QUANTUM TURING MACHINES
A LIGHT INTRODUCTION

note per la lezione speciale di Informatica Quantistica del 5 dicembre 2013

Andrea Masini
dipartimento di Informatica, Università di Verona

Hilbert Spaces

Definition *Complex Inner Product Space*). A *complex inner product space* is a vector space $\mathcal{H}$ on the field $\mathbb{C}$ equipped with a function $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ that satisfies the following properties:

1. $\langle \phi, \psi \rangle = \langle \psi, \phi \rangle^*$;
2. $\langle \psi, \psi \rangle$ is a non-negative real number;
3. if $\langle \psi, \psi \rangle = 0$ then $\psi = \mathbf{0}$;
4. $\langle c_1\phi_1 + c_2\phi_2, \psi \rangle = c_1^* \langle \phi_1, \psi \rangle + c_2^* \langle \phi_2, \psi \rangle$;
5. $\langle \phi, c_1\psi_1 + c_2\psi_2 \rangle = c_1 \langle \phi, \psi_1 \rangle + c_2 \langle \phi, \psi_2 \rangle$.

The function $\langle \cdot, \cdot \rangle$ is the inner product of $\mathcal{H}$ and induces a norm $|| \cdot ||_{\mathcal{H}}$ defined by $||\phi||_{\mathcal{H}} = \sqrt{\langle \phi, \phi \rangle}$.

Definition *Completeness*). Given the metric $d(\psi, \phi) = ||\psi - \phi||_{\mathcal{H}}$, an inner product space $\mathcal{H}$ is *complete* if any Cauchy sequence[3] $(\phi_n)_{n<\omega}$ is convergent.

cauchy-sequence $\forall \epsilon > 0. \exists N > 0. \forall n, m > N. d(\phi_n, \phi_m) < \epsilon.$

Definition **An Hilbert space H is a complex inner product space that is complete with respect to the distance induced by the inner product.**

Proposition Any finite dimensional inner product space is a Hilbert space

Definition Let H', H'' be Hilbert space, and let $U : H' \rightarrow H''$ be a linear surjection map. If for all ϕ, ψ, $\langle U\phi, U\psi\rangle_{H'} = \langle \phi, \psi\rangle_{H''}$ we say that U *is an unitary operator.*

(REMARK: each unitary operator is injective and therefore invertible)

The inverse of an unitary operator is denoted with $U^\dagger$ and is called Adjoint of U

Definition (finite dimensional spaces). Let H be a finite dimensional Hilbert space, and let $U : H \rightarrow H$ be a linear surjection map. The adjoint of U is the unique linear transform $U^\dagger: H \rightarrow H$ such that for all ϕ, ψ $\langle U\phi, \psi\rangle = \langle \phi, U^\dagger \psi\rangle$.

If $U^\dagger U$ is the identity, we say that U is a unitary operator.

Definition (Hilbert Basis). Let B a maximal orthonormal set in a Hilbert space H (whose existence is consequence of Zorn's lemma). B is said to be an Hilbert basis of H.

Definition (Hamel Basis). Let B a maximal linearly independent set in a Hilbert space H (whose existence is consequence of Zorn's lemma). B is said to be an Hamel basis of H.

Please note that the concept of a Hilbert basis is different from the concept of vector space basis (a maximal linearly independent set of vectors), the so-called Hamel basis. In fact it is possible to exhibit a space H with Hilbert basis M s.t. H is not finitely generated by M and therefore M is not a maximal linearly independent set of vectors. An orthonormal Hamel basis is usually called orthonormal basis.

In the finite dimensional case, the two concepts of a Hamel basis and a Hilbert basis coincide. This fails for the infinite dimensional cases [21].

