The mathematical model of a quantum circuit and the Grover search algorithm

Giorgio Ottaviani

Abstract

We introduce the qubits and the mathematical model of a quantum circuit. Two applications are presented, the Deutsch-Josza algorithm and the Grover search algorithm. This introduction is largely inspired from the excellent [Na], with a more geometric point of view. The two algorithms are explained with more details in the comprehensive text [NC].

Contents

1 Qubits

A *bit* is an element of $\{0,1\}$, which is accessible to humans.

Let U be a complex Hilbert space of dimension 2. A *qubit* is an element of $\mathbb{P}(U)$, which is not accessible to humans, but to God only.

We (humans) can have informations on the qubit space only by *measurements*, that will be considered later. The space $\mathbb{P}(U)$ is homeomorphic to a 2-dimensional sphere S^2. The space U is endowed with a Hermitian scalar product (sesquilinear, Hermitian and positive definite). It is customary to denote a preferred orthonormal basis of U by $|0\rangle$, $|1\rangle$ (*ket* in Dirac notation).

With the choice of a basis, we may identify $U=\mathbb{C}^2$. The quotient map

$\mathbb{C}^2 \setminus \{0\} \longrightarrow \mathbb{P}(\mathbb{C}^2) = S^2$ is the quotient by the action of $\mathbb{C}^*$. Since any $\lambda \in \mathbb{C}^*$ has a polar form $\lambda = re^{i\theta}$, the quotient can be performed in two steps, first by acting with $r \in \mathbb{R}^+$ and then by acting with $e^{i\theta} \in S^1$. The result is the factorization

$$\begin{tikzcd}
\mathbb{C}^2 \setminus \{0\} \arrow[rr] \arrow[dr, "p"] & & S^2 \\
& S^3 \arrow[ur, "h"'] &
\end{tikzcd} \tag{1.1}$$

where $p(v) = \frac{v}{|v|}$ and $h\colon S^3 \to S^2$ is the Hopf fibration, which deserves a separate study. In the physical literature, S^2 is called the Bloch sphere. Points of $\mathbb{P}^1(\mathbb{C}) = S^2$ correspond to S^1 fibers that, as we see now, carry a natural algebraic structure of subgroups (or lateral classes), and a natural metric structure of geodesics.

1.1 The Hopf fibration, algebraic aspects (Hamilton, Clifford)

The interesting point is that S^3 is a Lie group (the only spheres which are Lie groups are S^0, S^1 and S^3). The simplest way to find this group structure is to identify

$$\mathbb{C}^2 = \mathbb{H} = \langle 1, i, j, k \rangle_{\mathbb{R}},$$

the space of quaternions. The sphere S^3 is the subgroup of $\mathbb{H}$ of quaternions of unit norm. Recall that for $q \in \mathbb{H}$ is well defined the conjugate $\overline{q} \in \mathbb{H}$, we have the squared norm $q\overline{q} = |q|^2$ and every $q \in \mathbb{H} \setminus \{0\}$ is invertible with $q^{-1} = \frac{\overline{q}}{|q|^2}$. Decompose $\mathbb{H} = \mathbb{R} \oplus \mathbb{I}$, where $\mathbb{I} = \langle i, j, k \rangle_{\mathbb{R}}$, then we have a natural embedding $S^2 \subset \mathbb{I}$ (the sphere of unitary imaginary quaternions). S^3 contains several subgroups $S^1 \subset S^3$, one for any $n \in S^2 \subset \mathbb{I}$, defined by $\{e^{n\theta} = \cos\theta + n \sin\theta | \theta \in \mathbb{R}\}$. These subgroups are not normal, but we see now that the set of lateral classes S^3/S^1 endowes the structure of a manifold isomorphic to S^2. In the following Theorem we make the standard choice $n = i$, but the result remain true for any $n \in \mathbb{I}$.

Theorem 1.1. *The Hopf fibration $h\colon S^3 \to S^2$ has the analytic expression*

$$h(q) = q^{-1} i q$$

and can be identified with the quotient map $S^3 \to S^3/S^1$. The group S^3 acts on S^2 through the map h which is S^3-equivariant, in the sense that $\forall g \in S^3$ we have $h(g \cdot x) = g \cdot h(x)$.

Proof. It is straighforward to compute $\forall q = q_0 + q_1 i + q_2 j + q_3 k \in S^3$ (such that $q_0^2 + q_1^2 + q_2^2 + q_3^3 = 1$)

$$q^{-1} i q = i(q_0^2 + q_1^2 - q_2^2 - q_3^3) + j(2q_1q_2 - 2q_0q_3) + k(2q_0q_2 + 2q_1q_3) \in S^2 \subset \mathbb{I}$$

The stereographic projection from i, seen as "North Pole", to the complex plane spanned by the equator is

$$St\colon S^2 \to \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C})$$

with equation $St(xi+yj+zk) = \frac{y}{1-x}j + \frac{z}{1-x}k$. Now $St(q^{-1}iq) = k\left(\frac{q_0+q_1 i}{q_2+q_3 i}\right)$ which (apart from k which is needed to translate the result from the plane $\langle 1, i\rangle$ to the plane $\langle j, k\rangle$) is the projective abscissa of the point $(q_0+q_1 i, q_2+q_3 i) \in \mathbb{C}^2$. This shows the analytical expression of h. Note that $q^-1iq = i$ if an only if $q = e^{i\theta}$ for some $\theta \in \mathbb{R}$. The S^3-invariance is obvious as a quotient map to the set of lateral classes. □

