Exercise 1. ***Measurements and dephasing***

We will see how to write measurements using generalized Pauli operators. This helps us prove the uncertainty relation (1).

We saw that a mesurement described by a POVM $\{M_k\}_k$ corresponds to the following unitary evolution of the quantum system measured and a classical register,

$$|\text{ready to measure}\rangle\langle\text{ready to measure}| \otimes \rho \mapsto \sum_k |k\rangle\langle k| \otimes \sqrt{M_k}\rho\sqrt{M_k}^\dagger.$$

Tracing out the register, we obtain the map

$$\rho \mapsto \sum_k \sqrt{M_k}\rho\sqrt{M_k}^\dagger$$

on the quantum system.

(a) We start with the measurement of a single qubit. A measurement in the computational basis corresponds to the POVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and the evolution

$$\rho \mapsto |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|.$$

Show that the map above can also be written as

$$\rho \mapsto \frac{1}{2}\left(\rho + Z\rho Z^{-1}\right),$$

where Z is the Pauli-Z operator,

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Solution.

$$\begin{aligned} \rho + Z\rho Z^{-1} &= \rho + (|0\rangle\langle 0| - |1\rangle\langle 1|)\rho(|0\rangle\langle 0| - |1\rangle\langle 1|) \\ &= |0\rangle\langle 0|\rho|0\rangle\langle 0| + |0\rangle\langle 0|\rho|1\rangle\langle 1| + |1\rangle\langle 1|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1| \\ &\quad + |0\rangle\langle 0|\rho|0\rangle\langle 0| - |0\rangle\langle 0|\rho|1\rangle\langle 1| - |1\rangle\langle 1|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1| \\ &= 2(|0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|). \end{aligned}$$

(b) More generally, the measurement of a system of dimension d (like $\log d$ qubits) in an orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ can be described as a map

$$\rho \mapsto \sum_{k=0}^{d-1} |k\rangle\langle k|\rho|k\rangle\langle k|.$$

Show that this map can also be expressed as

$$\rho \mapsto \frac{1}{d}\sum_{n=0}^{d-1} Z^n \rho Z^{-n},$$

where Z is the generalized Pauli-Z operator,

$$Z = \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d}k}|k\rangle\langle k| = \begin{bmatrix} 1 & & & \\ & e^{\frac{2\pi i}{d}} & & \\ & & \ddots & \\ & & & e^{(d-1)\frac{2\pi i}{d}} \end{bmatrix}.$$

Solution. Exponentiating the generalized Pauli operator is straight-forward,

$$Z^n = \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} kn} |k\rangle\langle k|, \qquad Z^{-n} = \sum_{k=0}^{d-1} e^{-\frac{2\pi i}{d} kn} |k\rangle\langle k|.$$

We obtain

$$\begin{aligned}
\frac{1}{d}\sum_{n=0}^{d-1} Z^n \rho Z^{-n} &= \frac{1}{d}\sum_{n=0}^{d-1}\left(\sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} kn}|k\rangle\langle k|\right)\rho\left(\sum_{q=0}^{d-1} e^{-\frac{2\pi i}{d} qn}|q\rangle\langle q|\right)\\
&= \frac{1}{d}\sum_{n=0}^{d-1}\sum_{k,q=0}^{d-1} e^{\frac{2\pi i}{d}(k-q)n}\ |k\rangle\langle k|\rho|q\rangle\langle q|\\
&= \frac{1}{d}\left(\underbrace{\left[\sum_{n=0}^{d-1}\sum_{k=0}^{d-1}|k\rangle\langle k|\rho|k\rangle\langle k|\right]}_{k=q} + \underbrace{\left[\sum_{k\neq q}\left(\sum_{n=0}^{d-1} e^{\frac{2\pi i}{d}(k-q)n}\right)|k\rangle\langle k|\rho|q\rangle\langle q|\right]}_{k\neq q}\right)\\
&= \frac{1}{d}\left(\left[d\sum_{k=0}^{d-1}|k\rangle\langle k|\rho|k\rangle\langle k|\right] + \left[\sum_{k\neq q}\underbrace{\frac{-1+e^{2\pi i(k-q)}}{-1+e^{2\pi i(k-q)/d}}}_{=0,\text{ since } 0\neq k-q\in\mathbb{Z}/d}\ |k\rangle\langle k|\rho|q\rangle\langle q|\right]\right)\\
&= \sum_{k=0}^{d-1}|k\rangle\langle k|\rho|k\rangle\langle k|.
\end{aligned}$$

(c) Now we will see how to express a measurement in the complementary basis, $\{|\bar{k}\rangle\}$, with $|\bar{k}\rangle = F|k\rangle$. Here, F is the quantum Fourier transform, whose matrix representation is

$$F = \frac{1}{\sqrt{d}}\sum_{j,k=0}^{d-1} e^{\frac{2\pi i}{d}(jk)}|k\rangle\langle j|.$$

