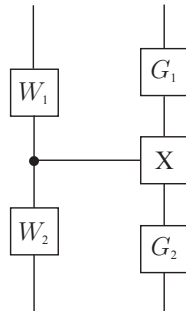


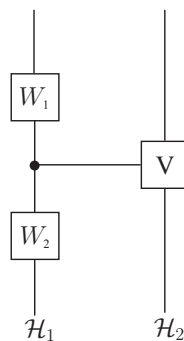
## 5 Análise dos Traços Parciais

Todo unitário  $U$  pode ser arbitrariamente bem aproximado pela composição de operadores CNOT e operadores unitários unipartidos (ou seja, aqueles que agem sobre um único fator tensorial). Nesta tese, optamos por trabalhar com operações não-locais bastante simples: a composição de um único operador CNOT com unitários unipartidos. Além da vantagem óbvia, que é a realização do experimento em laboratório de forma mais fácil, mostraremos adiante que tal escolha satisfaz nosso propósito de distinção ótima de estados quânticos não-ortogonais. Um diagrama representando a situação geral a ser considerada é o seguinte:

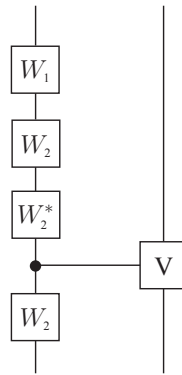


onde  $W_1$ ,  $W_2$ ,  $G_1$  e  $G_2$  são operadores unitários unipartidos, e  $X$  é tal que  $X|0\rangle = |1\rangle$  e  $X|1\rangle = |0\rangle$  (deve-se lembrar que CNOT's nada mais são do que operadores controle- $X$ , como representado acima).

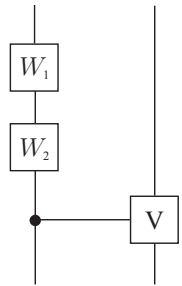
Uma primeira simplificação óbvia a ser feita é utilizarmos um operador controle- $V$ , onde  $V = G_1 X G_2$ , e nosso diagrama passa a ser o seguinte:



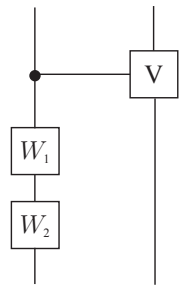
o qual é igual a



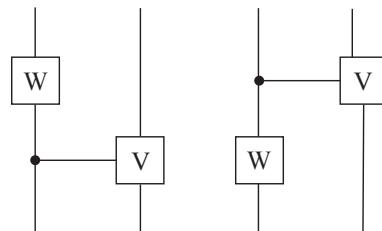
Após uma mudança de base em  $\mathcal{H}_1$ , obtemos:



Analogamente, poderíamos considerar outra mudança de base ainda no mesmo sistema, e então teríamos:



Se denotarmos  $W$  como a composição dos operadores  $W_1$  e  $W_2$ , os dois casos que de fato devemos estudar são:



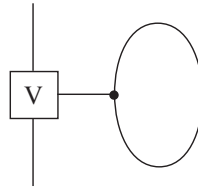
os quais são obviamente equivalentes, pois estão relacionados por uma mudança de base.

Por enquanto vamos considerar casos ainda mais simples, onde o operador  $W$  é a identidade. Ao final deste capítulo justificaremos tal simplificação.

Para suprir a eventual necessidade de ajuste na aparelhagem durante a realização empírica dos experimentos que propomos, consideraremos também que operadores *Swap* podem agir sobre os sistemas. Existem quatro maneiras de combinar *Swaps* (que são representados por  $S$ ) e um operador  $U$  tipo controle- $V$ , onde  $V$  é um unitário, e cada uma delas dá origem a um diagrama diferente de traço parcial. Em todos os quatro casos, nossos objetivos são encontrar o conjunto de matrizes  $V$  que distiguem dois vetores  $\varphi_1$  e  $\varphi_2$  não-ortogonais entre si, e verificar se existe  $V$  unitária tal que para quaisquer pares de vetores a probabilidade de distinção entre eles é ótima. No que se segue, usaremos o símbolo  $\stackrel{f}{=}$  para dizer que dois objetos são iguais a menos de um número complexo unimodular, isto é, a menos de uma *fase*.

**5.1**  
**Diagrama T.I**

O primeiro diagrama a ser considerado é:



E temos que

$$\text{Tr}_2(U) = I + V . \tag{5-1}$$

Nosso problema é distinguir entre os vetores  $\varphi_1$  e  $\varphi_2$ . Como o traço parcial de  $U$  é o operador calculado acima, isto é possível se e somente se

$$((I + V)\varphi_1, (I + V)\varphi_2) = 0 .$$

Seja  $W$  uma matriz unitária. Podemos reescrever esta equação como:

$$\begin{aligned} & (W(I + V)\varphi_1, W(I + V)\varphi_2) = 0 \\ \Leftrightarrow & (W(I + V)W^*W\varphi_1, W(I + V)W^*W\varphi_2) = 0 \\ \Leftrightarrow & ((I + WWVW^*)W\varphi_1, (I + WWVW^*)W\varphi_2) = 0 , \end{aligned}$$

ou seja,  $V$  distingue  $\varphi_1$  e  $\varphi_2$  se e somente se  $WWVW^*$  distingue  $W\varphi_1$  e  $W\varphi_2$ .

