Fundamentos de teoria quântica

Aula 6: Primitivas da informação quântica

Rafael Rabelo – rabelo@ifi.unicamp.br

Departamento de Física da Matéria Condensada
Instituto de Física "Gleb Wataghin"
Universidade Estadual de Campinas

Função informação

Seja X uma variável aleatória que assume valores em um alfabeto $\mathcal{A}_X = \{x\}$, cada valor x com probabilidade $p(x)$. Definimos a *função informação* $I(x)$ de forma que:

- $I(x) = I(p(x))$;
- $I(p(x))$ seja suave com respeito a $p(x)$;
- $I(p(x).q(y)) = I(p(x)) + I(q(y))$.

A função I é única (a menos de uma transformação afim):

$$I(p(x)) = -\log_2 (p(x)) .$$

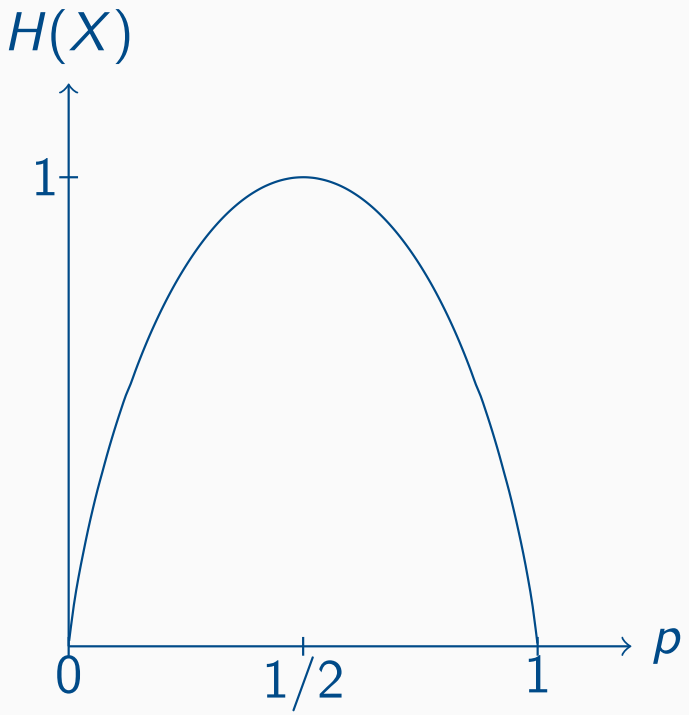
Entropia de Shannon

A *entropia de Shannon* de uma variável aleatória X, que assume valores no alfabeto $\mathcal{A}_X = \{x\}$, é o valor médio da informação de seus possíveis resultados:

$$H(X) = -\sum_{x \in \mathcal{A}_X} p(x) \log\left(p(x)\right).$$

Entropia de Shannon de um bit

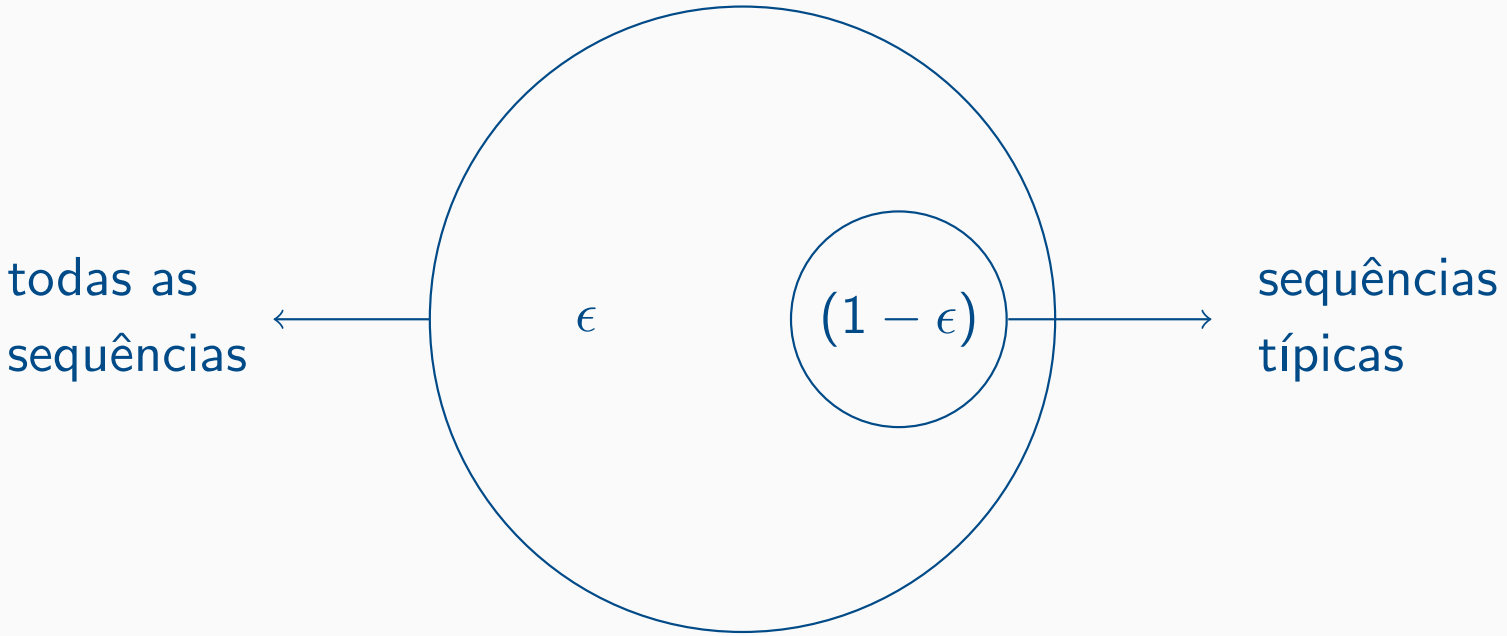
$$H(X) = -p \log p - (1-p) \log(1-p).$$



Compressão de dados

- Suponha que Alice joga uma moeda n vezes, e deseja comunicar os resultados obtidos a Bob.
- Ambos sabem que a moeda tem probabilidade p de se obter 'cara', e probabilidade $(1-p)$ de se obter 'coroa'.
- No fim de n jogadas, se n é grande, a *lei dos grandes números* nos garante que existe uma grande probabilidade de Alice obter uma sequência com np caras e $n(1-p)$ coroas. Sequências com essas características são ditas *típicas*.

Probabilidade das sequências típicas



Número de sequências típicas

Qual é o número N de sequências de n símbolos nas quais np são 'cara' e $n(1-p)$ são 'coroa'?

$$
\begin{aligned}
N = \binom{n}{np} &= \frac{n!}{(np)!\,[n(1-p)]!} \\
&\approx \frac{n^n}{(np)^{np}\,[n(1-p)]^{[n(1-p)]}} \qquad \text{[aprox. de Stirling]} \\
&= \frac{1}{p^{np}\,(1-p)^{n(1-p)}} \\
&= \frac{1}{2^{n[p\log(p)+(1-p)\log(1-p)]}} \\
&= 2^{nH(X)}.
\end{aligned}
$$

Teorema da compressão de dados

Suponha uma fonte associada a uma variável aleatória A, que produz bit a com probabilidade $p(a)$. Considere uma mensagem com n bits $(a_1, \ldots, a_n)$, *i. i. d.*, advindos desta fonte. Esta mensagem pode ser codificada em uma mensagem de m bits $(x_1, \ldots, x_m)$, e, posteriormente, decodificada, sem a introdução de erros,

$$(a_1, \ldots, a_n) \xrightarrow{C} (x_1, \ldots, x_m) \xrightarrow{D} (a_1, \ldots, a_n),$$

somente se $m \geq nH(A)$, no limite assintótico $n \to \infty$.

