Quantum Complexity Theory

Problem set 3: Entanglement and quantum communication **Solutions**

We use the Bell-state convention $|\beta_{ab}\rangle = (I \otimes X^b Z^a)|\Phi^+\rangle$. All post-measurement kets are specified up to global phase.

1. The Bell basis

(a) The four states are

ab	$\lvert\beta_{ab}\rangle$	ab	$\lvert\beta_{ab}\rangle$
00	$(\lvert00\rangle + \lvert11\rangle)/\sqrt{2}$	01	$(\lvert01\rangle + \lvert10\rangle)/\sqrt{2}$
10	$(\lvert00\rangle - \lvert11\rangle)/\sqrt{2}$	11	$(\lvert01\rangle - \lvert10\rangle)/\sqrt{2}$

Each is normalised. Opposite parities have disjoint support, and within each parity the $+$ and $-$ combinations are orthogonal. Thus the four states form an orthonormal basis.

(b) Using the suggested expansion,

$$\mathrm{CNOT}|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{ax}|x,b\rangle = H|a\rangle \otimes |b\rangle.$$

Applying H to the first qubit gives $|a,b\rangle$. Hence CNOT, then H on the first qubit, then computational-basis measurement distinguish the four Bell states with certainty.

(c) Under either partial trace the cross terms vanish, giving

$$\rho_A = \rho_B = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = I/2.$$

Each joint state is pure with mixed reduced states, so it is entangled. Every local measurement has probabilities determined by $I/2$, independently of a, b.

2. Teleportation

(a) Expanding in the order M, A, B and applying Alice's gates gives

$$\frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle)$$
$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)] = \frac{1}{2}\sum_{m,n=0}^{1}|m,n\rangle \otimes X^n Z^m|\psi\rangle.$$

(b) Each $X^n Z^m|\psi\rangle$ is normalised, so every outcome has probability $1/4$:

Outcome (m,n)	Bob's conditional state	Correction
00	$\lvert\psi\rangle$	I
01	$X\lvert\psi\rangle$	X
10	$Z\lvert\psi\rangle$	Z
11	$XZ\lvert\psi\rangle$	ZX

Bob applies X^n first and then Z^m: the correction is $Z^m X^n$, and $Z^m X^n X^n Z^m|\psi\rangle = |\psi\rangle$.

(c) Put $\rho = |\psi\rangle\langle\psi|$. Since $\rho + Z\rho Z = 2\,\mathrm{diag}(|\alpha|^2, |\beta|^2)$,

$$\rho_B = \frac{1}{4}\sum_{m,n=0}^{1} X^n Z^m \rho Z^m X^n$$
$$= \frac{1}{4}[\rho + Z\rho Z + X(\rho + Z\rho Z)X] = \frac{1}{2}\,\mathrm{diag}(1,1) = I/2.$$

Bob has the same reduced state before and after Alice's operations, independently of $|\psi\rangle$. Thus Alice's local operations cannot signal to him; the classical message is needed to recover the state. The protocol consumes one initially shared Bell pair and sends two classical bits from Alice to Bob, transferring one unknown qubit state. No qubit is sent during these steps. Alice's measured qubits are $|m,n\rangle$; their averaged state is $I_4/4$, independent of $|\psi\rangle$, so she retains no copy.

3. Superdense coding

(a) Applying X^b and then Z^a on Alice's qubit and relabelling $y = x \oplus b$ gives

$$(Z^a X^b \otimes I)|\Phi^+\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{1} (-1)^{a(x\oplus b)} |x \oplus b, x\rangle$$
$$= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{ay} |y, y \oplus b\rangle = |\beta_{ab}\rangle.$$

(b) After receiving A, Bob applies CNOT from A to B, followed by H on A. By Problem 1(b), this maps $|\beta_{ab}\rangle$ to $|a, b\rangle$. Computational-basis measurement recovers both bits with certainty.

(c) Before transmission, $\rho_B = \mathrm{Tr}_A |\beta_{ab}\rangle\langle\beta_{ab}| = I/2$, independently of a, b. Thus Alice's local encoding alone gives Bob no information about either bit. He can distinguish the four joint states once he receives A.

Superdense coding consumes one initially shared Bell pair and sends one qubit to communicate two classical bits. Teleportation consumes one Bell pair and sends two classical bits to transfer one unknown qubit state.

4. BB84: preparation and sifting

(a) For $(x, \theta) = (0,0), (1,0), (0,1), (1,1)$, the signals are $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, respectively. Since $H^2 = I$,

$$\Pr(y \mid x, \theta, \phi) = \left|\langle y|H^\phi H^\theta |x\rangle\right|^2 = \begin{cases} \delta_{x,y}, & \theta = \phi, \\ 1/2, & \theta \neq \phi. \end{cases}$$

(b) Independent uniform bases satisfy $\Pr(\theta = \phi) = 1/2$, so the expected sifted length is $N/2$. Every sifted bit has $y = x$ in the ideal honest protocol.