Ao tomarmos  $W = W_2 W_1$ , onde

$$W_1 \varphi_1 \stackrel{f}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad W_1 \varphi_2 \stackrel{f}{=} \begin{pmatrix} \epsilon \\ \sigma \sqrt{1 - \epsilon^2} \end{pmatrix}, \quad |\sigma| = 1$$

$$W_2 = \begin{pmatrix} 1 & 0 \\ 0 & \bar{\sigma} \end{pmatrix},$$

o problema de distinguir os vetores  $\varphi_1$  e  $\varphi_2$  transforma-se no problema de distinguir os vetores

$$W \varphi_1 \stackrel{f}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad W \varphi_2 \stackrel{f}{=} \begin{pmatrix} \epsilon \\ \sqrt{1 - \epsilon^2} \end{pmatrix}.$$

Vale ressaltar que, como  $W \varphi_2$  é um vetor normalizado, temos que  $0 \leq \epsilon \leq 1$ . Entretanto, se  $\epsilon = 0$ , então  $W \varphi_1$  e  $W \varphi_2$  são ortogonais entre si; se  $\epsilon = 1$ , então  $W \varphi_1 \stackrel{f}{=} W \varphi_2$ , ambos casos triviais. Assim, em todo nosso trabalho, vamos considerar  $0 < \epsilon < 1$ .

### 5.1.1

#### Distinção entre $\varphi_1$ e $\varphi_\epsilon$

Vamos agora estudar o conjunto de unitários  $V$  tais que  $I + V$  distinguem os vetores

$$\varphi_1 \stackrel{f}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad \varphi_\epsilon \stackrel{f}{=} \begin{pmatrix} \epsilon \\ \sqrt{1 - \epsilon^2} \end{pmatrix}.$$

Sabendo que a forma geral de uma matriz unitária 2 x 2 é

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta}\sigma & \bar{\alpha}\sigma \end{pmatrix},$$

onde  $|\sigma| = 1$  e  $|\alpha|^2 + |\beta|^2 = 1$ , a condição a ser satisfeita é a seguinte:

$$((I + V)\varphi_1, (I + V)\varphi_\epsilon) = 2\epsilon + 2\epsilon \operatorname{Re}(\alpha) + \sqrt{1 - \epsilon^2} \beta (1 - \bar{\sigma}) = 0. \quad (5-2)$$

Tomando  $\alpha = \eta \cos \theta$ ,  $\beta = \delta \sin \theta$ ,  $\sigma = e^{i\lambda}$ ,  $\eta = e^{i\tau}$ ,  $\delta = e^{i\xi}$ , podemos reescrevê-la como:

$$2\epsilon + 2\epsilon \cos \tau \cos \theta + \sqrt{1 - \epsilon^2} e^{i\xi} \sin \theta (1 - e^{-i\lambda}) = 0. \quad (5-3)$$

Vale ressaltar que sempre podemos supor  $0 \leq \theta \leq \pi/2$ , pois os demais quadrantes podem ser alcançados através de um ajuste conveniente das fases  $\tau$  e  $\xi$ . Voltando à equação, vamos igualar as partes imaginárias dos lados direito

e esquerdo:

$$\sqrt{1 - \epsilon^2} \sin \theta (\sin \xi - \sin(\xi - \lambda)) = 0.$$

Como  $0 < \epsilon < 1$ , então  $\sqrt{1 - \epsilon^2} \neq 0$ . Se  $\sin \theta = 0$ , teríamos  $\beta = 0$  e a condição de distinção seria escrita como  $2\epsilon + 2\epsilon \operatorname{Re}(\alpha) = 0$ . Ou seja,  $\operatorname{Re}(\alpha) = -1$ , e então  $V$  seria da forma  $\operatorname{diag}(-1, \sigma)$ . Este conjunto de matrizes  $V$  específicas é tal que  $(I + V)\varphi_1 = 0$ , e é topologicamente um círculo. Pela simetria do problema entre  $\varphi_1$  e  $\varphi_\epsilon$ , afirmamos que existe ainda um outro círculo de matrizes  $V$  tais que  $(I + V)\varphi_\epsilon = 0$ . Estes dois círculos interceptam-se no ponto  $V = -I$ . Uma outra opção para que equação acima seja satisfeita é a seguinte:

$$\sin \xi = \sin(\xi - \lambda),$$

cujas soluções independentes (a menos de múltiplos de  $2\pi$ ) são  $\lambda = 0$  e  $\lambda = 2\xi - \pi$ . Se  $\lambda = 0$ , então, por (5-2),  $1 - \bar{\sigma} = 0$ , e a condição de distinção seria  $2\epsilon + 2\epsilon \operatorname{Re}(\alpha) = 0$ , ou seja,  $\operatorname{Re}(\alpha) = -1$ . Teríamos então  $\alpha = -1$ , logo,  $\beta = 0$ , o que nos levaria a  $V = -I$ , exatamente o ponto de interseção dos dois círculos mencionados anteriormente. Vamos então assumir que  $\lambda = 2\xi - \pi$ . Voltando então à parte real da equação (5-3), temos que

$$C(V) = \epsilon + \epsilon \cos \tau \cos \theta + \sqrt{1 - \epsilon^2} \sin \theta \cos \xi = 0 \quad (5-4)$$

é a condição a ser satisfeita para que a matriz  $I + V$ , onde

$$V = \begin{pmatrix} e^{i\tau} \cos \theta & e^{i\xi} \sin \theta \\ e^{i\xi} \sin \theta & -e^{i(2\xi - \tau)} \cos \theta \end{pmatrix}, \quad (5-5)$$

seja capaz de distinguir os vetores  $\varphi_1$  e  $\varphi_\epsilon$ .

### 5.1.2

#### Distinção com Probabilidade Ótima

Nosso propósito nesta seção é verificar a existência de matrizes  $V$  do tipo (5-5) tais que  $I + V$  distinguem  $\varphi_1$  e  $\varphi_\epsilon$  com probabilidade ótima. Os valores ótimos da probabilidade de distinção de dois estados quânticos foram obtidos no artigo (19) de Jaeger e Shimony. Sejam  $r$  e  $1 - r$  as probabilidades de sortearmos um sistema preparado no estado  $\varphi_1$  e um sistema preparado no estado  $\varphi_\epsilon$ , respectivamente. Então afirmamos que:

$$P_{\text{best}} = \begin{cases} (1 - r)(1 - \epsilon^2) & \text{se } 0 \leq r \leq \frac{\epsilon^2}{1 + \epsilon^2} \\ 1 - 2\epsilon\sqrt{r(1 - r)} & \text{se } \frac{\epsilon^2}{1 + \epsilon^2} \leq r \leq \frac{1}{1 + \epsilon^2} \\ r(1 - \epsilon^2) & \text{se } \frac{1}{1 + \epsilon^2} \leq r \leq 1 \end{cases}$$

Na primeira faixa de  $r$ , o estado  $\varphi_1$  nunca é identificado com certeza; na terceira faixa, temos que o estado  $\varphi_\epsilon$  nunca é identificado com certeza; já na faixa intermediária, ambos os estados podem ser identificados com certeza. É nesta faixa em que vamos concentrar nossos estudos iniciais sobre probabilidade ótima de distinção de estados não-ortogonais.

Pelas equações (4-2) e (5-1), a probabilidade de distinguirmos corretamente entre  $\varphi_1$  e  $\varphi_\epsilon$  é dada por:

$$P = \frac{r}{4} \|(I + V)\varphi_1\|^2 + \frac{(1-r)}{4} \|(I + V)\varphi_\epsilon\|^2 .$$

Queremos verificar se existe  $V$  tal que a probabilidade de distinção é ótima, ou seja, tal que  $P = P_{\text{best}} = 1 - 2\epsilon\sqrt{r(1-r)}$ . Motivados por visualização gráfica das superfícies  $P - P_{\text{best}} = 0$  e aquela dada pela equação (5-4), assumiremos que o máximo da função  $P$  existe e tem um valor conhecido (a saber,  $P_{\text{best}}$ ). Introduziremos então uma variável  $\alpha$ , e nosso problema passa a ser resolver o seguinte sistema:

$$\begin{aligned} \frac{r}{4} \|(I + V)\varphi_1\|^2 &= \alpha P_{\text{best}} \\ \frac{(1-r)}{4} \|(I + V)\varphi_\epsilon\|^2 &= (1-\alpha)P_{\text{best}} \\ C(V) &= 0, \end{aligned}$$

onde  $V$  deve ser da forma (5-5). Consideremos agora as seguintes mudanças de variáveis:

$$\begin{aligned} \cos \tau &= x, & \sin \tau &= -\sqrt{1-x^2} \\ \cos \theta &= y, & \sin \theta &= \sqrt{1-y^2} \\ \cos \xi &= z, & \sin \xi &= -\sqrt{1-z^2} \end{aligned} .$$

Devemos ressaltar que os sinais de  $\sin \tau$ ,  $\sin \theta$  e  $\sin \xi$  foram escolhidos com base em visualização gráfica fornecida pelo Maple dos dois pontos de interseção  $(\tau, \theta, \xi)$  entre as superfícies  $P - P_{\text{best}} = 0$  e aquela dada pela equação (5-4). Um nos fornece  $V$ , e o outro,  $V^*$ .