Define $\forall q \in S^3$ the isomorphism $c_q \colon \mathbb{I} \to \mathbb{I}$, $c_q(v) = q^{-1}vq$. q has a polar form $q = \cos\frac{\theta}{2} + \frac{\mathrm{Imq}}{|\mathrm{Imq}|}\sin\frac{\theta}{2}$. Indeed the conjugation on $\mathbb{H}$ leaves invariant the two subspaces $\mathbb{R}$ and $\mathbb{I}$. The restriction to $\mathbb{R}$ (center of $\mathbb{H}$) is the identity, and the restriction to $\mathbb{I}$ that we have called c_q is the interesting part. If $q \neq \pm 1$ (which gives $\mathrm{Imq} \neq 0$) then c_q is a rotation through $\frac{\mathrm{Imq}}{|\mathrm{Imq}|}$ of an angle θ. In the special case when $q \in S^2 \subset \mathbb{I}$ then $-c_q$ is the symmetry with respect to the hyperplane with normal q. A bonus of the previous approach is that the map

$$\begin{array}{ccc} S^3 & \to & SO(3) \\ q & \mapsto & c_q \end{array}$$

is a 2: 1 covering. Indeed $c_q = c_{q'}$ if and only if $q = \pm q'$. This shows that $SO(3)$ is isomorphic to $\mathbb{P}^3(\mathbb{R})$ and that $\pi_1(SO(3)) = \mathbb{Z}_2$. The map from S^3 to $SU(2)$ which maps $(z, w) \in S^3 \subset \mathbb{C}^2$ to

$$\begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix} \tag{1.2}$$

is an isomorphism and it is the celebrated spin representation. The standard notation for the universal covering of $SO(3)$ is indeed $S^3 = Spin(3)$.

1.2 The Hopf fibration, metric aspects (Fubini, Study)

For every $n \in S^2 \subset \mathbb{I}$ we have a subgroup of S^3 given by $\{e^{n\theta} = cos\theta + n\sin\theta\}$ which is isomorphic to S^1. If we fix $i \in \mathbb{I}$ we have a well defined subgroup $S^1 \subset S^3$ and a corresponding Hopf map on the quotient $h \colon S^3 \to S^3/S^1 \simeq S^2$. S^1 acts by scalar multiplication on S^3 and points of $\mathbb{P}^1(\mathbb{C}) = S^2$ correspond to S^1-orbits on S^3.

Note also that the formula

$$\cos d(P, Q) = \mathrm{Re}\left(P \cdot \overline{Q}\right) \tag{1.3}$$

gives the geodesic distance $d(P, Q)$ of two points on S^3.

Lemma 1.2. 1. *Given $P \in S^3$, the orbit curve $e^{i\theta}P$ is a geodesic on S^3 and a fiber for the Hopf map. All geodesics through P have the form $e^{n\theta}P$ for some $n \in S^2 \subset \mathbb{I}$.*

2. *Given $P, Q \in S^3$ and the two orbits $e^{i\theta}P$, $e^{i\phi}Q$, the geodesic distance on S^3 between the point $e^{i\theta}P$ and the orbit $e^{i\phi}Q$ is equal to*

$$\arccos\sqrt{(P \cdot \overline{Q})(Q \cdot \overline{P})}$$

(where $\cdot$ is the Euclidean scalar product on $\mathbb{C}^2$) and it does not depend on θ. So any two orbits are "parallel" and the distance $d(S^1P, S^1Q)$ satisfies

$$\cos d(S^1P, S^1Q) = |\left(P \cdot \overline{Q}\right)|. \tag{1.4}$$

Proof. $e^{n\theta}P$ are "great circles" which makes obvious the first statement. Compute the polar form $P \cdot \overline{Q} = r \cdot e^{i\sigma}$. Now the geodesic distance of two points, one on each geodesic, is

$$\cos d = \mathrm{Re}\left(e^{i\theta}P \cdot \overline{e^{i\phi}Q}\right) = \mathrm{Re}(re^{i(\theta-\phi+\sigma)}) = r\cos(\theta - \phi + \sigma)$$

The minimum d is obtained for $\phi = \theta + \sigma$ and it is equal to $\arccos(r) = \arccos(\left|P \cdot \overline{Q}\right|)$. □

Proposition 1.3. *1. Let $q_1, q_2 \in \mathbb{I}$. Then*

$$q_1q_2 = -q_1 \cdot q_2 + q_1 \wedge q_2 \in \mathbf{R} \oplus \mathbf{I}$$

2. For $q_1, q_2 \in S^2 \subset \mathbb{I}$ the distance $d_{S^2}(q_1, q_2)$ can be computed as $-Re(q_1q_2)$ where the product is the quaternion product.

Proof. The statement in 1) is linear in q_1, q_2. Then it is enough to prove it when q_1, q_2 are chosen among the basis vector i, j, k and in this case it is a straightforward check.

2) is an immediate consequence of 1) and (1.3). □

□

The formula in 1.3 1) has an intrinsic beauty since it links the quaternion product, the scalar product and the cross product.