Definition (Span). Let H be an inner-product space and let $S \subseteq H$, the span of S is the inner product subspace of H defined by

$$\mathrm{span}(S)= \{\sum_{i\leq n} c_i s_i | c_i \in C, s_i \in S,\ n \in \mathbb{N}\}$$

Even if H is an Hilbert space, span(S) is not necessarily an Hilbert space

Let $\mathcal{S}$ a set such that $|\mathcal{S}| \leq \aleph_0$ and let $\ell^2(\mathcal{S})$ be the set

$$\left\{ \phi \mid \phi : \mathcal{S} \to \mathbb{C}, \sum_{s \in \mathcal{S}} |\phi(s)|^2 < \infty \right\}$$

equipped with:

(i) an inner sum $+ : \ell^2(\mathcal{S}) \times \ell^2(\mathcal{S}) \to \ell^2(\mathcal{S})$ defined by $(\phi + \psi)(s) = \phi(s) + \psi(s)$;
(ii) a multiplication by a scalar $\cdot : \mathbb{C} \times \ell^2(\mathcal{S}) \to \ell^2(\mathcal{S})$ defined by $(c \cdot \phi)(s) = c \cdot (\phi(s))$;
(iii) an inner product[4] $\langle \cdot, \cdot \rangle : \ell^2(\mathcal{S}) \times \ell^2(\mathcal{S}) \to \mathbb{C}$ defined by $\langle \phi, \psi \rangle = \sum_{s \in \mathcal{S}} \phi(s)^* \psi(s)$;

It is quite easy to show that $\ell^2(\mathcal{S})$ is an Hilbert space.
We call *quantum register* any normalized vector in $\ell^2(\mathcal{S})$.
The set $\mathcal{B}(\mathcal{S}) = \{|s\rangle : s \in \mathcal{S}\}$, where $|s\rangle : \mathcal{S} \to \mathbb{C}$ is defined by:

$$|s\rangle(t) = \begin{cases} 1 & \text{if } s = t \\ 0 & \text{if } s \neq t \end{cases}$$

is a Hilbert basis of $\ell^2(\mathcal{S})$, usually called the *computational basis* in the literature.

It is now interesting to distinguish two cases:

(1) $\mathcal{S}$ is *finite*: in this case $\mathcal{B}(\mathcal{S})$ is also an orthonormal (Hamel) basis of $\ell^2(\mathcal{S})$ and consequently *span*$(\mathcal{B}(\mathcal{S})) = \ell^2(\mathcal{S})$. $\ell^2(\mathcal{S})$ is isomorphic to $\mathbb{C}^{|\mathcal{S}|}$. With a little abuse of language, we can also say that $\ell^2(\mathcal{S})$ is "generated" or "spanned" by $\mathcal{S}$.

(2) $\mathcal{S}$ is *denumerable*: in this case it is easy to show that $\mathcal{B}(\mathcal{S})$ is a Hilbert basis of $\ell^2(\mathcal{S})$, but *it is not* a Hamel basis. In fact let us consider the subspace *span*$(\mathcal{B}(\mathcal{S}))$. We see immediately that *span*$(\mathcal{B}(\mathcal{S})) \subsetneq \ell^2(\mathcal{S})$[5] is an inner-product infinite dimensional space with $\mathcal{B}(\mathcal{S})$ as the Hamel basis, but *span*$(\mathcal{B}(\mathcal{S}))$ *is not* a Hilbert space because *it is not complete*

The careful reader immediately recognizes that $\ell^2(\mathcal{S})$ is the well known fundamental Hilbert space $\ell^2(\mathcal{S})$. There are strong relationships between *span*$(\mathcal{B}(\mathcal{S}))$ and $\ell^2(\mathcal{S})$, in fact it is possible to show (this is a standard result for ℓ^2) that *span*$(\mathcal{B}(\mathcal{S}))$ is a dense subspace of $\ell^2(\mathcal{S})$, and that $\ell^2(\mathcal{S})$ is the (unique!) *completion* of *span*$(\mathcal{B}(\mathcal{S}))$. This fact is important because in the main literature on quantum Turing machines, unitary transforms are usually defined on spaces like *span*$(\mathcal{B}(\mathcal{S}))$, but this could be problematic because *span*$(\mathcal{B}(\mathcal{S}))$ *is not a Hilbert space*. Anyway, this is not a real problem: it is possible to show that each unitary operator $\mathbf{U}$ in *span*$(\mathcal{B}(\mathcal{S}))$ has a standard extension in $\ell^2(\mathcal{S})$

Quantum Turing Machines

In the following we will assume to deal with a finite alphabet Σ with two distinguished symbols $1, \Box$, where $\Box$ represents the blank symbol and 1 is needed to represent integers. With α, β, eventually indexed, we will represent strings in Σ^* (λ denotes the empty string). The finite set Q is called set of states, and contains two distinguished states q_0 (the initial state) and q_f (the final state). Let $n \in \mathbb{N}$, with $\overline{n}$ we denote the string 1^{n+1}.