O sistema pode então ser reescrito da seguinte forma:

$$rxy = 2\alpha Z - r \tag{5-6}$$

$$\begin{aligned} (1-r)(\epsilon^2 xy + 2\epsilon\sqrt{1-\epsilon^2}z\sqrt{1-y^2} - (1-\epsilon^2)y(x(2z^2-1) + \\ + 2\sqrt{1-x^2}z\sqrt{1-z^2})) = 2(1-\alpha)Z - (1-r) \end{aligned} \tag{5-7}$$

$$\epsilon(1+xy) + \sqrt{1-\epsilon^2}\sqrt{1-y^2}z = 0 \tag{5-8}$$

onde  $Z$  é uma variável substituindo  $P_{\text{best}}$  em (5-6)-(5-8). Para resolver tal

sistema, procedemos como segue: a partir da primeira equação, obtemos uma expressão para  $x$ , que foi substituída na terceira equação. Ainda nesta terceira, obtemos uma expressão para  $z$ , e os dois resultados foram então substituídos na segunda equação, nos fornecendo uma equação apenas em  $y$ . Esta equação foi separada em duas partes cujos quadrados foram igualados. Aplicamos a substituição  $y^2 = 1 - w$ , e então chegamos a uma equação polinomial, de grau 2, em  $w$ . Claramente, qualquer qualquer acréscimo a  $P_{\text{best}}$  faz com que a solução seja perdida. Como o sistema inteiro foi reduzido a uma equação polinomial de grau 2, este fato implica que tal polinômio deve ter raiz dupla (ou seja, que os pontos de interseção mencionados sejam pontos de tangência).

O discriminante do polinômio de grau 2 em  $w$  é o seguinte:

$$\Delta = 4096Z^6r^6\epsilon^4(r-1)^2\alpha^5(\alpha-1)(\alpha^2Z^2+\alpha Z(1-2r-Z)+r(r-\epsilon^2r+Z-1+\epsilon^2)),$$

onde  $Z$  é uma variável substituindo  $P_{\text{best}}$  no sistema. As raízes distintas do discriminante são:

$$\alpha = 0, 1, \frac{2r-1+Z}{2Z},$$

as quais foram simplificadas utilizando-se a equação  $Z^2 - 2Z + 1 - 4\epsilon^2r + 4\epsilon^2r^2 = 0$ . Antes de prosseguir, é importante ressaltar que, como  $\alpha$  é uma parcela da probabilidade, devemos ter  $0 \leq \alpha \leq 1$ . Se  $\alpha = 0$ , então pelo sistema (5-6)-(5-8) teríamos que  $\|(I+V)\varphi_1\|^2 = 0$ , ou seja,  $\varphi_1$  jamais seria observado. Analogamente, se  $\alpha = 1$ ,  $\varphi_\epsilon$  jamais seria observado. Em ambos os casos, estaríamos em uma faixa de  $r$  diferente da que está sendo considerada. Tomaremos então  $\alpha = \frac{2r-1+Z}{2Z}$ , e vamos agora verificar se  $0 < \alpha < 1$ . Seja  $p = \sqrt{(1-r)/r}$ . Como  $\epsilon^2/(1+\epsilon^2) < r < 1/(1+\epsilon^2)$ , segue que  $\epsilon < p < 1/\epsilon$ . Podemos reescrever  $\alpha$  como:

$$\alpha = \frac{1-p\epsilon}{(1-p\epsilon)+p(p-\epsilon)},$$

o qual é obviamente positivo e menor do que 1.

Substituindo este valor no polinômio e resolvendo-o para  $w$ , chegamos a uma raiz dupla, como esperado, escrita em função de  $r$  e  $\epsilon$ , e assim está determinado  $y$ , já que  $y^2 = 1 - w$ . Os valores de  $x$  e  $z$  são obtidos através de substituição do mesmo  $\alpha$ . Para fins de simplificação, aplicamos novamente a substituição  $r = 1/(1+p^2)$  e obtemos então o seguinte:

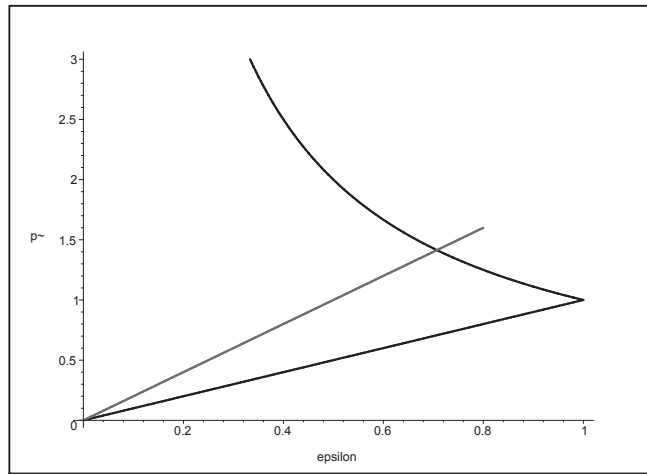
$$x = (1-2\epsilon p)\sqrt{\frac{1+p^2-2\epsilon p}{1+p^2+\epsilon p(8\epsilon p-4\epsilon^2p^2-6)}}$$

$$w = 1 - y^2 = \frac{4\epsilon p(\epsilon p - 1)^2}{1 + p^2 - 2\epsilon p}$$

$$z = \epsilon(\epsilon p - 1) \sqrt{\frac{1 + p^2 - 2\epsilon p}{\epsilon p(\epsilon p - 1)^2(1 - \epsilon^2)}}$$

Verificamos por Maple que estas expressões de fato satisfazem o sistema (5-6) – (5-8).