Theorem 1.4. *Let d_{S_n} be the round distance on S^n. S^3 acts as an isometry on itself, that is*

$$d_{S^3}(x, y) = d_{S^3}(g \cdot x, g \cdot y) \quad \forall g \in S^3$$

For any $x, y \in S^3$ we have

$$2d_{S^3}(S^1x, S^1y) = d_{S^2}(h(x), h(y))$$

Proof. Thanks to the group action, we may assume $x = 1$ and $h(x) = i$. Let $y = q_0 + q_1i + q_2j + q_3k$, $\beta = d_{S^2}(i, h(y))$, $\alpha = d_{s^3}(1, y)$. Then $\cos\beta = Re\left(i \cdot \overline{y^{-1}iy}\right)$ where $\cdot$ is the scalar product, $\cos\alpha = |1 \cdot \overline{y}| = q_0^2 + q_1^2$. We compute $\cos\beta = q_0^2 + q_1^2 - q_2^2 - q_3^2$, hence $\cos 2\alpha = 2\cos^2\alpha - 1 = 2(q_0^2 + q_1)^2 - (q_0^2 + q_1^2 + q_2^2 + q_3^2) = \cos\beta$ as we wanted. □

Given $\psi, \phi \in S^3$, the length of a geodesic between ψ and ϕ is

$$d(\phi, \psi) = \arccos\sqrt{\frac{\langle\psi|\phi\rangle\langle\phi|\psi\rangle}{\langle\psi|\psi\rangle\langle\phi|\phi\rangle}} \tag{1.5}$$

where $\langle\ |\ \rangle$ is the Hermitian inner product on $\mathbb{C}^2$.

Remark 1.5. *A special case in Theorem 1.4 is that orthonormal basis in $\mathbb{C}^2$ correspond through the Hopf fibration to antipodal points on the sphere S^2. Through the stereographic projection these pair of points correspond to pairs $z, w \in \mathbb{C} \cup \{+\infty\}$ such that*

$$w = -\frac{1}{\overline{z}}$$

Although not needed here, to complete the picture we show how to get the infinitesimal expression of Fubini-Study metric from the above. The proof (see [BZ]) is the same in any dimension, and we consider the metric induced by $S^{2n+1} \to \mathbb{P}^n\mathbb{C}$.

Theorem 1.6. *The round metric on S^1-orbits in S^{2n+1} induces the Fubini-Study metric on $\mathbb{P}^n\mathbb{C}$ which is*

$$ds^2 = \frac{dP \cdot d\overline{P}}{P\overline{P}} - \frac{(P \cdot d\overline{P})(\overline{P} \cdot dP)}{(P\overline{P})^2}$$

Proof. Now compute (recall that $\cos^2 x = 1 - x^2 + \ldots$)

$$1 - ds^2 + \ldots = \cos^2 d(P, P + dP) =$$

$$= \frac{(P\overline{P} + P \cdot d\overline{P})(P\overline{P} + \overline{P} \cdot dP)}{(P\overline{P})(P\overline{P})} \frac{1}{1 + \frac{(P \cdot d\overline{P} + \overline{P} \cdot dP)}{P\overline{P}} + \frac{dP \cdot d\overline{P}}{P\overline{P}}} =$$

where we used next formula (1.5), and the second denominator is $\frac{1}{P\overline{P}}(P+dP)(\overline{P}+d\overline{P})$, now set $x = \frac{(P \cdot d\overline{P} + \overline{P} \cdot dP)}{P\overline{P}}$, $y = \frac{(P \cdot d\overline{P})(\overline{P} \cdot dP)}{(P\overline{P})^2}$, $z = \frac{dP \cdot d\overline{P}}{P\overline{P}}$, we get

$$1 - ds^2 + \ldots = (1 + x + y)\frac{1}{1 + x + z} = (1 + x + y)(1 - x - z + x^2 + \ldots) =$$

$$= (1 - x^2 + x^2 + y - z + \ldots)$$

Hence

$$ds^2 = z - y$$

as we wanted. □

1.3 Hermitian product on tensor products

If $V_1, \ldots, V_k$ are complex Hilbert spaces (that we assume for simplicity of finite dimension), each V_i is endowed with a Hermitian scalar product q_i. Recall the unitary group $U(V_i, q_i)$ consists of $\{g \in GL(V_i) | q_i(x, y) = q_i(g \cdot x, g \cdot y) \quad \forall x, y \in V_i\}$

The group $U(V_1, q_1) \times \ldots \times U(V_k, q_k)$ acts in a natural way on the space $\mathrm{S}ym^{d_1} V_1 \otimes \ldots \otimes \mathrm{S}ym^{d_k} V_k$. The action is defined on decomposable elements as $(g_1, \ldots, g_k) \cdot v_1^{d_1} \otimes \ldots \otimes v_k^{d_k} = (g_1 \cdot v_1)^{d_1} \otimes \ldots \otimes (g_k \cdot v_k)^{d_k}$ and then extended by linearity.

Theorem 1.7. 1. *There is a unique scalar product q on $\mathrm{S}ym^{d_1} V_1 \otimes \ldots \otimes \mathrm{S}ym^{d_k} V_k$, called the Frobenius product, such that on decomposable elements*

$$q(v_1^{d_1} \otimes \ldots \otimes v_k^{d_k}, w_1^{d_1} \otimes \ldots \otimes w_k^{d_k}) = \prod_{i=1}^{k} q_i(v_i, w_i)^{d_i}$$

2. *q is the unique scalar product (up to scalar multiples) on $\mathrm{S}ym^{d_1} V_1 \otimes \ldots \otimes \mathrm{S}ym^{d_k} V_k$ which is $U(V_1, q_1) \times \ldots \times U(V_k, q_k)$-invariant.*

Proof. Uniqueness in 1) is clear since every element is sum of decomposable ones. To show existence we consider in each vector space a basis $(z_1, \ldots, z_{n_i})$ and a dual basis $(\partial_1, \ldots, \partial_{n_i})$ given by partial differential operators, define for elements $f = f_1 \otimes \ldots \otimes f_k \in \mathrm{S}ym^{d_1}V_1 \otimes \ldots \otimes \mathrm{S}ym^{d_k}V_k$ (other tensors are sum of these ones) $q(f, g) = \prod_{i=1}^{k} f_i(\partial_1, \ldots, \partial_{n_i})g$. It is straightforward to check that this definition satisfies the condition of the statement for decomposable elements.

