Quantum Computing based on Tensor Products
Basics and Illustrative Procedures

Guillermo Morales Luna

Computer Science Section
CINVESTAV-IPN

E-mail: gmorales@cs.cinvestav.mx

5-th International Workshop on Applied Category Theory
Graph-Operad Logic

Agenda

Agenda

Vector and Space Products

$\mathbb{U}, \mathbb{V}$: two vector spaces over $\mathbb{C}$.
$\mathcal{L}(\mathbb{U}, \mathbb{V})$: space of linear maps $\mathbb{U} \to \mathbb{V}$.
$\mathbb{U}^* = \mathcal{L}(\mathbb{U}, \mathbb{C})$: Dual space of $\mathbb{U}$. $u^* \in \mathbb{U}^*$, $u \in \mathbb{U}$, $\langle u^* | u \rangle := u^*(u)$.
$\langle \cdot | \cdot \rangle : \mathbb{U}^* \times \mathbb{U} \to \mathbb{C}$ is a bilinear map.
$\mathbb{U} \otimes \mathbb{V} = \mathcal{L}(\mathbb{V}^*, \mathbb{U})$: Tensor product of $\mathbb{U}$ and $\mathbb{V}$.

Fact

$\mathbb{U} \times \mathbb{V}$ is identified with a subset of $\mathbb{U} \otimes \mathbb{V}$.

$\Phi : \mathbb{U} \times \mathbb{V} \to \mathbb{U} \otimes \mathbb{V}$, $\forall (u, v) \in \mathbb{U} \times \mathbb{V}$, $\Phi(u, v) : [w^* \mapsto \langle w^* | v \rangle u] \in \mathcal{L}(\mathbb{V}^*, \mathbb{U})$.
Given $u \in \mathbb{U}$, $v \in \mathbb{V}$, $u \otimes v := \Phi(u, v) \in \mathcal{L}(\mathbb{V}^*, \mathbb{U})$: tensor product of u and v.

$$\begin{array}{ll} (zu) \otimes v = z(u \otimes v) & (u_1 + u_2) \otimes v = (u_1 \otimes v) + (u_2 \otimes v) \\ u \otimes (zv) = z(u \otimes v) & u \otimes (v_1 + v_2) = (u \otimes v_1) + (u \otimes v_2) \end{array}$$

The tensor product is not commutative, nor even for $\mathbb{U} = \mathbb{V}$.

Fact

If $\dim \mathbb{U} = m$ *and* $\dim \mathbb{V} = n$ *then* $\dim(\mathbb{U} \otimes \mathbb{V}) = mn$*.*

Namely, $\dim(\mathbb{V}^*) = n$ and $\dim(\mathcal{L}(\mathbb{V}^*, \mathbb{U})) = nm$. Thus, if $\mathbb{U} = \mathbb{C}^m$ and $\mathbb{V} = \mathbb{C}^n$ then, $\mathbb{U} \otimes \mathbb{V} = \mathbb{C}^{mn}$.

Fact

If $B_{\mathbb{U}} = \{u_0, u_1, \ldots, u_{m-1}\}$ *is a basis of* $\mathbb{U}$ *and* $B_{\mathbb{V}} = \{v_0, v_1, \ldots, v_{n-1}\}$ *is a basis of* $\mathbb{V}$ *then* $(u_i \otimes v_j)_{i<m, j<n}$ *is a basis of* $\mathbb{U} \otimes \mathbb{V}$*, where for each* i, j*,* $u_i \otimes v_j$ *is the map* $w^* = \sum_{k=0}^{n-1} w_k v_k^* \mapsto w_j u_i$*. This is called the product basis.*

If $B_{\mathbb{V}^*} = \{v_0^*, v_1^*, \ldots, v_{n-1}^*\}$ is a basis of $\mathbb{V}^*$, where $\langle v_{j_1}^* | v_{j_2} \rangle = \delta_{j_1 j_2}$.
The map $u_i \otimes v_j$ is represented by $D_{ij} = (\delta_{i_1 j_1 ij})_{i_1 < m, j_1 < n}$.
Given $u = \sum_{i=0}^{m-1} a_i u_i \in \mathbb{U}$, $v = \sum_{j=0}^{n-1} b_j v_j \in \mathbb{V}$, and $w^* = \sum_{j=0}^{n-1} c_j v_j^* \in \mathbb{V}^*$ then

$$(u \otimes v)(w^*) = \sum_{i=0}^{m-1} a_i \left(\sum_{j=0}^{n-1} b_j c_j \right) u_i = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_i b_j \, (u_i \otimes v_j) \, (w^*),$$

thus $u \otimes v = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_i b_j \, (u_i \otimes v_j)$.

