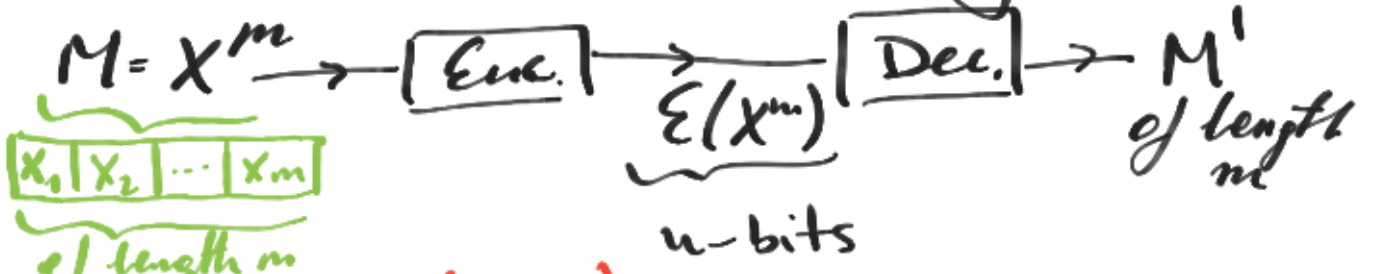
1. Quantum Compression

Recall Shannon Coding Theorem:



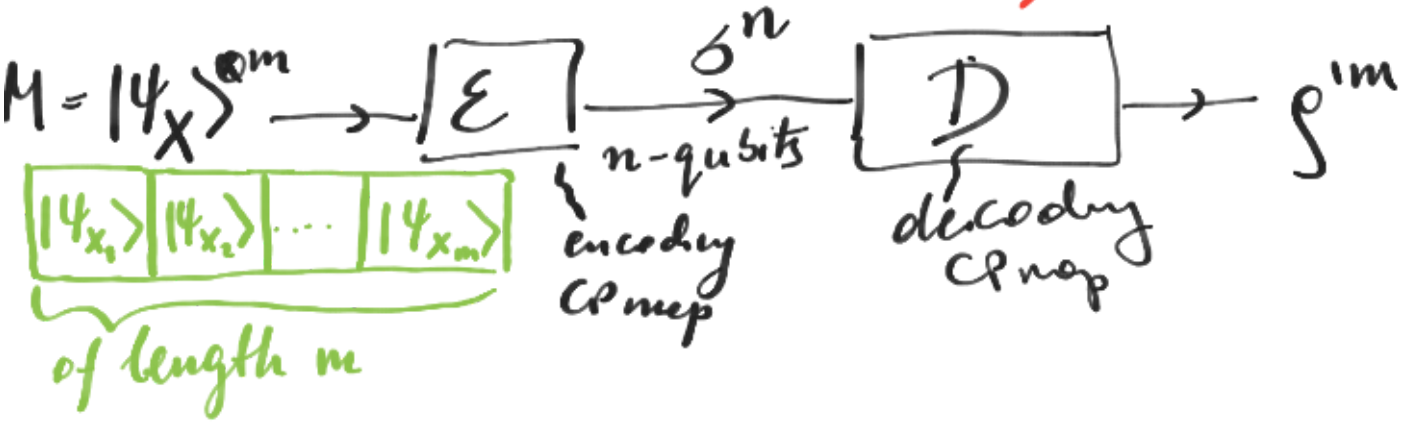
(M = M') for faithful compression

$$\text{Asymptotic compression rate: } R_\infty = \lim_{m\to\infty} \frac{n(m)}{m} \leq H(X)$$

"=" with Huffman codes

Q: What if we allow to encode (classical) information into (pure) quantum states?

X labels: $\{p(X), |\psi_X\rangle\}$ ensemble.



We want ρ'^m to faithfully represent every transmitted message M:

that

$\underbrace{|\psi_{x_1}\rangle, |\psi_{x_2}\rangle, \ldots, |\psi_{x_m}\rangle}_{|\psi_{\underline{x}}\rangle}$ occurs with $\underbrace{p(x_1)p(x_2)\ldots p(x_m)}_{p(\underline{x})}$

Still, it is an IID scenario, so that on average each symbol looks like: $\rho = \sum_{x=1}^{d} p(x)|\psi_x\rangle\langle\psi_x|$ and the whole message as: $\rho^{\otimes m} = \sum_{x_1,\ldots,x_m=1}^{d} p(\underline{x})|\psi_{\underline{x}}\rangle\langle\psi_{\underline{x}}|$

but not enough $F[\rho^{\otimes m}, \rho'^{\otimes m}] = 1$!