Uniqueness in 2) follows from the irreducibility of $\mathrm{S}ym^{d_1}V_1 \otimes \ldots \otimes \mathrm{S}ym^{d_k}V_k$

□

Note $\mathrm{S}ym^dV$ is not irreducible for the action of $SO(V)$, indeed the harmonic polynomials make an invariant subspace. As a consequence, there is a continuous family of orthogonally invariant scalar products on $\mathrm{S}ym^dV$.

1.4 Bra-ket Dirac's notation

The Hermitian product on a Hilbert space U allows to identify U with $U^\vee$. If coordinates are chosen with respect to a orthonormal basis, then the scalar product $q(x, y)$ can be written as $x^t \cdot \overline{y}$, where x, y are identified with their column of coordinates. In Dirac notation, this is written $x^t \cdot \overline{y} = \langle x|y\rangle$, assuming that $|y\rangle$ is a column vector and $\langle x|$ is a row vector.

$|y\rangle$ is called a ket vector.

$\langle x|$ is called a bra vector.

Alternatively, column vectors could be thought in U and row vectors could be thought in $U^\vee$. The notation is efficient in manipulating expressions, for example, after a basis $|0\rangle$ and $1\rangle$ is fixed, which correspond respectively to the column vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and we have the expression

$$|v\rangle = |0\rangle\langle 0|v\rangle + |1\rangle\langle 1|v\rangle$$

Note that the expression

$$|0\rangle\langle 0| + |1\rangle\langle 1|$$

corresponds to the identity operator. The expression $|v\rangle\langle v|x\rangle$ represents the projection of $|x\rangle$ on the line spanned by a versor $|v\rangle$. In this note we will use bra-ket notation with some freedom, in particulat if $|t\rangle \in V^q$ and $\langle s| \in (V^\vee)^r$, with $s \leq r$, we denote by $\langle s|t\rangle \in V^{r-s}$ the result of the contraction between t and s

2 Quantum circuits

A quantum circuit consists of three items

- *State* The state is initialized in a predefinite way. Its special feature is that it is not accessible, unless with a measurement.

- *Operations* The state evolves by applying operations, specified in advance in the form of an algorithm.

- *Measurement* At the end of the algorithm some information on the state can be obtained by a measurement.

2.1 State

We equip $(\mathbb{C}^2)^{\otimes q}$ (tensor product of q qubits) with the Hermitian product as in Theorem 1.7. This means that on decomposable elements $q(v_1 \otimes \ldots \otimes v_q, w_1 \otimes \ldots \otimes w_q) = \prod_{i=1}^{q} v_i \cdot (\overline{w_i})^t$. A state is an element of

$$\mathbb{P}((\mathbb{C}^2)^{\otimes q})$$

The q modes of $(\mathbb{C}^2)^{\otimes q}$ are called *registers.* Recall the qubits are not accessible, at the same time also states are not accessible. A orthonormal basis of $(\mathbb{C}^2)^{\otimes q}$ is denoted by $|0\ldots 00\rangle, |0\ldots 01\rangle, \ldots, |1\ldots 11\rangle$ and has 2^q elements, where

$|0\ldots 00\rangle = |0\rangle \otimes \ldots \otimes |0\rangle \otimes |0\rangle$, denoted $|0\rangle_q$,

$|0\ldots 01\rangle = |0\rangle \otimes \ldots \otimes |0\rangle \otimes |1\rangle$, denoted $|0\rangle_{q-1}|1\rangle$,

and so on.

As for qubits, it is convenient to consider states in the sphere

$$S^{2^{q+1}-1} \subseteq (\mathbb{C}^2)^{\otimes q}$$

and then consider equivalent two representatives if they differ by $e^{i\theta} \in S^1$. So our states $\psi \in S^{2^{q+1}-1}$ satisfy $\langle\psi|\psi\rangle = 1$.

In other words, we still have a diagram as in the single qubit case (1.1)

$$\begin{tikzcd}
(\mathbb{C}^2)^{\otimes q} \setminus \{0\} \arrow[rr] \arrow[dr, "p"] & & \mathbb{P}((\mathbb{C}^2)^{\otimes q}) \\
& S^{2^{q+1}-1} \arrow[ur, "h"] &
\end{tikzcd} \tag{2.1}$$

The sphere $S^{2^{q+1}-1}$ is no more a group for $q \geq 2$ and the algebraic description of lateral classes crashes, though S^1 is still a group acting on $S^{2^{q+1}-1}$ and the fibers of h are orbits for this group action . Still the metric description works, since the fibers of h are great circles S^1 which are "parallel", and the orbit distance descends to $\mathbb{P}((\mathbb{C}^2)^{\otimes q})$ as the Fubini-Study metric.

We may denote states as

$$|t\rangle = \sum_{j\in\{0,1\}^q} t_j|j\rangle$$

with $\sum_{j\in\{0,1\}^q} |t_j|^2 = 1$.

Definition 2.1. *A state is called a product state if it is decomposable. Otherwise is called entangled.*

In other words, states have a *rank*, the product states have rank 1, the entangled states have rank ≥ 2.

