Ph219/CS219: Quantum Computation

Winter 2006

Solutions to Problem Set 5

Problem 5.1

a) Reading the circuit diagram, $U_1 = (H\otimes I)\Lambda(P)(H\otimes I)$, where $\Lambda(P) = diag(1,1,1,i)$ and $H = \frac{1}{\sqrt{2}}(X+Z)$ [1]. We can express $H \otimes I$ and $\Lambda(P)$ in block form as

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ I & -I \end{pmatrix} \; ; \; \Lambda(P) = \begin{pmatrix} I & O_2 \\ O_2 & P \end{pmatrix} , \tag{1}$$

where I (resp. O_2) is the 2×2 identity (resp. zero) matrix. Thus,

$$U_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} I+P & I-P \\ I-P & I+P \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix} . \tag{2}$$

We note that $U_2 = (I\otimes H)\Lambda(P)(I\otimes H) = \textsc{swap}\; U_1 \;\textsc{swap}$, where the SWAP gate acts as $\textsc{swap}\colon |ij\rangle \mapsto |ji\rangle$ for $i,j \in \{0,1\}$. Therefore, U_2 can be obtained from U_1 in Eq. (2) by interchanging the second and third row and also the second and third column. The result is

$$U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix} . \tag{3}$$

Let $|u_1\rangle = |00\rangle$ and $|u_2\rangle = \frac{1}{\sqrt{3}}(|01\rangle+|10\rangle+|11\rangle)$. Then we can check $U_i|u_j\rangle = |u_j\rangle$ for all $i,j \in \{1,2\}$.

b) Let $|u_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and $|u_4\rangle = \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle - 2|11\rangle)$, so that the set $\{|u_i\rangle : i = 1,\ldots,4\}$ forms an orthonormal basis. Then, the unitary V that describes the transformation from the computation basis to this new basis is

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{6}} \end{pmatrix} . \tag{4}$$

[1] We use the shorthand notation for the Pauli matrices $X \equiv \sigma_{\rm x}$, $Y \equiv \sigma_{\rm y}$ and $Z \equiv \sigma_{\rm z}$.

Expressing U_1 and U_2 in the new basis amounts to conjugating them by V, or $U_i \mapsto (U_i)_{\text{new}} = VU_iV^\dagger$ for $i = 1, 2$. By explicit calculation

$$(U_1)_{\text{new}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{3+i}{4} & \frac{\sqrt{3}(-1+i)}{4} \\ 0 & 0 & \frac{\sqrt{3}(-1+i)}{4} & \frac{1+3i}{4} \end{pmatrix} , \tag{5}$$

$$(U_2)_{\text{new}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{3+i}{4} & \frac{\sqrt{3}(1-i)}{4} \\ 0 & 0 & \frac{\sqrt{3}(1-i)}{4} & \frac{1+3i}{4} \end{pmatrix} , \tag{6}$$

and we see that the two gates act trivially on the two-dimensional subspace spanned by $|u_1\rangle$ and $|u_2\rangle$, as expected.

c) From part (b), U_1 and U_2 restricted on the two-dimensional subspace on which they act non-trivially are

$$U_1 = \begin{pmatrix} \frac{3+i}{4} & \frac{\sqrt{3}(-1+i)}{4} \\ \frac{\sqrt{3}(-1+i)}{4} & \frac{1+3i}{4} \end{pmatrix} \; ; \; U_2 = \begin{pmatrix} \frac{3+i}{4} & \frac{\sqrt{3}(1-i)}{4} \\ \frac{\sqrt{3}(1-i)}{4} & \frac{1+3i}{4} \end{pmatrix} . \tag{7}$$