Funções entrópicas

- Entropia conjunta:

$$H(X, Y) = -\sum_{x,y} p(x, y) \log\left(p(x, y)\right).$$

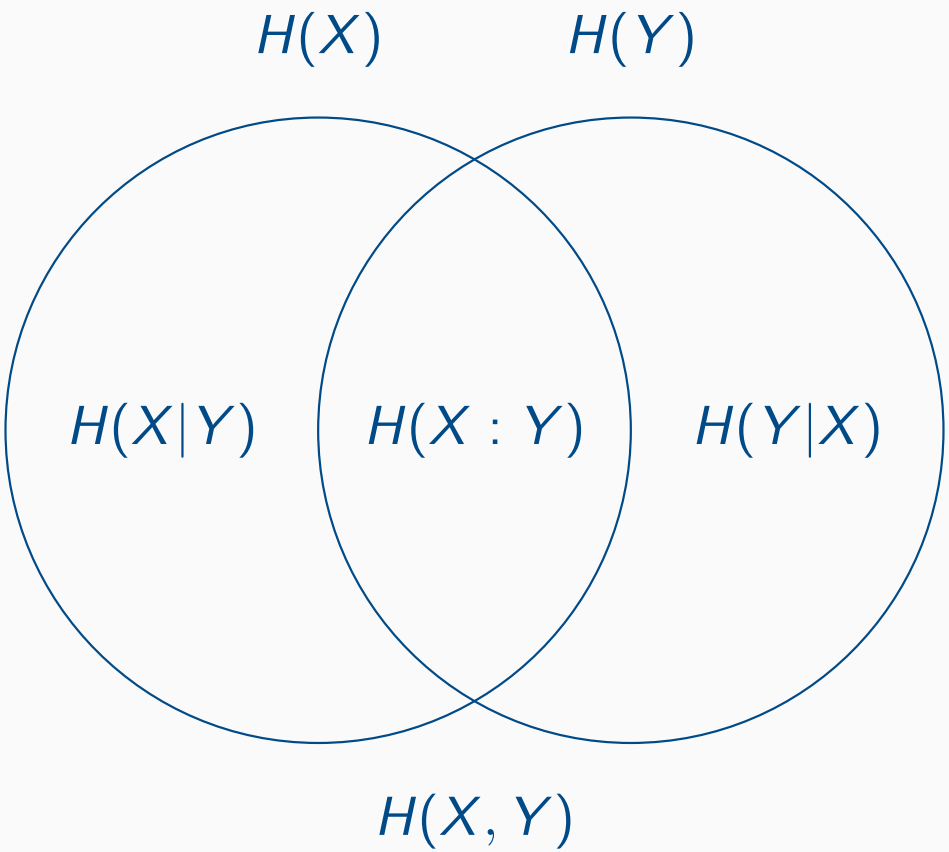
- Entropia condicional:

$$H(X|Y) = H(X, Y) - H(Y).$$

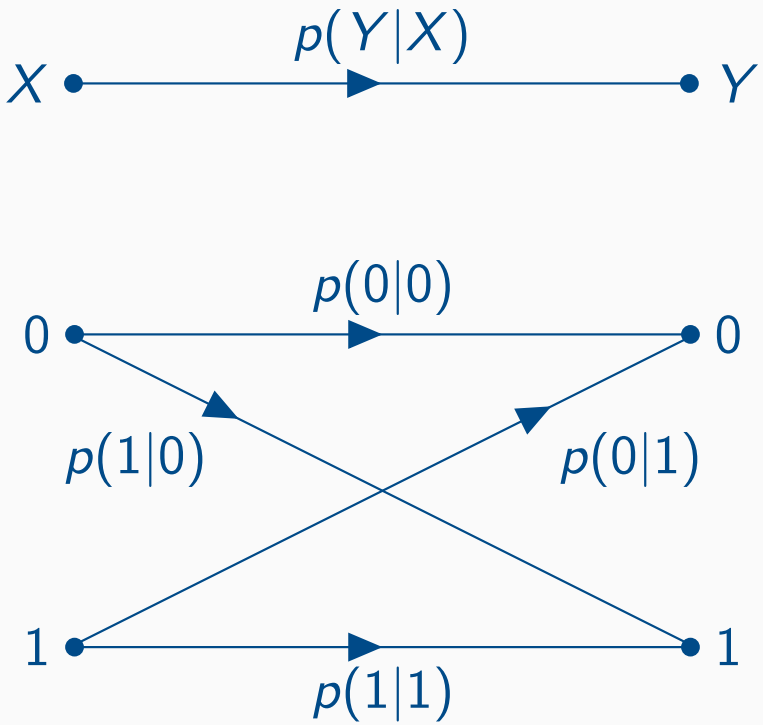
- Informação mútua:

$$\begin{aligned} H(X : Y) &= H(X) + H(Y) - H(X, Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$$

Diagrama



Canal de comunicação ruidoso



Capacidade do canal

A capacidade C de um canal ruidoso é definida como

$$C = \sup_{p(X)} H(X : Y).$$

O que motiva esta definição:

- O número aproximado de sequências típicas produzidas pela fonte de Alice é $N = 2^{nH(x)}$;
- para cada sequência observada por Bob, haverá, em média, $2^{nH(X|Y)}$ sequências que as podem ter gerado;
- assim, o número de sequências não redundantes é $2^{n[H(X)-H(X|Y)]} = 2^{nH(X:Y)}$.