NB. $F[\rho,\sigma] = \mathrm{Tr}\left\{\sqrt{\sqrt{\rho}\,\sigma\,\sqrt{\rho}}\right\}^2 = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

$\Rightarrow F[|\psi\rangle, |\phi\rangle] = |\langle\psi|\phi\rangle|^2$

$F[|\psi\rangle, \rho] = \langle\psi|\rho|\psi\rangle$

$\rightsquigarrow$ not for a given state ρ (which we know $\Rightarrow$ could just reprepare...)

$\rightsquigarrow$ transmission: information encoded in $|\psi_{\underline{x}}\rangle$ $\rightarrow$ recovered at the output despite probabilistic noise

Faithful compression:

$|\psi_{\underline{x}}\rangle\langle\psi_{\underline{x}}| \rightarrow \rho_{\underline{x}} = D[\mathcal{E}[|\psi_{\underline{x}}\rangle\langle\psi_{\underline{x}}|]]$

We want $\rho_{\underline{x}}$ to be close to $|\psi_{\underline{x}}\rangle$

on average!:

$$\bar{F} = \sum_{\underline{x}} p(\underline{x}) \langle \psi_{\underline{x}} | \rho'_{\underline{x}} | \psi_{\underline{x}} \rangle$$

$$= \sum_{\underline{x}} p(\underline{x}) \operatorname{Tr}\{ |\psi_{\underline{x}}\rangle\langle\psi_{\underline{x}}| \; \rho'_{\underline{x}} \}$$

Faithful compression with rate R:

(*) $\forall_{\varepsilon>0} \; \exists_{m_0} \; \forall_{m \geq m_0} \; \bar{F} > 1-\varepsilon$,

where # of qubits used for encoding : $n = R \cdot m$

Def.ⁿ von-Neumann entropy

$$S(\rho) = -\operatorname{Tr}\{\rho \log \rho\}$$

let $\rho = \sum_{\lambda} p_\lambda |e_\lambda\rangle\langle e_\lambda|$ eigenvalue (spectral) decomposition

$$\Rightarrow S(\rho) = -\sum_{\lambda} p_\lambda \log p_\lambda = H(\lambda)$$

Ok, then in eigenbasis we can write the average input message M as

$$\rho^{\otimes m} = \sum_{\lambda_1 \lambda_2 \ldots \lambda_m} \underbrace{p(\lambda_1) \ldots p(\lambda_m)} \, |e_{\lambda_1}\rangle\langle e_{\lambda_1}| \otimes \ldots \otimes |e_{\lambda_m}\rangle\langle e_{\lambda_m}|$$

$$= \sum_{\underline{\lambda}} p(\underline{\lambda}) \; |e_{\underline{\lambda}}\rangle\langle e_{\underline{\lambda}}|$$

$\underline{\lambda}$

where these are all orthogonal $\langle e_{\underline{\lambda}} | e_{\underline{\lambda}'} \rangle = \delta_{\underline{\lambda}\underline{\lambda}'}$

Can treat classically! ⟸

$$\Rightarrow \rho^{\otimes m} \approx \sum p(\underline{\lambda}) |e_{\underline{\lambda}}\rangle\langle e_{\underline{\lambda}}|$$

$(m \to \infty)$ $\underline{\lambda} \in$ typ. seq ⟸ Shannon theory!

$$P_T = \sum_{\underline{\lambda} \in \text{typ.seq}} |e_{\underline{\lambda}}\rangle\langle e_{\underline{\lambda}}|$$

m diagonal qubits

projector onto typical subspace of dimension : $2^{mH(\lambda)} = 2^{mS(\rho)}$ (m qubits)

⇒ From Shannon Coding Theorem: with help of λ label, as $m \to \infty$ it should be enough to use: $mH(\lambda) = mS(\rho)$ qubits

But how?