We can expand these 2×2 matrices in the basis of the Pauli matrices $\{I, X, Y, Z\}$. Let $U_1 = \alpha I + \beta X + \gamma Y + \delta Z$. Then, note that $\text{tr}(U_1) = 2\alpha = 1 + i$, or $\alpha = \sqrt{i/2}$. Also, $\text{tr}(U_1X) = 2\beta = \frac{\sqrt{3}}{2}(-1+i)$, or $\beta = \sqrt{i/2}\,(i\sqrt{3}/2)$. Similarly, $\text{tr}(U_1Y) = 2\gamma = 0$, or $\gamma = 0$, and finally $\text{tr}(U_1Z) = 2\delta = (1-i)/2$, or $\delta = \sqrt{i/2}\,(-i/\sqrt{2})$. Thus,

$$U_1 = \sqrt{i}\left(\frac{1}{\sqrt{2}}I - i\frac{1}{\sqrt{2}}\,\hat{n_1}\cdot\vec{\sigma}\right) , \tag{8}$$

where $\hat{n_1} = (-\sqrt{3}/2, 0, 1/2)^T$.

Repeating the same calculation for U_2 we find expansion coefficients $\alpha = \sqrt{i/2}$, $\beta = \sqrt{i/2}\,(-i\sqrt{3}/2)$, $\gamma = 0$, and $\delta = \sqrt{i/2}\,(-i/\sqrt{2})$. Thus,

$$U_2 = \sqrt{i}\left(\frac{1}{\sqrt{2}}I - i\frac{1}{\sqrt{2}}\,\hat{n_2}\cdot\vec{\sigma}\right) , \tag{9}$$

where $\hat{n_2} = (\sqrt{3}/2, 0, 1/2)^T$.

d) From part (c),

$$\begin{aligned} U_2^{-1}U_1 &= \sqrt{-i^2}\left(\tfrac{1}{\sqrt{2}}I + i\tfrac{1}{\sqrt{2}}\,\hat{n_2}\cdot\vec{\sigma}\right)\left(\tfrac{1}{\sqrt{2}}I - i\tfrac{1}{\sqrt{2}}\,\hat{n_1}\cdot\vec{\sigma}\right) \\ &= \tfrac{1}{2} - i\tfrac{1}{2}(\hat{n_1} - \hat{n_2})\cdot\vec{\sigma} + \tfrac{1}{2}(\hat{n_1}\cdot\vec{\sigma})(\hat{n_2}\cdot\vec{\sigma}) . \end{aligned} \tag{10}$$

We can now use the identity

$$(\hat{n_1} \cdot \vec{\sigma})(\hat{n_2} \cdot \vec{\sigma}) = \hat{n_1} \cdot \hat{n_2} + i\vec{\sigma} \cdot (\hat{n_1} \times \hat{n_2}) \ , \tag{11}$$

with $\hat{n_1} \cdot \hat{n_2} = -1/2$ and $\hat{n_1} \times \hat{n_2} = (0, \sqrt{3}/2, 0)^T$ and substitute in Eq. (10) to find

$$U_2^{-1} U_1 = \tfrac{1}{4} I - i \tfrac{\sqrt{15}}{4} \ \hat{k} \cdot \vec{\sigma} \ , \tag{12}$$

where $\hat{k} = (-\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}, 0)$. This is a rotation around the axis $\hat{k}$ by an angle θ such that $\cos(\frac{\theta}{2}) = \frac{1}{4}$.

Problem 5.2

a) Clearly a monic rational polynomial of degree one has a rational root, which $e^{i\frac{\theta}{2}}$ is not. We therefore try to find a monic rational polynomial of degree two. Since its coefficients are rationals, its roots must be complex conjugates of one another. We therefore obtain the polynomial

$$P(x) = (x - e^{i\frac{\theta}{2}})(x - e^{-i\frac{\theta}{2}}) = x^2 - 2\cos\left(\frac{\theta}{2}\right) x + 1 = x^2 - \frac{1}{2} x + 1 \ . \tag{13}$$

b) Let $A(x) = x^n - 1$, and consider the division of $A(x)$ by $P(x)$. Then

$$A(x) = P(x)Q(x) + R(x) \ , \tag{14}$$

for some rational polynomials $Q(x)$ and $R(x)$, where $R(x)$ has degree less than the degree of $P(x)$. But $A(a) = 0$ and $P(a) = 0$, which implies $R(a) = 0$. We have found that a is a root of $R(x)$, which is a contradiction because $P(x)$ is the minimal-degree rational polynomial with root a. The only way to avoid the contradiction is if $R(x) = 0$, $\forall x$. Thus, $A(x) = x^n - 1 = P(x)Q(x)$.