Devemos agora comprovar que estes valores de  $x$ ,  $y$  e  $z$  são de fato soluções do nosso problema, ou seja, que  $-1 < x < 1$ ,  $0 < y < 1$  e  $-1 < z < 0$  no interior da região de interesse, aquela limitada por  $0 < \epsilon < 1$  e  $\epsilon < p < 1/\epsilon$ :



Motivados pela figura acima, vamos considerar os segmentos de reta com inclinação  $\nu$  (onde  $1 < \nu < \infty$ ), cujas extremidades são a origem e um ponto na curva  $p = 1/\epsilon$  (e então  $0 < \epsilon < 1/\sqrt{\nu}$ ). Se as desigualdades forem satisfeitas para todo  $\nu$ , então concluímos que elas são verdadeiras em todo o interior da região em questão. Uma ferramenta será comum a todas as demonstrações a seguir: se uma expressão depende linearmente de  $\epsilon^2$ , e se, quando avaliada em  $\epsilon = 0$  e  $\epsilon = 1/\sqrt{\nu}$ , tiver valores ambos positivos ou ambos negativos, então afirmamos que tal expressão é positiva (ou, respectivamente, negativa) em  $0 < \epsilon < 1/\sqrt{\nu}$ .

As restrições a serem verificadas para  $x$  podem ser reescritas como  $0 < x^2 < 1$ . Sendo  $p = \nu\epsilon$ , temos que  $x^2$  é da forma  $\frac{A}{A+B}$ , onde  $A = (2\nu\epsilon^2 - 1)^2(2\nu\epsilon^2 - \nu^2\epsilon^2 - 1)$  e  $B = 4\epsilon^4\nu^2(\nu - 1)(\nu\epsilon^2 - 1)$ . Como  $A < 0$  e  $B < 0$ , então  $0 < x^2 < 1$ .

As restrições sobre  $y$  podem ser escritas em termos de  $w$  como  $0 < w < 1$ . Sendo  $p = \nu\epsilon$ , temos que  $w$  é da forma  $\frac{C}{C+D}$ , onde  $C = 4\epsilon^2\nu(\nu\epsilon^2 - 1)^2$  e  $B = 1 + \nu\epsilon^2(\nu + 8\epsilon^2\nu - 4\epsilon^4\nu^2 - 6)$ . Como  $A > 0$  e  $B > 0$ , segue que  $0 < w < 1$ .

Para  $z$ , devemos verificar inicialmente que o radicando do denominador é positivo. Substituindo  $p$  por  $\nu\epsilon$ , podemos escrevê-lo como  $E/F$ , onde  $E =$



$\nu\epsilon^2(\nu\epsilon^2 - 1)(1 - \epsilon^2)$  e  $F = 1 + \nu^2\epsilon^2 - 2\nu\epsilon^2$ . Como  $E > 0$  e  $F > 0$ , afirmamos que o radicando é positivo, como esperado. O numerador de  $z$  é  $(\nu\epsilon^2 - 1)\epsilon$ . Logo,  $z < 0$ . Para verificar a segunda desigualdade,  $z > -1$ , basta mostrar que  $z^2 < 1$ . Temos que  $z^2 = G/(G + H)$ , onde  $G = 2\nu\epsilon^2 - \nu^2\epsilon^2 - 1$  e  $H = \nu^2\epsilon^2 - \nu\epsilon^2 - \nu + 1$ . Como  $G < 0$  e  $H < 0$ , segue que  $z^2 < 1$ . Isto então conclui os estudos sobre probabilidade ótima de distinção dos estados  $\varphi_1$  e  $\varphi_\epsilon$  na faixa em que ambos podem ser identificados com certeza.