2.2 Operations (gates)

Operations are *unitary operators* on the "quantum register" $(\mathbb{C}^2)^{\otimes q}$. They can be described by $2^q \times 2^q$ matrices.

The operations have the form

$$v_1 \otimes \ldots \otimes v_q \mapsto U(v_1 \otimes \ldots \otimes v_q)$$

extended by linearity.

These operations are *linear* and *reversible.* Operations are represented as *gates*, operating on q registers. The first input where a series of operations can apply is chosen by convention as $|0\rangle_q$.

Special single-qubit gates operate on just one register, they correspond to operations like

$$v_1 \otimes v_2 \otimes \ldots \otimes v_q \mapsto U_1(v_1) \otimes v_2 \otimes \ldots \otimes v_q$$

extended by linearity. These single-qubit gates preserve the rank of a state. **In general a unitary operator destroys the rank of the states**.

As operations on classical bits are composed by few standard operations, also operations on quantum register can be defined by a few gates. The first single-qubit gates are the *Pauli* gates

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The X gate is equivalent to a NOT gate in classical registers. Up to scalar multiples, the Pauli matrices are the images of the quaternion basis through the spin representation (1.2).

The *Hadamard* gate is

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

Note that $H^2 = I$, H is a *square root of the identity.* Its importance comes from the following

Proposition 2.2. *The unitary matrix $H^{\otimes q}$ operates applying H to any single qubit and satisfies*

$$H^{\otimes q}|0\rangle_q = \frac{1}{\sqrt{2^q}} \sum_{j \in \{0,1\}^q} |j\rangle$$

note the target is the uniform superposition of all basis states.

Proof.

$$H^{\otimes q}|0\rangle_q = (H|0\rangle)^{\otimes q} = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)^{\otimes q} = \frac{1}{\sqrt{2^q}} \sum_{j \in \{0,1\}^q} |j\rangle$$

□

The CNOT (*controlled NOT*) gate is a two qubit-gate, operating on a control qubit and target qubit. If the control qubit is $|0\rangle$ nothing happens, while if the control qubit is $|1\rangle$ the target qubit is flipped.

With the basis $|00\rangle, |01\rangle, |10\rangle, |1\rangle$ the matrix of CNOT is

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

The reader is invited to browse [Na] at page 21, where it is shown that three successive CNOT can make a complete swap of two registers.

A very important remark for our purposes is that any function

$$f\colon \{0,1\}^n \to \{0,1\}^m$$

can be encoded in a gate on $n+m$ qubits in the following way

$$\begin{array}{cccc} U_f\colon & (\mathbb{C}^2)^{\otimes n}\otimes(\mathbb{C}^2)^{\otimes m} & \to & (\mathbb{C}^2)^{\otimes n}\otimes(\mathbb{C}^2)^{\otimes m} \\ & |x\rangle_n \otimes |y\rangle_m & \mapsto & |x\rangle_n \otimes |y\oplus f(x)\rangle_m \end{array} \tag{2.2}$$

where $\oplus$ is the sum in $(\mathbb{Z}_2)^{\oplus m}$.

For example, if $m=1$ and $n=2$, let f be the function such that
$f(00)=0, f(01)=1, f(10)=0, f(11)=1$,
then U_f is 8×8 with the following 4×4 block structure

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

Every U_f is a permutation matrix, hence it is unitary. In the case $m=1$ if we apply U_f to the state $|0\rangle_{n+1}$ we get $|0\rangle_n \otimes f(0)$, but if we first apply the Hadamard gate to the first n qubits and then apply U_f we get at the end

$$\frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n} |j\rangle \otimes |f(j)\rangle \tag{2.3}$$

which is pretty more interesting since it contains a superposition of all possible values of f. Another instructive example is to start from $|0\rangle_n \otimes 1$, and again apply the Hadamard gate to the first n qubits and then apply U_f, we get at the end

$$\frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n} |j\rangle \otimes |f(j)\oplus 1\rangle \tag{2.4}$$

Exercise 2.3. *Construct f such that U_f does not preserve the rank.*

Question Which inequalities exist between $\mathrm{rk}(t)$ and $\mathrm{rk}(U_f(t))$, depending on f ?

2.3 Measurement

A measurement can be considered as a special gate, which is degenerate and no more reversible. Moreover its effect is probabilistic. It is a slippy concept that contains both the difficulty and the power of quantum computing. Measurement is the only way we can make accessible some partial informations on a state.

We can measure only along orthonormal basis of a given register. Let $\{e_0^k, e_1^k\}$ be a orthonormal basis of register k. For any $|t\rangle \in (\mathbb{C}^2)^{\otimes q}$ consider the contraction $\langle e_j^k|t\rangle \in (\mathbb{C}^2)^{\otimes q-1} = \mathbb{C}^2 \otimes \ldots \widehat{\mathbb{C}^2} \ldots \otimes \mathbb{C}^2$. Note that

$$1 = \left||t\rangle\right|^2 = |\langle e_0^k|t\rangle|^2 + |\langle e_1^k|t\rangle|^2$$

Probabilistic procedure of measurement A measure on register k along the basis $\{e_0^k, e_1^k\}$ can have as output only e_0^k or e_1^k. Precisely

- the output is e_0^k with probability $|\langle e_0^k|t\rangle|^2$, in this case the state after the measurement becomes $\frac{|e_0^k\rangle\langle e_0^k|t\rangle}{|\langle e_0^k|t\rangle|}$.
- the output is e_1^k with probability $|\langle e_1^k|t\rangle|^2$, in this case the state after the measurement becomes $\frac{|e_1^k\rangle\langle e_1^k|t\rangle}{|\langle e_1^k|t\rangle|}$.