Definition (configurations) *The notion of configuration is standard, namely a configuration is a triple* $c = \langle \alpha, q, \beta \rangle \in \Sigma^* \times Q \times \Sigma^*$ *where:*

- q *is the current state;*
- α *represents the tape content at the left of the pointer, i.e. the longest string in* Σ^* *on the tape starting with a symbol different from* $\Box$*, such that the last symbol in* α *is in the cell predecessor of the current cell;*
- β *is the tape content at the right of the pointer, i.e. the longest string in* Σ^* *on the tape ending with a symbol different from* $\Box$ *such that the first symbol in* β *is the content of the current cell (if* $\beta = \lambda$ *the current cell contains* $\Box$*);*
- *an initial configuration has the shape* $\langle \lambda, q_0, \overline{n} \rangle$*;*
- *a final configuration has the shape* $\langle \alpha, q_f, \beta \rangle$*; the string* $\alpha + \beta$ *is called output;*
- *given a configuration* $c = \langle \alpha, q, \beta \rangle$*, with* $val[c]$ *we denote the number* n *if* $c = \langle \lambda, q_0, \overline{n} \rangle$ *(the* n *is the input) and the number of* $'1'$ *in* $\alpha\beta$ *if* c *is not initial.*

With $\mathcal{C}_{\Sigma,Q}$ we denote the set of possible configurations (we will omit the subscripts when the choice of Q and Σ is clear from the context). Elements of $\mathcal{C}_{\Sigma,Q}$ are denoted by C, D eventually indexed.

Definition (Hilbert space of configurations) *Given a set $\mathcal{C}_{\Sigma,Q}$ of configurations, with $\ell^2(\mathcal{C}_{\Sigma,Q})$ we will denote the infinite dimensional Hilbert space defined as follow.*

The set of vectors in $\ell^2(\mathcal{C}_{\Sigma,Q})$ is the set

$$\left\{ \phi \mid \phi : \mathcal{C}_{\Sigma,Q} \to \mathbb{C}, \sum_{C \in \mathcal{C}_{\Sigma,Q}} |\phi(C)|^2 < \infty \right\}$$

and equipped with:

1. *An inner sum $+ : \ell^2(\mathcal{C}_{\Sigma,Q}) \times \ell^2(\mathcal{C}_{\Sigma,Q}) \to \ell^2(\mathcal{C}_{\Sigma,Q})$ defined by $(\phi + \psi)(C) = \phi(C) + \psi(C)$;*
2. *A multiplication by a scalar $\cdot : \mathbb{C} \times \ell^2(\mathcal{C}_{\Sigma,Q}) \to \ell^2(\mathcal{C}_{\Sigma,Q})$ defined by $(a \cdot \phi)(C) = a \cdot (\phi(C))$;*
3. *An inner product[1] $< \cdot, \cdot >: \ell^2(\mathcal{C}_{\Sigma,Q}) \times \ell^2(\mathcal{C}_{\Sigma,Q}) \to \mathbb{C}$ defined by $< \phi, \psi >= \sum_{C \in \mathcal{C}_{\Sigma,Q}} \phi(C)^* \psi(C)$;*
4. *The Euclidian norm is defined as $\| \phi \| =< \phi, \phi >$.*

in order the inner product definition make sense, we must prove that the sum $\sum_{C \in \mathcal{C}} \phi(C)^* \psi(C)$ converges.

Definition 3 (computational basis) *The set of functions* $\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}} = \{|\mathsf{C}\rangle : C \in \mathcal{C}_{\Sigma,Q},\ |\quad : \mathcal{C}_{\Sigma,Q} \to \mathbb{C}\}$ *such that for each* C

$$|\mathsf{C}\rangle(D) = \begin{cases} 1 & \textit{if}\, C = D \\ 0 & \textit{if}\, C \neq D \end{cases}$$

is called <u>*computational basis*</u> *of* $\ell^2(\mathcal{C}_{\Sigma,Q})$.

