4. Quantum information and Quantum error correction

4.1 Measure of quantum information

classical random variable X that takes on values x_i with probabilities p_i ⇒ Shannon entropy

$$(1) \qquad S_{Sh} = -\sum_j p_j \log p_j$$

as measure of information.

consider orthogonal states with probabilities p_j

$$(2) \qquad x_j \longleftrightarrow |x_j\rangle \qquad \langle x_j | x_e \rangle = \delta_{je}$$

$$(3) \qquad \rho = \sum_j p_j |x_j\rangle\langle x_j|$$

Eq. (1) can be written as

$$(4) \qquad S_{Sh} = -\mathrm{Tr}\{\rho \log \rho\} = S_N$$

i.e. this is the von Neumann entropy. We now use S_N also as measure of information contained in a quantum state ρ

$$(5) \qquad \boxed{S_N = -\mathrm{Tr}\{\rho \log \rho\}}$$

rem.: the basis of the log is 2

<u>some properties</u> (some known and some new)

(i) pure state $\varrho = |\psi\rangle\langle\psi|$ $\boxed{S_N = 0}$

(ii) maximally mixed state $\varrho = \frac{1}{N}\mathbb{1}_N$ $\boxed{S_N = \log N}$

(iii)
$$\boxed{0 \leq S_N \leq \log(\dim \mathcal{H})} \qquad (6)$$

(iv) S_N is concave $\lambda_1, \lambda_2, \ldots, \lambda_n \geq 0$ $\sum_i \lambda_i = 1$

(7)
$$\boxed{S_N(\varrho) = S_N(\lambda_1\varrho_1 + \cdots \lambda_n \varrho_n) \geq \lambda_1 S_N(\varrho_1) + \cdots + \lambda_n S_N(\varrho_N)}$$

this reflects that if we know the decomposition $\varrho = \sum_i \lambda_i \varrho_i$ of a state we have more a-priori knowledge i.e. "measurement" of ϱ would yield <u>less</u> information

(v)
$$\boxed{S_N(U\varrho U^{-1}) = S_N(\varrho)} \quad \text{if } U^+ = U^{-1} \qquad (8)$$

(vi) <u>subadditivity</u>

$$\boxed{S_N(\varrho_{AB}) \leq S_N(\varrho_A) + S_N(\varrho_B)} \qquad (9)$$

where $\varrho_A = \mathrm{Tr}_B\{\varrho_{AB}\}$; $\varrho_B = \mathrm{Tr}_A\{\varrho_{AB}\}$

if ϱ factorizes, i.e. if $\varrho_{AB} = \varrho_A \cdot \varrho_B$

$$S_N(\varrho_A \varrho_B) = S_N(\varrho_A) + S_N(\varrho_B)$$

(ϱ_A, ϱ_B do not contain information about entanglement between A and B)

(vii) <u>strong subadditivity</u>

$$(10) \quad \boxed{S_N(\rho_{ABC}) + S_N(\rho_A) \leq S_N(\rho_{AB}) + S_N(\rho_{AC})}$$

This is <u>non-trivial</u>! It is basis for many formal proofs in quantum information theory.

(ix) <u>Araki-Lieb inequality</u>

$$(11) \quad \boxed{S_N(\rho_{AB}) \geq |S_N(\rho_A) - S_N(\rho_B)|}$$

this is in contrast to the classical case!! where

$$S_{Sh}(X,Y) \geq S_{Sh}(X), S_{Sh}(Y)$$

in q-mechanics it is however possible that

$$S_N(\rho_{AB}) < S_N(\rho_A), S_N(\rho_B)$$

even $S_N(\rho_{AB}) = 0$ if ρ_{AB} is pure but A and B are <u>entangled</u> and thus $S_N(\rho_A) = S_N(\rho_B) > 0$

