Shor's algorithm

Course at IUM Ch. Pittet

II

- A classical bit is formalised by the group $\mathbb{Z}/2\mathbb{Z}$ with two elements. It has two states which are 0 and 1.

- The memory (or register) of a classical computer with n bits is described as the n-dim. vector space
$$\underbrace{\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n} \text{ on the field } \mathbb{Z}/2\mathbb{Z}.$$
It has 2^n states which are the vectors of $(\mathbb{Z}/2\mathbb{Z})^n$.

- A computation is a finite sequence of gates. A gate is by definition a map $(\mathbb{Z}/2\mathbb{Z})^n \xrightarrow{g} (\mathbb{Z}/2\mathbb{Z})^n$. For example the NOT gate $g : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $x \longmapsto x+1$ exchanges 0 and 1.

- Let $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ be the complex vector space on the set $\mathbb{Z}/2\mathbb{Z}$:
$$\mathbb{C}[\mathbb{Z}/2\mathbb{Z}] = \{ \alpha \cdot \mathbf{0} + \beta \cdot \mathbf{1} \ : \ \alpha, \beta \in \mathbb{C} \}$$
$\simeq \mathbb{C}^2$ with basis vectors $e_0 = \mathbf{0}$ and $e_1 = \mathbf{1}$

- This is a 2-dimensional complex Hilbert space with scalar product

$$\langle (\alpha, \beta), (\alpha', \beta') \rangle \doteq \alpha \bar{\alpha}' + \beta \bar{\beta}' .$$

- A <u>quantum-bit</u> (q-bit) is the unit sphere in $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$:

$$S^3 = \{ \alpha \cdot \mathbf{0} + \beta \cdot \mathbf{1} \; : \; |\alpha|^2 + |\beta|^2 = 1 \} .$$
$$\alpha, \beta \in \mathbb{C}$$

- A <u>q-state</u> of a q-bit is any unit vector in $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ (that is any point in $S^3 \subset \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$).
- The elements $\mathbf{0}$ and $\mathbf{1}$ of the q-bit are the <u>fundamental states</u> of the q-bit. Hence any q-state is a <u>superposition</u>

$$\alpha \cdot 0 + \beta \cdot 1 \; : \; |\alpha|^2 + |\beta|^2 = 1$$

of the two fundamental states.

<u>N.B</u> the fundamental states $\mathbf{0}$ and $\mathbf{1}$ are two vectors of norm 1 which are orthogonal.

Tensor products Let V and W be two vector spaces over a field k. Let $F(V\times W)$ be the k-vector space over the set $V\times W$. That is $F(V\times W)$ is the set of formal linear combinaisons

$$\sum_{(v,w)\in V\times W} \alpha_{v,w}\cdot(v,w)$$

$\alpha_{v,w}\in k$ is zero exept for a finite number of $(v,w)\in V\times W$. Hence the set $V\times W$ is a basis of $F(V\times W)$.

Let $I < F(V,W)$ be the linear subspace generated by the elements

$$(\lambda_1 v_1+\lambda_2 v_2, w) - \lambda_1(v_1,w) - \lambda_2(v_2,w)$$
$$\lambda_1,\lambda_2\in k \quad v_1,v_2\in V,\ w\in W$$

$$(v, \lambda_1 w_1+\lambda_2 w_2) - \lambda_1(v,w_1) - \lambda_2(v,w_2)$$
$$\lambda_1,\lambda_2\in k,\ v\in V,\ w_1,w_2\in W.$$

The tensor product of V and W is by definition

$$V\otimes W := F(V\times W)/I .$$

The bilinear map

$$V\times W \to F(V\times W)/I$$
$$(v,w)\longmapsto (v,w)+I$$

is denoted $\quad \begin{array}{ccc} V \times W & \to & V \otimes W \\ (v, w) & \mapsto & v \otimes w \end{array}$

<u>Proposition</u> 1) The tensor product $V \otimes_k W$ has the following universal property: for any vector space E over k and any k bilinear map $\alpha : V \times W \to E$ there is a unique k-linear map $\tilde{\alpha}$:

$$\begin{tikzcd} V \times W \arrow[r, "\alpha"] \arrow[d] & E \\ V \otimes W \arrow[ur, "\tilde{\alpha}"] & \end{tikzcd}$$

commutes

i.e.

$$\tilde{\alpha}(v \otimes w) = \alpha(v, w) \quad \forall (v, w) \in V \times W$$

