2. An example of non-composable "qubit": Remote state preparation
   Setting: given qubits & qubits.
   Task: Alice wants to transmit pure quantum state \( |\psi\rangle \)
       that she "authors" (not just forwarding).

   Qn: Can her knowledge of \( |\psi\rangle \) save communication
       (relative to teleportation)?

   / insufficient method, but other did not applicable!

   Caution: Transmission need not be a TCP map on \( |x\rangle \langle y| \).
   eg, Alice teleports \( |x_0\rangle \).

   Initially a curiosity, but finds app in cheaper q. encryption
   and communication complexity as well.
Check if students are familiar with this result.

Lemma: If Alice and Bob share $|\psi_0\rangle = \frac{1}{\sqrt{d+1}} \sum_{i=0}^{d} |i\rangle$, and Alice applies measurement with POVM $\{A_k\}$.

Then conditioned on getting outcome $k$, Bob's state is $\frac{M_k^T}{\text{Tr}M_k}$. 
Example in 1699:

- Alice & Bob share 1 qubit: $|\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$

- Alice comes up with $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{R}$

- Define a POVM $\{M_0, M_1\}$, $M_0 = 14 \times 14^T$, $M_1 = I - M_0$

Alice applies the measurement on $A$.

From Lemma:

If outcome is "0", then Bob has $14 \times 14^T$

"1", I - $14 \times 14^T = 14^T \times 14^L$

where $14^L = -b|0\rangle + a|1\rangle$

- Alice sends the measurement outcome $K$ to Bob.

- Bob applies $I$ or $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ for $K = 0, 1$ resp.

- Either case output $\psi^+ = |\psi\rangle$

So "one qubit" sent with 1 qubit & 1 qubit!
Why this example does not contradict optimality of RSP?

1. Protocol not working $V_{14} \neq C^2$
   
   But this can be resolved!

2. When discussing “qbits”, sender’s operations are “oblivious”
   - independent of the state to be sent
   - that info is NOT accessible given a specimen

3. Only works for pure states, not part of a state
   potentially entangled with a reference system not
   in Alice’s possession. RSP does not create “good enough”
   qbits. So optimality of TP (coming from (3) which
   applies only to computationally good qbits) does not apply.
How much communication is needed for RSP of ANY $|w| \in G^d$?

- Exact case: unresolved in general
- Exact case: if $|w| \in G^d$ is also "oblivious" to Bob, meaning that he receives no more info about $|w|$ beyond a single specimen, then $2 \log d$ bits are needed. (Li, Shor 02)
- Exact case: if Bob's decoding is restricted to Pauli operators, then $2 \log d$ bits needed. (Nayak).

- Approx case: $\approx \log d$ bits suffice.

Idea similar to Lo 99.
Idea for approx RSP:

Recall:

\[ |\psi\rangle \rightarrow |\psi\rangle \quad \text{measurement test depends on } \psi \]

\[ |\psi\rangle \rightarrow |U_k\rangle \rightarrow |\psi\rangle \quad \text{if measurement outcome } = k \]

Necessary condition for RSP:

\[ \exists U_k, \rho_k \text{ s.t. } |1^d\rangle \in \rho_k^d, \sum_{k \in \mathbb{C}} \rho_k U_k^\dagger |1^d\rangle U_k = |1^d\rangle \]

Also sufficient by choosing \( M_k = [U_k 1^d U_k^\dagger + \rho_k] \)

But \( \bullet \) gives an encryption scheme as \( d^2 \) terms necessary.

So no gain over teleportation.

Surprise: \( \bullet \) can be relaxed to give approx RSP & approx encryption where \# terms \( \approx O(d^2) \)!
In BHLSWo3: for large $d$,

\[ \exists t \text{ unitaries } U_k \in U(C^d) \]

s.t. \[ \forall 1 \leq k \leq d \],

\[ \| \frac{1}{t} \sum_{k=1}^{d} U_k|y_k\rangle \langle y_k^*| U_k^* \|_F \leq \frac{\epsilon}{d} \]

where \[ t = \frac{134 \cdot \log d}{\epsilon^2} \].

NB: $t$ reduced to \[ \frac{150 \cdot \log (\frac{d}{\epsilon})}{\epsilon^2} \].

Proof idea:

Consider $U_1|y_1\rangle \langle y_1^*| U_1^*$ as an operator-valued RV

and ask how quickly $t$ samples $U_k|y_k\rangle \langle y_k^*| U_k^*$

have empirical average \[ \frac{1}{t} \sum_{k=1}^{d} U_k|y_k\rangle \langle y_k^*| U_k^* \]

converging
to the theoretical average \[ \frac{\epsilon}{d} \].

Actual proof: a little technical. Possible term project.

NB \[ \epsilon \leftrightarrow \epsilon \]

\[ \frac{1}{t} \sum_{k=1}^{d} U_k|y_k\rangle \langle y_k^*| U_k^* \|_F \leq \frac{1+\epsilon}{d} \]
Consequences of (**):

1. RSP of any $(y) \in C^d$ can be done with prob $\geq 1 - \varepsilon$
   with log $d$ bits and log $t = \log d + \frac{1}{\varepsilon}$ bits.

