10 Communication protocols using entanglement and the no-cloning theorem

10.1 Dense coding

10.1.1 The Bell basis

It will be convenient here to let $X := \sigma_x$ and $Z := \sigma_z$. These operators are hermitian and unitary. Therefore, $X^2 = \mathbb{1}$ and $Z^2 = \mathbb{1}$, and it follows that, for any $j \in \mathbb{Z}$,

$$X^j = \begin{cases} \mathbb{1} \text{ if } j \text{ is even, and} \\ X \text{ if } j \text{ is odd,} \end{cases} \tag{10.1}$$

and similarly for Z^j. Furthermore, $\mathrm{Tr}X = \mathrm{Tr}Z = \mathrm{Tr}XZ = 0$.

Given a system AB where A and B are qubits, we define for $i, j \in \{0, 1\}$

$$|\beta_{ij}\rangle_{\mathsf{AB}} := X^i_{\mathsf{A}} Z^j_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}} |\phi^+\rangle_{\mathsf{AB}}. \tag{10.2}$$

Using the properties of the Pauli X and Z operators mentioned above and the fact that $\mathrm{Tr}_{\mathsf{B}}\phi^+_{\mathsf{AB}} = \mathbb{1}_{\mathsf{A}}/d_{\mathsf{A}}$ (where $\phi^+_{\mathsf{AB}} = |\phi^+\rangle\langle\phi^+|_{\mathsf{AB}}$) we have

$$\langle\beta_{i'j'}|\beta_{ij}\rangle = \mathrm{Tr}_{\mathsf{AB}} X^i_{\mathsf{A}} Z^j_{\mathsf{A}} \phi^+_{\mathsf{AB}} Z^{j'}_{\mathsf{A}} X^{i'}_{\mathsf{A}} = \frac{1}{2}\mathrm{Tr}_{\mathsf{A}} X^i_{\mathsf{A}} Z^j_{\mathsf{A}} \mathbb{1}_{\mathsf{A}} Z^{j'}_{\mathsf{A}} X^{i'}_{\mathsf{A}} = \frac{1}{2}\mathrm{Tr}_{\mathsf{A}} X^{i+i'}_{\mathsf{A}} Z^{j+j'}_{\mathsf{A}}. \tag{10.3}$$

The operator $X^{i+i'}_{\mathsf{A}} Z^{j+j'}_{\mathsf{A}}$ has trace zero unless $i + i'$ and $j + j'$ are both even, in which case it is equal to $\mathbb{1}_{\mathsf{A}}$, which has trace 2. Since $i, j, i', j' \in \{0, 1\}$, this happens precisely when $i = i'$ and $j = j'$, so

$$\langle\beta_{i'j'}|\beta_{ij}\rangle = \delta_{i'i}\delta_{j'j}.$$

So $\{|\beta_{ij}\rangle_{\mathsf{AB}} : i, j \in \{0, 1\}\}$ is an orthonormal basis for a two qubit Hilbert space. It is known as the **Bell basis**.

10.1.2 The dense coding protocol

Suppose Alice wishes to transmit a message of two bits $M = (M_1, M_2)$, $\mathcal{A}_M = \{0, 1\}^2$, $P_M(m) = 1/4$ for all m, to Bob by sending just one qubit. The definition of the Bell basis (10.2) suggests a way to do this if Alice and Bob already possess qubits A and B, respectively, in the state ϕ^+_{AB}:

1. Alice performs unitary $X^{M_1}_{\mathsf{A}} Z^{M_2}_{\mathsf{A}}$ on A. The state of AB is now $|\beta_{M_1M_2}\rangle\langle\beta_{M_1M_2}|_{\mathsf{AB}}$.

2. Alice sends the qubit A to Bob.

3. Bob measures in the Bell basis to decode the message. That is, Bob measures the POVM $E : \{0, 1\}^2 \to \mathcal{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ with $E(\,(i, j)\,) = |\beta_{ij}\rangle\langle\beta_{ij}|_{\mathsf{AB}}$ obtaining a result $\hat{M}$. Clearly, $\Pr(\hat{M} = M) = 1$.