Vamos agora concentrar nossos estudos na primeira faixa de  $r$ , onde  $P_{\text{best}} = (1-r)(1-\epsilon^2)$ . Neste caso, sabemos que o estado  $\varphi_1$  nunca é observado, ou seja,  $\|(I + V)\varphi_1\|^2 = 0$ . Como  $V$  é da forma (5-5), a condição  $(I + V)\varphi_1 = 0$  é satisfeita se  $\sin\theta = 0$  e  $e^{i\tau} = -1$ , ou seja,  $\theta = 0$  (já que  $0 \leq \theta \leq \pi/2$ , como mencionado na seção (5.1.1)) e  $\tau = \pi$ . Logo,  $V$  deve ter o seguinte formato:

$$V = \begin{pmatrix} -1 & 0 \\ 0 & e^{2i\xi} \end{pmatrix}$$

A probabilidade de distinguirmos corretamente entre  $\varphi_1$  e  $\varphi_\epsilon$  é então dada por:

$$\begin{aligned} P &= \frac{(1-r)}{4} \|(I + V)\varphi_\epsilon\|^2 \\ &= \frac{(1-r)}{4} (1 - \epsilon^2) ((1 + \cos(2\xi))^2 + \sin^2(2\xi)) . \end{aligned}$$

Logo, temos que  $P$  é igual a  $P_{\text{best}} = (1-r)(1-\epsilon^2)$  se e somente se  $(1 + \cos(2\xi))^2 + \sin^2(2\xi) = 4$ . Como  $\pi/2 \leq \xi \leq 3\pi/2$ , segue que  $\xi = \pi$ . Assim,

$$V = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

é tal que os vetores  $\varphi_1$  e  $\varphi_\epsilon$  são distinguidos com probabilidade ótima.

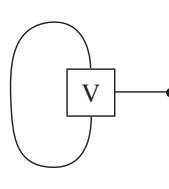
Para a terceira faixa de  $r$ , quando  $\varphi_\epsilon$  nunca é observado, a condição a ser satisfeita por  $V$  é  $(I + V)\varphi_\epsilon = 0$ , a qual é bem complicada. Entretanto, nosso problema tem uma simetria óbvia: distinguir entre  $\varphi_1$  e  $\varphi_\epsilon$  é o mesmo que distinguir entre  $\varphi_\epsilon$  e  $\varphi_1$ . Logo, a existência de uma matriz  $V$  tal que  $I + V$  distingue otimamente os dois vetores, na primeira faixa de  $r$ , garante a existência de uma matriz  $\tilde{V}$  tal que a probabilidade máxima também é alcançada, na terceira faixa de  $r$ .

Concluindo: para qualquer par de vetores  $\varphi_1$  e  $\varphi_\epsilon$  a serem distinguidos (sendo  $r$  e  $1 - r$  a probabilidade de sortearmos um sistema que tenha sido preparado no estado  $\varphi_1$  ou no estado  $\varphi_\epsilon$ , respectivamente), sempre existe uma

matriz  $V$  unitária tal que  $I + V$  distingue os dois vetores com probabilidade ótima.

## 5.2 Diagrama T.II

O próximo diagrama a ser considerado é o seguinte:



Temos que

$$L = \text{Tr}_2(SUS) = 2P_0 + \text{Tr}(V)P_1 = \begin{pmatrix} 2 & 0 \\ 0 & \text{Tr}(V) \end{pmatrix},$$

a qual já é uma matriz diagonal. Como um de seus autovalores é igual a 2, seguindo o critério estabelecido na seção (4.2), afirmamos que para cada matriz unitária  $V$  existem pares de vetores distinguíveis otimamente.

Vamos agora estabelecer condições para identificar os pares de vetores que podem ser distinguidos por este diagrama. Sejam  $\varphi_1 = (a, b)$  e  $\varphi_2 = (c, d)$ . Afirmamos que a condição para que tais vetores possam ser distinguidos é  $(L\varphi_1, L\varphi_2) = (\varphi_1, L^*L\varphi_2) = 0$ . Para este diagrama, temos que  $L^*L = 4P_0 + |\text{Tr}(V)|^2P_1$ . Seja  $\text{Tr}(V) = Re^{iA}$ . Como  $V$  é uma matriz unitária, temos que  $0 \leq R \leq 2$ . Podemos então escrever  $L^*L = 4P_0 + R^2P_1$ , e a condição de distinção é reescrita como  $4\bar{a}c + R^2\bar{b}d = 0$ . Sem perda de generalidade, podemos aplicar uma fase global a  $\varphi_1$  e tomar  $a = 1$ . Analogamente, uma fase global aplicada a  $\varphi_2$  nos permite tomar  $d = 1$ . A condição de distinção é agora dada por  $4c + R^2\bar{b} = 0$ , e então  $c = -R^2\bar{b}/4$ . Observe que se  $b = 0$ , então  $c = 0$ , e assim  $\varphi_1 = (1, 0)$  e  $\varphi_2 = (0, 1)$ , dois vetores trivialmente distinguidos, já que são ortogonais entre si. Assumiremos então que  $b \neq 0$ . Como a razão entre  $c$  e  $\bar{b}$  é uma constante real, podemos tomar  $c = |c|e^{i\lambda}$  e  $\bar{b} = |b|e^{i\lambda}$ . Devidamente normalizados, os vetores  $\varphi_1$  e  $\varphi_2$  devem então ser escritos da seguinte forma:

$$\varphi_1 = \frac{1}{\sqrt{1 + |b|^2}} \begin{pmatrix} 1 \\ |b|e^{i\lambda} \end{pmatrix}, \quad \varphi_2 = \frac{1}{\sqrt{1 + \frac{R^4}{16}|b|^2}} \begin{pmatrix} -\frac{R^2}{4}|b| \\ e^{i\lambda} \end{pmatrix}.$$

Ou seja, os dois vetores devem ficar no mesmo meridiano da esfera de Bloch, exceto nos polos.

