\vec{x},\theta) = \exp(-i\theta\widehat{\sigma}_x) = \begin{pmatrix}\cos\theta & -i\sin\theta\\ -i\sin\theta & \cos\theta\end{pmatrix}$$

Example 21. Rotation around $y-$axis:

$$\widehat{R}(\vec{y},\theta) = \exp(-i\theta\widehat{\sigma}_y) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Example 22. Rotation around $z-$axis:

$$\widehat{R}(\vec{z},\theta) = \exp(-i\theta\widehat{\sigma}_z) = \begin{pmatrix} \exp(-i\theta) & 0 \\ 0 & \exp(i\theta) \end{pmatrix}$$

Remark 23. These operators rotate vector components anticlockwise by an angle θ, they are so-called "active rotations".

2.3.3. Poincare' vs. Bloch spheres

Compare the so-called Poincare' sphere (related to polarizations) on the left vs. the Bloch sphere (on the right):

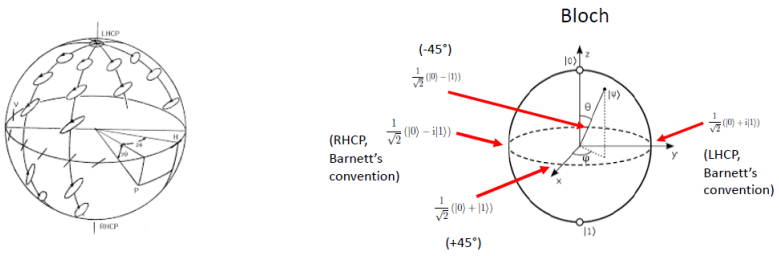

Fig. From "Operators", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

Though some analogies can be made between both, notice these spheres are rotated w.r.t. each other. On the Poincaré sphere, traditionally all the purely linear polarizations are around the equator, and the two purely circular polarizations (LHCP, RHCP) at the two poles, with all other places corresponding to elliptical polarization. As for the Bloch sphere, on the Poincaré sphere antipodal points correspond to orthogonal states.

2.4. Time evolution operator & Schroedinger equation

The time evolution operator is given by the following unitary operator,

$$\widehat{U}(t) = \exp(-i\widehat{H}t/\hbar)$$

with $\widehat{H}$ the Hamiltonian operator (representing the total energy: kinetic plus potential), which as we know represents an observable.

The Schroedinger equation is

$$i\hbar\frac{d}{dt}|\psi\rangle(t) = \widehat{H}|\psi\rangle(t)$$

If you remember your Diff. Eq.'s course, you might expect that a formal solution of this equation is

$$|\psi\rangle(t) = \exp(-i\widehat{H}t/\hbar)|\psi\rangle(0) = \widehat{U}(t)|\psi\rangle(0)$$

3. Classical cryptography

The simplest system in this context is the single-key cryptosystem. We summarize its specifics below.

- There's a secret key shared by Alice and Bob. This key is a number, that we will denote by K, say

$$K = 10110101011110001010\cdots$$

- Alice uses K to encrypt a message ("plaintext" P) to produce a ciphertext C.

- The ciphertext is a function of the plaintext and the key, that is

$$C = C(P, K)$$

- The plaintext can be recovered using the key, and it's a function of the ciphertext and the key,

$$P = P(C, K)$$

3.1. Substitution cipher

In the substitution cipher, we replace each letter by a symbol. Let's assume \$ is the first symbol in the ciphertext: there are 26 possible letters (in our alphabet) for it. For the second symbol (let's say @ for example) there are 25 possibilities, and so on. This implies that there are 26! possible translations. If we use Stirling's approximation to the factorial, we have

$$n! \approx \sqrt{2\pi n}(n/e)^n$$

so under this approximation,

$$26! \approx 13 \times 10^{26}$$

and clearly going through all of them is not possible. However, substitution cipher is easy to crack if one considers letter frequencies. For example:

- The most common letter in English is E, which occurs 12.7% of the time in this language. \

- Letter Q occurs around 0.1% of the time, etc.

Remark 24. This method is used by the character Sherlock Holmes in "The adventure of the dancing men".

Proposition 25. *Criterion for perfect secrecy (Shannon, 1949):*

If $\{p_i\}$ is the set of possible plaintexts (messages) and if $\{c_i\}$ is the set of possible ciphertexts, then the criterion for perfect secrecy is

$$P(p_i|c_j) = P(p_i) \quad \forall i, j$$

We can interpret the result above as follows. The probability for the message being the plaintext p_i given that the ciphertext was c_j in the equality is independent of which ciphertext we have, only depending on the probability of occurrence of the plaintext p_i. In other words, discovering the ciphertext provides no information on the plaintext.

If we use Bayes' theorem, we have that

$$P(p_i|c_j)P(c_j) = P(c_j|p_i)P(p_i) \implies P(c_j|p_i) = \frac{P(p_i|c_j)P(c_j)}{P(p_i)} = P(c_j)$$

so any given ciphertext is equally likely to have been generated by any plaintext.