10.1.3 The necessity of entanglement

Suppose Alice and Bob have systems A and B, respectively, in a state σ_{AB} and Alice wished to transmit a uniformly distributed message M to Bob by sending system A to him. The most general protocol has Alice perform some operation $\mathcal{N}(M)^{\mathsf{A}\leftarrow\mathsf{A}}$ on A depending on the message she wants to send, then send A to Bob, who measures a POVM $E : \mathcal{A}_M \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ whose result $\hat{M}$ is his estimate of the message. The probability of success is

$$\Pr(\hat{M} = M) = \sum_{m\in\mathcal{A}_M} P_M(m) \Pr(\hat{M} = m|M = m) \tag{10.4}$$

$$= \sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}E(m)_{\mathsf{AB}}\mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}} \otimes \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{B}}\sigma_{\mathsf{AB}}. \tag{10.5}$$

If σ_{AB} is separable, then

$$\sigma_{\mathsf{AB}} = \sum_x p(x)\mathcal{A}(x)_{\mathsf{A}} \otimes \beta(x)_{\mathsf{B}} \tag{10.6}$$

were p is a probability distribution and, for all x, $\alpha(x)$ and $\beta(x)$ are density operators. In this case,

$$\Pr(\hat{M} = M) = \sum_x p(x) \sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}E(m)_{\mathsf{AB}}(\mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}}\alpha(x)_{\mathsf{A}}) \otimes \beta(x)_{\mathsf{B}} \tag{10.7}$$

$$\leq \sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}_{\mathsf{AB}}E(m)_{\mathsf{AB}}(\mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}}\alpha(x^*)_{\mathsf{A}}) \otimes \beta(x^*)_{\mathsf{B}} \tag{10.8}$$

$$= \sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}_{\mathsf{A}}E'(m)_{\mathsf{A}}(\mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}}\alpha(x^*)_{\mathsf{A}}) \tag{10.9}$$

where x^* is the choice of x which maximises

$$\sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}E(m)_{\mathsf{AB}}(\mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}}\alpha(x)_{\mathsf{A}}) \otimes \beta(x)_{\mathsf{B}},$$

and E' is the POVM with

$$E'(m)_{\mathsf{A}} := \mathrm{Tr}_{\mathsf{B}}E(m)_{\mathsf{AB}}\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}}.$$

To see that this is a POVM we use a frequently useful fact about the partial trace

Proposition 1 (Partial trace cyclicity)**.** For any $J_{\mathsf{A}} \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$ and $L_{\mathsf{AB}} \in \mathcal{L}(\mathcal{H}_{\mathsf{AB}})$,

$$\mathrm{Tr}_{\mathsf{A}}J_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}L_{\mathsf{AB}} = \sum_i (\mathrm{Tr}J_{\mathsf{A}}G_{\mathsf{A}}^{(i)}) \otimes F_{\mathsf{B}}^{(i)} = \sum_i (\mathrm{Tr}G_{\mathsf{A}}^{(i)}J_{\mathsf{A}}) \otimes F_{\mathsf{B}}^{(i)} = \mathrm{Tr}_{\mathsf{A}}L_{\mathsf{AB}}J_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}$$

where we used the existence of a product basis for $\mathcal{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ to write $L_{\mathsf{AB}} = \sum_i G_{\mathsf{A}}^{(i)} \otimes F_{\mathsf{B}}^{(i)}$ for some (not necessarily positive or hermitian) operators $G_{\mathsf{A}}^{(i)}$ and $F_{\mathsf{B}}^{(i)}$.

Note that it is certainly *not* generally true that $\mathrm{Tr}_{\mathsf{A}}K_{\mathsf{AB}}L_{\mathsf{AB}} = \mathrm{Tr}_{\mathsf{A}}L_{\mathsf{AB}}K_{\mathsf{AB}}$. Using partial trace cyclicity we have, for all m,

$E'(m)_{\mathsf{A}} := \mathrm{Tr}_{\mathsf{B}}E(m)_{\mathsf{AB}}\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}} = \mathrm{Tr}_{\mathsf{B}}\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}}^{1/2}E(m)_{\mathsf{AB}}\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}}^{1/2}$ and hence $E'(m)_{\mathsf{A}} \geq 0$.