Segue então que  $a = 1/\sqrt{1+|b|^2}$  e  $d = 1/\sqrt{1+\frac{R^4}{16}|b|^2}$ . Juntando-se a isto o fato de que  $0 \leq R \leq 2$ , conclui-se facilmente que a condição para que os vetores  $\varphi_1 = (a, b)$  e  $\varphi_2 = (c, d)$  possam ser distinguidos por este diagrama é  $ac \leq bd$ .

Nossa próxima tarefa é verificar que os pares de vetores distinguíveis sempre podem ser distinguidos com probabilidade ótima. Para isto, vamos verificar quais deles satisfazem a equação  $P = P_{\text{best}}$ , onde  $P$  representa a probabilidade de que eles sejam distinguidos (4-2) e  $P_{\text{best}}$  é uma das expressões de probabilidade ótima fornecidas na seção (2.4). Considerando a primeira de tais expressões, temos:

$$\begin{aligned} P = P_{\text{best}} &\Leftrightarrow \frac{r}{4}\|L\varphi_1\|^2 + \frac{1-r}{4}\|L\varphi_2\|^2 = 1 - 2\sqrt{r(1-r)}|\langle\varphi_1|\varphi_2\rangle| \\ &\Leftrightarrow \frac{r}{4} \frac{(4 + R^2|b|^2)}{(1 + |b|^2)} + \frac{1-r}{4} \frac{\left(\frac{R^4|b|^2}{4} + R^2\right)}{\left(1 + \frac{R^4|b|^2}{16}\right)} \\ &= 1 - 2\sqrt{r(1-r)} \frac{|b| \left(1 - \frac{R^2}{4}\right)}{\sqrt{1 + |b|^2} \sqrt{1 + \frac{R^4|b|^2}{16}}} \end{aligned}$$

Como nenhum dos termos desta equação depende da fase de  $b$ , podemos tomar  $b$  real. Mais ainda, podemos tomar  $b$  positivo, pois os termos dependem apenas de  $|b|$ .

Fazendo a substituição  $R^2 = S$ , utilizamos o Maple para resolver esta equação para  $S$ , obtendo os seguintes resultados:

$$S = 4, \pm \frac{4}{rb^2} \sqrt{r(1-r + (1-2r)b^2)}.$$

Extraindo então a raiz quadrada de cada um deles, obtemos os valores que  $R$  pode assumir. Observe que os resultados imaginários não devem ser considerados, pois  $R$  é real, por definição. O valor  $R = 2$  nos levaria a um caso trivial, como já foi discutido na seção (4.2):  $L$  seria igual a  $\text{diag}(2, 2)$ , um múltiplo de uma matriz unitária, e só seria capaz de distinguir vetores que já fossem ortogonais entre si. Analisando os outros resultados, como  $R$  deve ser positivo, podemos afirmar que

$$R = 2(\sqrt{r(1-r + (1-2r)b^2)}/(rb^2))^{1/2} \quad (5-9)$$

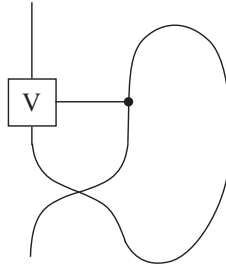
Ou seja, esta é uma relação que  $R$  e  $b$  devem satisfazer para que  $\varphi_1$  e  $\varphi_2$  possam ser distinguidos otimamente.

Concluimos então que, dados dois vetores distinguíveis, e a probabilidade  $r$ , a distinção será ótima se e somente se o valor  $R$  calculado a partir do produto interno satisfaz (5-9).

**5.3**

**Diagrama T.III**

O terceiro diagrama a ser considerado é o seguinte:



O traço parcial é dado por:

$$L = \text{Tr}_2(US) = P_0 + VP_1 = \begin{pmatrix} 1 & l_1 \\ 0 & l_3 \end{pmatrix},$$

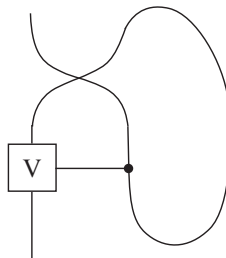
onde  $l_1 = e^{i\xi} \sin \theta$  e  $l_3 = e^{i(\lambda-\tau)} \cos \theta$ , valores estes obtidos na seção (5.1.1), por ser  $V$  uma matriz  $2 \times 2$  unitária geral.

Utilizando o Maple, obtemos os seguintes autovalores para a matriz  $|L|$ :  $\sqrt{1 \pm \sin \theta}$ . Obviamente, nenhum deles pode ser igual a 2, e então, novamente pelo critério da seção (4.2), afirmamos que os pares de vetores distinguidos pelo diagrama III nunca são distinguidos com probabilidade ótima.