Teorema de Shannon

Seja R a taxa média de transmissão de informação através de um canal ruidoso. Se $R < C$, então, para todo $\epsilon > 0$, existe um código de tamanho n cuja máxima probabilidade de erro é ϵ, para n grande o suficiente.

Teorema da não-clonagem

Não existe nenhum mapa M completamente positivo e traço-preservante capaz de clonar perfeitamente todo estado quântico $|\psi\rangle$:

$$\nexists\, M : M\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle\,,\ \forall\ |\psi\rangle \in \mathcal{H}.$$

Teorema da não-clonagem: prova para unitárias

- Suponha que exista U que clone corretamente dois estados $|\psi\rangle$ e $|\phi\rangle$:

$$U\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle$$
$$U\left(|\phi\rangle\,|0\rangle\right) = |\phi\rangle\,|\phi\rangle\,.$$

- Tomando o produto interno entre as duas equações, obtemos

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2\,.$$

- Para que satisfaçam a equação acima, $|\psi\rangle$ e $|\phi\rangle$ devem necessariamente ser ortogonais.

Teorema da dilatação de Stinespring

Seja $M : \mathcal{D}_{\mathcal{H}_A} \to \mathcal{D}_{\mathcal{H}_A}$ um mapa completamente positivo e traço-preservante, atuando sobre os operadores densidade de um espaço de Hilbert $\mathcal{H}_A$. Então existe um espaço de Hilbert $\mathcal{H}_B$ e uma operação unitária U em $\mathcal{H}_A \otimes \mathcal{H}_B$ tal que

$$M[\rho] = \mathrm{Tr}_B \left(U \left(\rho \otimes |0\rangle\langle 0| \right) U^\dagger \right),$$

para todo ρ.

Teorema da não-clonagem: prova para mapas gerais

- O teorema de dilatação de Stinespring nos diz que qualquer mapa M pode ser implementado por meio de uma unitária e um sistema auxiliar.
- Suponha, pois, que exista U que clone corretamente dois estados $|\psi\rangle$ e $|\phi\rangle$:

$$U\left(|\psi\rangle|0\rangle|0\rangle\right) = |\psi\rangle|\psi\rangle|\alpha\rangle$$
$$U\left(|\phi\rangle|0\rangle|0\rangle\right) = |\phi\rangle|\phi\rangle|\beta\rangle\,.$$

- Por linearidade,

$$\begin{aligned} U\left[\left(|\psi\rangle + |\phi\rangle\right)|0\rangle|0\rangle\right] &= |\psi\rangle|\psi\rangle|\alpha\rangle + |\phi\rangle|\phi\rangle|\beta\rangle \\ &\neq \left(|\psi\rangle + |\phi\rangle\right)\left(|\psi\rangle + |\phi\rangle\right)|\delta\rangle\,. \end{aligned}$$

Fidelidade

Uma importante figura de mérito para se avaliar a semelhança entre dois estados quânticos é a *fidelidade*. Dados dois operadores densidade ρ e σ atuando no mesmo espaço de Hilbert, a fidelidade $F(\rho, \sigma)$ entre eles é definida como

$$F(\rho, \sigma) = \left[\mathrm{Tr} \left(\sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right) \right]^2 .$$

Se $\rho = |\psi\rangle\langle\psi|$ e $\sigma = |\phi\rangle\langle\phi|$,

$$F(\rho, \sigma) = |\langle\psi|\phi\rangle|^2 .$$

Clonagem trivial

- Seja $|\psi\rangle$ o estado do qubit que se quer clonar. Prepare um segundo qubit no estado $|0\rangle$, e, com probabilidade $1/2$, troque os qubits.
- O estado da cópia após o protocolo é

$$\rho = \frac{1}{2}\left(|\psi\rangle\langle\psi| + |0\rangle\langle 0|\right).$$