Schumacher compression: $R_\infty = S(\rho)$

Encoding $\mathcal{E}$:
Project onto typical subspace T and send $n = mS(\rho)$-qubit representation of M: $|4_{\underline{\nu}}\rangle \approx |4_{\underline{\lambda}}\rangle$, $\underline{\lambda} \in T$

$$\rho' = D[\mathcal{E}[\rho]] = P_T \rho P_T + \mathcal{E}_1(\rho)$$

$P_T \rho P_T$: λ-representation of n qubits was sent

$\mathcal{E}_1(\rho) = |0\rangle\langle 0|^{\otimes m} \mathrm{Tr}\{\rho(\mathbb{1} - P_T)\}$: $|0\rangle\langle 0|^{\otimes m}$ was sent

for everything out of T just send a fixed (atypical) state

PROOF: Let $\mathrm{Tr}\{\rho^{\otimes m} P_T\} = 1 - \delta$. then

$$\bar{F} = \sum_x p(x)\, \mathrm{Tr}\{ |\psi_x\rangle\langle\psi_x| D\mathcal{E}(|\psi_x\rangle\langle\psi_x|) \} =$$

$$= \sum_x p(x)\, \mathrm{Tr}\{ \psi_x (P_T \psi_x P_T + |0\rangle\langle 0| \mathrm{Tr}\{\rho P_T^\perp\}) \}$$

$$\geq \sum_x p(x) [\mathrm{Tr}\{\psi_x P_T \psi_x P_T\} + \underbrace{\langle 0|\psi_x|0\rangle \mathrm{Tr}\{\rho P_T^\perp\}}_{\geq 0}]$$

$$\geq \sum_x p(x)\, \mathrm{Tr}\{\psi_x P_T \psi_x P_T\}$$

$$\{ |\psi_x\rangle = \alpha_x |\psi_x\rangle + \beta_x |\psi_x^\perp\rangle ;\ |\psi\rangle \in T$$

$$\ldots = \sum_x p(x) |\alpha_x|^4 \geq \sum_x p(x)(1-|\beta_x|^2)^2$$

but $\mathrm{Tr}\{\rho^{\otimes m} P_T\} = \sum_x p(x) \langle\psi_x| P_T |\psi_x\rangle =$

$$= 1 - \sum_x p(x) |\beta_x|^2$$

$$\geq 1-\delta$$

$$\Rightarrow \sum_x p(x) |\beta_x|^2 \leq \delta$$

$$\ldots = 1 - \sum_x p(x) 2|\beta_x|^2 + \sum_x p(x) |\beta_x|^4$$

$$\geq 1 - 2\delta$$

thm $\bar{F} \geq 1 - \underbrace{2\delta}_{\epsilon \text{ in } (*)}$

typicality: $\delta \to 0$ as $m \to \infty \Rightarrow \bar{F} \to 1$

$\Rightarrow R_\infty = S(\rho)$ is a faithful compression rate

[Schumacher 1995]

2) Definitions of quantum entropies

- Quantum Mutual Information

$$S(A:B) = \underbrace{S(\rho_A)}_{S(A)} + \underbrace{S(\rho_B)}_{S(B)} - \underbrace{S(\rho_{AB})}_{S(A,B)}$$

- Quantum Conditional Entropy

$$S(A|B) = \underbrace{S(\rho_{AB})}_{S(A,B)} - \underbrace{S(\rho_B)}_{S(B)}$$

$\Rightarrow$ can be negative !!!

- Quantum Relative Entropy (q. K-L divergence)

$$S(\rho_A \| \rho_B) = \mathrm{Tr}\{\rho \lg \rho\} - \mathrm{Tr}\{\rho \lg \sigma\}$$

Properties of S:

(i) $S(\rho \| \sigma) \geq 0$

(ii) subadditivity: $S(A,B) \leq S(A) + S(B)$

(iii) strong subadditivity: $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$

$$S(A:B) \leq S(A:BC)$$

(iv) Let $\mathcal{E}$ be a CPTP map on B

s.t. $\rho_B' = \mathcal{E}(\rho_B)$

then $S(A:B') \leq S(A:B)$

(v) $S\left(\sum_x p_x |x\rangle\langle x| \otimes \rho_x\right) = H(x) + \sum_x p_x S(\rho_x)$

cl $\leftrightarrow$ quantum

for $\langle x|x'\rangle = \delta_{xx'}$

Proofs: 🏠

(i) $\rho = \sum_i p_i |i\rangle\langle i|$, $\sigma = \sum_k \tilde{p}_k |e_k\rangle\langle e_k|$

$$S(\rho\|\sigma) = \sum_i p_i \lg p_i - \sum_i p_i \langle i|\lg\sigma|i\rangle$$

$$= \sum_i p_i \left(\lg p_i - \sum_k |\langle i|e_k\rangle|^2 \lg \tilde{p}_k\right) \geq$$

concavity of log $\geq \sum_i p_i \left(\lg p_i - \lg \underbrace{\sum_k \tilde{p}_k |\langle i|e_k\rangle|^2}_{q_i}\right)$