c) Let $A(x) = \sum_l a_l x^l$, $B(x) = \sum_m b_m x^m$ and

$$C(x) = \sum_k c_k x^k = A(x)B(x) = \sum_{l,m} a_l b_m x^{l+m} \ . \tag{15}$$

It is clear that $C(x)$ is integral. Suppose it is not primitive. Then there exists a prime p that divides all coefficients c_k. In contrast, p does not divide all coefficients a_l (or else $A(x)$ would not be primitive), and let a_r be the lowest-order coefficient of $A(x)$ that is not divisible by p. Similarly, p does not divide all b_m, and let b_s be the lowest-order coefficient of $B(x)$ that is not divisible by p. Consider the $(r+s)$-th order coefficient of $C(x)$. From Eq. (15),

$$c_{r+s} = a_r b_s + \sum_{l \neq r,\ m \neq s \ : \ l+m = r+s} a_l \ b_m \ . \tag{16}$$

Now, c_{r+s} is divisible by p and so is every term in the sum on the right-hand side. Indeed, for each term in the sum, either $l < r$ and a_l is divisible by p or $m < s$ and then b_m is divisible by p. Hence, Eq. (16) implies that $a_r b_s$ is also divisible by p and so at least one of a_l or b_s is divisible by p which leads to a contradiction. To avoid the contradiction, we conclude $C(x)$ is primitive.

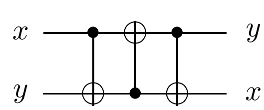
d) Let r be the lowest common denominator of the coefficients of $A(x)$. Therefore, r is the lowest integer such that we can write $rA(x) = \tilde{A}(x)$ with $\tilde{A}(x)$ integral. We can show that $\tilde{A}(x)$ is primitive. Indeed, if it is not primitive, then there exists integer $k > 1$ such that $\frac{1}{k}\tilde{A}(x)$ is integral, or equivalently $\frac{r}{k}A(x)$ is integral. But $A(x)$ is monic, which means that the highest-order coefficient of $\frac{r}{k}A(x)$ is $\frac{r}{k}$. Since $\frac{r}{k}A(x)$ is integral, k must divide r. We have found a new integer $\frac{r}{k}$ less than r for which $\frac{r}{k}A(x) = \tilde{A}'(x)$, where $\tilde{A}'(x) \equiv \frac{1}{k}\tilde{A}(x)$ is integral. This is a contradiction because r is the lowest integer for which this is true. We conclude that $\tilde{A}(x)$ is primitive. Similarly, we can write $B(x) = \frac{1}{s}\tilde{B}(x)$ for some integer s and for $\tilde{B}(x)$ a primitive integral polynomial.

Now, $P(x) = A(x)B(x) = \frac{1}{rs}\tilde{A}(x)\tilde{B}(x)$, where $P(x)$ is by assumption a monic integral polynomial. Using part (c), $\tilde{A}(x)\tilde{B}(x)$ is primitive integral since $\tilde{A}(x)$ and $\tilde{B}(x)$ are primitive integral. Since $P(x)$ is integral, rs divides all coefficients of $\tilde{A}(x)\tilde{B}(x)$. This leads to a contradiction because $\tilde{A}(x)\tilde{B}(x)$ is primitive, unless $rs = 1$ or equivalently $r = 1$ and $s = 1$.

e) Assume a is a root of unity (i.e., $a^n = 1$ for some integer n) and $P(x)$ is the minimal-degree monic rational polynomial that has a as a root. Then part (b) implies that there exists monic rational polynomial $Q(x)$ such that $x^n - 1 = P(x)Q(x)$. Finally, from part (d), since $x^n - 1$ is monic integral, it follows that $P(x)$ must be integral. QED

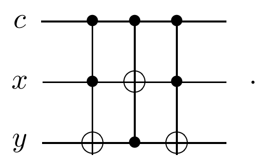
Problem 5.3

a) We want to construct a controlled-SWAP gate, so let's first consider the following circuit that implements the SWAP gate using three CNOT gates.