2) Let $A : V \to E$, $B : W \to F$ be k-linear maps between k vector spaces. There is a unique k-linear map $A \otimes B : V \otimes W \to E \otimes F$ s.t.

$$\begin{tikzcd} V \times W \arrow[r, "A \times B"] \arrow[d] & E \times F \arrow[d] \\ V \otimes W \arrow[r, "A \otimes B"] & E \otimes F \end{tikzcd}$$

commutes i.e. $\forall (v, w) \in V \times W$

$$A(v) \otimes A(w) = (A \otimes B)(v \otimes w) .$$

<u>Proof:</u> 1) By def. of $F(V \times W)$, there is a unique k-lin. ext. of α to $F(V \times W)$ into E. The bilin. of α implies that this extension is 0 on I.

2) $\begin{array}{ccccc} V \times W & \to & E \times F & \to & E \otimes F \\ (v, w) & \mapsto & (A(v), B(w)) & \to & A(v) \otimes B(w) \end{array}$ is k bilinear

hence 2) follows from 1).

Tensor product of finite dimensional Hilbert spaces

Let V and W be two finite dimensional complex Hilbert spaces.
Let $v_1, \dots, v_m$, $w_1, \dots, w_n$ be orthonormal basis i.e. $(v_i, v_j)_V = \delta_{ij}$ $(w_i, w_j)_W = \delta_{ij}$
then $v_i \otimes w_j$ is an orthonormal basis of $V \otimes W$ for the scalar product

$$(v \otimes w, v' \otimes w')_{V \otimes W} := (v, v')_V \cdot (w, w')_W$$

- The n-th tensor product $\left(\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]\right)^{\otimes n}$ of the 2-dimensional Hilbert space $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ is a complex Hilbert space of dim. 2^n:

$$\left(\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]\right)^{\otimes n} = \left\{ \sum_{I \in (\mathbb{Z}/2\mathbb{Z})^n} \alpha_I e_I : \alpha_I \in \mathbb{C} \right\}$$

$$e_I = e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n} \qquad I = (i_1, \dots, i_n), \; i_k \in \{0, 1\}$$

$e_1 = 1$, $e_0 = 0$. Th product is

$$(e_I, e_J) = \prod_{k=1}^{n} (e_{i_k}, e_{j_k}) = \delta_{I,J} .$$

That is: it is the complex Hilbert space with orthonormal basis e_I, $I \in (\mathbb{Z}/2\mathbb{Z})^n$:

$$\langle e_I, e_J \rangle = \begin{cases} 1 & \text{if } I = J \\ 0 & \text{if } I \neq J \end{cases} .$$

- The <u>memory</u> (or register) of a quantum computer with n q-bits is described as the $(2^{n+1}-1)$-unit sphere in $\left(\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]\right)^{\otimes n}$: $\dim_{\mathbb{C}} \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n} = \left(\dim_{\mathbb{C}} \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]\right)^n = 2^n$, $\dim_{\mathbb{R}} = 2^{n+1}$

$$S^{2^{n+1}-1} = \left\{ \sum_{I \in (\mathbb{Z}/2\mathbb{Z})^n} \alpha_I \cdot e_I \ : \ \sum_{I \in (\mathbb{Z}/2\mathbb{Z})^n} |\alpha_I|^2 = 1 \right\}$$

- It is made of the 2^n <u>fundamental states</u> e_I, $I \in (\mathbb{Z}/2\mathbb{Z})^n$ and their superpositions:

$$\sum_{I \in (\mathbb{Z}/2\mathbb{Z})^n} \alpha_I e_I \ : \ \sum_{I \in (\mathbb{Z}/2\mathbb{Z})^n} |\alpha_I|^2 = 1 .$$

- A <u>quantum computation</u> is a finite sequence of <u>quantum gates</u>. A <u>quantum gate</u> is a unitary <u>transformation</u>

$$\mathcal{U} : \left(\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]\right)^{\otimes n} \longrightarrow \left(\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]\right)^{\otimes n}$$

that is a $\mathbb{C}$-linear map from $\left(\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]\right)^{\otimes n}$ into itself which preserves the Hilbert structure:

$$\langle \mathcal{U}(v), \mathcal{U}(w) \rangle = \langle v, w \rangle$$
$$\forall\, v, w \in \left(\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]\right)^{\otimes n} .$$

By definition a <u>q-state</u> is an element $v \in S^{2^n-1} \subset \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n}$.
The image of v under a q-gate $\mathcal{U}$ is $\mathcal{U}(v)$. It is again a q-state because $\|\mathcal{U}(v)\| = \|v\| = 1$.