The original quantum state is no longer recoverable. If t has a basis expression involving e_0^k, e_1^k at register k, only the summands containing e_0^k (respectively e_1^k) survive in the above first (respectively second) case.

Example 2.4. $|t\rangle = p|00\rangle + \sqrt{1-p^2}|11\rangle$ *(entangled state, with* $p \in [0,1] \subset \mathbb{R}$*) is measured in the first register as* $|0\rangle$ *with probability* p^2*, after this measurement the state becomes* $|00\rangle$ *and the measurement with respect to the second register gives* $|0\rangle$ *with probability* 1*, the state remains* $|00\rangle$*.*

$|t\rangle$ *is measured in the first register as* $|1\rangle$ *with probability* $1-p^2$*, after this measurement the state becomes* $|11\rangle$ *and the measurement with respect to the second register gives* $|1\rangle$ *with probability* 1*, the state remains* $|11\rangle$*.*

This confirms the fact that mesurements with respect to different registers are not independent (see Proposition 2.11) .

In conclusion, after the measurement of $|t\rangle$ *on both registers, we get (the final probability is obtained as the product of the probabilities involved)* $|00\rangle$ *with probability* p^2 *and* $|11\rangle$ *with probability* $1-p^2$*. The output* $|01\rangle$ *and* $|10\rangle$*, although possible, are never obtained in this case (compare with Corollary 2.7).*

Remark 2.5. *The procedure implies the following basic but important principle. If a measurement is repeated twice on the same register* k*, the second time it is obtained the same output of the first measurement with probability* 1*. Note that if the second measurement is done on another register different from* k*, then a third measurement on the register* k *can give a different output.*

Lemma 2.6. *Measuring with a second register m gives the following tree of probabilities*

$$|t\rangle \begin{cases} \frac{|e_0^k\rangle\langle e_0^k|t\rangle}{|\langle e_0^k|t\rangle|} & \begin{cases} \frac{|e_0^ke_0^m\rangle\langle e_0^ke_0^m|t\rangle}{|\langle e_0^ke_0^m|t\rangle|} \text{ with probability } |\langle e_0^ke_0^m|t\rangle|^2 \\ \frac{|e_0^ke_1^m\rangle\langle e_0^ke_1^m|t\rangle}{|\langle e_0^ke_1^m|t\rangle|} \text{ with probability } |\langle e_0^ke_1^m|t\rangle|^2 \end{cases} \\ \\ \frac{|e_1^k\rangle\langle e_1^k|t\rangle}{|\langle e_1^k|t\rangle|} & \begin{cases} \frac{|e_1^ke_0^m\rangle\langle e_1^ke_0^m|t\rangle}{|\langle e_1^ke_0^m|t\rangle|} \text{ with probability } |\langle e_1^ke_0^m|t\rangle|^2 \\ \frac{|e_1^ke_1^m\rangle\langle e_1^ke_1^m|t\rangle}{|\langle e_1^ke_1^m|t\rangle|} \text{ with probability } |\langle e_1^ke_1^m|t\rangle|^2 \end{cases} \end{cases}$$

Proof. After the first measurement of register k we get $t_1 = \frac{|e_i^k\rangle\langle e_i^k|t\rangle}{|\langle e_i^k|t\rangle|}$ with probability $|\langle e_i^k|t\rangle|^2 = ||e_i^k\rangle\langle e_i^k|t\rangle|^2$. After the second measurement of register m we get

$$t_2 = \frac{|e_j^m\rangle\langle e_j^m|t_1\rangle}{|\langle e_j^m|t_1\rangle|} \tag{2.5}$$

with probability $|\langle e_j^m|t_1\rangle|^2 = \left||e_j^m\rangle\langle e_j^m|t_1\rangle\right|^2 = \frac{\left||e_i^ke_j^m\rangle\langle e_i^ke_j^m|t\rangle\right|^2}{|\langle e_i^k|t\rangle|^2}$. Since t_1 appears in (2.5) both at numerator and denominator, it can be replaced in this formula, up to scalar multiples, by $|e_i^k\rangle\langle e_i^k|t\rangle$ getting the expression

$$t_2 = \frac{|e_i^ke_j^m\rangle\langle e_i^ke_j^m|t\rangle}{|\langle e_i^ke_j^m|t\rangle|}$$

By the conditional probability formula we get that the final probability is

$$\frac{\left||e_i^ke_j^m\rangle\langle e_i^ke_j^m|t\rangle\right|^2}{|\langle e_i^k|t\rangle|^2} \cdot |\langle e_i^k|t\rangle|^2 = \left||e_i^ke_j^m\rangle\langle e_i^ke_j^m|t\rangle\right|^2$$

□

Continuing in this way for all q registers (in any order) gives at the end the following fundamental

Corollary 2.7.

$$|t\rangle = \sum_{j\in\{0,1\}^q} |j\rangle t_j \text{ with } t_j = \langle j|t\rangle \in \mathbb{C}$$

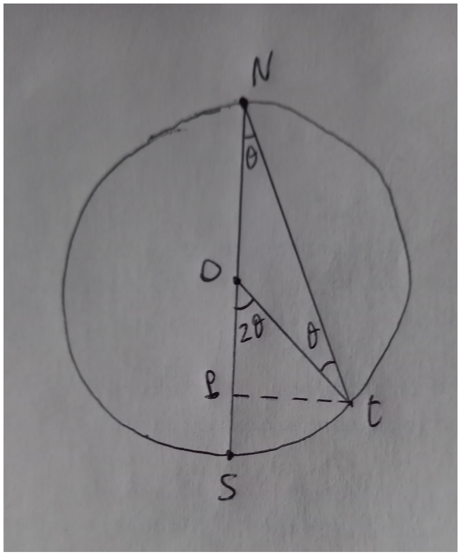
is measured as $|j\rangle$ with probability $|t_j|^2$.