- A fidelidade média da cópia, sobre todos os possíveis $|\psi\rangle$, é

$$\begin{aligned} F &= \frac{1}{2}\times 1 + \frac{1}{2}\times\left(\frac{1}{4\pi}\int_0^{2\pi} d\phi \int_{-1}^{1} d\left(\cos\theta\right)\left|\langle\phi|0\rangle\right|^2\right) \\ &= \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2}\int_{-1}^{1} d\left(\cos\theta\right)\frac{1+\cos\theta}{2}\right) = \frac{3}{4}. \end{aligned}$$

O protocolo de Bužec-Hillery

A *máquina de Bužec-Hillery* é uma clonadora universal, simétrica e ótima de $1 \to 2$ qubits, que se utiliza de 3 qubits na sua operação. Sua atuação nos estados da base é

$$|0\rangle|0\rangle|0\rangle \to \sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}(|0\rangle|1\rangle + |1\rangle|0\rangle)|1\rangle\,;$$

$$|1\rangle|0\rangle|0\rangle \to \sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}(|1\rangle|0\rangle + |0\rangle|1\rangle)|0\rangle\,.$$

O protocolo de Bužec-Hillery

Sua atuação em um estado geral é

$$|\psi\rangle\,|0\rangle\,|0\rangle \to \sqrt{\frac{2}{3}}\,|\psi\rangle\,|\psi\rangle\,|\psi^*\rangle + \sqrt{\frac{1}{6}}\,(|\psi\rangle\,|\psi_\perp\rangle + |\psi_\perp\rangle\,|\psi\rangle)\,|\psi_\perp^*\rangle\,,$$

onde $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, $|\psi^*\rangle = \alpha^*\,|0\rangle + \beta^*\,|1\rangle$ e $|\psi_\perp\rangle$ é o estado ortogonal a $|\psi\rangle$.

Discriminação não-ambígua de dois estados puros

- Suponha que Bob recebe um qubit em um de dois estados puros, $|\psi\rangle$ e $|\phi\rangle$, sendo $|\langle\psi|\phi\rangle| = S$ e deseja discriminá-los de forma não-ambígua.
- Sejam $|\psi_\perp\rangle$ e $|\phi_\perp\rangle$ os estados ortogonais a $|\psi\rangle$ e $|\phi\rangle$, respectivamente.
- Suponha que Bob realiza o POVM

$$\{\eta\,|\psi_\perp\rangle\langle\psi_\perp|\,, \eta\,|\phi_\perp\rangle\langle\phi_\perp|\,, \mathbb{1} - \eta\,|\psi_\perp\rangle\langle\psi_\perp| - \eta\,|\phi_\perp\rangle\langle\phi_\perp|\}\,,$$

  onde $\eta = 1/\left(1+S\right)$.
- A obtenção do primeiro resultado implica que o estado era $|\phi\rangle$;
- a obtenção do segundo resultado implica que o estado era $|\psi\rangle$;
- o terceiro resultado é inconclusivo, e ocorre com probabilidade S.

Estados de Bell e matrizes de Pauli

Os estados de Bell são:

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right),$$
$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right).$$

É possível modificar os quatro estados de Bell operando localmente sobre eles com as matrizes de Pauli. Por exemplo:

$$(\sigma_x \otimes \mathbb{1})\left|\phi^{+}\right\rangle = \left|\psi^{+}\right\rangle;$$
$$(\sigma_y \otimes \mathbb{1})\left|\phi^{+}\right\rangle = \left|\psi^{-}\right\rangle;$$
$$(\sigma_z \otimes \mathbb{1})\left|\phi^{+}\right\rangle = \left|\phi^{-}\right\rangle.$$

Codificação superdensa

- Suponha que Alice e Bob compartilham um sistema de dois qubits no estado $|\phi^+\rangle$.
- Alice codifica dois bit no sistema, operando somente em seu qubit:

$$\begin{aligned}
00: &\quad (\mathbb{1}\otimes\mathbb{1})\,|\phi^+\rangle = |\phi^+\rangle\,;\\
01: &\quad (\sigma_x\otimes\mathbb{1})\,|\phi^+\rangle = |\psi^+\rangle\,;\\
10: &\quad (\sigma_y\otimes\mathbb{1})\,|\phi^+\rangle = |\psi^-\rangle\,;\\
11: &\quad (\sigma_z\otimes\mathbb{1})\,|\phi^+\rangle = |\phi^-\rangle\,.
\end{aligned}$$

