(2) An example of non-composable "qbit" : remote state preparation

Setting : given ebits & cbits.

Task: Alice wants to transmit <u>pure</u> quantum state $|\psi\rangle$ that she "authors" (not just forwarding)

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

↳ sufficient method, but lower bd <u>not applicable</u>!

- Caution: transmission need not be a TCP map on $|\psi\rangle\langle\psi|$.
  eg Alice teleports $|\psi\rangle^{\otimes 2}$.

- 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 & Bob share $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$

and Alice applies meas with POVM $\{M_k\}$.

Then conditioned on getting outcome k

Bob's state is $\frac{M_k^T}{\mathrm{Tr}\, M_k}$.

Example in Lb 99 :

- Alice & Bob share 1 ebit $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$
- Alice comes up with $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{R}$
- Define a POVM $\{M_0, M_1\}$, $M_0 = |\psi\rangle\langle\psi|^T$, $M_1 = I - M_0$

  Alice applies the meas on A.

- From lemma :

  If outcome is "0" , then Bob has $|\psi\rangle\langle\psi|$

  . . . . "1" , ... $I - |\psi\rangle\langle\psi| = |\psi^\perp\rangle\langle\psi^\perp|$

  where $|\psi^\perp\rangle = -b|0\rangle + a|1\rangle$.

- Alice sends the 1-bit 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 $= |\psi\rangle$

So "one qubit" sent with 1 ebit & 1 cbit !

Why this example does not contradict optimality of RSP?

① Protocol not working $\forall |\psi\rangle \in \mathbb{C}^2$

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 comparably good qbits) does not apply.

How much communication is needed for RSP of <u>ANY</u> $|\psi\rangle \in \mathbb{C}^d$?

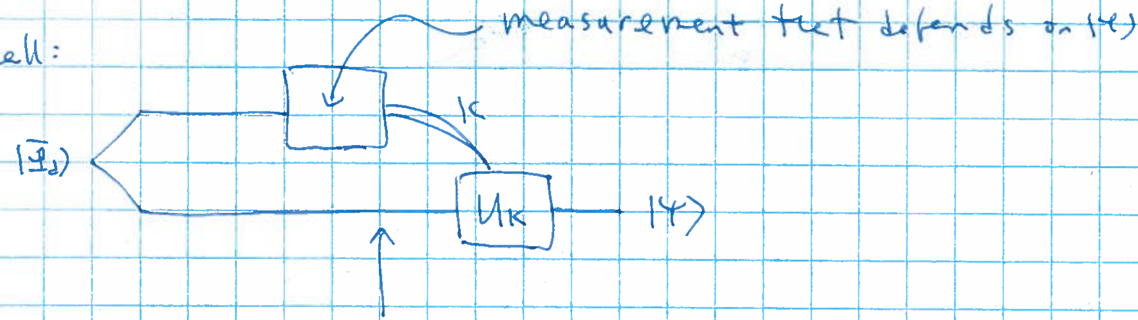
- Exact case: unresolved in general
- Exact case: If protocol is also "oblivious" to Bob, meaning that he receives no more info about $|\psi\rangle$ beyond a single specimen, then $2\log d$ cbits are needed (L, Shor 02)
- Exact case: if Bob's decoding is restricted to Pauli operations, then $2\log d$ cbits needed. (Nayak).

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

  Idea similar to Lo 99.

Idea for approx RSP:

Recall:



$U_k^\dagger |\psi\rangle\langle\psi| U_k$ if measurement outcome $= k$

Necessary condition for RSP:

$$\exists\, U_k, p_k \ \text{ s.t. } \ \forall |\psi\rangle \in \mathbb{C}^d, \quad \sum_k p_k U_k^\dagger |\psi\rangle\langle\psi| U_k \overset{(*)}{=} \frac{I}{d}.$$

Also sufficient by choosing $M_k = \left[d\, p_k\, U_k^\dagger |\psi\rangle\langle\psi| U_k\right]^T$.

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

So no gain over teleportation.

Surprise: (*) can be relaxed to give approx RSP & approx Q encryption where # terms $\approx O(d)$!