   Pf: Choose $M_k = \frac{1}{1+\varepsilon} \cdot \frac{d}{t} \left( U_k \cdot (1 + \varepsilon) U_k^t \right)^t$

   Then $\sum_{k=1}^{t} M_k^T \preceq \frac{1}{1+\varepsilon} \cdot \frac{d}{t} \sum_{k=1}^{t} U_k \cdot (1 + \varepsilon) U_k^t \preceq \frac{1}{1+\varepsilon} \cdot \frac{d}{t} \cdot \frac{1+\varepsilon}{d} \leq 1$

2. Let $M_{t+1} = I - \sum_{k=1}^{t} M_k \succeq 0$

   $\{M_k\}_{k=1}^{t+1}$ is $\Phi VM$.

Bob can decode if out come $K \neq t+1$.

$\text{Prob} (K = t+1) = \text{Tr} \left( M_{t+1} \cdot \frac{\frac{d}{t}}{d} \right)$

Alice's reduced state

$$= \text{Tr} \left( \left( I - \frac{\varepsilon}{d} M_k \right) \cdot \frac{d}{t} \right)$$

Each has trace $\frac{d}{t} \cdot \text{Tr} (U_k U_k^t) = 1 - \frac{\varepsilon}{1+\varepsilon}$

$$\geq \varepsilon^{1+\varepsilon} \leq \varepsilon.$$
NB: This RSP scheme is &-close to exact.

Almost oblivious to Bob:

Given $k=1, 2, \ldots, t$, he has $M_k \oplus x_k \oplus \mu_k^t$

Each $k$ occurs equally probably, indep. of $M_k$.

Note though if $k=t+1$, $M_{t+1}$ has a small
dependence on $x_t$. This is the only place
Leung-Shor 02 did not apply!

The PVM on
\[ \begin{array}{c}
\sum \frac{1}{t+1} = k \\
\end{array} \]

Cannot be constructed!

Cannot change RSP to a teleportation-like protocol

Alice's ob's do not depend on $x_t$

Preserves ent w/ any reference sites

Can be composed \ldots

Requires 2log $d$ bits.

Alice's ob's depend on $y_t$.

Preserves ent w/ any reference sites.
2) Approx encryption of \( \mathbb{H} \in \mathbb{C}^d \) can be done

with \( \log d + \ell(\varepsilon) \) key bits.

\[ \widetilde{PH} = \frac{1}{t} \sum_{k=1}^{t} \text{vec}(U_k)^* U_k \quad \text{s.t.} \quad \frac{1}{2} \| A_k \|_2 \leq \frac{\varepsilon}{d} \]

Then

\[ \| A \|_2 \leq \varepsilon \]

If the key \( k \) has \( \| k \| = \frac{\varepsilon}{2} \), and \( E_k(\cdot) = U_k \cdot U_k^* \)

\( D_k(\cdot) = U_k^2 - U_k \cdot U_k \)

Then Eve sees the state \( \frac{1}{t} \sum_{k=1}^{t} U_k(1 \cdot 1 k) U_k^* \)

which has 1-norm distance \( \leq \varepsilon \) from \( \frac{\varepsilon}{d} \).

She can't tell which state she has \( \| w_p \| \geq \frac{1}{2} + \frac{\varepsilon}{4} \).

**NB:** Exact BGN.

\[ \begin{array}{cccc}
R & \downarrow & \uparrow & B \\
A \downarrow U_k & & & U_k^2 \\
1P & \uparrow & S & 1P
\end{array} \]

\[ \text{So protect against eavesdropping by doubling the side to } k \rightarrow k, k'. \]
Approx.

14) \( A \frac{\mathbf{U}_k}{\mathbf{U}_k^*} \rightarrow \mathbb{C} \)

In fact if we apply approx 2 to part of an ent state:

\[ \text{State is rank } k \approx \frac{150}{d^2} \log(\frac{1}{\varepsilon}) \]

Very different from \( k \).

Info about \( k \) and \( 14 \) may be leaked.

Conclusion: the \( 2 \) (and key bits required for)

Gives classical

more one may have purification\( \rightarrow \)


decomposite transmitted system from

its purification. logod key bits suff for

or states that are pure or whose purification is NOT

with one.
(3) First example showing that, for \( R_o, R_i \) TCP maps,
\[
\| R_o(14 \times 41) - R_i(14 \times 41) \|_1 \leq \varepsilon
\]

Need not imply \( R_o \approx R_i \).

\[
F_i = R_o(y) = \frac{1}{t} \sum_{k=1}^{t} \text{mc } P \text{ } X_k^t
\]

\[
R_i(y) = \frac{3}{2}
\]

NB: if one of \( R_o, R_i \) \( \approx \) identity map,

then \( \| R_o(14 \times 41) - R_i(14 \times 41) \|_1 \leq \varepsilon \implies R_o \approx R_i \)
Additional note: SP of known quantum state

If Alice knows of a \( d^2 \)-bin pure quantum state \( |\psi\rangle \), and Alice & Bob share \( \log d \) ebits,

Bob can receive \( |\psi\rangle \) in his laboratory (with fidelity \( \geq 1-2\Delta^2 \)).

If Alice transmits \( \log d + 2.5 \log \log d + 2.5 \log d + \log 1753 \)

Detail: 0307221, 6407049, A1

NB: Q states known to the sender can behave rather classically.