≥ 0 [by K-L divergence / classical relative entropy]

(ii) $\rho = \rho_{AB}$, $\sigma = \rho_A \otimes \rho_B$

$S(\rho\|\sigma) = \mathrm{Tr}\{\rho \lg\rho\} - \mathrm{Tr}\{\rho \lg\sigma\}$

$$= -S(A,B) - \mathrm{Tr}\{\rho_{AB} \lg[(\rho_A \otimes \mathbb{1})(\rho_B \otimes \mathbb{1})]\}$$

$$= -S(A,B) - S(A) - S(B) \geq 0$$

(iii) proof is not straightforward unlike the classical case, but intuitively ...

(iv) $S(A:B') \leq S(A:B'C')$

$$\rho_{AB'} = \sum_i \overset{A}{\mathbb{1}} \otimes \overset{B}{K_i}(\rho_{AB}) \overset{A}{\mathbb{1}} \otimes \overset{B}{K_i^+}$$

Stinespring Thm:

$$\rho_{AB'C'} = \overset{A}{\mathbb{1}} \otimes \overset{BC'}{U}(\rho_{AB} \otimes |0\rangle\langle 0|) \overset{A}{\mathbb{1}} \otimes \overset{BC'}{U^+}$$

unitary

$$S(\rho_{AB'C'}) = S(\rho_{AB} \otimes |0\rangle\langle 0|) =$$

$$= S(\rho_{AB}) + \underbrace{S(|0\rangle\langle 0|)}_{0}$$

$$S(A:B') \leq S(A) + S(B',C') - S(A,B',C')$$

$$S(B') \qquad S(A,B)$$

$$\leq S(A:B)$$

(v) $S\left(\sum_x p_x |x\rangle\langle x| \otimes \rho_x\right) = S\left(\sum_{x,r} p_x \lambda_r^{(x)} |x\rangle\langle x| \otimes |\xi_r^{(x)}\rangle\langle \xi_r^{(x)}|\right)$

$$= -\sum_{x,r} p_x \lambda_r^{(x)} \lg p_x \lambda_r^{(x)} =$$

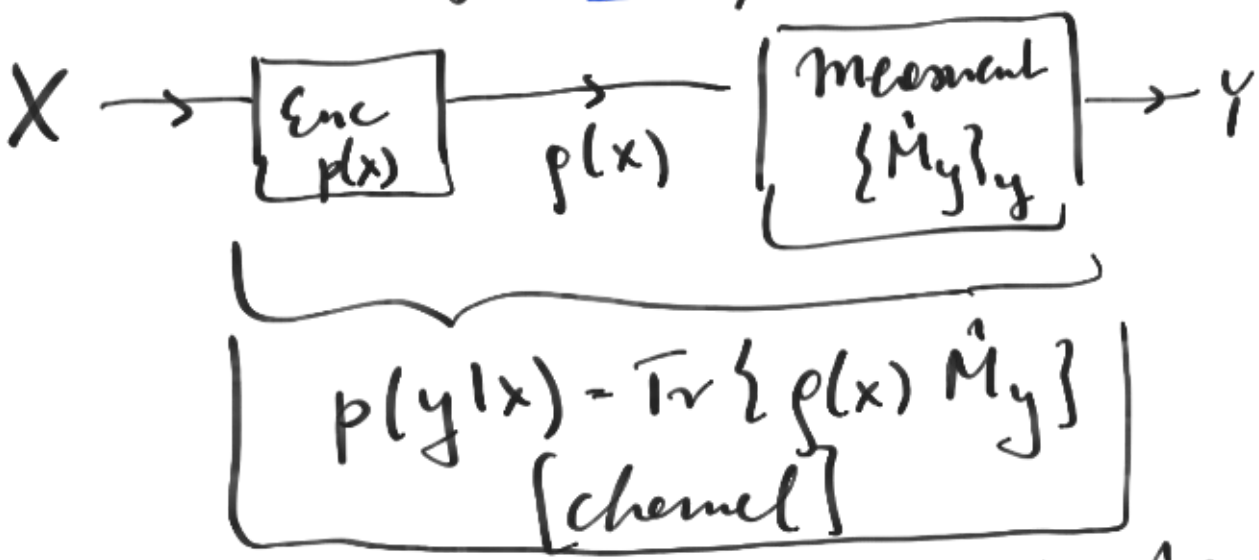
$$= -\sum p_x \lg p_x - \sum_x p_x \sum_r \lambda_r^{(x)} \lg \lambda_r^{(x)}$$