<u>example</u> $\quad |\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\rho_A = \mathrm{Tr}_B\{|\Phi_+\rangle\langle\Phi_+|\} = \frac{1}{2}\mathbb{1} = \rho_B \qquad (S_N \to S)$$

$$S(\rho_A) = S(\rho_B) = 1 \quad \text{but} \quad S(\rho_{AB}) = 0$$

smallest Hilbert space with non-zero S_N : $\mathbb{C}^2$
(spin 1/2)

$$(12) \qquad \boxed{\mathcal{H} = \{|0\rangle, |1\rangle\} \qquad \text{qubit}}$$

a general qubit state has the form

$$(13) \qquad \boxed{\rho = \frac{1}{2}\left(\mathbb{1} + \vec{s}\cdot\vec{\sigma}\right)} \qquad \vec{\sigma} = \sigma_x \vec{e}_x + \sigma_y \vec{e}_y + \sigma_z \vec{e}_z$$

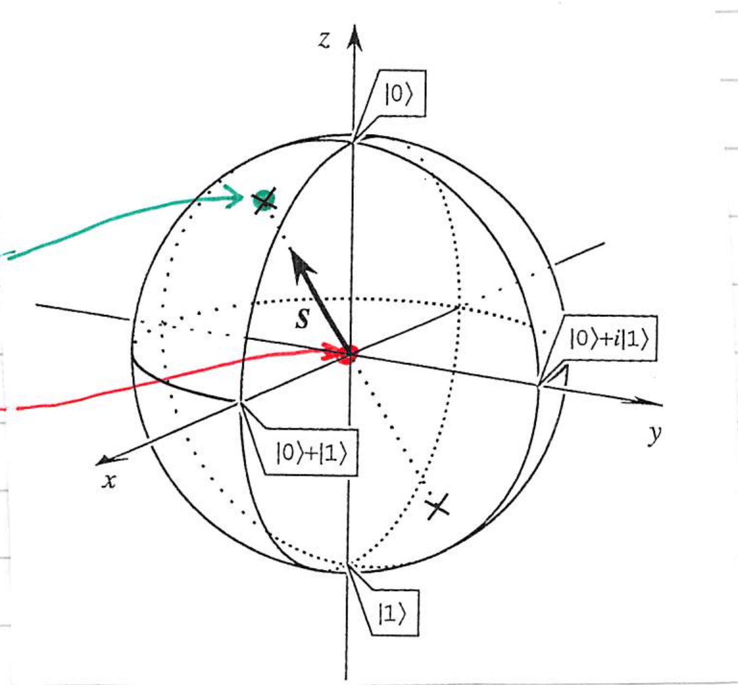
and $\vec{s} \in \mathbb{R}^3$ with $|\vec{s}| \leq 1$ called <u>polarization vector</u>

obviously $s_i = \mathrm{Tr}\{\rho\,\sigma_i\}$; diagonalizing (13) yields

$$(14) \qquad \rho = \frac{1}{2}\left(1+|s|\right)|\uparrow_s\rangle\langle\uparrow_s| + \frac{1}{2}\left(1-|s|\right)|\downarrow_s\rangle\langle\downarrow_s|$$

representation on the Bloch sphere

- pure states $|\vec{s}| = 1$
- max. mixed state $|\vec{s}| = 0$



4.2 quantum information transfer

There is a generalization of Shannons noiseless coding theorem to qubits

pure states: Schumacher theorem

(15) In order to encode (store) the quantum information of n copies of a pure state $\rho = |\psi\rangle\langle\psi|$ a Hilbert space $\mathcal{H}_0$ is required in the limit $n \to \infty$ with

$$\log(\dim \mathcal{H}_0) = n\, S_N(\rho)$$

thus to transfer n qubits each in state ρ over a lossless channel $n S_N(\rho)$ qubits need to be transferred

- example: Alice wants to send to Bob a qbit word of length 3

(16) $$|\psi\rangle = |\psi_1\rangle|\psi_2\rangle|\psi_3\rangle \qquad |\psi_i\rangle \in \left\{ \begin{matrix} |\uparrow_x\rangle \\ |\uparrow_z\rangle \end{matrix} \right.$$

can be done most efficiently using only 4 states

(17) $$\{|000\rangle, |100\rangle, |010\rangle, |001\rangle\}$$

instead of the $2^3 = 8$ possible combinations of $|\uparrow_x\rangle$ and $|\uparrow_z\rangle$

one can easily calculate

$$|\langle 000|\psi\rangle|^2 = \left|\cos^2\left(\frac{\pi}{8}\right)\right|^3 = 0.6219$$