**5.4**

**Diagrama T.IV**

O quarto e último diagrama a ser estudado é o seguinte:



Temos que

$$L = \text{Tr}_2(SU) = P_0 + P_1V = \begin{pmatrix} 1 & 0 \\ l_2 & l_3 \end{pmatrix},$$

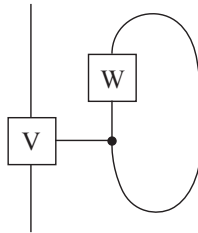
onde  $l_2 = -e^{i(\lambda-\xi)} \sin \theta$  e  $l_3 = e^{i(\lambda-\tau)} \cos \theta$ , valores estes obtidos na seção (5.1.1), como antes.

Utilizando novamente o Maple, obtemos os seguintes autovalores para a matriz  $|L|$ :  $\sqrt{1 \pm \sin \theta}$ . Assim como no diagrama III, chegamos então à mesma conclusão: os pares de vetores distinguidos pelo diagrama IV nunca são distinguidos com probabilidade ótima.

### 5.5 Resultados para operadores não-triviais

Para concluir este capítulo, devemos voltar à questão da simplificação do operador  $W$ , proposta anteriormente. Para isso, vamos verificar que ao tomarmos  $W$  não-trivial (ou seja, diferente do operador identidade) em cada um dos diagramas de traço parcial, não há melhores resultados sobre distinção de estados quânticos.

Se  $W$  não fosse o operador identidade, o diagrama T.I seria reescrito como:



Observe que

$$L = \text{Tr}_2(I \otimes WP_0 + V \otimes WP_1) = w_{00}I + w_{11}V,$$

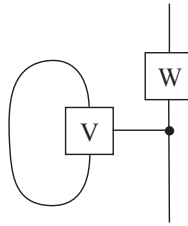
onde  $w_{ij}$ ,  $i, j = 0, 1$ , são as entradas da matriz  $W$ . De acordo com o critério apresentado na seção 4.2, os pares de vetores distinguidos por este diagrama são distinguidos com probabilidade ótima se e somente se  $|L|$  possui um autovalor igual a 2. Entretanto,

$$L^*L = (|w_{00}|^2 + |w_{11}|^2)I + 2\text{Re}(w_{00}^*w_{11}V),$$

e como  $\text{Re}(w_{00}^*w_{11}V)$  tem autovalores reais de módulo menor ou igual a 1,  $L^*L$  terá um autovalor igual a 4 se e somente se  $|w_{00}|^2 + |w_{11}|^2 = 2$ , ou seja,  $|w_{00}|^2 = |w_{11}|^2 = 1$ , e então  $W$  deve ser diagonal. Se este for o caso, temos, a menos de uma fase global,  $L = I + V'$ , onde  $V'$  nada mais é do que  $V$  multiplicada por um número unimodular. Ou seja, o poder de distinção neste

caso é o mesmo do diagrama T.I. No caso em que  $W$  não é diagonal, não há distinção ótima.

Para o diagrama T.II, teríamos:

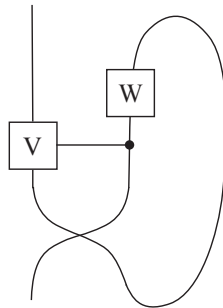


Observe que

$$\begin{aligned} L = \text{Tr}_2(SUS) &= \text{Tr}_2(S(I \otimes WP_0 + V \otimes WP_1)S) \\ &= W(2P_0 + \text{Tr}(V)P_1), \end{aligned}$$

temos o mesmo traço parcial do diagrama T.II, a menos de uma multiplicação por unitário. Logo, o poder de distinção não é alterado se  $W$  não for a identidade.

Para o diagrama T.III, teríamos:

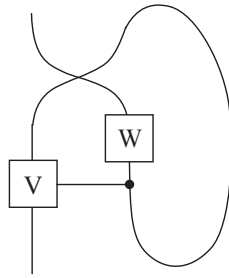


Observe que

$$\begin{aligned} L = \text{Tr}_2(US) &= \text{Tr}_2((I \otimes WP_0 + V \otimes WP_1)S) \\ &= WP_0 + VWP_1 \\ &= (WP_0W^* + VWP_1W^*)W, \end{aligned}$$

o qual é equivalente ao traço parcial do diagrama T.III original através de uma mudança de base. Ou seja, em termos de poder de distinção de estados quânticos através de traços parciais, os diagramas T.III original e T.III alterado são equivalentes.

Por fim, o diagrama T.IV alterado:



Este caso é completamente análogo ao do diagrama T.III: o poder de distinção é o mesmo do diagrama original T.IV.

Conclui-se então que, em todos os casos, ao considerarmos  $W$  não-trivial, os resultados sobre distinção de estados quânticos são piores ou exatamente iguais aos que já tínhamos obtido com  $W$  sendo o operador identidade.