$$= H(X) + \sum_x p_x S(\rho_x)$$

---

2. Holevo bound (or theorem)

⇒ Reliably (faithfully) encoding and decoding (classical) information into/from quantum states.



⇒ $p(x,y) = p(x)\, p(y|x) = p(x)\, \mathrm{Tr}\{\rho(x) \hat{M}_y\}$

Theorem:

$$I(X:Y) \leq \underbrace{S(\bar{\rho}) - \sum_x p(x) S(\rho(x))}$$

$\bar{\rho} = \sum_x p(x) \rho(x)$ $\qquad$ χ - Holevo quantity

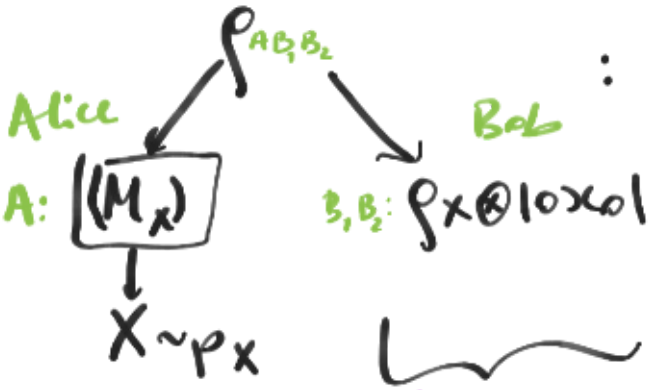
(Holevo) bound on accessible information.
(best one known)

$p(x)$ $\qquad$ $\rho(x)$

Proof:

Consider $\rho_{AB_1B_2} = \sum_x p_x |x\rangle\langle x|_A \otimes \rho_x^{(B_1)} \otimes |0\rangle\langle 0|_{B_2}$ (① ② ③)

with $\langle x|x'\rangle = \delta_{xx'}$



: Hilde [remote state preparation] according to the ensemble $\{p_x, \rho_x\}$

RSP

$\mathcal{E}$: ← $\{\hat{M}_y\}$ + Neumark Dilation →

$$\rho_{AB'B'} = \mathcal{E}[\rho_{AB_1B_2}] = \sum_x p_x |x\rangle\langle x| \otimes \sum_y \sqrt{\hat{M}_y}\rho_x\sqrt{\hat{M}_y} \otimes |y\rangle\langle y| \otimes |0\rangle\langle 0| \otimes |y\rangle\langle y|$$

$$S(A:BC) \overset{(iv)}{\geq} S(A:B'C') \overset{(iii)\ \text{str. subad.}}{\geq} S(A:C')$$

$$S(A:BC) = S(A) + S(B) - S(A,BC) \quad (①\ ②\ ⑤)$$
$$= H(X) + S(\bar{\rho}) - \sum_x p_x S(\rho_x) - H(X)$$
$$= S(\bar{\rho}) - \sum_x p_x S(\rho_x)$$

$$S(A:C') = S(\rho_A) + S(\rho_{C'}) - S(\rho_{AC'})$$
$$= H(X) + H(Y) - H(X,Y)$$

$$\rho_{AC'} = \sum_x \underbrace{p_x \, \mathrm{Tr}\{\rho_x \hat{M}_y\}}_{p(x,y)} \; |x\rangle\langle x| \otimes |y\rangle\langle y|$$

$$\ldots = I(X:Y)$$

$$\Rightarrow I(X:Y) \leq S(\bar{\rho}) - \sum_{x=1}^{d} p_x S(\rho_x)$$

where $\bar{\rho} = \sum_{x=1}^{d} p_x \rho_x$

Important consequence:

given n qubits, so that $\bar{\rho} \in \mathcal{B}(\mathbb{C}_2^{\otimes n})$

$$I(X:Y) \leq S(\bar{\rho}) = H(\lambda_{\bar{\rho}}) \leq \lg 2^n = n$$

n-bits!