- Alice envia seu qubit a Bob.
- Bob realiza uma medição projetiva sobre o par de qubits na base de Bell, e é capaz de distinguir perfeitamente entre os quatro estados.
- Bob adquire dois bits de informação, tendo recebido um único qubit de Alice.

Teleportação quântica

- Alice deseja enviar um qubit em um estado arbitrário $|\psi\rangle$ para Bob.
- Suponha que Alice e Bob compartilham um outro sistema de dois qubits, no estado de Bell $|\phi^+\rangle$.
- Alice realiza sobre seus dois qubits uma medição projetiva na base dos estados de Bell.
- Alice informa a Bob o resultado da medição (2 bits).
- Baseado na informação recebida, Bob opera sobre seu qubit, que termina no estado $|\psi\rangle$.

Teleportação quântica

O estado do sistema anterior à medição de Alice é:

$$
\begin{aligned}
|\psi\rangle \left|\phi^{+}\right\rangle &= (\alpha |0\rangle + \beta |1\rangle)(|00\rangle + |11\rangle)/\sqrt{2} \\
&= \{[\alpha |00\rangle + \beta |10\rangle]|0\rangle + [\alpha |01\rangle + \beta |11\rangle]|1\rangle\}/\sqrt{2} \\
&= \{[\alpha (\left|\phi^{+}\right\rangle + \left|\phi^{-}\right\rangle) + \beta (\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle)]|0\rangle + \\
&\quad [\alpha (\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle) + \beta (\left|\phi^{+}\right\rangle - \left|\phi^{-}\right\rangle)]|1\rangle\}/2 \\
&= \{\left|\phi^{+}\right\rangle (\alpha |0\rangle + \beta |1\rangle) + \left|\phi^{-}\right\rangle (\alpha |0\rangle - \beta |1\rangle) + \\
&\quad \left|\psi^{+}\right\rangle (\beta |0\rangle + \alpha |1\rangle) - \left|\psi^{-}\right\rangle (\beta |0\rangle - \alpha |1\rangle)\}/2.
\end{aligned}
$$

Teleportação quântica

- O estado do sistema anterior à medição de Alice é:

$$|\psi\rangle\left|\phi^{+}\right\rangle = \left\{\left|\phi^{+}\right\rangle(\alpha|0\rangle + \beta|1\rangle) + \left|\phi^{-}\right\rangle(\alpha|0\rangle - \beta|1\rangle) + \left|\psi^{+}\right\rangle(\beta|0\rangle + \alpha|1\rangle) - \left|\psi^{-}\right\rangle(\beta|0\rangle - \alpha|1\rangle)\right\}/2.$$

- Após a medição, o estado do qubit de Bob dependerá do resultado obtido por Alice:

$$\begin{aligned}
|\phi^{+}\rangle: &\quad \alpha|0\rangle + \beta|1\rangle &&= |\psi\rangle\,;\\
|\phi^{-}\rangle: &\quad \alpha|0\rangle - \beta|1\rangle &&= \sigma_z|\psi\rangle\,;\\
|\psi^{+}\rangle: &\quad \beta|0\rangle + \alpha|1\rangle &&= \sigma_x|\psi\rangle\,;\\
|\psi^{-}\rangle: &\quad \beta|0\rangle - \alpha|1\rangle &&= \sigma_y|\psi\rangle\,.
\end{aligned}$$

- Basta, portanto, que Bob opere em seu qubit com a matriz de Pauli adequada, que ele obtém o estado $|\psi\rangle$.

Tomografia de estados quânticos

O operador densidade ρ de um sistema quântico de dimensão d tem $d^2 - 1$ parâmetros reais.

Tomografia é o processo de se estimar os parâmetros de um estado a partir dos resultados de medições realizadas sobre várias cópias do sistema.