Note that F is unitary ($F^\dagger = F^{-1}$). A measurement in this basis corresponds to the map

$$\rho \mapsto \sum_{k=0}^{d-1}|\bar{k}\rangle\langle\bar{k}|\rho|\bar{k}\rangle\langle\bar{k}| = \sum_{k=0}^{d-1}\left(F|k\rangle\langle k|F^\dagger\right)\ \rho\ \left(F|k\rangle\langle k|F^\dagger\right).$$

Consider the generalized Pauli-X operator,

$$X = \left(\sum_{k=1}^{d-1}|k-1\rangle\langle k|\right) + |d-1\rangle\langle 0| = \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ 1 & & & 0\end{bmatrix}.$$

Show that we can write a measurement in the complementary basis as

$$\rho \mapsto \frac{1}{d}\sum_{n=0}^{d-1} X^n\rho X^{-n}.$$

Hint: start by showing that $X^n = FZ^nF^\dagger$.

Solution. We start with

$$\begin{aligned}
FZF^\dagger &= \left(\frac{1}{\sqrt{d}}\sum_{j,k=0}^{d-1} e^{\frac{2\pi i}{d}(jk)}|k\rangle\langle j|\right)\left(\sum_{q=0}^{d-1} e^{\frac{2\pi i}{d}q}|q\rangle\langle q|\right)\left(\frac{1}{\sqrt{d}}\sum_{j',k'=0}^{d-1} e^{-\frac{2\pi i}{d}(k'j')}|k'\rangle\langle j'|\right)\\
&= \frac{1}{d}\sum_{j,k=0}^{d-1}\sum_{q=0}^{d-1}\sum_{j',k'=0}^{d-1} e^{\frac{2\pi i}{d}[jk+q-j'k']}\ |k\rangle\langle j|q\rangle\langle q|k'\rangle\langle j'|\\
&= \frac{1}{d}\sum_{k=0}^{d-1}\sum_{q=0}^{d-1}\sum_{j'=0}^{d-1} e^{\frac{2\pi i}{d}[qk+q-j'q]}\ |k\rangle\langle j'|\\
&= \frac{1}{d}\sum_{k,j=0}^{d-1}\sum_{q=0}^{d-1} e^{2\pi i q\frac{k+1-j}{d}}\ |k\rangle\langle j|\\
&= \frac{1}{d}\left(\underbrace{\left[\sum_{j=0}^{d-1}\sum_{q=0}^{d-1}|j-1 \mod d\rangle\langle j|\right]}_{j=k+1 \mod d} + \underbrace{\left[\sum_{j\neq k+1\ldots}\left(\sum_{q=0}^{d-1} e^{2\pi i q\frac{k+1-j}{d}}\right)\ |k\rangle\langle j|\right]}_{j\neq k+1 \mod d}\right)\\
&= \frac{1}{d}\left(d\left[\sum_{j=0}^{d-1}|j-1 \mod d\rangle\langle j|\right] + \left[\sum_{j\neq k+1\ldots}\underbrace{\frac{-1+e^{2\pi i(k+1-j)}}{-1+e^{2\pi i(k+1-j)/d}}}_{=0,\text{ since } 0\neq k+1-j\in\mathbb{Z}/d}\ |k\rangle\langle j|\right]\right)\\
&= \sum_{j=0}^{d-1}|j-1 \mod d\rangle\langle j| = X.
\end{aligned}$$

The exponentiated version of this transformation is simply

$$\begin{aligned}
X^n &= (FZF^\dagger)(FZF^\dagger)\ldots(FZF^\dagger)\\
&= FZ\underbrace{F^\dagger F}_{\mathbb{1}}Z\underbrace{F^\dagger F}_{\mathbb{1}}\ldots\underbrace{F^\dagger F}_{\mathbb{1}}ZF^\dagger\\
&= FZ^nF^\dagger,
\end{aligned}$$

because F is unitary. The post-measurement state is given by

$$\begin{aligned}
\sum_{k=0}^{d-1}|\bar{k}\rangle\langle\bar{k}|\rho|\bar{k}\rangle\langle\bar{k}| &= \sum_{k=0}^{d-1}\left(F|k\rangle\langle k|F^\dagger\right)\ \rho\ \left(F|k\rangle\langle k|F^\dagger\right)\\
&= F\left(\sum_{k=0}^{d-1}|k\rangle\langle k|(F^\dagger\rho F)|k\rangle\langle k|\right)F^\dagger\\
&= F\left(Z^n(F^\dagger\rho F)Z^{-n}\right)F^\dagger\\
&= \sum_{n=0}^{d-1}\left(FZ^nF^\dagger\right)\rho\left(FZ^{-n}F^\dagger\right)\\
&= \sum_{n=0}^{d-1}X^n\rho X^{-n}.
\end{aligned}$$

Exercise 2. *Entropic uncertainty relations*

In the lecture, we proved an entropic uncertainty relation for complementary observables X and Z on a single qubit A, conditioned on side information B.