Theorem 4 *The set* $\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}$ *is an Hilbert basis of* $\ell^2(\mathcal{C}_{\Sigma,Q})$.

Please note that the inner product space $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$ defined by:

$$span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}) = \left\{ \sum_{i=1}^{n} c_i s_i \mid c_i \in \mathbb{C}, s_i \in \mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}, n \in \mathbb{N} \right\}.$$

is a proper inner product subspace of $\ell^2(\mathcal{C}_{\Sigma,Q})$, but it is not an Hilbert Space (this means that $\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}$ is not an Hamel basis of $\ell^2(\mathcal{C}_{\Sigma,Q})$).

The completion of $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$ (denoted by $c{-}span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$) is a space isomorphic to $\ell^2(\mathcal{C}_{\Sigma,Q})$.

Theorem *1.* $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$ *is a dense subspace of* $\ell^2(\mathcal{C}_{\Sigma,Q})$*;*

2. $\ell^2(\mathcal{C}_{\Sigma,Q})$ *is the (unique! up to isomorphism)* *completion* *of* $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$*.*

This fact is important because in the main literature on quantum Turing machines, unitary operators are defined by linearity on $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$ not directly on $\ell^2(\mathcal{C}_{\Sigma,Q})$. This is not a real problem, since it is possible to show that:

Theorem *Each unitary operator* $\mathbf{U}$ *in* $span(\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}})$ *has an unique extension in* $\ell^2(\mathcal{C}_{\Sigma,Q})$

Definition 7 (computable numbers) *A real number* x *is called computable if there exists a deterministic Turing machine that on input* 1^n *computes a binary representation of an integer* $m \in \mathbb{Z}$ *such that* $|\frac{m}{2^n} - x| \leq \frac{1}{2^n}$*.*

Let us call $\tilde{\mathbb{C}}$*, the computable complex number, the set of complex numbers such that the real and imaginary parts are computable.*

Definition (quantum configurations). *An elements* $\phi \in \ell^2(\mathcal{C}_{\Sigma,Q})$ *is called quantum configuration (q-configuration) if* $\sum_{C\in\mathcal{C}} |\phi(C)|^2 = 1$. *A q-configuration* C *is* <u>*computable*</u> *(c–configuration) if* $\phi(\mathcal{C}_{\Sigma,Q}) \subseteq \tilde{\mathbb{C}}$.

The set of q-configurations is denoted by $q\mathcal{C}_{\Sigma,Q}$*; the set of c–configurations is denoted by* $q\tilde{\mathcal{C}}_{\Sigma,Q}$. *The elements of* $q\mathcal{C}_{\Sigma}Q$ *are denoted by* $|\phi\rangle, |\psi\rangle$ *possibly indexed; the elements of* $q\tilde{\mathcal{C}}_{\Sigma,Q}$ *are denoted by* $\|\phi\rangle\rangle, \|\psi\rangle\rangle$ *possibly indexed.*

Definition . *[pre-Quantum Turing Machine] Given a set* Q *of states and the alphabet* Σ*, a pre-Quantum Turing Machine is a triple* $M = \langle \Sigma, Q, \delta \rangle$ *where*

$$\delta : Q \times \Sigma \to ((\Sigma \times Q \times \{L, R\}) \to \tilde{\mathbb{C}})$$

satisfies, for any $a \in \Sigma$:

$$\textstyle\sum_{b\in\Sigma, q'\in Q, m\in\{L,R\}} |\delta(q,a)(b,q',m)|^2 = 1;$$

δ *is the* <u>*quantum transition function*</u>.

Definition (time evolution operator). *Let $M = \langle \Sigma, Q, \delta \rangle$ be a pre-Quantum Turing machine , and let us consider the linear operator $W_M : \mathsf{CB}_{\mathcal{C}_{\Sigma,Q}} \to \mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}$ defined on the Hilbert basis $\mathsf{CB}_{\mathcal{C}_{\Sigma,Q}}$ in the following way. If $C = \langle \alpha, q, a\beta \rangle$ then*

$$W_M(|\mathsf{C}\rangle) = \sum_{b \in \Sigma, q' \in Q, m \in \{L,R\}} \delta(q,a)(b,q',m)|\mathsf{C}_{\mathsf{b},\mathsf{q}',\mathsf{m}}\rangle$$

*where each $C_{b,q',m}$ is classically defined, i.e. it is the new configuration obtained by replacing in C the current symbol a with b, changing the current state from q to q' and moving the control in direction m (the technical details are standard, see [**?**]).*

The unique extension $U_M : \ell^2(\mathcal{C}_{\Sigma,Q}) \to \ell^2(\mathcal{C}_{\Sigma,Q})$ of W_M is called <u>time evolution operator</u> of M.