<u>Examples</u>

- <u>The quantum NOT gate</u>

$$\mathcal{U} : \mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \to \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$$
$$\alpha \cdot \mathbf{0} + \beta \cdot \mathbf{1} \longmapsto \alpha \cdot \mathbf{1} + \beta \cdot \mathbf{0}$$

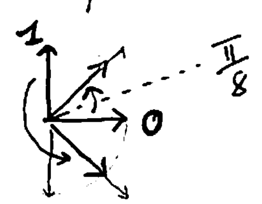
has matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{U}(2, \mathbb{C})$.
It permutes the two fundamental states: $\mathcal{U}(\mathbf{0}) = \mathbf{1}$, $\mathcal{U}(\mathbf{1}) = \mathbf{0}$.

- <u>The Walsh-Hadamard transformations</u>

- $$W : \mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \to \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$$
$$\alpha \cdot \mathbf{0} + \beta \cdot \mathbf{1} \mapsto \frac{\alpha+\beta}{\sqrt{2}} \cdot \mathbf{0} + \frac{\alpha-\beta}{\sqrt{2}} \cdot \mathbf{1}$$

has matrix $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

reflexion of axe $\frac{\pi}{8}$ in the real plane generated by $\mathbf{0}$ and $\mathbf{1}$



$$W^2 = \text{identity}$$

i.e. W is a unitary involution.

- $W_n : \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n} \to \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n}$

$W_n := \underbrace{W \otimes \cdots \otimes W}_{n \text{ times}}$ is $\mathbb{C}$ lin. by def.

It is unitary because the tensor product of two unit. transf. is again a unit. transf.

- $\underline{n=2}$ orth. normal basis for $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \otimes \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ is $0 \otimes 0$, $0 \otimes 1$, $1 \otimes 0$, $1 \otimes 1$.

$W_2(0 \otimes 1) = W(0) \otimes W(1) = \frac{1}{\sqrt{2}}(0+1) \otimes \frac{1}{\sqrt{2}}(0-1)$

$= \frac{1}{2}\left[0\otimes 0 - 0 \otimes 1 + 1 \otimes 0 - 1 \otimes 1\right]$.

The matrix of W_2 in the above basis is

$$\left[\begin{array}{cc|cc} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \hline 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{array}\right] \cdot \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & \multicolumn{2}{c}{\multirow{2}{*}{$-\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$}} \\ 1 & -1 & & \end{array}\right] \in \mathcal{U}(4, \mathbb{C}).$$

- $W_n^2 = (W \otimes \cdots \otimes W)^2 = W^2 \otimes \cdots \otimes W^2 = id \otimes \cdots \otimes id$
$= id_{\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n}}$. Hence W_n is a unitary involution $\forall n$.

- $W_n(0 \otimes 0 \otimes \cdots \otimes 0) = W(0) \otimes \cdots \otimes W(0)$
$= \frac{1}{2^{n/2}}(0+1) \otimes \cdots \otimes (0+1)$

$= \frac{1}{2^{n/2}} \sum_{(i_1, \dots, i_n) \in (\mathbb{Z}/2\mathbb{Z})^n} e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n}$ <u>is the uniform superposition of all fundamental states</u>.

$\begin{pmatrix} e_0 = 0 \\ e_1 = 1 \end{pmatrix}$

The standard oracle and the left regular representation

- Any classical computation $f : (\mathbb{Z}/2\mathbb{Z})^m \to (\mathbb{Z}/2\mathbb{Z})^n$ can be simulated by a quantum computation. To explain how we recall what is the left-regular representation of a finite group.