(a) Generalize the proof of the uncertainty relation for an abritrary quantum system A, and complementary observables X and Z, obtaining

$$H(X|B) + H(Z|B) \geq \log|A| + H(A|B). \tag{1}$$

Hint: follow the proof from the lecture, and use the result from Exercise 1.

Solution. [I am changing the notation from the lecture; namely, the names of subsystems are different.]

Consider a system AB in initial state ρ_{AB}. A measurement

(b) Use this relation to prove the Maassen-Uffink relation for complementary observables,

$$H(X) + H(Z) \geq \log|B|. \tag{2}$$

Solution. If system B is trivial, we can write $\rho_{AB} = \rho_A \otimes |0\rangle\langle 0|_B$. In this case, B does not give us any extra information about the state of A: $H(A|B)_{\rho_A \otimes \sigma_B} = H(A)_{\rho_A}$. Recall that the non-conditioned von Neumann entropy cannot be negative, $H(A)_\rho \geq 0$.

Note that in the formulation of (1) it is implicit that there is a map $\mathcal{E}_{A\to Z}$ that corresponds to the measurement in a basis (Z), and a map $\mathcal{F}_{A\to X}$ that corresponds to the measurement in the complementary basis (X). In other words, the entropy $H(Z|B)$ is evaluated on state $\mathcal{E}_{A\to Z} \otimes \mathcal{I}_B\ (\rho_{AB})$.

Finally, note that

$$\mathcal{E}_{A\to Z} \otimes \mathcal{I}_B\ (\rho_A \otimes |0\rangle\langle 0|_B) = \mathcal{E}_{A\to Z}(\rho_A) \otimes |0\rangle\langle 0|_B.$$

We have

$$\begin{aligned}
H(X|B)_{\mathcal{F}_{A\to X}\otimes\mathcal{I}_B(\rho_A\otimes|0\rangle\langle 0|_B)} + H(Z|B)_{\mathcal{E}_{A\to Z}\otimes\mathcal{I}_B(\rho_A\otimes|0\rangle\langle 0|_B)} &\geq \log|A| + H(A|B)_{\rho\otimes|0\rangle\langle 0|_B} \Leftrightarrow \\
H(X|B)_{\mathcal{F}_{A\to X}(\rho_A)\otimes|0\rangle\langle 0|_B} + H(Z|B)_{\mathcal{E}_{A\to Z}(\rho_A)\otimes|0\rangle\langle 0|_B} &\geq \log|A| + H(A|B)_{\rho\otimes|0\rangle\langle 0|_B} \Leftrightarrow \\
H(X)_{\mathcal{F}_{A\to X}(\rho_A)} + H(Z)_{\mathcal{E}_{A\to Z}(\rho_A)} &\geq \log|A| + H(A)_{\rho_A} \\
&\geq \log|A|.
\end{aligned}$$

By the way, this relation is the reason why we sometimes call these two bases (computational and complementary) the Z and X bases, respectively.

Exercise 3. *The uncertainty game*

We will see a "practical" application of the entropic uncertainty relation (1). Consider the following setting: two players, Alice and Bob, sit in separate labs. Bob sends one qubit to Alice, she performs one of two measurements (X or Z) at random, and then tells Bob her choice of measurement. Now Bob has to guess the output of Alice's measurement.

(a) Suppose that Bob only has a classical memory (like a notepad) in his lab. What is his best strategy? What is the state of the qubit he should send to Alice, and what is his uncertainty about the measurement outcome?

Solution. First let's apply the uncertainty relation to see how well Bob can perform. The best he can do is to prepare a qubit in a pure state, send it to Alice, and keep a record of the state he sent (sending Alice a mixed state is equivalent to forgetting exactly what pure state he sent her, which cannot help him). The joint state of the qubit he sends to Alice, A, and his notebook, B, is $|\psi\rangle_A|\text{“}\psi\text{”}\rangle_B$, and the entropy $H(A|B) = 0$. We get

$$\begin{aligned}
H(X|B) + H(Z|B) &\geq \log|A| + H(A|B) \\
&= 1 + 0.
\end{aligned}$$

This tells us that Bob will always have one bit of uncertainty about Alice's measurement outcome. For example, suppose that he sends state $|0\rangle$ to Alice. If Alice chooses to measure in the Z basis, then he knows the outcome of her measurement: it has to be 0. However, if Alice picks the X basis, $\{|+\rangle, |-\rangle\}$, she could get each outcome with equal probability, and Bob cannot predict it. In this example, we have $H(Z|B) = 0$ and $H(X|B) = 1$, which shows that this choice of initial state is optimal for the purpose of minimizing $H(X|B) + H(Z|B)$.