Definition (Quantum Turing Machine). *A pre-Quantum Turing Machine is a <u>Quantum Turing Machine i</u> (QTM) iff the time evolution operator U_M is unitary.*

Theorem *[local conditions for unitariety] Let $M = \langle \Sigma, Q, \delta \rangle$ be a QTM, the time evolution operator U_M is unitary iff:*

(1) $\forall q \in Q, a \in \Sigma$

$$\sum_{p \in Q, b \in \Sigma, d \in \{L,R\}} |\delta(q,a,b,p,d)|^2 = 1$$

(2) $\forall (q,a),(q',a') \in Q \times \Sigma$ *with* $(q,a) \neq (q',a')$

$$\sum_{p \in Q, b \in \Sigma, d \in \{L,R\}} \delta(q',a',b,p,d)^* \delta(q,a,b,p,d) = 0$$

(3) $\forall (q,a,b),(q',a',b') \in Q \times \Sigma \times \Sigma$

$$\sum_{p \in Q} \delta(q',a',b',p,L)^* \delta(q,a,b,p,R) = 0$$

Theorem *Let $M = \langle \Sigma, Q, \delta \rangle$ be a pre–quantum TM; if U_M is an isometry in $\ell^2(\mathcal{C}_{\Sigma,Q})$ then it is also unitary.*

The previous result is important, since for an infinite dimensional Hilbert space $\mathcal{H}$ (e.g. $\ell^2(\mathcal{C}_{\Sigma,Q})$), we have that $U : \mathcal{H} \to \mathcal{H}$ is unitary iff $\forall x, y \in \mathcal{H}, \langle Ux, Uy \rangle = \langle x, y \rangle$ (it is an isometry) and moreover $U(\mathcal{H}) = \mathcal{H}$ (it is surjective). The condition of surjectivity is not necessary in the case of finite dimensional Hilbert spaces, since in this case each isometry is also surjective.

Definition *A q–configuration* $|\phi\rangle = \sum e_i|\mathsf{C_i}\rangle$ *is called* *initial* *if all the* C_i *are initial, and is called* *final* *if all the* C_i *are final.*

Definition (computation)**.** *Let* M *be a QTM and let* U_M *be the associated time evolution operator. Given an a initial q–configuration* $|\phi\rangle$*, a computation for* M *is a denumerable sequence* $\{|\phi_\mathsf{i}\rangle\}_{i\in\omega}$ *s.t.*

(1) $|\phi_\mathsf{0}\rangle = |\phi\rangle$*;*
(2) $|\phi_\mathsf{i}\rangle = U_M^i(|\phi\rangle)$.

Therefore, given a QTM M, each computation is univocally determined by its initial q–configuration.

We denote a computation of a QTM M with initial q–configuration $|\phi\rangle$ with $K^M_{|\phi\rangle}$. If $K^M_{|\phi\rangle} = \{|\phi_\mathsf{i}\rangle\}_{i\in\mathbb{N}}$ we denote with $(K^M_{|\phi\rangle})_i$ the q–configuration $|\phi_\mathsf{i}\rangle$.

It is important to observe that, strictly speaking, QTM-s does not have finite computations.

Definition (denumerable multiset). *Given a set A, a multiset on A is a function $m_A : A \to \mathbb{N}$ (which gives the multiplicity of an element). Let $\alpha = |m_A^{-1}(\mathbb{N} - \{0\})|$, m_A is finite (denumerable) if $\alpha < \aleph_0$ ($\alpha = \aleph_0$). With $2m^A$ we denote the set of all, at most denumerable, multisets on A.*

As usual we will use freely the usual set–theoretic operation on multisets. In particular, given a set A, $\emptyset$ denotes the constant-0 multiplicity function $m_A(i) = 0$.