Products of Linear Maps

U_1, U_2: vector spaces of dimensions m_1, m_2. $K : U_1 \to U_2$ linear.
The dual $K^* : U_2^* \to U_1^*$ is defined by

$$\forall u_1 \in U_1\ ,\ u_2 \in U_2 :\ \langle K^*(u_2^*)|u_1\rangle = \langle u_2|K(u_1)\rangle.$$

Fact

If K is represented, with respect to basis B_{U_1} and B_{U_2}, by $M_K \in \mathbb{C}^{m_2 \times m_1}$ then K^* is represented by its Hermitian $M_K^H \in \mathbb{C}^{m_1 \times m_2}$.

V_1, V_2: other two vector spaces of dimensions n_1, n_2. $L : V_1 \to V_2$ linear.
$K \otimes L : U_1 \otimes V_1 \to U_2 \otimes V_2$ is such that

$$\forall u_1 \in U_1\ ,\ v_1 \in V_1 :\ (K \otimes L)(u_1 \otimes v_1) = K(u_1) \otimes L(v_1).$$

Fact

If K is represented, with respect to the basis B_{U_1} and B_{U_2}, by the matrix $M_K \in \mathbb{C}^{m_2 \times m_1}$ and L is represented, with respect to the basis B_{V_1} and B_{V_2}, by the matrix $M_L \in \mathbb{C}^{n_2 \times n_1}$ then $(K \otimes L)$ is represented, with respect to the product basis, by the following tensor product matrix:

$$M_K \otimes M_L = \begin{bmatrix} m_{00}^{(K)} M_L & m_{01}^{(K)} M_L & \cdots & m_{0,m_1-1}^{(K)} M_L \\ m_{10}^{(K)} M_L & m_{11}^{(K)} M_L & \cdots & m_{1,m_1-1}^{(K)} M_L \\ \vdots & \vdots & \ddots & \vdots \\ m_{m_2-1,0}^{(K)} M_L & m_{m_2-1,1}^{(K)} M_L & \cdots & m_{m_2-1,m_1-1}^{(K)} M_L \end{bmatrix} \in \mathbb{C}^{m_2 n_2 \times m_1 n_1}.$$

U: m-dimensional vector space, $K : U \to U$ linear: $K^{\otimes 1} = K$,
$K^{\otimes n} = K^{\otimes (n-1)} \otimes K$: n-th tensorial power.

If $M_K = (m_{ij})_{i,j<m}$ represents K, then $M_{K^{\otimes n}} = \left(m_{ij}^{(n)}\right)_{i,j<m^n}$ represents $K^{\otimes n}$.

Let's write each $i < m^n$ in base m: $i = \sum_{j=0}^{n-1} \xi_j m^j = (\xi_{n-1} \cdots \xi_1 \xi_0)_m = (\xi)_m$.
If $\xi = \xi_{n-1} \cdots \xi_1 \xi_0$, let $\mathrm{car}(\xi) = \xi_0$ and $\mathrm{cdr}(\xi) = \xi_{n-1} \cdots \xi_1$

$$\begin{aligned} (\xi)_m &= m(\mathrm{cdr}(\xi))_m + \mathrm{car}(\xi) \ , \\ \mathrm{car}(\xi) &= (\xi)_m \bmod m \ \text{ and} \\ (\mathrm{cdr}(\xi))_m &= ((\xi)_m - \mathrm{car}(\xi))/m. \end{aligned}$$

Then

$$m^{(n)}_{\xi(i),\xi(j)} = m^{(n-1)}_{\mathrm{cdr}(\xi(i)),\mathrm{cdr}(\xi(j))} \cdot m_{\mathrm{car}(\xi(i)),\mathrm{car}(\xi(j))} \qquad (1)$$

Agenda

Measurement Principle

Complex matrices. $\mathbb{C}^{m\times n}$: space of $(m \times n)$-matrices with complex entries

Transpose conjugate. $M = (m_{ij})_{i,j} \in \mathbb{C}^{m\times n} \ \Rightarrow \ M^H = \left(m^H_{ji}\right)_{ji} = (\overline{m_{ij}})_{ji}$

Unitary matrix. $M^H M = \mathbf{1}_{nn}$. $M|_{E_m} : E_m \to E_m$.

