Maximum privacy without coherence, zero-error

arXiv:1509.01300

Debbie Leung[1] and Nengkun Yu[1,2,3]

Zero-error Information, Operators, and Graphs

Taipei, August 29, 2016

1: University of Waterloo

2: University of Technology Sydney

3: University of Guelph

Result:

$\exists$ family of channels N_d w/ input dim d^2, quantum output dim d, and with $P_0(N_d) = \log d$ and $Q_0(N_d) = 0$.

Zero-error private capacity

Zero-error quantum capacity

Result:

$\exists$ family of channels N_d w/ input dim d^2, quantum output dim d,

and with $P_0(N_d) = \log d$ and $Q_0(N_d) = 0$.

Zero-error private capacity

Zero-error quantum capacity

log d max given the quantum output dim

can't be less 0

max difference

Prior work (L, Li, Smith, Smolin 2014):

$\exists$ family of channels N_d w/ input dim d^2, quantum output dim d,

and with $P(N_d) = \log d$ and $Q(N_d) < 1$.

regular
private capacity

transmission
happens to be ZE

regular
quantum capacity

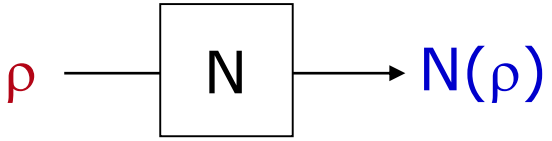
lower bounded
by ≈ 0.6

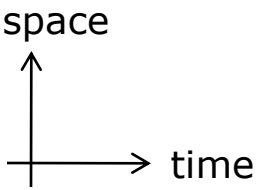
Our contribution: showing $Q_0(N_d) = 0$.

Noisy quantum channels

input from
sender Alice

output to
receiver Bob

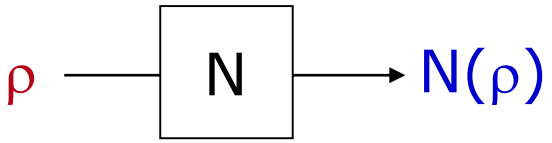


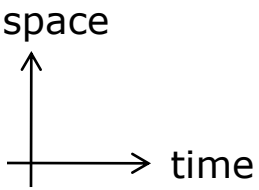


Noisy quantum channels

input from
sender Alice

output to
receiver Bob





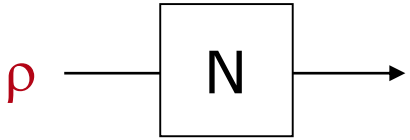
Linear, trace-preserving, completely positive

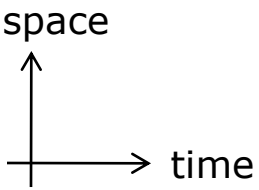
Most general evolution (as long as the quantum system has no prior correlation with the environment)