In BHLSW03: for large d.

$\exists\, t$ unitaries $U_k \in \mathcal{U}(\mathbb{C}^d)$

s.t. $\forall\, |\psi\rangle \in \mathbb{C}^d$, $\quad \left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$ (**)

where $t = \frac{134\, d \log d}{\varepsilon^2}$.

NB: t reduced to $\frac{150\, d}{\varepsilon^2} \log\left(\frac{1}{\varepsilon}\right)$. [Aubrun08]

Proof idea:

Knowing that $\int \underbrace{dU}_{\text{Haar meas}} \; U |\psi\rangle\langle\psi| U^\dagger = \frac{I}{d}$

Consider $U|\psi\rangle\langle\psi|U^\dagger$ as an operator-value RV

and ask how quickly t samples $U_k|\psi\rangle\langle\psi|U_k^\dagger$

have empirical average $\sum_k U_k|\psi\rangle\langle\psi|U_k^\dagger$ converging

to the theoretical average $\frac{I}{d}$?

Actual proof: a little technical. Possible term project.

NB (**) $\Leftrightarrow$ $\left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger \right\|_\infty \leq \frac{1+\varepsilon}{d}$

Consequences of (**):

(1) RSP of any $|\psi\rangle \in \mathbb{C}^d$ can be done with prob $\geq 1-\varepsilon$ with $\log d$ ebits and $\log t \approx \log d + f(\varepsilon)$ cbits.

Pf: choose $M_k = \frac{1}{1+\varepsilon} \cdot \frac{d}{t} \left(U_k |\psi\rangle\langle\psi| U_k^+ \right)^T$

Then $\sum_{k=1}^{t} M_k^T = \frac{1}{1+\varepsilon} \cdot d \cdot \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^+$

$\left\| \sum_{k=1}^{t} M_k^T \right\|_\infty \leq \frac{1}{1+\varepsilon} \cdot d \cdot \frac{1+\varepsilon}{d} \leq 1$

$\therefore$ Let $M_{t+1} = I - \sum_{k=1}^{t} M_k \geq 0$

$\therefore \{M_k\}_{k=1}^{t+1}$ is a POVM.

Bob can decode if outcome $k \neq t+1$.

$\text{Prob}(k=t+1) = \text{tr}\left(M_{t+1} \times \frac{I}{d} \right)$

Alice's reduced state

$= \text{tr}\left[\left(I - \sum_{k=1}^{t} M_k \right) \frac{I}{d} \right]$

each has trace $\frac{d}{(1+\varepsilon)t}$

$= \text{tr}\left(\frac{I}{d}\right) - \text{tr}\, \frac{1}{d} \sum_{k=1}^{t} M_k = 1 - \frac{1}{1+\varepsilon}$

$= \varepsilon/1+\varepsilon \leq \varepsilon.$

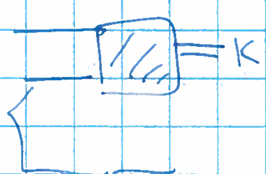
NB: This RSP scheme is ε-close to exact.

Almost oblivious to Bob:

Given $K = 1, 2, \ldots t$, he has $M_K |\psi\rangle\langle\psi| M_K^\dagger$

each K occurs equiprobably, indep of $|\psi\rangle$.

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

The POVM on 

cannot be constructed!

Cannot change RSP to a teleportation-like protocol

RSP:

Alice op's depend on $|\psi\rangle$

Pure state only

$\Downarrow$

* log d cbits suffices.

Teleportation-like protocol:

Alice op's do not depend on $|\psi\rangle$

Preserves ent w/ any reference sys

Can be composed ...

$\Downarrow$

* Requires 2 log d cbits.

(2) Approx encryption of $|\psi\rangle \in \mathbb{C}^d$ can be done with $\log d + f(\varepsilon)$ key bits.