(18)

$$|\langle 100|\psi\rangle|^2 = |\langle 010|\psi\rangle|^2 = |\langle 001|\psi\rangle|^2 = \left[\cos^2\left(\frac{\pi}{8}\right)\right]^2 \sin^2\frac{\pi}{8}$$
$$= 0.1067$$

i.e. for a random qbit word the probability to find it in the subspace spanned by (17) is

(19) $$p_{success} = 0.6219 + 3 \cdot 0.1067 = 0.9419$$

for $n \to \infty$ $\qquad p_{success} \to 1$

For mixed states the generalization is less trivial. Here we introduce an alphabet of orthogonal mixed states ϱ_j

(20) $$\mathrm{Tr}\{\hat{\varrho}_i \hat{\varrho}_j\} \sim \delta_{ij}$$

If then a general state is decomposed into ϱ_j

(21) $$\hat{\varrho} = \sum_j p_j \hat{\varrho}_j$$

$$S(\hat{\varrho}) = -\mathrm{Tr}\{\varrho \log \varrho\} = -\sum_j \mathrm{Tr}\{p_j \hat{\varrho}_j \log(p_j \hat{\varrho}_j)\}$$

(22) $$= \underbrace{-\sum_j p_j \log p_j}_{\text{classical information in } \{p_j\}} \underbrace{- \sum_j p_j \mathrm{Tr}\{\hat{\varrho}_j \log \hat{\varrho}_j\}}_{\text{from mixedness of alphabet}}$$

Holevo information

$$\chi(\rho) = S(\hat{\rho}) + \sum_j p_j \, \mathrm{Tr}\{\hat{\rho}_j \log \hat{\rho}_j\}$$
(23)
$$= S(\hat{\rho}) - \sum_j p_j \, S(\hat{\rho}_j)$$

Holevo conjecture

To transfer a n qubit-word of mixed states ρ_j which appear with probability p_j:

$$n \, \chi(\{p_j, \hat{\rho}_j\}) \le n \, S(\rho) \qquad n \to \infty$$

qubits are needed.

4.3 quantum error correction

many ideas of classical error correction can be transferred, however there are two specialities

(i) qubits have more than bit flip errors

(ii) the state of a qubit should not be measured during transfer

qubit errors

result from coupling of qubit $\{|0\rangle, |1\rangle\}$ to environment $\{|E\rangle\}$

- spin flip

$$(24)\qquad \begin{aligned} |0\rangle|E\rangle &\longrightarrow |1\rangle|E_{01}\rangle \\ |1\rangle|E\rangle &\longrightarrow |0\rangle|E_{10}\rangle \end{aligned}$$

- dephasing

$$(25)\qquad \begin{aligned} |0\rangle|E\rangle &\longrightarrow |0\rangle|E_{00}\rangle \\ |1\rangle|E\rangle &\longrightarrow |1\rangle|E_{11}\rangle \end{aligned}$$

in the course of interaction the environment states become more and more orthogonal

$$(26)\qquad \begin{aligned} \langle E_{01}(t)|E_{10}(t)\rangle &\xrightarrow{t\to\infty} 0 \\ \langle E_{00}(t)|E_{11}(t)\rangle &\longrightarrow 0 \end{aligned}$$

this yields to the following evolution of the reduced density matrix starting from $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\rho_0 = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \xrightarrow{\text{spin flip}} \begin{pmatrix} |\beta|^2 & \alpha^*\beta\langle E_{01}(t)|E_{10}(t)\rangle \\ \alpha\beta^*\langle E_{10}(t)|E_{01}(t)\rangle & |\alpha|^2 \end{pmatrix}$$