Noisy quantum channels

input from
sender Alice

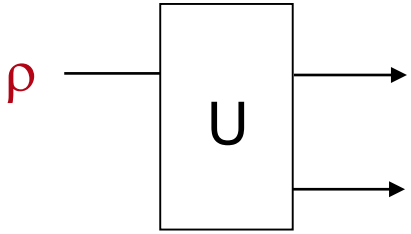
output to
receiver Bob





input from
sender Alice

output to
receiver Bob

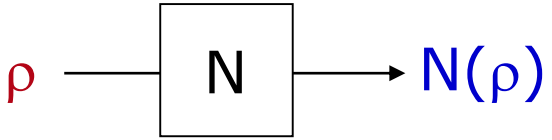


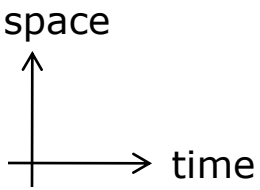
leakage to
environment Eve

Noisy quantum channels

input from sender Alice

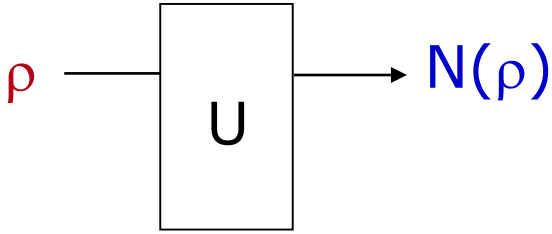
output to receiver Bob





input from sender Alice

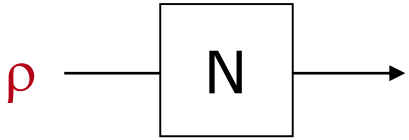
output to receiver Bob

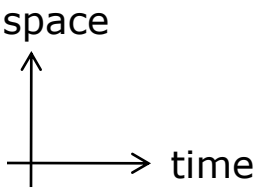


Noisy quantum channels

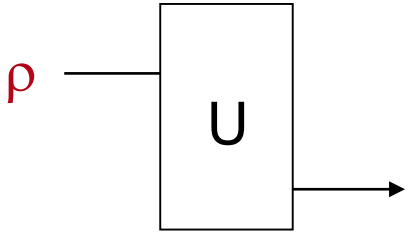
input from
sender Alice

output to
receiver Bob





input from
sender Alice

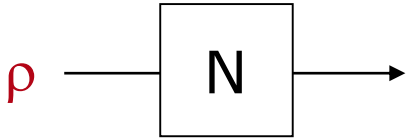


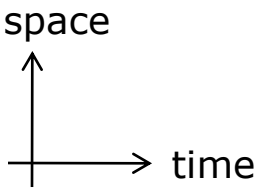
leakage to
environment Eve

Noisy quantum channels

input from sender Alice

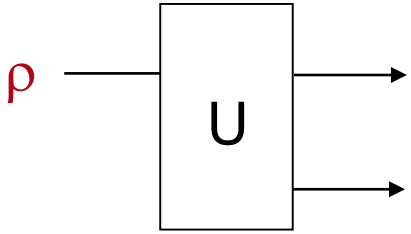
output to receiver Bob





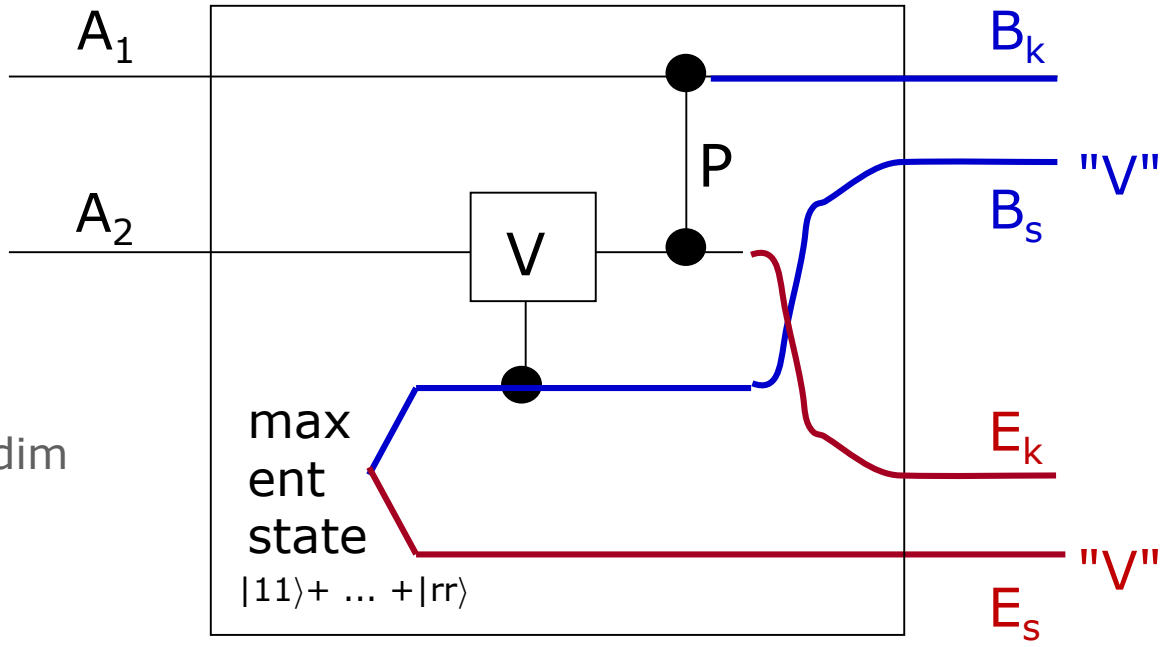
input from sender Alice

output to receiver Bob



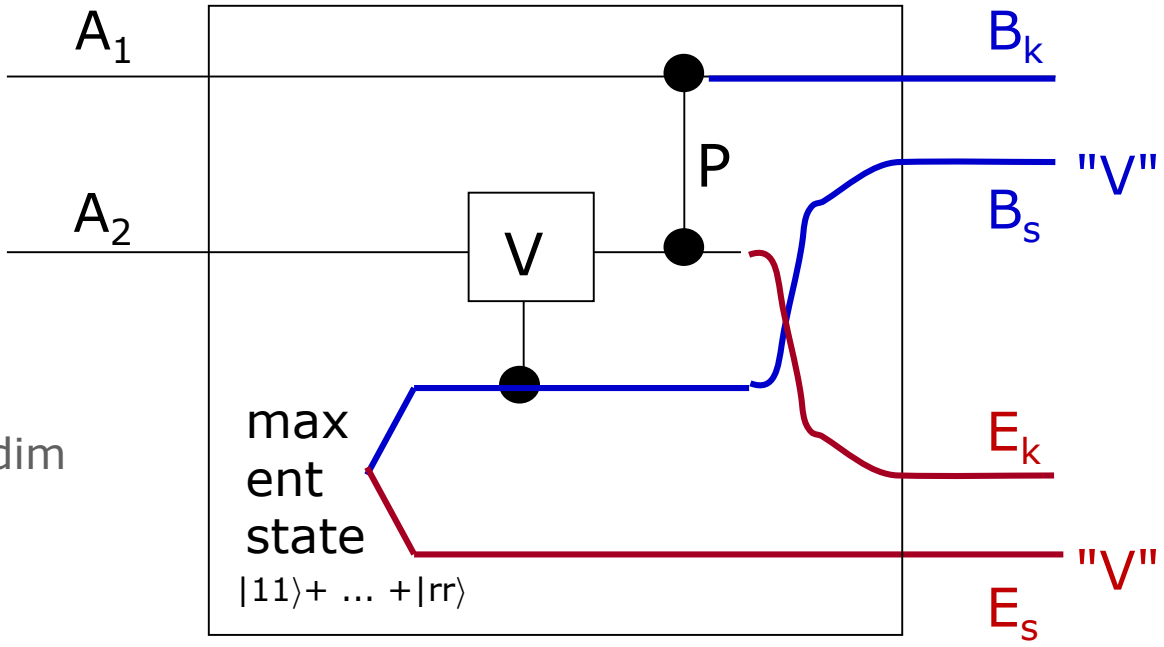
leakage to environment Eve

The channel N_d:



$A_{1,2}$: d-dim
$d_{in} = d^2$

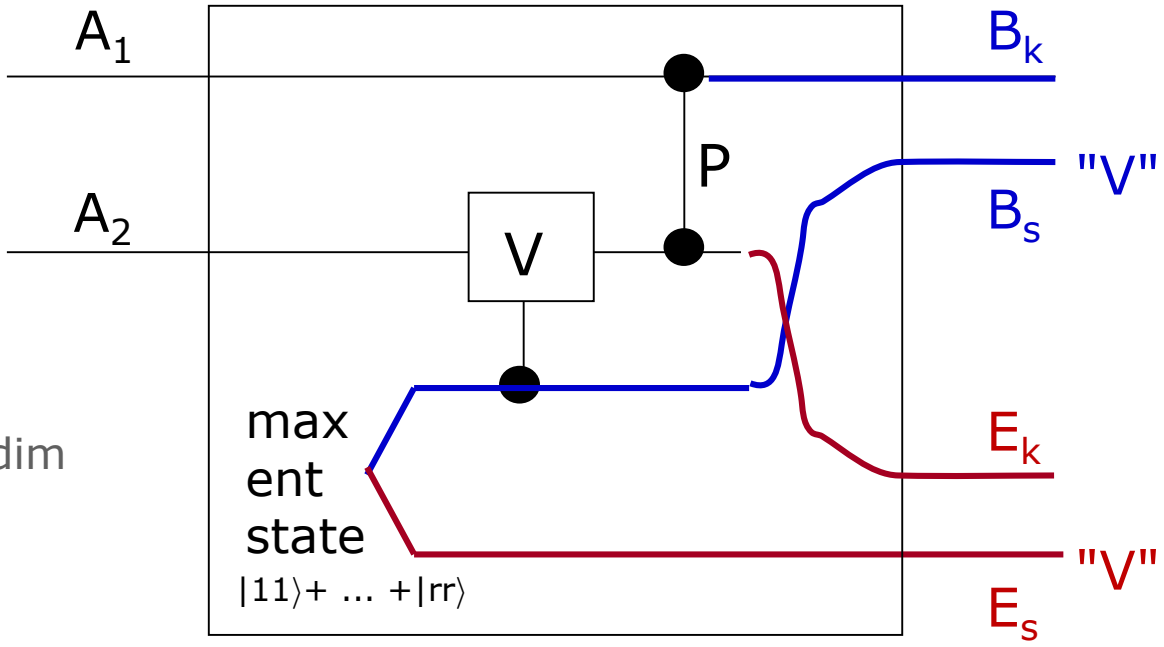
The channel N_d:



$A_{1,2}$: d-dim
$d_{in} = d^2$

V: random element of a unitary 2-design (e.g., Clifford group).

The channel N_d:

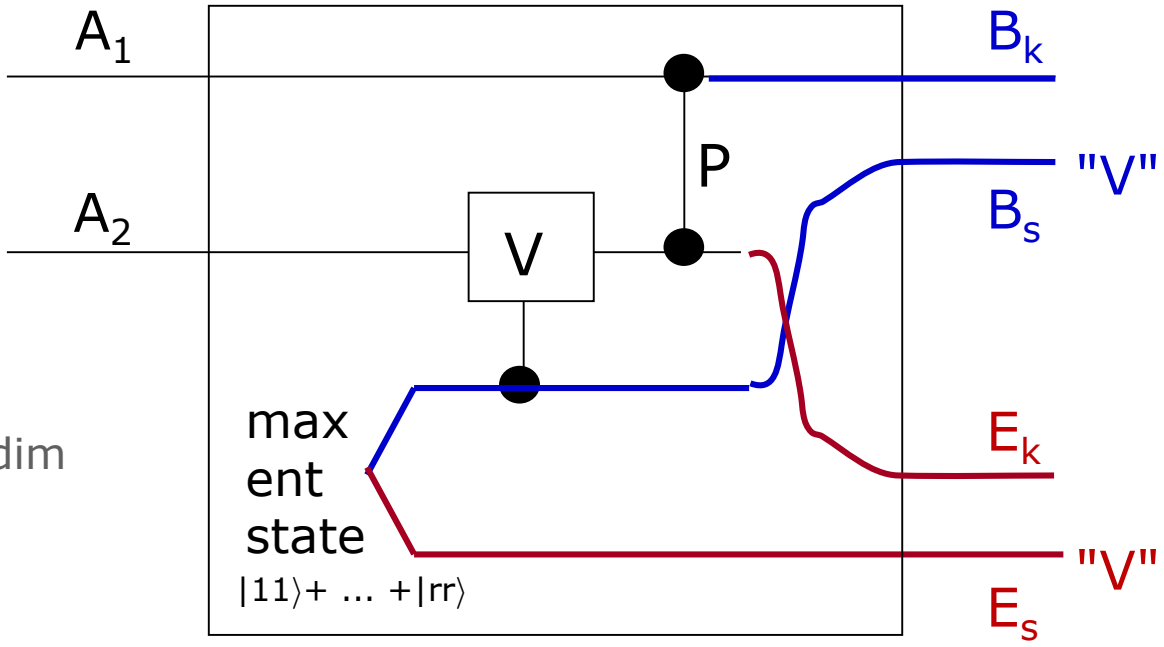


$A_{1,2}$: d-dim
$d_{in} = d^2$

V: random Clifford gate,

$P|ij\rangle = \omega^{ij}|ij\rangle$, ω primitive d^{th} root of unity

The channel N_d:



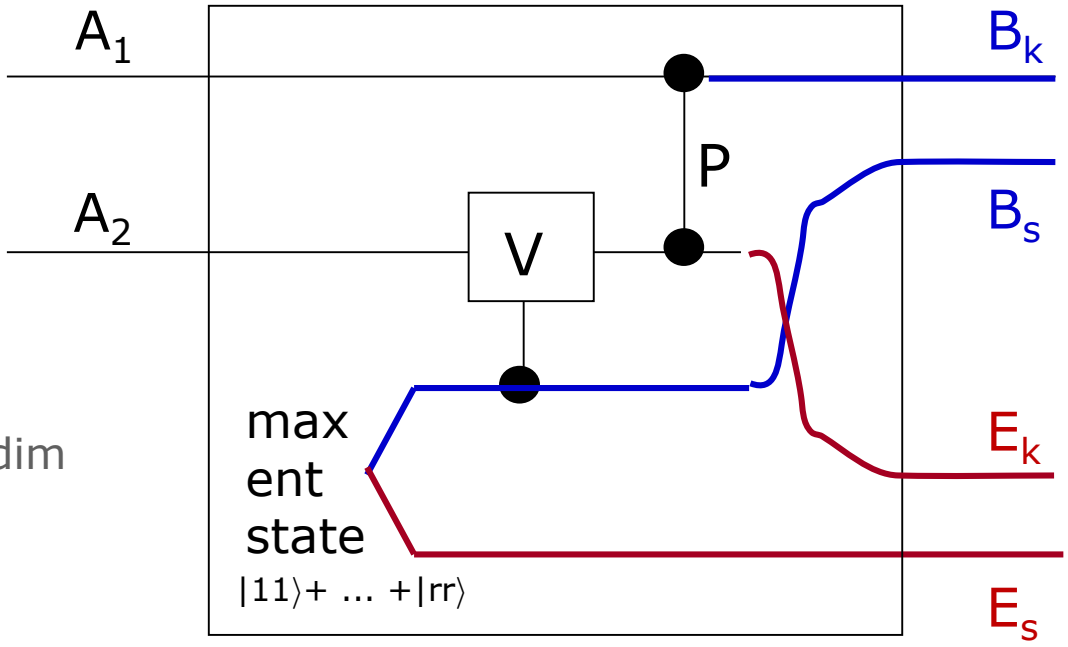
$A_{1,2}$: d-dim
$d_{in} = d^2$

V: random Clifford gate,

$P|ij\rangle = \omega^{ij}|ij\rangle$, ω primitive d^{th} root of unity

If A_1 is $|i\rangle$, apply Z^i to A_2 , $Z = \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^{d-1} \end{pmatrix}$

The channel N_d:



N takes A_1A_2 to B_kB_s

N^c takes A_1A_2 to E_kE_s

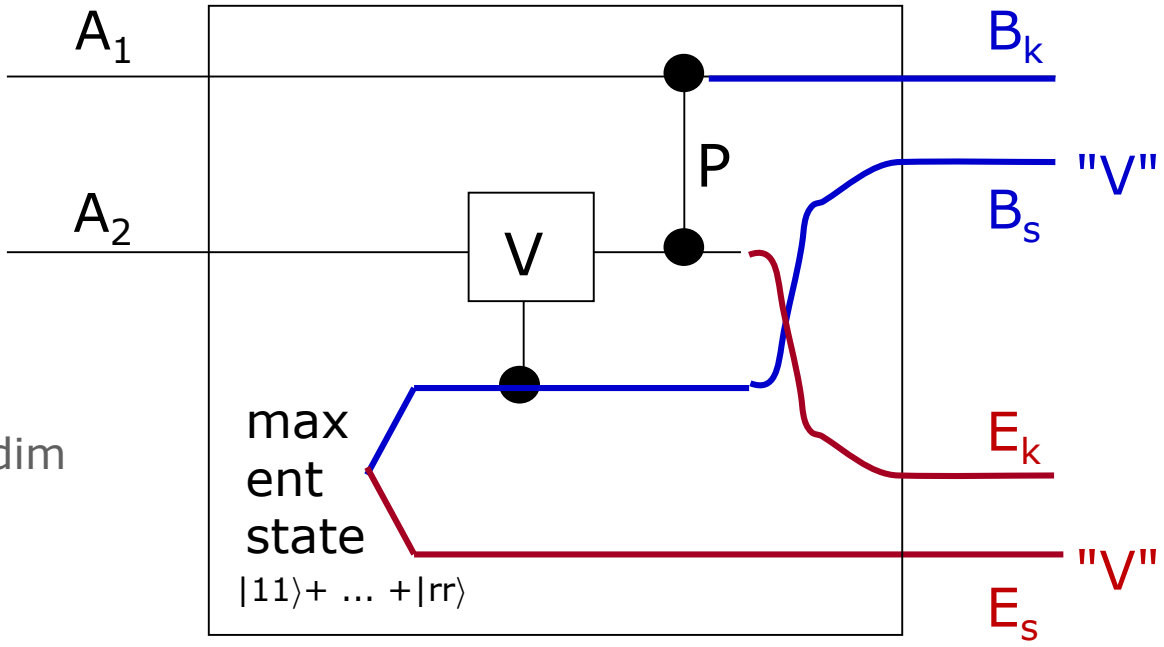
$A_{1,2}$: d-dim
$d_{in} = d^2$

V: random Clifford gate,

$P|ij\rangle = \omega^{ij}|ij\rangle$, ω primitive d^{th} root of unity

If A_1 is $|i\rangle$, apply Z^i to A_2 , $Z = \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^{d-1} \end{pmatrix}$

Why $P_0(N_d) = \log d$:



$A_{1,2}$: d-dim
$d_{in} = d^2$

The Choi state is an exact p-bit (HHHO03) with log d key-bits. (Note achievable in 1-shot.)

Why it's not obvious $Q_0(N_d) = 0$:

- The channel N_d together with classical feedback or with entanglement has a high zero-error quantum capacity

- Superactivation in zero-error capacities of a quantum channel

  Duan 2009, Chen-Cubitt-Harrow 2011, Cubitt-Smith 2012
  Shirokov-Shulman-2014, Shirokov-Shulman-2015, Shirokov 2015