(c) Averaging over the bit gives

$$\rho_\theta = \frac{1}{2} \sum_x H^\theta |x\rangle\langle x| H^\theta = \frac{I}{2}.$$

All measurement statistics are therefore independent of θ. This establishes basis hiding before the announcement. It does not establish bit secrecy: averaging over the basis while fixing the bit gives the distinct states

$$\rho_x^{\text{bit}} = \frac{1}{2} \sum_\theta H^\theta |x\rangle\langle x| H^\theta = \frac{I}{2} + \frac{(-1)^x}{4}(X + Z).$$

5. BB84: intercept-resend

(a) On a sifted position Bob uses Alice's basis. If Eve uses that basis too, she obtains x and resends the correct state, so Bob's error probability is 0. If Eve uses the other basis, her resent state gives either Bob outcome with probability $1/2$, so the error probability is $1/2$.

(b) Eve's basis agrees with Alice's with probability $1/2$, independently of sifting. Hence

$$q = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

If each signal is attacked independently with probability f, the sifted error rate is $q = f/4$.

(c) For the attack on every signal, each tested sifted position agrees with probability $3/4$. Independence gives

$$\Pr(\text{no detected error}) = \left(\frac{3}{4}\right)^m, \qquad \Pr(\text{detection}) = 1 - \left(\frac{3}{4}\right)^m.$$

The disclosed test bits are publicly known and cannot contribute to the secret key. Passing this test alone does not establish security against arbitrary attacks.

6. Monogamy of a Bell pair

(a) In the expansion $|\Omega\rangle = \sum_{a,b} |\beta_{ab}\rangle|e_{ab}\rangle$,

$$\langle\beta_{ab}|\rho_{AB}|\beta_{ab}\rangle = \langle e_{ab} \mid e_{ab}\rangle = \delta_{a0}\delta_{b0}.$$

Thus every $|e_{ab}\rangle$ except $|e_{00}\rangle$ vanishes, and $\|e_{00}\| = 1$. Hence $|\Omega\rangle = |\Phi^+\rangle_{AB} \otimes |e_{00}\rangle_E$.

(b) Purify ρ_{ABE} to $|\widetilde{\Omega}\rangle_{ABER}$. Its AB marginal is still $|\Phi^+\rangle\langle\Phi^+|$, so (a), with ER in place of E, gives $|\widetilde{\Omega}\rangle_{ABER} = |\Phi^+\rangle_{AB}|e\rangle_{ER}$. Tracing out R,

$$\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+| \otimes \mathrm{Tr}_R|e\rangle\langle e| = |\Phi^+\rangle\langle\Phi^+| \otimes \rho_E.$$

(c) Tracing out B gives $\rho_{AE} = (I_A/2) \otimes \rho_E$. For a rank-one projector P_x in either measurement basis, Eve's unnormalised conditional state is

$$\mathrm{Tr}_A\big[(P_x \otimes I_E)\rho_{AE}(P_x \otimes I_E)\big] = \tfrac{1}{2}\rho_E.$$

Each outcome has probability $1/2$, and Eve's normalised conditional state is always ρ_E. Since A is uncorrelated with E, it cannot form another Bell pair with a qubit in E.

7. Shared correlations and BB84 (extension)

(a)

$$\rho_{AB} = \tfrac{1}{2}|00\rangle\langle 00| + \tfrac{1}{2}|11\rangle\langle 11|, \qquad \langle Z_A Z_B\rangle = 1, \qquad \langle X_A X_B\rangle = 0.$$

This is a mixture of product states, so A, B are not entangled. Measuring all three qubits in the computational basis gives 000 or 111, each with probability $1/2$; Eve therefore learns Alice's bit. There is no contradiction with Problem 6: the AB marginal is not a Bell pair.

(b) The Bell states obey

$$(Z \otimes Z)|\beta_{ab}\rangle = (-1)^b|\beta_{ab}\rangle, \qquad (X \otimes X)|\beta_{ab}\rangle = (-1)^a|\beta_{ab}\rangle.$$

Write $\tau_{AB} = \sum_j \lambda_j |v_j\rangle\langle v_j|$. For either observable O, each $\langle v_j|O|v_j\rangle \le 1$. Since their weighted average is 1, every positive-weight component has expectation 1. Moreover, $\|(I - O)|v_j\rangle\|^2 = 2(1 - \langle v_j|O|v_j\rangle) = 0$, so each lies in the $+1$ eigenspace. The common $+1$ eigenspace is $\mathrm{span}\{|\beta_{00}\rangle\}$; hence $\tau_{AB} = |\Phi^+\rangle\langle\Phi^+|$.

(c) Since H is real and symmetric,

$$(\langle x|H^\theta \otimes I)|\Phi^+\rangle = \frac{1}{\sqrt{2}} H^\theta|x\rangle.$$

Thus x is uniform and Bob's conditional state is the BB84 state $H^\theta|x\rangle$. Under the exact premise of (b), Problem 6 gives $\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+| \otimes \rho_E$. Eve's conditional state is ρ_E for every x, θ, so announcing θ reveals no information about the unannounced bit x. An error-free finite sample cannot establish this exact premise: the attack in Problem 5 escapes detection on m tested sifted positions with probability $(3/4)^m > 0$.

Protocol references. Teleportation: Bennett et al., *Phys. Rev. Lett.* **70**, 1895 (1993). Superdense coding: Bennett and Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992). BB84: Bennett and Brassard, *Quantum cryptography: Public key distribution and coin tossing* (1984).