Hermitian matrix. $M^H = M$

Set of states. $\mathbb{C}^{m\times 1}$

Unit Euclidean sphere. $E_m = \{\mathbf{v} \in \mathbb{C}^m | 1 = \mathbf{v}^H \mathbf{v} =: \langle \mathbf{v}|\mathbf{v}\rangle\}$.

Canonical basis. $\mathbf{e}_j = (\delta_{ij})_{i<m}$

Connotation

A state $\mathbf{v} = (v_{i1})_{i<m}$ outputs index i with probability $|v_{i1}|^2 = \mathrm{Re}(v_{i1})^2 + \mathrm{Im}(v_{i1})^2$.

Measurement Principle

Being at $\mathbf{v} = (v_{i1})_{i<m}$, with probability $|v_{i1}|^2$:

- The index i is output and
- the computing control is transferred to the state $\mathbf{e}_i$.

This principle is applied just once at the end of any quantum algorithm, it ptoduces a halting state.

If m is a power of 2:

Quantum gate. Any square $(m \times m)$-unitary matrix $U \in \mathbb{C}^{m \times m}$.

Quantum algorithm. Composition of a finite number of quantum gates, followed by a measurement.

For the particular case of $m = 2$,

- $\mathbf{e}_0 = [1 \;\; 0]^T$ and $\mathbf{e}_1 = [0 \;\; 1]^T$: Canonical basis of $\mathbb{C}^2$
- $\mathbf{e}_0$ is identified with the truth value false, or zero, and $\mathbf{e}_1$ with the truth value true, or one.
- qubit: $z_0\mathbf{e}_0 + z_1\mathbf{e}_1$, with $z_0, z_1 \in \mathbb{C}$, $|z_0|^2 + |z_1|^2 = 1$
- $\mathbb{H}_1 = \mathbb{C}^2$, $\mathbb{H}_n = \mathbb{H}_{n-1} \otimes \mathbb{H}_1$.
- $\dim(\mathbb{H}_n) = 2^n$, with basis $B_{\mathbb{H}_n} = \left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right)_{\varepsilon_{n-1},\ldots,\varepsilon_1,\varepsilon_0\in\{0,1\}}$

Conventional Dirac's "ket" notation

$$\begin{aligned} |\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0\rangle &:= \mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0} \\ &= \mathbf{e}_{\varepsilon_{n-1}}\otimes\cdots\otimes\mathbf{e}_{\varepsilon_1}\otimes\mathbf{e}_{\varepsilon_0} \\ &=: |\varepsilon_{n-1}\rangle\cdots|\varepsilon_1\rangle|\varepsilon_0\rangle \end{aligned} \quad (2)$$

- $[\![0, 2^n - 1]\!] \approx \{0,1\}^n$, $i \leftrightarrow \varepsilon = \varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0$
- Information word of length n: $\mathbf{z} \in E_{2^n} \Rightarrow \mathbf{z} = \sum_{\varepsilon\in\{0,1\}^n} z_{\varepsilon}\mathbf{e}_{\varepsilon}$

Agenda

Quantum Gates

Identity

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $I : \mathbb{H}_1 \to \mathbb{H}_1$ is the identity operator.