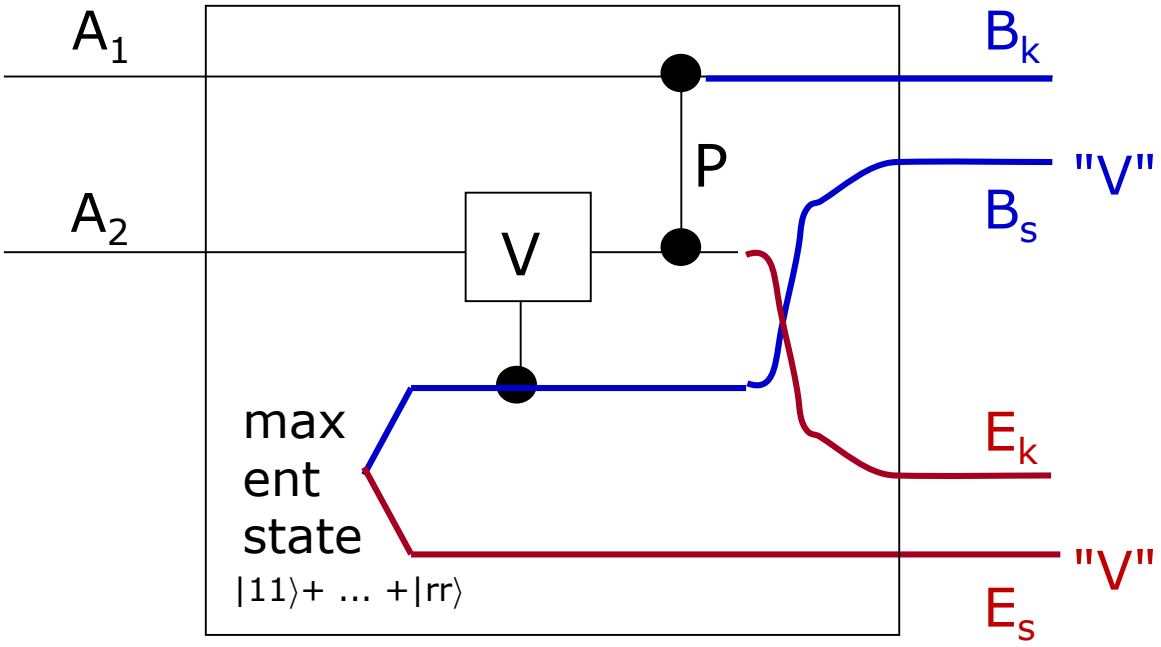
  In particular:

  - there are two channels each with no asymptotic zero-error classical capacity, but has positive joint zero-error quantum capacity (superactivation of all 3 capacities)

  - for every n, there is a channel with no n-shot zero-error quantum capacity, but positive asymptotic zero-error quantum capacity.

The non-commutative graph of N_d:

Duan-Severini-Winter & Weaver



Kraus operator for each k and V:

$$(I \otimes \langle k|)P(I \otimes V)\otimes V\rangle = (Z_k \otimes \langle k|V)\otimes|V\rangle$$

$G(N_d)$ = span{$E^\dagger F$: E,F Kraus ops}

= span{$Z_{k-l}\otimes V^\dagger|l\rangle\langle k|V : 1 \leq l,k \leq d, V \in$ 2-design}

The non-commutative graph of N_d:

Duan-Severini-Winter & Weaver

$G(N_d) = \text{span}\{E^\dagger F: E,F \text{ Kraus ops}\}$

$= \text{span}\{Z_{k-l} \otimes V^\dagger |l\rangle\langle k| V : 1 \leq l,k \leq d,\ V \in \text{2-design}\}$

Shirokov-Shulman 2015:

If G(N) constains all matrices diagonal in some basis, or if G(N) is closed under multiplication, then N cannot be superactivated.

NB $Z \otimes I \notin G(N_d)$, $Z \otimes Z$, $I \otimes Z \in G(N_d)$, so, neither condition holds, so cannot conclude $Q_0(N_d) = 0$.

Open problem: can other channels activate N_d ?

cf (regular) $Q(N_d \otimes \text{50/50 erasure channel}) \approx O(\log d)$.

Lemma (Cubitt-Smith-2012):

One can transmit quantum data through 1 use of a q channel N

iff $\exists\, |\alpha\rangle, |\beta\rangle$ s.t.

$$\mathrm{tr}\,[N(|\alpha\rangle\langle\alpha|)\, N(|\beta\rangle\langle\beta|)] = 0 \qquad (1)$$

$$\mathrm{tr}\,[N(|\alpha+\beta\rangle\langle\alpha+\beta|)\, N(|\alpha-\beta\rangle\langle\alpha-\beta|)] = 0 \qquad (2)$$

where $|\alpha \pm \beta\rangle = (|\alpha\rangle \pm |\beta\rangle)/\sqrt{2}$

Proof sketch for $Q_0(N_d) = 0$:

- characterize $|\alpha\rangle$, $|\beta\rangle$ satisfying condition (1) for 1 use of N_d
- generalize to $N_d^{\otimes n}$
- show condition (2) must fail

$\therefore\ \forall n$, no quantum data can be transmitted through $N_d^{\otimes n}$

Lemma 1:

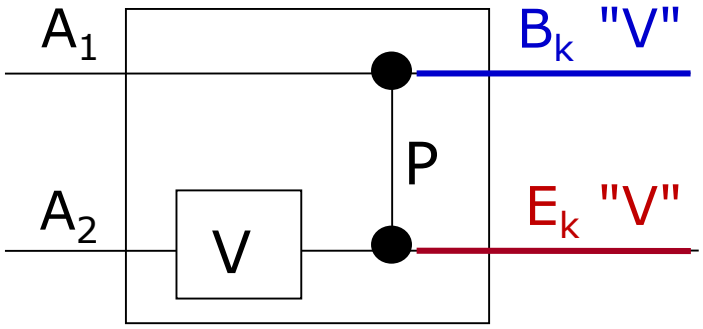
Let $|\alpha\rangle=\sum_{i=1}^{d} |i\rangle\ |\alpha_i\rangle$, $|\beta\rangle =\sum_{i=1}^{d} |i\rangle\ |\beta_i\rangle$.

Then, $\mathrm{tr}\,[N_d(|\alpha\rangle\langle\alpha|)\ N_d(|\beta\rangle\langle\beta|)] = 0$ iff $\forall_i\ |\alpha_i\rangle|\beta_i\rangle = 0$.

i.e., no overlap in the computation basis in system A_1.

Pf: for each V, let $|\alpha'\rangle = P(I \otimes V)|\alpha\rangle$; $\rho^V = \mathrm{tr}_2\ |\alpha'\rangle\langle\alpha'|$
$|\beta'\rangle = P(I \otimes V)|\beta\rangle$; $\sigma^V = \mathrm{tr}_2\ |\beta'\rangle\langle\beta'|$.