Pf: If $\left\| \frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger - \frac{I}{d} \right\|_\infty \leq \frac{\varepsilon}{d}$

then $\| \quad \cdots\cdots \quad \|_1 \leq \varepsilon$

If the key k has $p_k = \frac{1}{t}$, and $E_k(\cdot) = U_k \cdot U_k^\dagger$

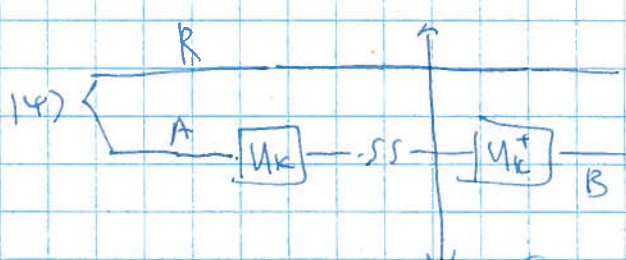
$D_k(\cdot) = U_k^\dagger \cdot U_k$

then Eve sees the state $\frac{1}{t} \sum_{k=1}^{t} U_k |\psi\rangle\langle\psi| U_k^\dagger$

which has 1-norm distance $\leq \varepsilon$ from $\frac{I}{d}$.

She can't tell which state she has wp $\geq \frac{1}{2} + \frac{\varepsilon}{4}$.

NB: Exact QEnc:

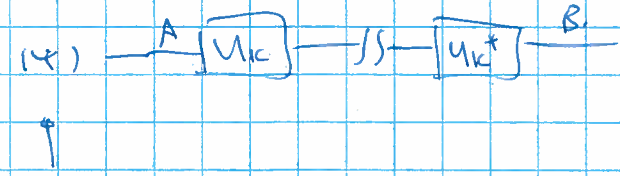


Needed for building 'P' into composition

$\rightarrow$ state $= \left(\mathrm{tr}_A |\psi\rangle\langle\psi| \right)_R \otimes \rho_0$

So protect against eavesdropper hold side info R.

Approx Enc:

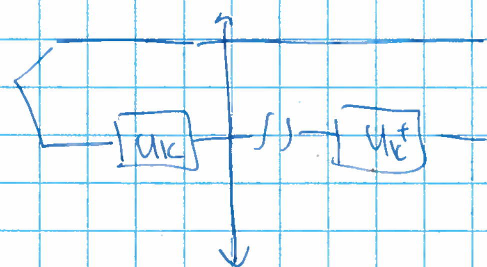


pure state, no side info

no sys correlated with it.

$\approx \log d$ key bits sufficient.

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



say $|\psi\rangle$.

State is rank $t \approx \frac{150\, d}{\varepsilon^2} \log(\frac{1}{\varepsilon})$.

Very diff from $\frac{I}{d}$.

Info about k and $|\psi\rangle$ may be leaked.

not Q vs classical

more Enc may have purification vs Enc not have purification

Conclusion: the $\underline{2 \log d}$ key bits requirement for encrypting q. states come from the need to <u>decorrelate</u> transmitted system from its purification. $\log d$ key bits suff for q states that are pure nor whose purification is <u>NOT</u> with Enc.

(3) first example showing that, for R_0, R_1 TCP maps,

$$\| R_0(|\psi\rangle\langle\psi|) - R_1(|\psi\rangle\langle\psi|) \|_1 \leq \varepsilon$$

Need not imply $R_0 \approx R_1$.

Pf: $R_0(\rho) = \frac{1}{t} \sum_{k=1}^{t} U_k \rho U_k^+$

$R_1(\rho) = \frac{I}{d}$.

NB: if one of $R_0, R_1 \approx$ identity map,

then $\| R_0(|\psi\rangle\langle\psi|) - R_1(|\psi\rangle\langle\psi|) \|_1 \leq \varepsilon \Rightarrow R_0 \approx R_1$

Additional note: SP of known quantum state

If Alice knows of a d^2-dim pure quantum state $|\Psi\rangle$,

and Alice & Bob share $\log d$ ebits,

Bob can receive $|\Psi\rangle$ in his laboratory (with fidelity $\geq 1-2\sqrt{\alpha}$)

If Alice transmits $\log d + 2.5 \log\log d + 2.5 \log(\frac{1}{\alpha}) + \log 1753$

Detail: 0307221, 0407049, AI

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