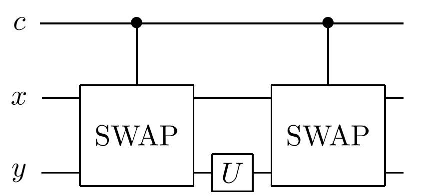


Indeed, this circuit implements the SWAP gate since $(x, y) = (0, 0)$ triggers none of the CNOTs, $(x, y) = (1, 1)$ triggers the first and third CNOT which have the same direction and cancel out (since $\text{CNOT}^2 = I$), while $(x, y) = (0, 1)$ and $(x, y) = (1, 0)$ trigger two CNOTs with opposite directions leading to a swap of the bit values.

To implement a controlled-SWAP we need to control each of the three gates in this circuit from some control bit c. But a controlled-CNOT is nothing other than a Toffoli gate! So our controlled-SWAP circuit is

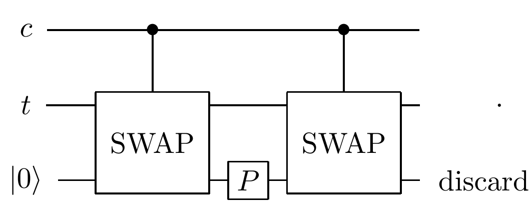


b) We consider the following circuit



When the control bit is $c = 0$, the controlled-SWAP gates are not activated and the circuit applies U on the third input y. If on the other hand $c = 1$, both controlled-SWAP gates are activated. First x and y are interchanged, then U is applied on x, and finally x and y are interchanged again. Overall, U is applied on the second qubit x. So the control bit c determines on which bit, x or y, the gate U will be applied and leaves the other input unchanged.

We want to make the gate $\Lambda(P)$ that applies P on the target (t) if the control (c) is in state $|1\rangle$ and does nothing otherwise. Imagine we use the circuit above with $U = P$, and connect the two inputs of the $\Lambda(P)$ we want to simulate to the first two inputs of this circuit. We don't care what is connected in the third input to that circuit, so we can just put any arbitrary input there, say $|0\rangle$. Then, if $c = 0$ the gate P is only applied on the third input which is arbitrary and the second input is left unchanged. If $c = 1$, P acts on the second input. Overall, we have simulated the $\Lambda(P)$ gate with the following circuit



c) Since $\Lambda(P) = diag(1,1,1,i)$,

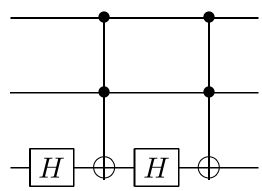
$$\begin{aligned} \Lambda(P)_R : \quad & |x,y,0\rangle \mapsto diag(1,1,1,0)|x,y,0\rangle + diag(0,0,0,1)|x,y,1\rangle \\ & |x,y,1\rangle \mapsto -diag(0,0,0,1)|x,y,0\rangle + diag(1,1,1,0)|x,y,1\rangle \ . \end{aligned} \tag{17}$$

Therefore $\Lambda(P)_R$ acts trivially on all inputs except for those with $x = y = 1$. In that case, it leaves the first two qubits unchanged and it maps the third qubit from $|0\rangle \mapsto |1\rangle$ and from $|1\rangle \mapsto -|0\rangle$. But this mapping corresponds to a XZ gate, since

$$XZ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ . \tag{18}$$

Thus, $\Lambda(P)_R$ applies a XZ gate on the third qubit when the first two qubits are in state $|1,1\rangle$ and does nothing otherwise. Hence it is a controlled-controlled-XZ, or $\Lambda(P)_R = \Lambda^2(XZ)$.

d) Recall that $HXH = Z$ and $H^2 = I$. Therefore $(I \otimes I \otimes H)\Lambda^2(X)(I \otimes I \otimes H) = \Lambda^2(Z)$. Then, $\Lambda^2(XZ) = \Lambda^2(X)\Lambda^2(Z) = \Lambda^2(X)(I \otimes I \otimes H)\Lambda^2(X)(I \otimes I \otimes H)$, or schematically

$\Lambda^2(XZ) =$  .