Remark 2.8. *Recall that the choice of a orthonormal basis corresponds to the choice of a line in $\mathbb{R}^3$ by Remark 1.5. The reader with a knowledge of Quantum Mechanics will note that the counterintuitive behaviour of the procedure of measurement corresponds exactly to the Stern-Gerlach experiment (see [NC, 1.5.1]) regarding the measure of electron spin. This is one of the ways quantum computers can be physically constructed, at least in principle.*

The probability appearing in the procedure of measurement have a simple geometric interpretation in the case of a single qubit, as in the following Lemma.

Lemma 2.9. *Let $t \in S^2$ be measured along an axis v pointing on N, let call $N - S$ (North-South) the line spanned by v, so that the only possible measurement are N or S. Let P be the euclidean orthogonal projection of t on the v axis. Then the measure of t*

- *gives S with probability $\frac{\overline{NP}}{2}$*
- *gives N with probability $\frac{\overline{SP}}{2}$.*

Proof. In the Hopf fibration formalism we have $|t\rangle = \sqrt{1-p^2}|0\rangle + p|1\rangle$, where $|0\rangle$ has image the North Pole N and $|1\rangle$ has image the South Pole S. The angle θ between t and $|1\rangle$ satisfies $\cos\theta = p$. Look at picture 

where by Theorem 1.4 we have $\overset{\frown}{St} = 2\theta$, hence we compute $\overline{Nt} = 2\cos\theta$, $\overline{NP} = 2\cos^2\theta = 2p^2$ as we wanted. □

Remark 2.10. *Measurement can be physically feasible only with respect to some distinguished basis. In [NC, exerc. 4.33] it is observed that the measurement with respect to any basis can be obtained by a unitary basis tranform followed by the measurement with respect to the basis $|0\rangle$, $|1\rangle$.*

Proposition 2.11. *The measurements at any different registers of a state t are independent if and only if t is a product state (not entangled).*

Proof. [BC, 2.3]. □

3 The Deutsch-Josza algorithm

This is a toy algorithm which shows, in a special case, the advantage of quantum algorithms on classical ones. Define a function $f\colon \{0,1\}^n \to \{0,1\}$ to be *balanced* if the two fibers $f^{-1}(0)$ and $f^{-1}(1)$ are two subsets of the same cardinality 2^{n-1}. These functions are in some sense opposite to the *constant* functions, where one fiber has the maximum cardinality 2^n and the second one is empty.

Alice secretly chooses one function, which can be only balanced or constant, and prepares it in a black box. Bob wishes to discover if the function chosen by Alice is balanced or constant and he can evaluate the black box choosing any input value. How many attempts are necessary to Bob ? If Bob is lucky two attempts can be enough to say that the function is not constant, hence balanced. But a winning strategy requires in the worst case at least $2^{n-1}+1$ attempts. This is the easy classical story, and we wish to see what happens if Alice and Bob are allowed to use quantum circuits.

In a quantum world, Alice prepares her black box in the form of a unitary transform U_f like in (2.2). It is a unitary matrix of size $n+1$. The surprising fact is that Bob, using a quantum computer, can discover with certainty the nature of f by just one evaluation through the operation U_f.

This is the following *Deutsch-Josza algorithm*

1. Start with the input state $|\underbrace{0\ldots 0}_{n}1\rangle$
2. Apply the Hadamard transform to all $n+1$ registers, we get $\sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
3. Apply U_f
4. Apply the Hadamard transform to the first n registers.
5. Measure the first n registers: $\begin{cases}\text{if the output is } \ |0\rangle_n \text{ then } f \text{ is constant with probability } 1,\\ \text{if the output is } \neq |0\rangle_n \text{ then } f \text{ is balanced with probability } 1.\end{cases}$

The intriguing feature of this algorithm is that the probabilistic answer of the measurement has been converted to get deterministic answers. The reason why the algorithm works is hidden in step 3. Each summand obtained after step 2. has the form $\frac{|x\rangle}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ and it is transformed in itself if $f(x)=0$ while it has a sign change if $f(x)=1$.

Hence, if f is constant, the output can be just the same or with a global sign change. Applying again the Hadamard transform we get the input state or with just a sign change (at least on the first n registers), so the measurement on the first n registers gives $|0\rangle_n$ with probability 1.

If f is balanced the situation is different, exactly half of summands obtained after step 2. are transformed in itself, the other half have a sign change. Now performing the step 4. we see an interesting result. Each $|x\rangle$ goes to $(\frac{|0\rangle+|01\rangle}{\sqrt{2}})(\frac{|0\rangle+|01\rangle}{\sqrt{2}})(\frac{|0\rangle-|01\rangle}{\sqrt{2}})\ldots$ where $+$ or $-$ appears depending if 0 or 1 appears in x at the corresponding register. Expanding this expression, the summand $|0\rangle_n$ appears always with a $+$, then taking in account the sign changes due to the effect of U_f on exactly half of the summands, the final coefficient of $|0\rangle_n$ vanishes. By Corollary 2.7 it follows that the output $|0\rangle_n$ appears with probability 0, as we wanted.