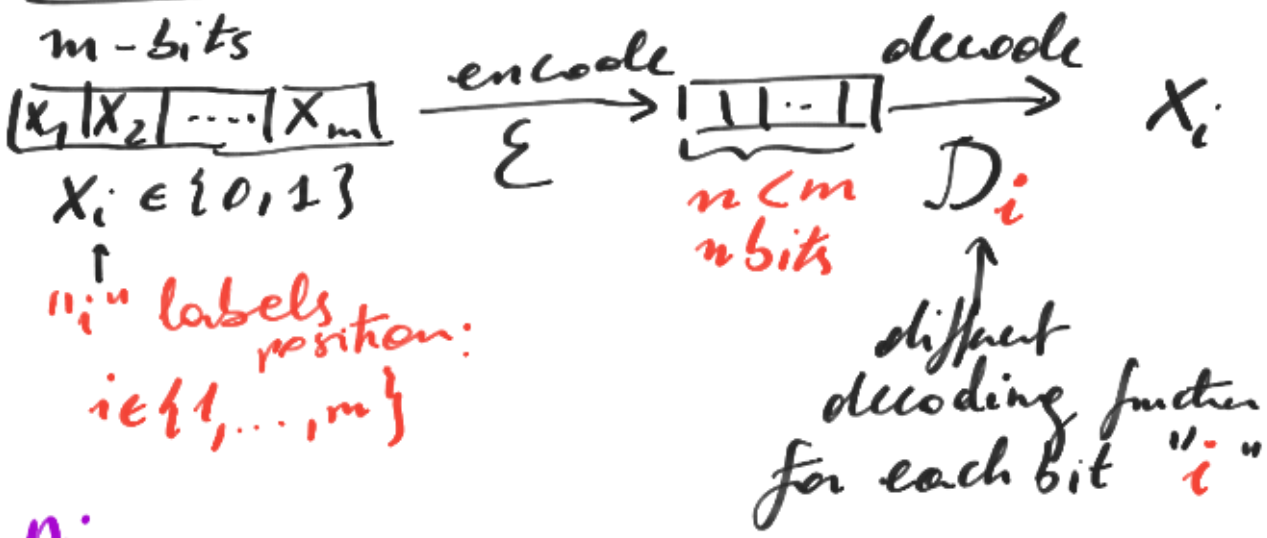
$\Rightarrow$ We can reliably (accessible information) encode and decode into n qubits only n bits of information.

So is there any advantage in using quantum states (light/matter) as storage of information??? (eg. quantum computers)

Simple example:

Quantum Random Access Codes

RACs (classical)



Aim:

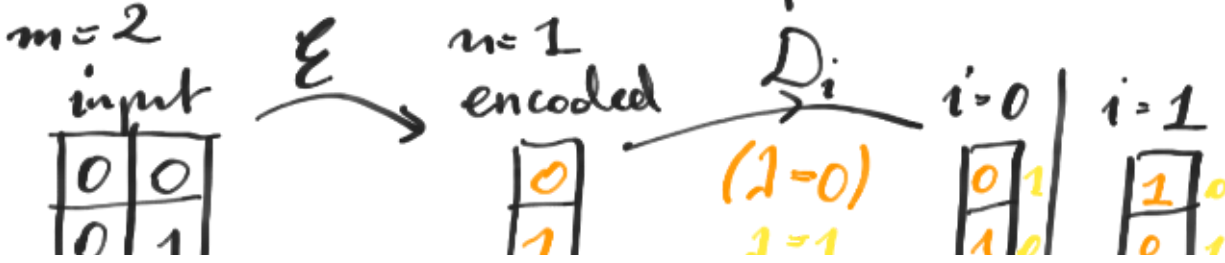
For each "i" construct decoding D_i such that the bit X_i is recovered with probability ("random" in the name) at least $> p$.

$\Rightarrow$ This is then RAC (m, n, p)

- m: input bits
- n: encoded bits
- p: each x_i recovered with $> p$.