$\mathrm{tr}\,[N_d(|\alpha\rangle\langle\alpha|)\ N_d(|\beta\rangle\langle\beta|)] = 0$
iff $\forall_V\ \mathrm{tr}\ \rho^V \sigma^V = 0$
iff $E_V\ \mathrm{tr}\ \rho^V \sigma^V = 0$
$\|$
$\langle x|A|x\rangle$



where $|x\rangle = \sum_{i=1}^{d} |i\rangle|\alpha_i\rangle|\beta_i^c\rangle$,
$A = M\otimes(I - \Phi) + |\nu\rangle\langle\nu|\otimes\Phi$, $M>0$, $|\nu\rangle = 1/\sqrt{d}\ \sum_{i=1}^{d} |i\rangle$

If $|x\rangle \in \mathrm{null}(A)$, $\mathrm{tr}_2|x\rangle\langle x| \propto \Phi$, a contradiction unless $|x\rangle = 0$.

Lemma n:

Let $|\alpha\rangle=\sum_{i1,..,in} |i_1...i_n\rangle|\alpha_{i1,..,in}\rangle$, $|\beta\rangle =\sum_{i1,..,in} |i_1...i_n\rangle|\beta_{i1,..,in}\rangle$.

Then $\mathrm{tr}\,[N_d^{\otimes n} (|\alpha\rangle\langle\alpha|) N_d^{\otimes n} (|\beta\rangle\langle\beta|)] = 0$

iff $\forall_{i1,..,in} |\alpha_{i1,..,in}\rangle|\beta_{i1,..in}\rangle = 0.$

Pf: similar to 1-shot case:

$\mathrm{tr}\,[N_d^{\otimes n} (|\alpha\rangle\langle\alpha|) N_d^{\otimes n} (|\beta\rangle\langle\beta|)] = 0$

iff $\langle x|A^{\otimes n}|x\rangle = 0$

where $|x\rangle = \sum_{i1,...,in} |i_1...i_n\rangle\ |\alpha_{i1,..,in}\rangle|\beta_{i1,...,in}{}^c\rangle$,

$A = M\otimes(I - \Phi) + |\nu\rangle\langle\nu|\otimes\Phi$, $M>0$, $|\nu\rangle = 1/\sqrt{d}\ \sum_{i=1}^{d} |i\rangle$

So, $0 = \langle x|A^{\otimes n}|x\rangle \geq$ constant $* \langle x|I^{\otimes n}\otimes(I - \Phi)^{\otimes n}|x\rangle$

So, $0 = \langle x|I^{\otimes n}\otimes(I - \Phi)^{\otimes n}|x\rangle$

Let $m = \mathrm{tr}_1|x\rangle\langle x|$. So, $m \geq 0$, PPT, and $\mathrm{tr}\, m(I - \Phi)^{\otimes n} = 0$.

By Yu-Duan-Ying-2014, $m = 0$. So, $\forall_{i1,..,in} |\alpha_{i1,..,in}\rangle|\beta_{i1,..in}\rangle = 0.$

Lemma n:

Let $|\alpha\rangle = \sum_{i1,..,in} |i_1 \ldots i_n\rangle |\alpha_{i1,..,in}\rangle$, $|\beta\rangle = \sum_{i1,..,in} |i_1 \ldots i_n\rangle |\beta_{i1,..,in}\rangle$.

Then $\mathrm{tr}\,[N_d^{\otimes n}(|\alpha\rangle\langle\alpha|)\, N_d^{\otimes n}(|\beta\rangle\langle\beta|)] = 0$

iff $\forall_{i1,..,in}\ |\alpha_{i1,..,in}\rangle |\beta_{i1,..in}\rangle = 0.$

If $\mathrm{tr}\,[N_d^{\otimes n}(|\alpha\rangle\langle\alpha|)\, N_d^{\otimes n}(|\beta\rangle\langle\beta|)] = 0$ (1)

& $\mathrm{tr}\,[N_d^{\otimes n}(|\alpha+\beta\rangle\langle\alpha+\beta|)\, N_d^{\otimes n}(|\alpha-\beta\rangle\langle\alpha-\beta|)] = 0$ (2)

For each $i_1, \ldots, i_n$,

at most one of $|\alpha_{i1,..,in}\rangle$, $|\beta_{i1,..in}\rangle$ nonzero, and

at most one of $|\alpha_{i1,..,in}\rangle + |\beta_{i1,..in}\rangle$, $|\alpha_{i1,..,in}\rangle - |\beta_{i1,..in}\rangle$ nonzero.

$\therefore |\alpha_{i1,..,in}\rangle = |\beta_{i1,..in}\rangle = 0$, a contradiction.

Theorem:

For any natural number n, N_d^n cannot send any quantum data with zero error.