Also, $\sum_m E'(m)_{\mathsf{A}} = \mathrm{Tr}_{\mathsf{B}}(\sum_m E(m)_{\mathsf{AB}})\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}} = \mathrm{Tr}_{\mathsf{B}}\mathbb{1}_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}\mathbb{1}_{\mathsf{A}} \otimes \beta(x^*)_{\mathsf{B}} = \mathbb{1}_{\mathsf{A}}$, so E' is indeed a POVM.

Defining $\rho(m)_{\mathsf{A}} := \mathcal{N}(m)^{\mathsf{A}\leftarrow\mathsf{A}}\alpha(x^*)_{\mathsf{A}}$ we have

$$\Pr(\hat{M} = M) \leq \sum_{m\in\mathcal{A}_M} P_M(m)\mathrm{Tr}_{\mathsf{A}}E'(m)_{\mathsf{A}}\rho(m)_{\mathsf{A}}, \tag{10.10}$$

so there is a protocol where Bob measures only A which does as well as any protocol using a separable state σ_{AB}. In Example Sheet 1, Q. 13, you showed that in this situation, for a uniformly distributed message ($P_M(m) = 1/|\mathcal{A}_M|$), $\Pr(\hat{M} = M) \leq d_{\mathsf{A}}/|\mathcal{A}_M|$. So, if $M = 4$ and $d_{\mathsf{A}} = 2$ as in the superdense coding protocol, then without using entanglement, the success probability will be no more than one half.

10.2 The no-cloning theorem

Theorem 2 (The no-cloning theorem)**.** There is no "cloning operation" $\mathcal{C}^{\mathsf{QQ}'\leftarrow\mathsf{Q}}$ such that, for all state vectors $|\psi\rangle_{\mathsf{Q}}$,

$$\mathcal{C}^{\mathsf{QQ}'\leftarrow\mathsf{Q}}|\psi\rangle\langle\psi|_{\mathsf{Q}} = |\psi\rangle\langle\psi|_{\mathsf{Q}} \otimes |\psi\rangle\langle\psi|_{\mathsf{Q}'}$$

Proof. If $\mathcal{C}^{\mathsf{QQ}'\leftarrow\mathsf{Q}}$ is an operation, then there is an isometry $V \in \mathcal{L}(\mathcal{H}_{\mathsf{Q}}, \mathcal{H}_{\mathsf{Q}} \otimes \mathcal{H}_{\mathsf{Q}'} \otimes \mathcal{H}_{\mathsf{E}})$ such that $\mathcal{C}^{\mathsf{QQ}'\leftarrow\mathsf{Q}}|\psi\rangle\langle\psi|_{\mathsf{Q}} = \mathrm{Tr}_{\mathsf{E}}V|\psi\rangle\langle\psi|_{\mathsf{Q}}V^\dagger$. Since $\mathrm{Tr}_{\mathsf{E}}V|\psi\rangle\langle\psi|_{\mathsf{Q}}V^\dagger$ is supposed to be a pure state for any $|\psi\rangle_{\mathsf{Q}}$, we know (from the Schmidt decomposition) that $V|\psi\rangle_{\mathsf{Q}}$ must be a product state w.r.t. the QQ' / E bipartition, and should satisfy

$$V|0\rangle_{\mathsf{Q}} = |0\rangle_{\mathsf{Q}} \otimes |0\rangle_{\mathsf{Q}'} \otimes |\eta_0\rangle_{\mathsf{E}}, V|1\rangle_{\mathsf{Q}} = |1\rangle_{\mathsf{Q}} \otimes |1\rangle_{\mathsf{Q}'} \otimes |\eta_1\rangle_{\mathsf{E}} \tag{10.11}$$