Definition (the sets $\mathcal{M}$ and $\mathcal{M}_1$). *Let us consider the following sets:*

$$\mathcal{M} = \left\{ |\mathsf{v}\rangle \mid |\mathsf{v}\rangle : \mathbb{N} \to m2^{\mathbb{C}}, \sum_{i \in \mathbb{N}, d \in \mathbb{C}} (|\mathsf{v}\rangle(i)(d))|d|^2 \leq 1 \right\}$$

$$\mathcal{M}_1 = \left\{ |\mathsf{v}\rangle \mid |\mathsf{v}\rangle : \mathbb{N} \to m2^{\mathbb{C}}, \sum_{i \in \mathbb{N}, d \in \mathbb{C}} (|\mathsf{v}\rangle(i)(d))|d|^2 = 1 \right\}$$

The element of $\mathcal{M}$ ($\mathcal{M}_1$) are called <u>quasi–register</u> (<u>register</u>).
A (quasi–)register $|\mathsf{v}\rangle$ is called <u>computable</u> if $|\mathsf{v}\rangle(\mathbb{N}) \subseteq m2^{\tilde{\mathbb{C}}}$; (computable) registers are denoted with ($\|\mathsf{v}\rangle\rangle, \|\mathsf{w}\rangle\rangle \ldots$) $|\mathsf{v}\rangle, |\mathsf{w}\rangle \ldots$).

Definition (numerical evaluation of quantum configurations). *The numerical evaluation of quantum configurations* $\mathbf{val} : q\mathcal{C}_{\Sigma,Q} \to \mathcal{M}$ *is defined in the following way:*

$$(\mathbf{val}|\phi\rangle)(k)(d) = |\,\{C \mid \mathbf{val}[C] = k, d = |\phi\rangle(C)\}\,|$$

Let $\{|\phi_{\mathsf{i}}\rangle\}_{i\in\omega}$ *be a computation, with* $\mathbf{val}(\{|\phi_{\mathsf{i}}\rangle\}_{i\in\omega})$ *we denote the sequence* $\{\mathbf{val}|\phi_{\mathsf{i}}\rangle\}_{i\in\omega}$ *in* $\mathcal{M}$*.*

Definition (probabilities).

(1) *Let* $|\phi\rangle = \sum e_i|\mathsf{C}_{\mathsf{i}}\rangle$ *be a q–configuration, we associate to* $|\phi\rangle$ *a real number in* $\mathbb{R}_{[0,1]}$ *denoted with* $\mathbf{P}^n_{|\phi\rangle}$ *in the following way: (i) if each* C_i *is not final,* $\mathbf{P}^n_{|\phi\rangle} = 0$ *otherwise* $\mathbf{P}^n_{|\phi\rangle} = \sum_{q_f\in C_k,\mathbf{val}[C_k]=n} |e_k|^2$.

(2) *Moreover let* $K^M_{|\phi\rangle} = \{|\phi_{\mathsf{i}}\rangle\}_{i\in\omega})$*, with* $\mathbf{P}[K^M_{|\phi\rangle}, n]$ *we denote the number* $sup\{\mathbf{P}^n_{|\phi_{\mathsf{i}}\rangle}\}_{i\in\mathbb{N}}$.

(3) *Let us denote with* $\mathbf{P}^n_{|\mathsf{v}\rangle}$ *the number* $\sum_{d\in\mathbb{C}}(|\mathsf{v}\rangle(n)(d))|d|^2 \in \mathbb{R}_{[0,1]}$.