Further open problem

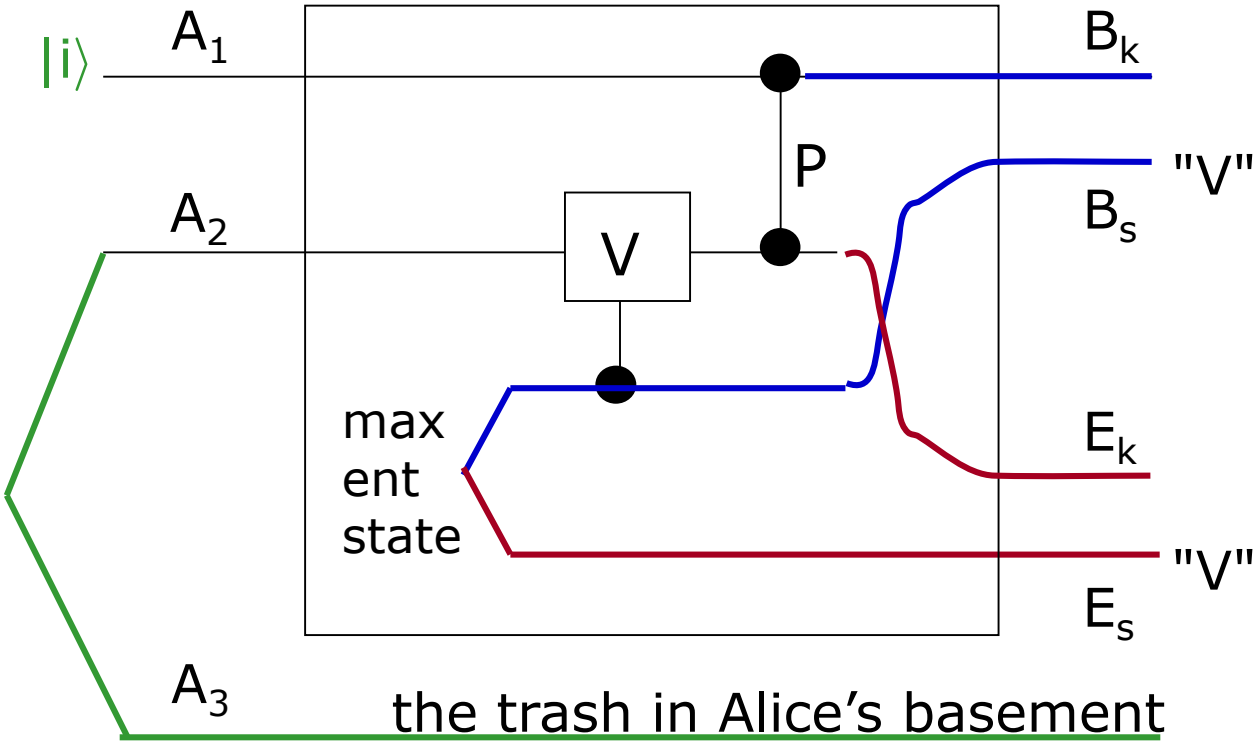
How to characterize when a quantum channel has no zero-error quantum capacity?

- Thank you!

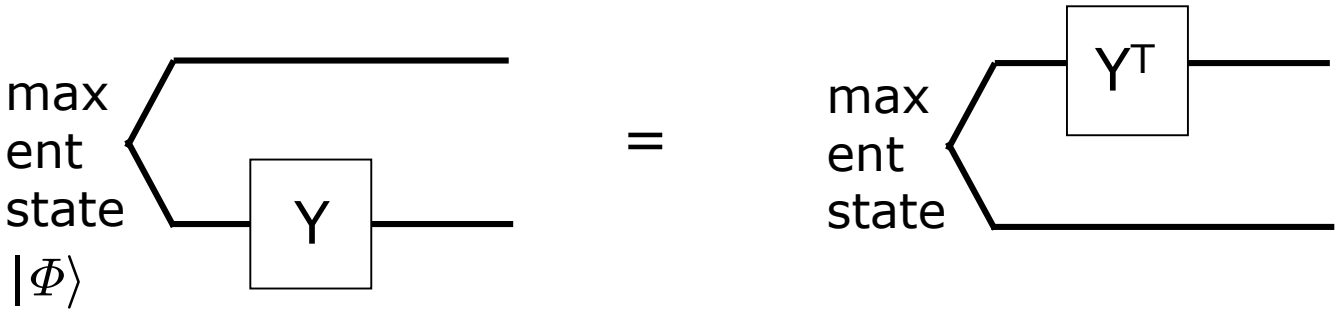
Alternative Pf from 1st principle.

Why $P_0(N_d) = \log d$:

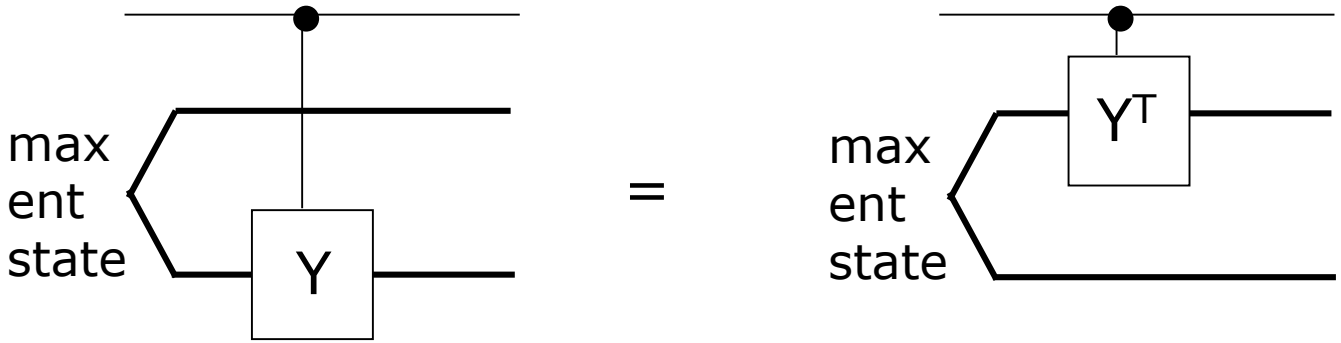
Let Alice's private message be $i \in \{1,2,\cdots,d\}$.
She inputs $|i\rangle$ into A_1, and half of a max ent state into A_2, holding the other half in A_3.