Problem 5.4

a) Choosing orthonormal bases $\{|i\rangle_A\}$ and $\{|j\rangle_{A'}\}$ for systems A and A', the swap operator is $S_{AA'} = \sum_{i,j} (|i\rangle\langle j|)_A \otimes (|j\rangle\langle i|)_{A'}$. Then, with $\rho_A = \mathrm{tr}_B(|\psi\rangle\langle\phi|)_{AB} = \rho_{A'}$,

$$\begin{aligned} \mathrm{tr}_{ABA'B'} & \left[(S_{AA'} \otimes I_{BB'}) \left(|\phi\rangle\langle\phi|_{AB} \otimes |\phi\rangle\langle\phi|_{A'B'} \right) \right] = \mathrm{tr}_{AA'} \left[S_{AA'}(\rho_A \otimes \rho_{A'}) \right] \\ &= \sum_{k,l} \langle k|_A \langle l|_{A'} \left[\sum_{i,j} (|i\rangle\langle j|)_A \otimes (|j\rangle\langle i|)_{A'} \right] (\rho_A \otimes \rho_{A'}) |k\rangle_A |l\rangle_{A'} \\ &= \sum_{i,j,k,l} \delta_{ik}\delta_{jl} (\rho_A)_{jk} (\rho'_A)_{il} = \sum_{k,l} (\rho_A)_{lk} (\rho_A)_{kl} = \sum_l (\rho_A^2)_{ll} = \mathrm{tr}_A \rho_A^2 \ . \end{aligned} \tag{19}$$

b) The constant C multiplying $\Pi_{AA'}$ can be determined from the requirement that the average state is normalized, or equivalently $\mathrm{tr}(C\,\Pi_{AA'}) = 1$. But $\mathrm{tr}\,\Pi_{AA'} = d_{\mathrm{sym}}$ where $d_{\mathrm{sym}} = d(d+1)/2$ is the dimension of the symmetric subspace of AA'. To see this, let's construct an explicit orthonormal basis for the symmetric subspace. The states $|i\rangle_A \otimes |i\rangle_{A'}$ for $i = 1, \ldots, d$ are clearly symmetric, and there are d such states. Furthermore, consider the states $\left(|i\rangle_A \otimes |j\rangle_{A'} + |j\rangle_A \otimes |i\rangle_{A'}\right)/\sqrt{2}$ for $i \neq j$, which are also symmetric and linearly independent from the previous ones. There are $\binom{d}{2} = d(d-1)/2$ such states, giving a total of $d + d(d-1)/2 = d(d+1)/2$ linearly independent basis states spanning the symmetric subspace of AA'. Therefore, $C = 1/d_{\rm sym} = [d(d+1)/2]^{-1}$.

c) Using part (b), $\Big\langle |\phi\rangle\langle\phi|_{AB} \otimes |\phi\rangle\langle\phi|_{A'B'} \Big\rangle = C\, \Pi_{AB;A'B'}$, where $C = \frac{2}{d_A d_B (d_A d_B + 1)}$ since $dim(AB) = d_A d_B$. Taking the average on both sides of Eq. (19),

$$\begin{aligned} \Big\langle {\rm tr}_A \rho_A^2 \Big\rangle &= {\rm tr}_{ABA'B'} \Big[(S_{AA'} \otimes I_{BB'}) \Big\langle |\phi\rangle\langle\phi|_{AB} \otimes |\phi\rangle\langle\phi|_{A'B'} \Big\rangle \Big] \\ &= \tfrac{C}{2}\, {\rm tr}_{ABA'B'} \left[(S_{AA'} \otimes I_{BB'})(I_{ABA'B'} + S_{AB;A'B'}) \right] \\ &= \tfrac{C}{2}\, {\rm tr}_{ABA'B'} \left[S_{AA'} \otimes I_{BB'} + I_{AA'} \otimes S_{BB'} \right] . \end{aligned} \tag{20}$$