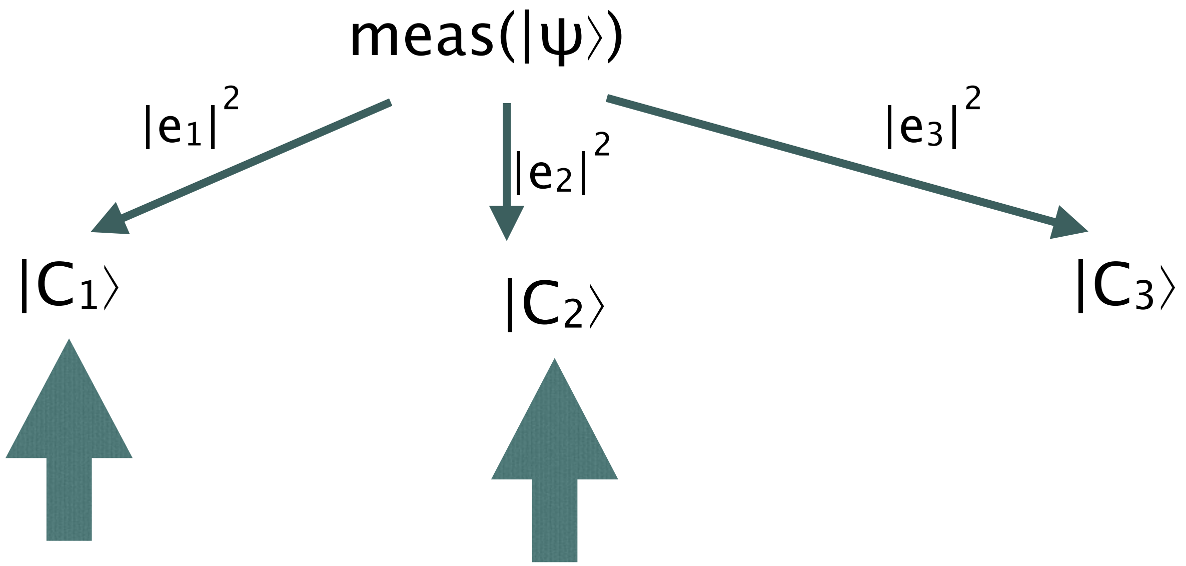
How to read the result of a computation?

The approach of Bernstein and Vazirani

Definition When the q-configuration $|\psi\rangle = \sum e_i|C_j\rangle$ is observed or measured, configuration C_i is seen with probability $|e_i|^2$. Moreover, the superposition of M is updated to $\psi' = |C_i\rangle$

What it happens if we make a measurement of a NON final q-configuration?

$|\psi\rangle = e_1|C_1\rangle + e_2|C_2\rangle + e_3|C_3\rangle$ with C_1, C_2 not final and C_3 final



we have destroyed the quantum computation

In order to supersede the problem Bernstein and Vazirani propose in [?] to consider only QTM where all the computations in superposition have the same length. More precisely:

"A final configuration of a QTM is any configuration in state qf . If when QTM M is run with input x, at time T the superposition contains only final configurations, and at any time less than T the superposition contains no final configuration, then M halts with running time T on input x."

Even their choice is well motivated by the use of QTM in order to solve classical decision problems, it is highly unsatisfactory in order to develop a truly quantum theory of computable function.

It is in fact quite easy to observe that the QTM of Bernstein and Vazirani ar not robust enough to admit quantum inputs but only classical ones.

The approach of Deutsch.

Deutsch assumes to enrich the quantum Turing machines with a termination bit T. At the beginning of a computation the bit T is set to 0 and during the computation the termination bit T is set to 1 when the machine enters in a final configuration. Following this approach the form of a generic q–configuration is:

$$|\phi\rangle = |\mathsf{T} = 0\rangle \otimes \sum e_i|\mathsf{C}'_\mathsf{i}\rangle + |\mathsf{T} = 1\rangle \otimes \sum d_j|\mathsf{C}''_\mathsf{j}\rangle.$$

not final

final

The observer periodically measures T (in a non destructive way):

(1) if the result of the measurement of T gives the value 0 the computation continues with the new (collapsed) q–configuration

$$|\psi'\rangle = \frac{|\mathsf{T}=0\rangle \otimes \sum e_i |\mathsf{C}'_\mathsf{i}\rangle}{\sum |e_i|^2}.$$

(2) if the result of the measurement of T gives the value 0, then $|\mathsf{psi}\rangle$ collapses (with probability $\sum |e_j|^2$) to

$$|\psi''\rangle = \frac{|\mathsf{T}=1\rangle \otimes \sum d_j |\mathsf{C}''_\mathsf{j}\rangle}{\sum |d_j|^2}.$$

Immediately after the collapse the observer makes a further measurement of the component $\frac{\sum d_j |\mathsf{C}''_\mathsf{j}\rangle}{\sum |d_j|^2}$ in order to read-back the result.

Even if this approach gives correct observational results, each observation changes the superpositions during a computation.