Rotation

For $t \in [-\pi, \pi]$, $Rot_t = \begin{bmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{bmatrix} : \mathbb{H}_1 \to \mathbb{H}_1$

If $\mathbf{x}_p = \sqrt{p}\,\mathbf{e}_0 + \sqrt{1-p}\,\mathbf{e}_1$ then

$$Rot_t(\mathbf{x}_p) = \left(\cos(t)\sqrt{p} - \sin(t)\sqrt{1-p}\right)\mathbf{e}_0 + \left(\cos(t)\sqrt{1-p} + \sin(t)\sqrt{p}\right)\mathbf{e}_1.$$

For $t_{0p} = \cos^{-1}(-\sqrt{p})$, $Rot_{t_{0p}}(\mathbf{x}_p) = -\mathbf{e}_0$: gives 0 with probability $(-1)^2 = 1$.
For $t_{1p} = \cos^{-1}(\sqrt{1-p})$, $Rot_{t_{1p}}(\mathbf{x}_p) = \mathbf{e}_1$: gives 1 with probability 1.
A rotation acts as an interference, either constructive or destructive.

Negation

$N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Clearly, $N : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \begin{bmatrix} z_1 \\ z_0 \end{bmatrix}$. N is unitary and it switches signals. Geometrically it is “a reflection along the main diagonal”.

Hadamard

$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Clearly, $H : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{bmatrix} z_0 + z_1 \\ z_0 - z_1 \end{bmatrix}$. H is unitary and it “reflects the complex plane with respect to the axis x and then it rotates counterclockwise an angle of $\frac{\pi}{4}$ radians”.

$N^{\otimes n} : \mathbb{H}_n \to \mathbb{H}_n$ acts as the "$(2^n - 1)$-complement", i.e. when it is evaluated at the basic vectors

$$N^{\otimes n}\left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right) = \mathbf{e}_{\delta_{n-1}\cdots\delta_1\delta_0} \quad (3)$$

where $(\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0)_2 + (\delta_{n-1}\cdots\delta_1\delta_0)_2 = 2^n - 1$.

$H^{\otimes n} : \mathbb{H}_n \to \mathbb{H}_n$ is such that

$$H^{\otimes n}(\mathbf{e}_{0\cdots 0}) = \frac{1}{(\sqrt{2})^n}\left(\sum_{\boldsymbol{\varepsilon}\in\{0,1\}^n} \mathbf{e}_{\boldsymbol{\varepsilon}}\right) \quad (4)$$

e.g. acting in the first basic vector $\mathbf{e}_{0\cdots 0}$ it produces the state that "averages" all the basic vectors with uniform weights.

Controlled negation

$C : \mathbb{H}_2 \to \mathbb{H}_2$, $\mathbf{e}_x \otimes \mathbf{e}_y \mapsto \mathbf{e}_x \otimes \mathbf{e}_{x \oplus y}$ ($\oplus$: xor). The second qubit is the negation of the first input qubit if the second qubit was "on". Second input qubit serves as "control" to negate the first input qubit: "argument".

C is not the tensor product of two unitary maps over $\mathbb{H}_1$.

Commuted controlled negation. $D : \mathbb{H}_2 \to \mathbb{H}_2$, $(\mathbf{x}, \mathbf{y}) \mapsto D(\mathbf{x}, \mathbf{y}) = C(\mathbf{y}, \mathbf{x})$. W.r.t. canonical basis of $\mathbb{H}_2$,

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \;,\; D = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

C and D generate a subgroup under the “composition” operation:

$\circ$	I	C	D	CD	DC	CDC
I	I	C	D	CD	DC	CDC
C	C	I	CD	D	CDC	DC
D	D	DC	I	CDC	C	CD
CD	CD	CDC	C	DC	I	D
DC	DC	D	CDC	I	CD	C
CDC	CDC	CD	DC	C	D	I

This group is presented by its unit I (the identity map), two generators C, D and the relation $CDC = DCD$. The group is isomorphic to S_3.
Namely, if $\rho = (1, 2)$ is the reflection and $\phi = (1, 2, 3)$ is the order 3 cycle, then $C \leftrightarrow \rho$, $D \leftrightarrow \rho \circ \phi$.

Reverse

$R_2 = CDC : \mathbb{H}_2 \to \mathbb{H}_2$. $R_2(\mathbf{e}_i \otimes \mathbf{e}_j) = \mathbf{e}_j \otimes \mathbf{e}_i$.

$$R_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

For each $n \geq 2$:

$$R_n = R_2^{\otimes n} \left(\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0}\right) = \mathbf{e}_{\varepsilon_0\varepsilon_1\cdots\varepsilon_{n-1}} \quad (5)$$

The operator reverses the “input word”.