3.2. (Gilbert) Vernam cipher

This is the simples perfectly secure cipher (one-time pad). In this case, the key is a random sequence of bits at least as long as the plaintext (where the plaintext is also a sequence of bits). The ciphertext is obtained by bit-wise addition modulo 2. In practice, this is achieved by applying an "exclusive OR" (XOR) operation to every bit of the message and the corresponding bit in the key. First, let's define the XOR operation by a table below:

$$\begin{gathered}\text{INPUT} \to \text{OUTPUT} \\ (A, B) \to A\text{XOR}B \\ (0,0) \to 0 \\ (0,1) \to 1 \\ (1,0) \to 1 \\ (1,1) \to 0\end{gathered}$$

Now, let's present an example on how this cipher works.

Example 26. Let's say the original message (plaintext) was the following sequence of bits

$$P = 01110011\cdots$$

and the secret key is the following random sequence of bits

$$K = 10011010\cdots$$

so the encrypted message is given by

$$C = \begin{matrix} 01110011\cdots \\ \text{XOR} \\ 10011010\cdots \end{matrix} = 11101001\cdots$$

The encrypted message can be transmitted over an insecure channel. If one doesn't have the key, it can't be deciphered. On the other hand, if one has the key, the message can be decrypted easily by applying XOR again. Notice, under the notation

$$A\text{XOR}B = \text{XOR}(A, B)$$

that

$$(A, B) \to A\text{XOR}B \to (A\text{XOR}B, B) \to \text{XOR}(A\text{XOR}B, B)$$
$$(0,0) \to 0 \to (0,0) \to 0$$
$$(0,1) \to 1 \to (1,1) \to 0$$
$$(1,0) \to 1 \to (1,0) \to 1$$
$$(1,1) \to 0 \to (0,1) \to 1$$

so, by the table above we have

$$\text{XOR}(A\text{XOR}B, B) = A$$

The issue with this private-key cryptography is how to share the key between A(lice) and B(ob). It seems that the only safe way is sending a courier with the random numbers representing the key, which might not be the most practical and is expensive. Then, most common cryptography everyday uses then public keys.

3.3. Public-key cryptography

The idea of public-key cryptography is that certain math operations are easy in the forward direction, but hard backwards. Some examples of this are multiplication and factoring. It works by Bob generating two keys, an enciphering key called e, and a deciphering key called d. Bob publishes e, but keeps d secret. Alice will use e to encode her message. The current standard is the RSA scheme (by Rivest, Shamir, Adleman), which is used over the internet for "digital signatures". We'll explain it below.

3.3.1. RSA scheme

1. Bob finds two large prime numbers p and q, and calculates $m = p \times q$, which is easy.
2. Then he finds two numbers e and d s.t. $d \times e = 1 \mod (p-1)(q-1)$. It should be commented that there are efficient algorithms for this.
3. The public key is m and e. The private key is d on the other hand.
4. Alice encodes her message x by applying the transformation

$$x \to x^e \mod m$$

5. The message can be retrieved using the following result (which is exact and quite useful for our purposes):

$$(x^e \mod m)^d \mod m = x \mod m$$

where $x \mod m$ is the original message. So Bob only needs to use his secret key d.

Remark 27. It is thought that the difficulty of breaking the RSA scheme is equivalent to that of factoring m into the primes p and q. If one knows p, q, then it's true that finding d from e, m is relatively easy.

The question is, how big should m be? Numbers of order 10^{90} can be factored into their primes with today's computers in less than a day, so we need larger numbers than that. BTW, in July 2012 the number RSA-212 $\approx 7 \times 10^{212}$ was factored as part of a challenge (the prize was $30,000).

Notice RSA numbers are semi-primes (composed of exactly two primes). The current challenge, for $75K, is to factor RSA-896, which has 270 decimal digits:

RSA-896 = 412023436986659543855531365332575948179811699844327982845455626433876445565248426198098870423161841879261420247188869492560931776375033421130982397485150944909106910269861031862704114880866970564902903653658867433731720813104105190864254793282601391257624033946373269391

On the other hand, computational power doubles every two years (by Moore's law arguments), and quantum computers are able to factor in exponentially shorter time than classical computers via Shor's algorithm. This means that, eventually, public key protocols will be obsolete.

3.4. Conclusions

- In the classical realm, we have to choose between private-key protocol (expensive) or public-key protocols (cheap but not perfectly secure).
- Quantum Mechanics, as we will show during the course, offers an alternative which actually has the best of both worlds. Namely, it allows public key distribution and it's guaranteed to be secure by the laws of Physics. Moreover, it doesn't require random numbers to be shared by the parties beforehand.

References

[1] "Operators", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

[2] Quantum Information, by Stephen M. Barnett (Oxford University Press, ISBN 978-0-19-852763-3).

[3] "Classical cryptography", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

[4] "Quantum Information", Chapter 2. Lecture notes by J. Preskill (available online).