Just for fun, we can compute Bob's probability of guessing the outcome correctly: it's 1 if Alice picks Z (which happens with probability 1/2), and 1/2 if Alice picks X (which happens with probability 1/2), because in this case he may as well try a random guess. His total probability of guessing correctly is 3/4.

(b) Now imagine that Bob has a quantum memory: he can prepare two qubits in any state, send one to Alice and keep the other. What should he do now, and how frequently will he guess correctly?

Solution. In this case, Bob can prepare two qubits in a maximally entangled state, $(|00\rangle + |11\rangle)/\sqrt{2}$, and send one to Alice. After Alice tells him the measurement basis, he only needs to measure his qubit in the same basis to obtain the same outcome.

We can demonstrate this explicitly. When Alice measures in basis Z, the POVM elements are $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Let's call A Alice's qubit, A' Alice's classical register (which saves the measurement outcome), B Bob's qubit, and B' Bob's register.

The initial state of the four systems is

$$|\text{ready to measure}\rangle_{A'} \otimes \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \otimes |\text{ready to measure}\rangle_{B'}$$

After Alice measures her qubit A, the global state becomes

$$\begin{aligned}
&\sum_{k=0}^{1} |k\rangle\langle k|_{A'} \otimes \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B \otimes \mathbb{1}_{B'}\right) \left(\frac{(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)}{2} \otimes |\text{ready}\rangle\langle\text{ready}|_{B'}\right) \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B \otimes \mathbb{1}_{B'}\right) \\
&= \sum_{k=0}^{1} |k\rangle\langle k|_{A'} \otimes \frac{|kk\rangle\langle kk|_{AB}}{2} \otimes |\text{ready}\rangle\langle\text{ready}|_{B'}.
\end{aligned}$$

If now Bob measures his qubit B in the same basis, the global state evolves to

$$\begin{aligned}
&\sum_{q=0}^{1} \left(\mathbb{1}_{A'} \otimes \mathbb{1}_A \otimes |q\rangle\langle q|_B\right) \left(\sum_{k=0}^{1} |k\rangle\langle k|_{A'} \otimes \frac{|kk\rangle\langle kk|_{AB}}{2}\right) \left(\mathbb{1}_{A'} \otimes \mathbb{1}_A \otimes |q\rangle\langle q|_B\right) \otimes |q\rangle\langle q|_{B'} \\
&= \sum_{k=0}^{1} |k\rangle\langle k|_{A'} \otimes \frac{|kk\rangle\langle kk|_{AB}}{2} \otimes |k\rangle\langle k|_{B'} \\
&= \frac{1}{2} \sum_{k=0}^{1} |\phi_k\rangle\langle\phi_k|, \qquad |\phi_k\rangle = |k\rangle_{A'} |k\rangle_A |k\rangle_B |k\rangle_{B'},
\end{aligned}$$

so the outcome in Bob's register is always the same as Alice's.

What if Alice measures her qubit in the X basis, $\{|+\rangle, |-\rangle\}$? We can write the initial state of the two qubits in this basis,

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) &= \frac{1}{\sqrt{2}} \left(\frac{|+\rangle + |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle + |-\rangle}{\sqrt{2}} + \frac{|+\rangle - |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle - |-\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2\sqrt{2}} \left(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle + |++\rangle - |+-\rangle - |-+\rangle + |--\rangle\right) \\
&= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \\
&= \frac{1}{\sqrt{2}} \sum_{k=+,-} |kk\rangle.
\end{aligned}$$

Since the POVM elements of a measurement in the X basis are precisely $\{|+\rangle\langle +|, |-\rangle\langle -|\}$, the previous result applies, and the final state after Alice and Bob's measurements is

$$\frac{1}{2} \sum_{k=+,-} |\psi_k\rangle\langle\psi_k|, \qquad |\psi_k\rangle = |k\rangle_{A'} |k\rangle_A |k\rangle_B |k\rangle_{B'},$$

which means again that Bob's register always shows the same output as Alice's.

In short, the post-measurement state of the two qubits after Alice's measurement, conditioned on Alice's outcome, is

Alice's outcome	X	Z
0 (+)	$\|{++}\rangle$	$\|00\rangle$
1 (−)	$\|{--}\rangle$	$\|11\rangle$

.

Applying the uncertainty relation to the initial, maximally entangled, state gives us

$$\begin{aligned}
H(X|B) + H(Z|B) &\geq \log|A| + H(A|B) \\
&= 1 - 1 = 0.
\end{aligned}$$