Example:

RAC $(2, 1, p)$



in general:

$$\xi : \{0,1\}^2 \times R \longrightarrow \{0,1\}$$
$$V_i : D_i : \{0,1\} \times R \longrightarrow \{0,1\}$$

source of randomness, e.g., toss a coin

try:

$$\xi(x,y) = x \oplus y$$

toss a coin $\lambda \in \{0,1\}$ with $p(\lambda=0) = p(\lambda=1) = \frac{1}{2}$

given λ: $D_i(x,\lambda) = x \oplus (\lambda \oplus i)$

$\Rightarrow$ bad strategy ☹ $\rightarrow$ $P = \frac{1}{2}$

same as guessing randomly with $p = \frac{1}{2}$ of getting the value of i^{th} bit right.

For all $\mathcal{E}$ & D_i : $(2, 1, p = \frac{1}{2})$

(*) For proof see: Ambainis, Nayak, Ta-Shma, Vazirani 1999

but:

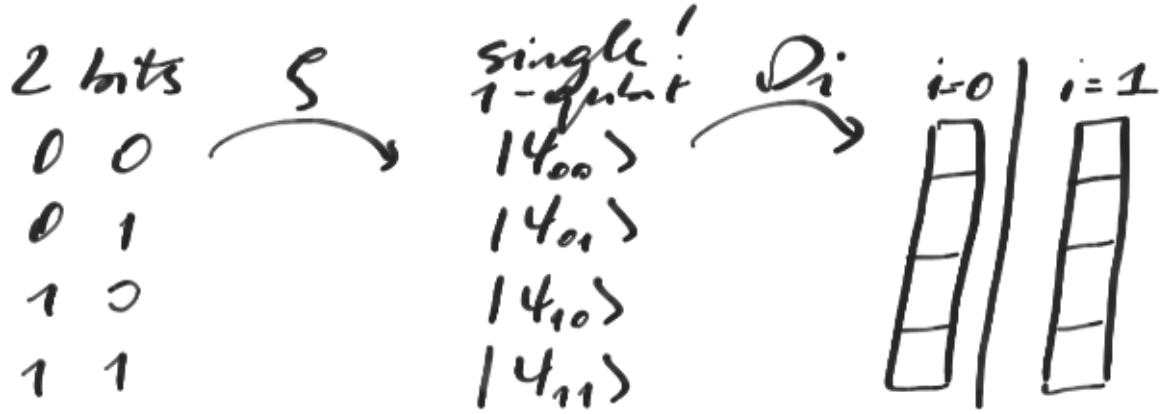
Quantum RAC (QRAC)

(m, n, p) — again, probability of recovering each x_i of m-bits

m-bits, n-qubits

Exemple: QRAC $\left(2, 1, \cos^2 \frac{\pi}{8}\right)$

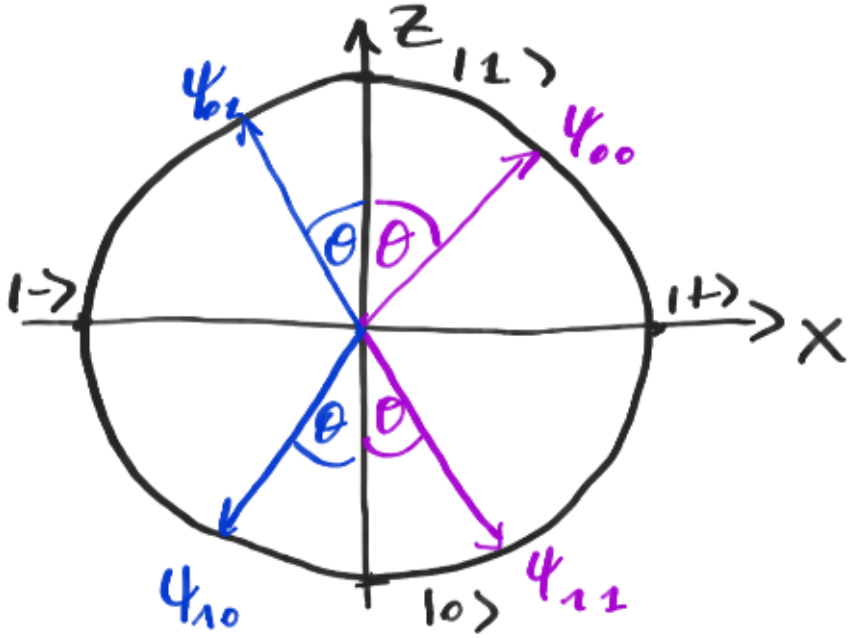
much better than classical ⇐ ≈ 0.85



Encoding

$$|\psi_{00}\rangle = \sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$$
$$|\psi_{01}\rangle = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$$
$$|\psi_{10}\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$$
$$|\psi_{11}\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$$