But, ${\rm tr}_{AA'}(S_{AA'}) = {\rm tr}(2\,\Pi_{AA'} - I_{AA'}) = 2\frac{d_A(d_A+1)}{2} - d_A^2 = d_A$. And therefore, ${\rm tr}_{ABA'B'}\,(S_{AA'} \otimes I_{BB'}) = {\rm tr}_{AA'}(S_{AA'})\ d_B^2 = d_A d_B^2$. Similarly, we can calculate ${\rm tr}_{ABA'B'}\,(I_{AA'} \otimes S_{BB'}) = d_A^2 d_B$, and substituting in Eq. (20),

$$\Big\langle {\rm tr}_A \rho_A^2 \Big\rangle = \tfrac{d_A d_B^2 + d_A^2 d_B}{d_A d_B (d_A d_B + 1)} = \tfrac{d_A + d_B}{d_A d_B + 1} . \tag{21}$$

d) We first calculate

$$\begin{aligned} ||\rho_a - \tfrac{1}{d_A} I_A||_2^2 &= {\rm tr}\left(\left(\rho_A - \tfrac{1}{d_A} I_A\right)^\dagger \left(\rho_A - \tfrac{1}{d_A} I_A\right) \right) \\ &= {\rm tr}\rho_A^2 + \tfrac{1}{d_A^2} {\rm tr} I_A - \tfrac{2}{d_A} {\rm tr}\rho_A \\ &= {\rm tr}\rho_A^2 + \tfrac{1}{d_A^2}\, d_A - \tfrac{2}{d_A} = {\rm tr}\rho_A^2 - \tfrac{1}{d_A} . \end{aligned} \tag{22}$$

And so, using part (c),

$$\Big\langle ||\rho_a - \tfrac{1}{d_A} I_A||_2^2 \Big\rangle = \Big\langle {\rm tr}\rho_A^2 \Big\rangle - \tfrac{1}{d_A} = \tfrac{d_A + d_B}{d_A d_B + 1} - \tfrac{1}{d_A} \leq \tfrac{1}{d_A} + \tfrac{1}{d_B} - \tfrac{1}{d_A} = \tfrac{1}{d_B} . \tag{23}$$

Thus, using the Cauchy-Schwarz inequality,

$$\Big\langle ||\rho_a - \tfrac{1}{d_A} I_A||_2 \Big\rangle \leq \sqrt{\tfrac{1}{d_B}} . \tag{24}$$

e) Let $M = \rho_A - \frac{1}{d_A} I_A$. Since M is Hermitian, we can write it in the basis $\{|\mu\rangle\}$ that diagonalizes it as $M = \sum_{\mu=1}^d \lambda_\mu |\mu\rangle\langle\mu|$. Then, $||M||_1 = {\rm tr}\sqrt{M^\dagger M} = \sum_{\mu=1}^d |\lambda_\mu|$. On the other hand, $||M||_2 = \sqrt{{\rm tr}(M^\dagger M)} = \sqrt{\sum_{\mu=1}^d |\lambda_\mu|^2}$. Now, using the Cauchy-Schwarz inequality again,

$$\Big\langle |\lambda_\mu| \Big\rangle \leq \sqrt{\Big\langle |\lambda_\mu|^2 \Big\rangle} \Rightarrow \tfrac{1}{d} \sum_{\mu=1}^d |\lambda_\mu| \leq \sqrt{\tfrac{1}{d} \sum_{\mu=1}^d |\lambda_\mu|^2} \Rightarrow ||M||_1 \leq \sqrt{d} ||M||_2 . \tag{25}$$

And using the bound on $\left\langle ||M||_2 \right\rangle$ from part (d),

$$\left\langle ||M||_1 \right\rangle \leq \sqrt{d_A}\left\langle ||M||_2 \right\rangle \leq \sqrt{\frac{d_A}{d_B}}\ . \tag{26}$$