The group algebra $\mathbb{C}[G]$

- Let G be a finite group and let $\mathbb{C}[G]$ be the complex vector space on G: $\mathbb{C}[G] = \{ \sum_{g \in G} a_g \cdot g \ : \ a_g \in \mathbb{C} \}$ this is a complex Hilbert space of dimension $|G|$ with orthonormal basis $\{ g \in G \}$
$\langle g, h \rangle = \delta_{g,h} = \begin{cases} 1 & g = h \\ 0 & g \neq h \end{cases}$.
It is <u>an algebra</u> for the product
$$\sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{g,h \in G} a_g b_h (g \cdot h).$$

- The <u>left-regular representation</u> of G is the group homomorphism
$$\lambda : G \to \mathcal{U}(\mathbb{C}[G])$$
$$g \mapsto \left(\sum_{h \in G} a_h \cdot h \mapsto \sum_{h \in G} a_h (g \cdot h) \right)$$

$\langle \lambda(g) a, \lambda(g) b \rangle = \langle ga, gb \rangle = \delta_{ga, gb}$
$= \delta_{a,b} = \langle a, b \rangle$ hence $\lambda(g)$ is unitary. $\forall a, b, g \in G$

$\lambda(g)^{-1} = \lambda(g^{-1})$ $\qquad \lambda(gh) = \lambda(g) \circ \lambda(h)$

<u>Proposition</u> (standard oracle)

Let $f: (\mathbb{Z}/2\mathbb{Z})^m \to (\mathbb{Z}/2\mathbb{Z})^n$ be a map.

Consider the basis $\{I \otimes J\}$, $I \in (\mathbb{Z}/2\mathbb{Z})^m$, $J \in (\mathbb{Z}/2\mathbb{Z})^n$ of $\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^m] \otimes \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$.

1) The map

$$I \otimes J \mapsto I \otimes \lambda(f(I))(J)$$

is a permutation of the basis $\{I \otimes J\}_{I \in (\mathbb{Z}/2\mathbb{Z})^m,\ J \in (\mathbb{Z}/2\mathbb{Z})^n}$

2) Let $I_1, \dots, I_{2^m}$ resp. $J_1, \dots, J_{2^n}$ be an ordering of the elements of $(\mathbb{Z}/2\mathbb{Z})^m$, resp. $(\mathbb{Z}/2\mathbb{Z})^n$. (For example we can choose the lex order: $(00\cdots 0), (0\cdots 01), \dots, (1\cdots\cdots 1)$).

The matrix of the induced linear transf. U_f of $\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^m] \otimes \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$ in the basis:

$I_1 \otimes J_1, \dots I_1 \otimes J_{2^n},$

$I_2 \otimes J_1 \dots, I_2 \otimes J_{2^n},$

$\vdots$

$I_{2^m} \otimes J_1, \dots, I_{2^m} \otimes J_{2^n}$

is a diagonal block matrix

$$\begin{bmatrix} \boxed{\lambda(f(I_1))} & & 0 \\ & \ddots & \\ 0 & & \boxed{\lambda(f(I_{2^m}))} \end{bmatrix}$$

where each diagonal block is the permutation matrix of $\lambda(f(I_k))$, $k = 1, \dots, 2^m$, in the basis $J_1, \dots, J_{2^m}$.

3) The values of f are recovered as

$$U_f\big(I \otimes \underbrace{(0,\dots,0)}_{n}\big) = f(I) \quad \forall\, I \in \left(\mathbb{Z}/2\mathbb{Z}\right)^m$$

4) The transformation U_f of the Hilbert product $\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^m] \otimes \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$ is a unitary involution.

<u>Proof</u>: 1) $\lambda : (\mathbb{Z}/2\mathbb{Z})^n \to U\left(\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]\right)$ is a unitary repres,

and $\lambda(f(I))(J) = f(I) + J$ permutes the basis vectors $J \in (\mathbb{Z}/2\mathbb{Z})^n$ of $\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$.

2), 3) obviously follows from 1).

4) Follows from 2) and the fact that

$$\lambda(f(I)) \circ \lambda(f(I)) = \lambda(f(I) + f(I))$$

$$= \lambda\big(\underset{\substack{\cap \\ (\mathbb{Z}/2\mathbb{Z})^n}}{(0,\dots,0)}\big) = id \qquad \blacksquare$$

<u>Def</u> If we identify

$$\mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^m] \otimes \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n] \overset{\overset{\text{isom. of Hilb. spaces}}{\downarrow}}{\cong} \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes m} \otimes \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n}$$

$$(i_1 \cdots i_m) \otimes (j_1 \cdots j_n) \longmapsto e_{i_1} \otimes \cdots \otimes e_{i_m} \otimes e_{j_1} \otimes \cdots \otimes e_{j_n}$$

we get a unitary involution, also denoted U_f, of $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes m} \otimes \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n}$.
It is called the <u>standard oracle</u> of f