(27)

$$\xrightarrow{\text{dephasing}} \begin{pmatrix} |\alpha|^2 & \alpha\beta^*\langle E_{00}(t)|E_{11}(t)\rangle \\ \alpha^*\beta\langle E_{11}(t)|E_{00}(t)\rangle & |\beta|^2 \end{pmatrix}$$

in both cases non-diagonal terms decay

"decoherence"

in general

$$(28)\quad \begin{array}{l} |0\rangle|E\rangle \\ |1\rangle|E\rangle \end{array} \xrightarrow{U(t)} \begin{array}{l} |0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle \\ |0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle \end{array}$$

this can be written as:

$$(30)\quad (\alpha|0\rangle+\beta|1\rangle)|E\rangle \longrightarrow \begin{array}{l} (\alpha|0\rangle+\beta|1\rangle)|E_0\rangle \\ +(\alpha|1\rangle+\beta|0\rangle)|E_x\rangle \\ +(\alpha|0\rangle-\beta|1\rangle)|E_z\rangle \\ +(-\alpha|1\rangle+\beta|0\rangle)|E_y\rangle \end{array}$$

$$= (\hat{I}|\psi_0\rangle)|E_0\rangle + (\hat{X}|\psi_0\rangle)|E_x\rangle + (\hat{Y}|\psi_0\rangle)|E_y\rangle + (\hat{Z}|\psi_0\rangle)|E_z\rangle$$

where

$$(31)\quad \hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{Y} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

spin flip — both — dephasing

$$(32)\quad \hat{Y} = \hat{Z}\hat{X}$$

$\Rightarrow$ **error correcting code should correct in addition to spin flip X also dephasing Z and combination ZX**

3-qubit code corrects spin flip X

error operation

$$(33)\quad \hat{M} = (1-p)\hat{I} + p\hat{X}$$

this is just the classical repetition code $k=1, n=3, d=3$

$$|0\rangle \rightarrow |0,0,0\rangle \qquad |1\rangle \rightarrow |1,1,1\rangle \tag{34}$$

- how to create code without measurement of state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i.e. without knowing α, β ?

CNOT operation (unitary)

$$|\psi\rangle|\phi\rangle \xrightarrow{\text{CNOT}} |\psi\rangle|\tilde{\phi}\rangle \tag{35}$$

leaves $|\psi\rangle$ unchanged

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \hat{X} \tag{36}$$

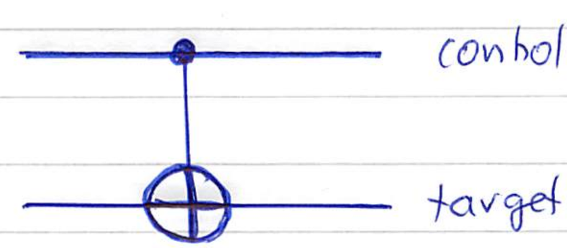
projector to basis of control bit

operation on target bit

if $|x\rangle, |y\rangle \in \{|0\rangle, |1\rangle\}$

$$\text{CNOT}\,|x\rangle|y\rangle = \underbrace{|x\rangle\,|y + x \bmod 2\rangle}_{\text{entanglement of control + target}} \tag{37}$$

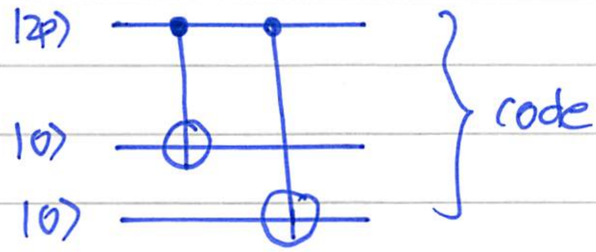
$$\begin{aligned} |00\rangle &\longrightarrow |00\rangle \\ |01\rangle &\longrightarrow |01\rangle \\ |10\rangle &\longrightarrow |11\rangle \\ |11\rangle &\longrightarrow |10\rangle \end{aligned} \tag{38}$$



(i) encoding in 3-qubit code

(39) $$(\alpha|0\rangle + \beta|1\rangle)\,|0\rangle|0\rangle \longrightarrow \alpha|000\rangle + \beta|111\rangle$$

$2 \times$ CNOT



(ii) interaction with environment

$\alpha|000\rangle + \beta|111\rangle$	probability
$\alpha|000\rangle + \beta|111\rangle$	$(1-p)^3$
(40) $\alpha|100\rangle + \beta|011\rangle$	$p(1-p)^2$
$\alpha|010\rangle + \beta|101\rangle$	$p(1-p)^2$
$\alpha|001\rangle + \beta|110\rangle$	$p(1-p)^2$
other	$\mathcal{O}(p^2)$ small !