for some $|\eta_0\rangle_{\mathsf{E}}$ and $|\eta_1\rangle_{\mathsf{E}}$, and, with $|+\rangle_{\mathsf{Q}} := \frac{1}{\sqrt{2}}(|0\rangle_{\mathsf{Q}} + |1\rangle_{\mathsf{Q}})$, we would like $V|+\rangle_{\mathsf{Q}}$ to be equal to $|+\rangle_{\mathsf{Q}} \otimes |+\rangle_{\mathsf{Q}'} \otimes |\eta_+\rangle_{\mathsf{E}}$, for some $|\eta_+\rangle_{\mathsf{E}}$. However, by (10.11) and the linearity of V, we have

$$V|+\rangle_{\mathsf{Q}} = \frac{1}{\sqrt{2}}(|0\rangle_{\mathsf{Q}} \otimes |0\rangle_{\mathsf{Q}'} \otimes |\eta_0\rangle_{\mathsf{E}} + |1\rangle_{\mathsf{Q}} \otimes |1\rangle_{\mathsf{Q}'} \otimes |\eta_1\rangle_{\mathsf{E}}). \tag{10.12}$$

This state is clearly not of the form that we require: In fact, the state of subsystem Q is the maximally mixed state, when it should be the pure state $|+\rangle\langle+|_{\mathsf{Q}}$! □

10.3 Teleportation

Suppose that Alice is given a system Q. She wants to transmit the state of Q to Bob, but she can only transmit classical information to him. The protocol has to work whatever the state of Q is, but Alice doesn't know which state it is.

Suppose Alice simply measures some POVM E on Q alone and sends the result M to Bob, who prepares a state $\sigma(M)_{\mathsf{B}}$. The overall operation $\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{Q}}$ takes states of Q to states of B is

$$\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{Q}} : \rho_{\mathsf{Q}} \mapsto \sum_{m\in\mathcal{A}_M} \sigma(m)_{\mathsf{B}}\mathrm{Tr}_{\mathsf{Q}}E(m)_{\mathsf{Q}}\rho_{\mathsf{Q}}.$$

An operation of this form is called a **measure-prepare operation**. The procedure works iff $\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{Q}} = \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{Q}}$. But if this were true, then Alice could copy the message M and send it to Bob (with system B) and Bertha (with system B') who could also prepare $\sigma(M)$. The operation from Q to $\mathsf{B}'\mathsf{B}$

$$\mathcal{C}^{\mathsf{B}'\mathsf{B}\leftarrow\mathsf{Q}} : \rho_{\mathsf{Q}} \mapsto \sum_{m\in\mathcal{A}_M} \rho(m)_{\mathsf{B}'} \otimes \rho(m)_{\mathsf{B}}\mathrm{Tr}_{\mathsf{Q}}E(m)_{\mathsf{Q}}\rho_{\mathsf{Q}}$$

would be a cloning operation, and we know that these don't exist!

10.3.1 Teleporting the state of a qubit

Suppose that $d_{\mathsf{Q}} = 2$ and that Alice and Bob start with qubits A and B, respectively, in the state ϕ^+_{AB}. Alice is given a qubit Q whose state she must transmit to Bob. Consider the following protocol:

- Alice measures the Bell basis PVM on QA obtaining a result $M = (M_1, M_2)$. To be precise, we mean the PVM with

$$E(\,(i,j)\,) = |\beta_{ij}\rangle\langle\beta_{ij}|_{\mathsf{QA}} = (X^i_{\mathsf{Q}} Z^j_{\mathsf{Q}} \otimes \mathbb{1}_{\mathsf{A}})\phi^+_{\mathsf{QA}}(Z^j_{\mathsf{Q}} X^i_{\mathsf{Q}} \otimes \mathbb{1}_{\mathsf{A}}). \tag{10.13}$$

- She sends M to Bob.
- Bob performs the unitary $X^{M_1}_{\mathsf{B}} Z^{M_2}_{\mathsf{B}}$ on his qubit.

We claim that the overall operation from Q to B is $\mathbf{id}^{\mathsf{B}\leftarrow\mathsf{Q}}$. Let's work out the state of B conditional on $M = (i,j)$, which we will call $\rho^{(i,j)}_{\mathsf{B}}$, immediately after Alice measures. To do this we will use the "transpose trick", which you were asked to prove in example sheet 1. A proof is given in the solutions for that sheet.