4 Grover search algorithm

Grover search algorithm can be used all the times a brute force search is needed to detect a particular candidate β from a long list of size N. Its surprising feature is that the search can be done with high probability in $O(\sqrt{N})$ steps, instead of the $N/2$ steps which are needed in a classical search, just to get the answer with probability > 0.5. Label the list with the basis of size 2^n of n qubits. Our candidate β is codified by a characteristic function f, such that

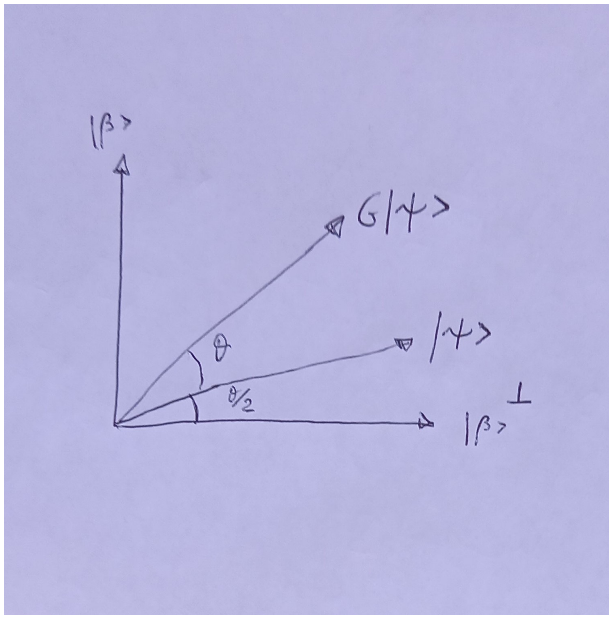
$$\begin{cases} f(x) = 1 & \text{if } x = \beta \\ f(x) = 0 & \text{if } x \neq \beta \end{cases}$$

The function defines a unitary transform U_f of size $n+1$ which, as in the Deutsch-Josza algorithm, can be conveniently applied starting from the uniform state $H^{\otimes n}|\underbrace{0\ldots0}_{n}1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2}} \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ The result of U_f is simply a sign flip in the summand where $x = \beta$. So we have a unitary map O_β which works as

$$\begin{cases} O_\beta(|x\rangle) = & -|x\rangle \quad \text{if } x = \beta \\ O_\beta(|x\rangle) = & |x\rangle \quad \text{if } x \neq \beta \end{cases}$$

The goal is to find the state β, while the simplest thing to be found is the uniform state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$.

The idea is to give a geometric interpretation of O_β restricted to the real plane $\big\langle|\beta\rangle, |\psi\rangle\big\rangle_{\mathbb{R}}$. It is obviously a symmetry through the line $\langle\beta^\perp\rangle$ as in the picture, where $\langle\beta^\perp\rangle = frac1\sqrt{2^n-1}\sum_{x\neq\beta}|x\rangle$ We can then compose with a symmetry through $\big\langle|\psi\rangle\big\rangle$ which is $2|\psi\rangle\langle\psi| - 2I$. Such a unitary operator can be constructed by means of the Hadamard operator H and other elementary bricks ([Na, **?**]) but we skip this point. Call $\theta/2$ the angle between $|\beta\rangle^\perp$ and$|\psi\rangle$. The composition $G = (2|\psi\rangle\langle\psi| - 2I) \cdot O_\beta$ is called the Grover operator and, being the composition of two symmetries, it acts on the plane $\big\langle|\beta\rangle, |\psi\rangle\big\rangle_{\mathbb{R}}$ as a rotation of angle θ (see the picture).



The angle $\theta/2$ satisfies $\cos(\theta/2) = |\beta\rangle^{\perp} \cdot |\psi\rangle = \frac{2^n-1}{\sqrt{2^n(2^n-1)}} = \sqrt{1-\frac{1}{2^n}}$. Hence by Taylor approximation

$$\cos(\theta/2) = 1 - \theta^2/8 + \ldots, \qquad \sqrt{1-\frac{1}{2^n}} = 1 - \frac{1}{2^{n+1}} + \ldots$$

and we get

$$\frac{\theta^2}{8} \sim \frac{1}{2^{n+1}}$$

and finally

$$\theta \sim \frac{1}{\sqrt{2^{n-2}}}$$

The best number of iterations needed to get a state close to β is when $k\theta \sim \pi/2$, hence with $k \sim \frac{\pi}{2\theta} \sim \frac{\pi}{4}\sqrt{2^n}$ which confirms that the number of iterations is approximatively $O(\sqrt{N})$ as promised.

In conclusion, the algorithm consists in applying $\sim \frac{\pi}{4}\sqrt{2^n}$ times the operator G to the uniform state ψ (which in turn can be obtained as $H^{\otimes n}|0\rangle_n$ as in Proposition 2.2. At the end a measurement on the computational basis gives β with high probability.

In [NC, 6.1] there is an (easy) generalization to the case where we search for one among M possible solutions in a list of N elements. Here the number of iterations gros as $O(\sqrt{N/M})$.

References

[BZ] I. Bengtsson, K. Zyczkowski, Geometry of quantum states, An introduction to quantum entanglement, Cambridge, 2006

[BC] C. Bocci, L. Chiantini, An introduction to Algebraic Statistics with Tensors, Springer, 2019

[NC] M. Nielsen I. Chuang, Quantum Computation and Quantum Information, Cambridge 2016

[Na] G. Nannicini, An introduction to quantum computing, without the physics. SIAM Rev. 62 (2020), no. 4, 936–981 , arXiv:1708.03684