(iii) error detection $k=1, n=3, d=3$

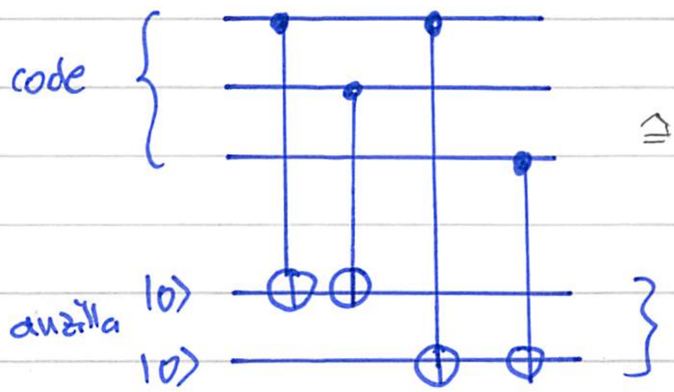
$\Rightarrow$ parity check matrix $n-k=2 \times n=3$

(41) $$\underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

important property

$$\underline{\underline{H}}\begin{pmatrix}0\\0\\0\end{pmatrix} = \underline{\underline{H}}\begin{pmatrix}1\\1\\1\end{pmatrix} = 0$$

this can be used to detect error without measurement of code!



$$\hat{=} \quad H^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

measurement of error syndrom

X error in qubit j: $\hat{X}_j$

e.g. $\hat{X}_2 |x,0,y\rangle = |x,1,y\rangle = |x, 0\oplus 1, y\rangle$

$\hat{X}_2 |x,1,y\rangle = |x,0,y\rangle = |x, 1\oplus 1, y\rangle$

i.e in general

(42) $$\hat{X}_2 |x,y,z\rangle = |x, y\oplus 1, z\rangle = |xyz \oplus \underbrace{010}\rangle$$

$\Rightarrow$ classical error

$$\underline{\underline{H}} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \underline{\underline{H}} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \underline{\underline{H}} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

all errors in the code (40) up to 1 bit flip can be detected

$$\Rightarrow \quad \begin{array}{l|l|} (\alpha|000\rangle + \beta|111\rangle) & |00\rangle \\ (\alpha|100\rangle + \beta|011\rangle) & |11\rangle \\ (\alpha|010\rangle + \beta|101\rangle) & |10\rangle \\ (\alpha|001\rangle + \beta|110\rangle) & |01\rangle \end{array}$$

error syndrom

(iv) error correction

$$\begin{aligned}
\text{if } |00\rangle &\Rightarrow \hat{I}_1 \hat{I}_2 \hat{I}_3 \\
|10\rangle &\Rightarrow \hat{I}_1 \hat{X}_2 \hat{I}_3 \\
|01\rangle &\Rightarrow \hat{I}_1 \hat{I}_2 \hat{X}_3 \\
|11\rangle &\Rightarrow \hat{X}_1 \hat{I}_1 \hat{I}_2
\end{aligned}$$

Hamming inequality

(43) a linear code for k qubits which can correct 3 independent errors ($\hat{X}, \hat{Y}, \hat{Z}$) in η qubits has to have at least n qubits

$$2^k \sum_{i=0}^{\eta} 3^i \binom{n}{i} \leq 2^n$$

the smallest code that can correct all possible errors in <u>one</u> qubit is therefore $(k=1, \eta=1)$

(44) $$2 \cdot 3 \binom{n}{1} = 6n \leq 2^n$$

$\Rightarrow$ $n = 5$ or larger

such a code can be constructed, it is however not very handy a very important class of codes are the so-called stabilizer codes

they make use of the fact that the possible errors forms a group

$$\pm \{I, X, Y, Z\}$$

one can show that "good" stabilizer codes exist were good means

$[n, k, d = 2t+1]$ $\qquad R = \frac{k}{n} \longrightarrow$ finite

$\qquad p = \frac{t}{n} \longrightarrow$ finite

(max. error probability per qubit)

one can show that good codes exist for $\boxed{p < 0.0946}$

remark: All of the discussion assumes that the coding, error detection and error correction steps themselves do not contribute errors. To include the latter one has to add additional encodings $\Rightarrow$ fault tolerant coding and error correction

one can show that this is possible if $\boxed{p \lesssim 1-10^{-4}}$ tough!