Pauli matrices

The matrices

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ , \ \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ , \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{6}$$

- Hermitian and unitary: for $j = 0, 1, 2, 3$, $\sigma_j \sigma_j = \mathbf{1}_2$
- They conform a basis of $\mathbb{C}^{2\times 2}$:

$$\forall A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \in \mathbb{C}^{2\times 2}\ \exists c_0, c_1, c_2, c_3 : \ A = c_0\sigma_0 + c_1\sigma_1 + c_2\sigma_2 + c_3\sigma_3 \tag{7}$$

namely
$(c_0, c_1, c_2, c_3) = \frac{1}{2}\left((a_{00} + a_{11}), (a_{01} + a_{10}), i(a_{01} - a_{10}), (a_{00} - a_{11})\right).$

- The following relations hold: for $1 \leq j, k \leq 3$

$$\sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{jk}\mathbf{1}_2 \quad (8)$$

$$\sigma_j\sigma_k = \delta_{jk}\mathbf{1}_2 + i\sum_{\ell=1}^{3}\varepsilon_{jk\ell}\sigma_\ell \quad (9)$$

where $\varepsilon_{jk\ell} \in \{-1, 0, 1\}$,
$|\varepsilon_{jk\ell}| = 1 \Leftrightarrow \{j, k, \ell\} = \{1, 2, 3\}$ and
$\varepsilon_{jk\ell} = 1 \Leftrightarrow (j, k, \ell)$ is a clockwise rotation.

- For a qubit $\mathbf{z} = z_0\mathbf{e}_0 + z_1\mathbf{e}_1$, with $|z_0|^2 + |z_1|^2 = 1$, we have that $\sigma_1\mathbf{z} = z_1\mathbf{e}_0 + z_0\mathbf{e}_1$ and $\sigma_2\mathbf{z} = -iz_1\mathbf{e}_0 + iz_0\mathbf{e}_1$ are bit-flip errors in $\mathbf{z}$, while $\sigma_3\mathbf{z} = z_0\mathbf{e}_0 - z_1\mathbf{e}_1$ is a phase-flip error in $\mathbf{z}$.

Quantum speed-up

Any state in $\mathbb{H}_n$, $\sigma(\mathbf{z}) = \sum_{\varepsilon\in\{0,1\}^n} z_\varepsilon \mathbf{e}_\varepsilon$ is determined by 2^n coordinates. If $U : \mathbb{H}_n \to \mathbb{H}_n$ is a quantum operator, the target state $\sigma(U\mathbf{z})$ consists also of 2^n coordinates.

A calculus involving an exponential number of terms is performed in just "one step" of the quantum computation.

Agenda

Observables

$\mathbb{H}$: finite dimensional Hilbert space over $\mathbb{C}$ $\quad E_{\mathbb{H}}$: unit sphere.

$H : \mathbb{H} \to \mathbb{H}$ is selfadjoint if $\forall \mathbf{x}, \mathbf{y} \in \mathbb{H}\ \langle \mathbf{x}|H\mathbf{y}\rangle = \langle H\mathbf{x}|\mathbf{y}\rangle$, or $\overline{H}^T = H$.

A selfadjoint map is also called an observable.

For any observable H, there exists an orthonormal basis of $\mathbb{H}$ consisting of eigenvectors of H. Let $(\mathbf{f}_i)_i$ be such a basis.

Then for any $\mathbf{z} = \sum_i a_i \mathbf{f}_i \in E_{\mathbb{H}}$, with $\sum_i |a_i|^2 = 1$,

$$\langle \mathbf{z}|H\mathbf{z}\rangle = \left\langle \sum_i a_i \mathbf{f}_i | H\left(\sum_j a_j \mathbf{f}_j\right)\right\rangle = \left\langle \sum_i a_i \mathbf{f}_i | \sum_j a_j \lambda_j \mathbf{f}_j \right\rangle = \sum_i \lambda_i |a_i|^2 = E(\lambda_i)$$

$\langle \mathbf{z}|H\mathbf{z}\rangle$ is the expected observed value of $\mathbf{z}$ under H.