Proposition 3 (Transpose trick)**.** If $d_{\mathsf{Q}} = d_{\mathsf{R}}$ and $J_{\mathsf{Q}} \in \mathcal{L}(\mathcal{H}_{\mathsf{Q}})$ then

$$J_{\mathsf{Q}} \otimes \mathbb{1}_{\mathsf{R}} |\phi^+\rangle_{\mathsf{QR}} = \mathbb{1}_{\mathsf{Q}} \otimes J^T_{\mathsf{R}} |\phi^+\rangle_{\mathsf{QR}} \text{ where } J_{\mathsf{R}} = \mathbf{id}^{\mathsf{R}\leftarrow\mathsf{Q}} J_{\mathsf{Q}}. \tag{10.14}$$

Using the measurement postulate and the expression (10.13) we find

$$\begin{aligned}
\Pr(M=(i,j))\rho^{(i,j)}_{\mathsf{B}} =& \mathrm{Tr}_{\mathsf{QA}} E(\,(i,j)\,)_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} \rho_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} E(\,(i,j)\,)_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} && (10.15)\\
=& \mathrm{Tr}_{\mathsf{QA}} \rho_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} E(\,(i,j)\,)_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} && (10.16)\\
=& \mathrm{Tr}_{\mathsf{QA}} (Z^j_{\mathsf{Q}} X^i_{\mathsf{Q}} \rho_{\mathsf{Q}} X^i_{\mathsf{Q}} Z^j_{\mathsf{Q}}) \otimes \phi^+_{\mathsf{AB}} \phi^+_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} && (10.17)
\end{aligned}$$

Let J_{Q} be any operator on $\mathcal{H}_{\mathsf{Q}}$. Using the transpose trick twice we have

$$J_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} \phi^+_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} = \mathbb{1}_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} \mathbb{1}_{\mathsf{Q}} \otimes J^T_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}} \phi^+_{\mathsf{QA}} \otimes \mathbb{1}_{\mathsf{B}} = \mathbb{1}_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} \phi^+_{\mathsf{QA}} \otimes J_{\mathsf{B}} \tag{10.18}$$

where $J_{\mathsf{A}} := \mathbf{id}^{\mathsf{A}\leftarrow\mathsf{Q}} J_{\mathsf{Q}}$ and $J_{\mathsf{B}} := \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{Q}} J_{\mathsf{Q}}$. Futhermore, we note that

$$\mathrm{Tr}_{\mathsf{QA}} \mathbb{1}_{\mathsf{Q}} \otimes \phi^+_{\mathsf{AB}} \phi^+_{\mathsf{QA}} \otimes J_{\mathsf{B}} = \frac{1}{d_{\mathsf{A}}} \mathrm{Tr}_{\mathsf{A}} \phi^+_{\mathsf{AB}} \mathbb{1}_{\mathsf{A}} \otimes J_{\mathsf{B}} = \frac{1}{d_{\mathsf{A}} d_{\mathsf{B}}} J_{\mathsf{B}}.$$

Taking $J_{\mathsf{Q}} = Z^j_{\mathsf{Q}} X^i_{\mathsf{Q}} \rho_{\mathsf{Q}} X^i_{\mathsf{Q}} Z^j_{\mathsf{Q}}$ in (10.17) and using these facts we have

$$\Pr(M=(i,j))\rho^{(i,j)}_{\mathsf{B}} = \frac{1}{4} Z^j_{\mathsf{B}} X^i_{\mathsf{B}} \rho_{\mathsf{B}} X^i_{\mathsf{B}} Z^j_{\mathsf{B}},$$

so, for all $(i,j) \in \{0,1\}^2$, $\Pr(M=(i,j)) = 1/4$ and $\rho^{(i,j)}_{\mathsf{B}} = Z^j_{\mathsf{B}} X^i_{\mathsf{B}} \rho_{\mathsf{B}} X^i_{\mathsf{B}} Z^j_{\mathsf{B}}$. By applying the unitary operation, Bob always ends up with the state $\rho_{\mathsf{B}} = \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{Q}} \rho_{\mathsf{Q}}$ as described.