Tomografia de um qubit com MPs

O estado de um qubit pode ser escrito como:

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{v}.\vec{\sigma}\right) = \frac{1}{2}\begin{pmatrix} 1+v_z & v_x - iv_y \\ v_x + iv_y & 1-v_z \end{pmatrix}.$$

Realizando-se as medições dos observáveis σ_x, σ_y e σ_z:

$$\langle\sigma_x\rangle = v_x, \quad \langle\sigma_y\rangle = v_y, \quad \langle\sigma_z\rangle = v_z.$$

Tomografia de um qubit com POVMs

Um POVM x com operardores $\left\{E_{a|x}\right\}$ é dito informacionalmente completo (IC) se qualquer estado ρ pode ser escrito como combinação linear dos elementos do POVM:

$$\rho = \sum_{a} \alpha_a E_{a|x}.$$

Um IC-POVM deve conter pelo menos $d^2 - 1$ elementos linearmente independentes.

Entropia de von Neumann

A entropia de von Neumann de um sistema quântico no estado ρ é definida como:

$$\begin{aligned} S(\rho) &= -\mathrm{Tr}\left(\rho \log\left(\rho\right)\right) \\ &= -\sum_i \lambda_i \log\left(\lambda_i\right), \end{aligned}$$

onde λ_i são os autovalores de ρ.

Funções entrópicas

- Entropia conjunta:

$$S(\rho_{AB}) = -\mathrm{Tr}\left(\rho_{AB}\log\left(\rho_{AB}\right)\right).$$

- Entropia condicional

$$S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_B).$$

- Informação mútua

$$S(\rho_A : \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}).$$

Codificação com sistemas quânticos: cota de Holevo

- Suponha que Alice prepare um sistema quântico em um dos estados ρ_a, com probabilidade $p(a)$, com $a = 1, \ldots, k$.
- Bob recebe o sistema e realiza sobre ele um POVM $\{E_b\}_{b=1}^{m}$, na intenção de aprender o valor de a.
- A cota de Holevo é uma cota superior na informação acessível a Bob:

$$H(A:B) \leq S(\rho) - \sum_a p(a) S(\rho_a),$$

onde $\rho = \sum_a p(a)\rho_a$. A cota é saturada somente se os estados ρ_a são mutuamente comutativos

Teorema da codificação sem perdas de Schumacher

Suponha uma fonte que produz estados $|\psi_a\rangle \in \mathcal{H}$, com probabilidade $p(a)$, com $a = 1, \ldots, k$. A fonte é representada pelo estado misto $\rho = \sum_a p(a) |\psi_a\rangle\langle\psi_a|$. Considere n cópias de sistemas quânticos *i. i. d.*, advindos desta fonte. Elas podem ser codificadas em um sistema de dimensão m, e, posteriormente, decodificados, sem a introdução de erros,

$$\rho^{\otimes n} \xrightarrow{C} \sigma \xrightarrow{D} \rho^{\otimes n},$$

somente se $m \geq 2^{nS(\rho)}$, no limite assintótico $n \to \infty$.

Estados simétricos

Seja $\rho^{(n)}$ um operador densidade atuando em $\mathcal{H}^{\otimes n}$. O estado $\rho^{(n)}$ é dito *simétrico* se é invariante sob quaisquer permutações dos subsistemas.

Estados trocáveis

Seja $\rho^{(n)}$ um operador densidade atuando em $\mathcal{H}^{\otimes n}$. O estado $\rho^{(n)}$ é dito *trocável* se é simétrico e se, para todo $m > 0$, existe um estado simétrico $\rho^{(n+m)}$ atuando em $\mathcal{H}^{\otimes (n+m)}$ tal que o operador densidade de quaisquer n subsistemas é $\rho^{(n)}$.

Teorema de de Finetti quântico

Seja $\rho^{(n)}$ um operador densidade trocável atuando em $\mathcal{H}^{\otimes n}$. Então, $\rho^{(n)}$ pode ser escrito unicamente na forma

$$\rho^{(n)} = \int_{\mathcal{D}_{\mathcal{H}}} p\left(\rho\right) \rho^{\otimes n} d\rho,$$

onde $p\left(\rho\right)$ é uma distribuição de probabilidades normalizada no espaço $\mathcal{D}_{\mathcal{H}}$ de operadores densidade atuando sobre $\mathcal{H}$.