Standard deviation

$$\triangle H : \mathbb{H} \to \mathbb{R}\ ,\ \mathbf{x} \mapsto \triangle H(\mathbf{x}) = \sqrt{\langle H^2\mathbf{x}|\mathbf{x}\rangle - \langle H\mathbf{x}|\mathbf{x}\rangle^2}.$$

Let $H_1, H_2 : \mathbb{H} \to \mathbb{H}$ be two observables. Then $\forall \mathbf{x} \in \mathbb{H}$:

$$\langle H_2 \circ H_1 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | H_2 \circ H_1 \mathbf{x} \rangle = \langle H_1 \circ H_2 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | H_1 \circ H_2 \mathbf{x} \rangle = |\langle H_1 \mathbf{x} | H_2 \mathbf{x} \rangle|^2,$$

and, from the Schwartz inequality, it follows $|\langle H_1 \mathbf{x} | H_2 \mathbf{x} \rangle|^2 \leq \|H_1 \mathbf{x}\|^2 \|H_2 \mathbf{x}\|^2$.

Robertson-Schrödinger Inequality

$$\frac{1}{4} |\langle (H_1 \circ H_2 - H_2 \circ H_1) \mathbf{x} | \mathbf{x} \rangle|^2 \leq \|H_1 \mathbf{x}\|^2 \|H_2 \mathbf{x}\|^2. \quad (10)$$

$[H_1, H_2] = H_1 \circ H_2 - H_2 \circ H_1$: Commutator .
H_1, H_2 are compatible observables if $[H_1, H_2] = 0$.

Heisenberg Principle of Uncertainty

For any two observables H_1, H_2 and any $\mathbf{z} \in E_{\mathbb{H}}$,

$$|\triangle H_1(\mathbf{z})|^2 |\triangle H_2(\mathbf{z})|^2 \geq \frac{1}{4} \left| \langle \mathbf{z} | \, [H_1, H_2] \, \mathbf{z} \rangle \right|^2 . \tag{11}$$

If the observables are incompatible, whenever H_1 is measured with greater precision, H_2 will be with lesser precision, and conversely.
A state $\mathbf{z}$ is decomposable if is of the form $\mathbf{z}_1 \otimes \cdots \otimes \mathbf{z}_n = \sigma(\mathbf{z})$, with $\mathbf{z}_i \in \mathbb{H}_1$. A non-decomposable state is an entangled state.

Agenda

Evaluation of Boolean Functions

- $V = \{0, 1\}$: set of classical truth values
- There are 2^{2^n} Boolean functions $V^n \to V$
- There are 2^{n2^n} functions $V^n \to V^n$
- Each of the 2^n assignments $\varepsilon = (\varepsilon_{n-1}, \dots, \varepsilon_1, \varepsilon_0) \in V^n$ corresponds with an $\mathbf{e}_\varepsilon \in \mathbb{H}_n$ of the canonical basis of $\mathbb{H}_n$.

Let $f : V^n \to V$ be a Boolean function.

- U_f: a permutation $2^{n+1} \times 2^{n+1}$-matrix s.t. $U_f(\mathbf{e}_\varepsilon \otimes \mathbf{e}_0) = (\mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)})$.
- U_f is an unitary matrix

Let $A \subset V^n$ and $a = \mathrm{card}(A)$. If $\mathbf{u}_A = \frac{1}{\sqrt{a}} \sum_{\varepsilon \in A} \mathbf{e}_\varepsilon \otimes \mathbf{e}_0$ then $U_f(\mathbf{u}_A) = \frac{1}{\sqrt{a}} \sum_{\varepsilon \in A} \mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)}$.

In just one step, the weighted average of the images of all the assignments in A is obtained. A final measurement selects a pair $\mathbf{e}_\varepsilon \otimes \mathbf{e}_{f(\varepsilon)}$, with $\varepsilon \in A$, each with probability $\frac{1}{a}$.