Bloch picture:



Decoding

"1" "0"

$D_{i=0}$: Measure in $\{|0\rangle, |1\rangle\}$ basis ⇒ output 1 or 0

$D_{i=1}$: Measure in $\{|+\rangle, |-\rangle\}$ basis ⇒ output 0 or 1

"0" "1" respectively

NB : • when $\theta = 0$ ⇒ measure in $\{|0\rangle, |1\rangle\}$

⇒ we perfectly recover first bit ($i=0$)

• when $\theta = \frac{\pi}{2}$ ⇒ measure in $\{|+\rangle, |-\rangle\}$

→ we perfectly recover second bit ($i=1$)

Exercice 1

$$\max_{0 \le \theta \le \frac{\pi}{2}} p(\text{outcome} = x_i) = \cos^2 \frac{\pi}{8} \approx 0.85$$

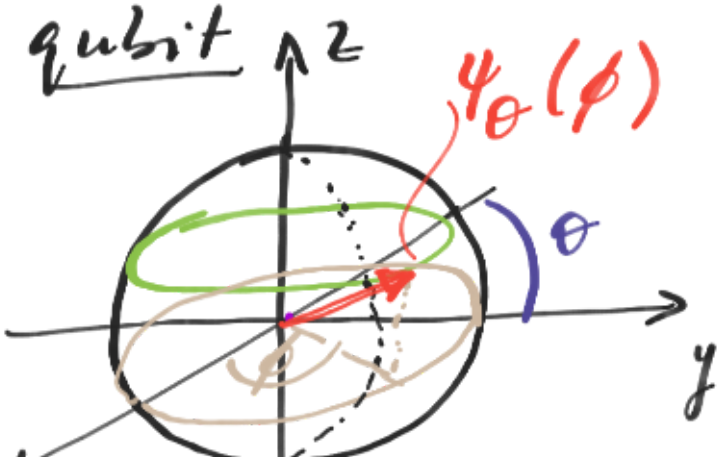
$$= \frac{2+\sqrt{2}}{4}$$

for $\theta_{opt} = \frac{\pi}{4}$

Example

a) Compression with states equally distributed around a parallel

b) Encoding + Decoding with ... (Holevo)



Messages $\phi \sim p(\phi) = \frac{1}{2\pi}$ ← flat around the circle

θ – fixed (parameter)

encoding: bits | ϕ_1 | ϕ_2 | ϕ_3 | .. | ϕ_m |

pure states | $|\psi_\theta(\phi_1)\rangle$ | $|\psi_\theta(\phi_2)\rangle$ | .... | $|\psi_\theta(\phi_m)\rangle$ |

Schumacher compression

$$R_\infty = \frac{n(m)}{m} = S(\bar\rho)$$

$$\bar\rho = \int_0^{2\pi} d\phi\, p(\phi)\ |\psi_\theta(\phi)\rangle\langle\psi_\theta(\phi)|$$

$$\text{⌂} = h\left(\frac{1+\sin\theta}{2}\right)$$

hint: $\rho_\phi = \frac{1}{2}(\mathbb{1} + \underline{r}_\phi \cdot \underline{\sigma})$

$$\bar\rho = \int d\phi\, p(\phi)\, \rho_\phi = \frac{1}{2}\left[\mathbb{1} + \left(\int d\phi\, p(\phi)\, \underline{r}_\phi\right)\cdot\underline{\sigma}\right]$$

$$\langle \underline{r}_\phi \rangle_\phi = \int d\phi\, p(\phi) \begin{pmatrix} \cos\phi\cos\theta \\ \sin\phi\cos\theta \\ \sin\theta \end{pmatrix}$$

Holevo bound, on accessible information
⇒ encoding into $\{\psi_\theta(\phi), \psi_\theta(\phi)\}$

$$I(X:Z) \leq S(\bar{\rho}) - \int d\phi\, p(\phi)\, S(|\psi_\theta(\phi)\rangle)$$

$S(|\psi\rangle) = 0$ for pure states!

$$= S(\bar{\rho})$$
$$= h\left(\frac{1+\sin\theta}{2}\right) \leq \log 2 = 1$$

"=" for $\theta = 0$