Agenda

Deutsch-Jozsa's Algorithm

Let $V = \{0, 1\}$ be the set of classical truth values. Among the $2^2 = 4$ Boolean functions $f : V \to V$, two are constant and two are balanced.

$$f_0 : \begin{array}{ccc} 0 & \mapsto & 0 \\ 1 & \mapsto & 0 \end{array} \;,\; f_1 : \begin{array}{ccc} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \end{array} \;,\; f_2 : \begin{array}{ccc} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{array} \;,\; f_3 : \begin{array}{ccc} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \end{array}$$

Deutsch-Jozsa's problem

Decide, for a given f, whether it is constant or balanced "in just one computing step".

Let U_f be the permutation $2^2 \times 2^2$-matrix s.t.

$$U_f(\mathbf{e}_x \otimes \mathbf{e}_z) = (\mathbf{e}_x \otimes \mathbf{e}_{(z+f(x)) \bmod 2}).$$

U_f is an unitary matrix and is similar to the “controlled negation” gate.
Using Hadamard's operator H, let $H_2 = H \otimes H$.
$H(\mathbf{e}_0) = \mathbf{x}_0 = \frac{1}{\sqrt{2}}(\mathbf{e}_0 + \mathbf{e}_1)$ and
$H(\mathbf{e}_1) = \mathbf{x}_1 = \frac{1}{\sqrt{2}}(\mathbf{e}_0 - \mathbf{e}_1) \in \mathbb{H}_1$ hence
$H_2(\mathbf{e}_0 \otimes \mathbf{e}_1) = H(\mathbf{e}_0) \otimes H(\mathbf{e}_1) = \mathbf{x}_0 \otimes \mathbf{x}_1 = \frac{1}{2}(\mathbf{e}_{00} - \mathbf{e}_{01} + \mathbf{e}_{10} - \mathbf{e}_{11}) \in \mathbb{H}_2$.

$$\begin{aligned} U_f(\mathbf{x}_0 \otimes \mathbf{x}_1) &= \frac{1}{2}(\mathbf{e}_{0,f(0)} - \mathbf{e}_{0,\overline{f(0)}} + \mathbf{e}_{1,f(1)} - \mathbf{e}_{1,\overline{f(1)}}) \\ &= \begin{cases} \mathbf{x}_0 \otimes \mathbf{x}_1 & \text{if } f = f_0 \\ \mathbf{x}_1 \otimes \mathbf{x}_1 & \text{if } f = f_1 \\ -\mathbf{x}_1 \otimes \mathbf{x}_1 & \text{if } f = f_2 \\ -\mathbf{x}_0 \otimes \mathbf{x}_1 & \text{if } f = f_3 \end{cases} \end{aligned}$$

$$
H_2 U_f H_2(\mathbf{e}_0 \otimes \mathbf{e}_1) = H_2 U_f(\mathbf{x}_0 \otimes \mathbf{x}_1) = \begin{cases} H\mathbf{x}_0 \otimes H\mathbf{x}_1 & \text{if } f = f_0 \\ H\mathbf{x}_1 \otimes H\mathbf{x}_1 & \text{if } f = f_1 \\ -H\mathbf{x}_1 \otimes H\mathbf{x}_1 & \text{if } f = f_2 \\ -H\mathbf{x}_0 \otimes H\mathbf{x}_1 & \text{if } f = f_3 \end{cases}
$$

$$
= \begin{cases} \mathbf{e}_0 \otimes \mathbf{e}_1 & \text{if } f = f_0 \\ \mathbf{e}_1 \otimes \mathbf{e}_1 & \text{if } f = f_1 \\ -\mathbf{e}_1 \otimes \mathbf{e}_1 & \text{if } f = f_2 \\ -\mathbf{e}_0 \otimes \mathbf{e}_1 & \text{if } f = f_3 \end{cases}
$$

The quantum procedure $H_2 U_f H_2$, from the basic vector $\mathbf{e}_0 \otimes \mathbf{e}_1$ is producing a vector of the form $\varepsilon \mathbf{e}_S \otimes \mathbf{e}_1$ where $\varepsilon \in \{-1, 1\}$ is a sign and S is a signal indicating whether f is balanced or not. S coincides with $f(0) \oplus f(1)$. The measurement principle outputs $\mathbf{e}_S \otimes \mathbf{e}_1$ with probability $\varepsilon^2 = 1$. It gives the value S from the first qubit.