The transpose trick

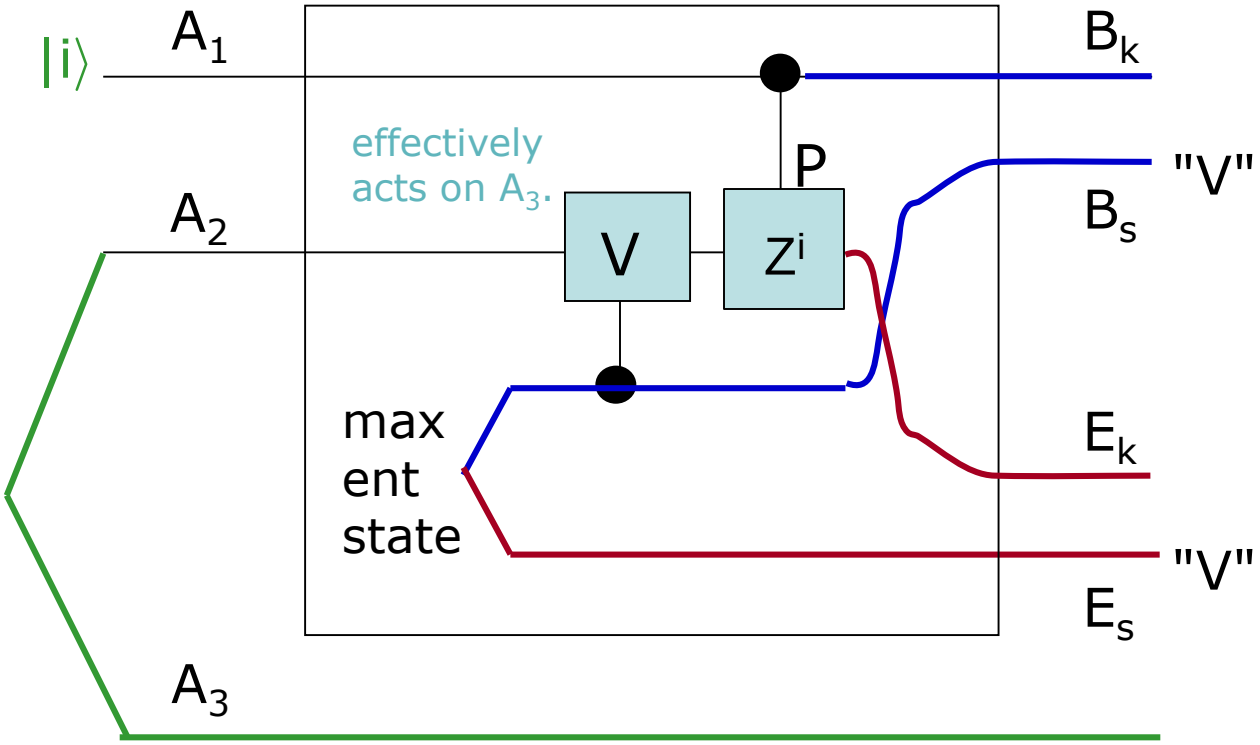


$$(IY)|\Phi\rangle = (IY^T)|\Phi\rangle$$



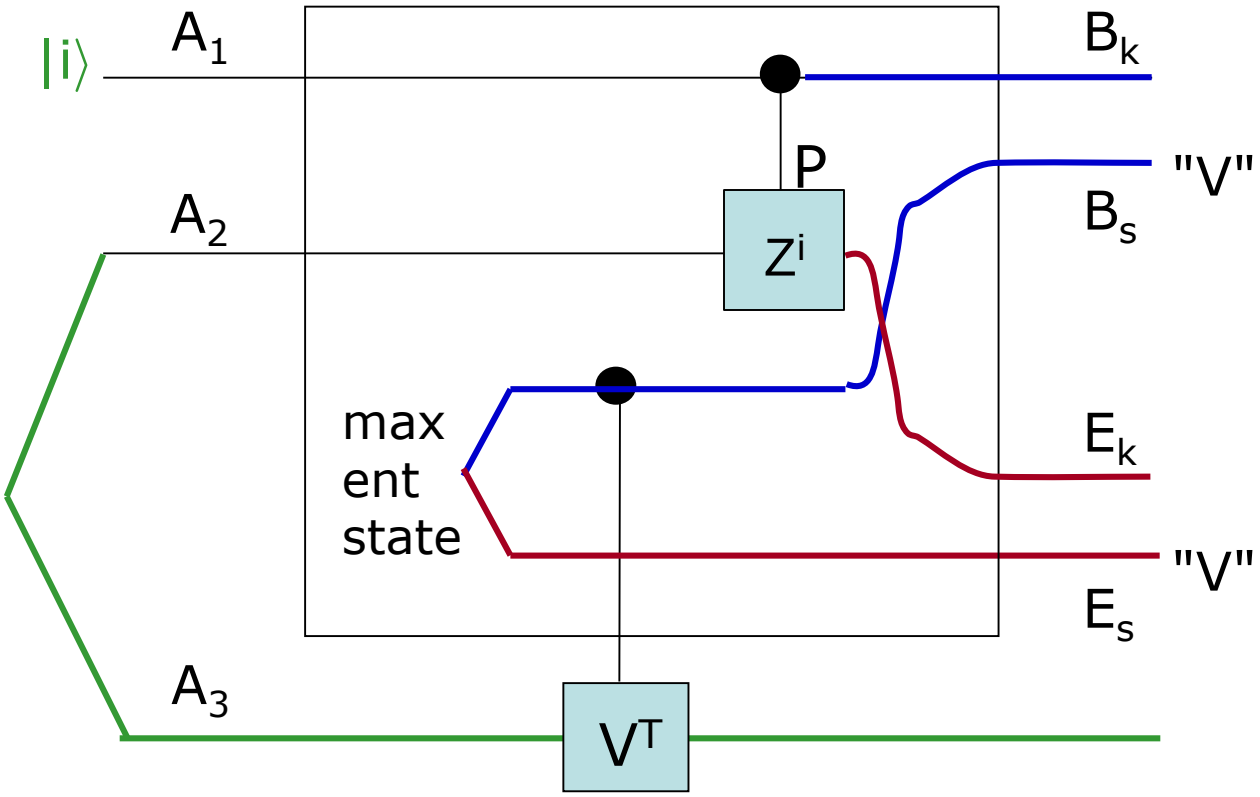
Why $P_0(N_d) = \log d$:

Let Alice's private message be $i \in \{1,2,\cdots,d\}$.
She inputs $|i\rangle$ into A_1, and half of a max ent state into A_2, holding the other half in A_3.



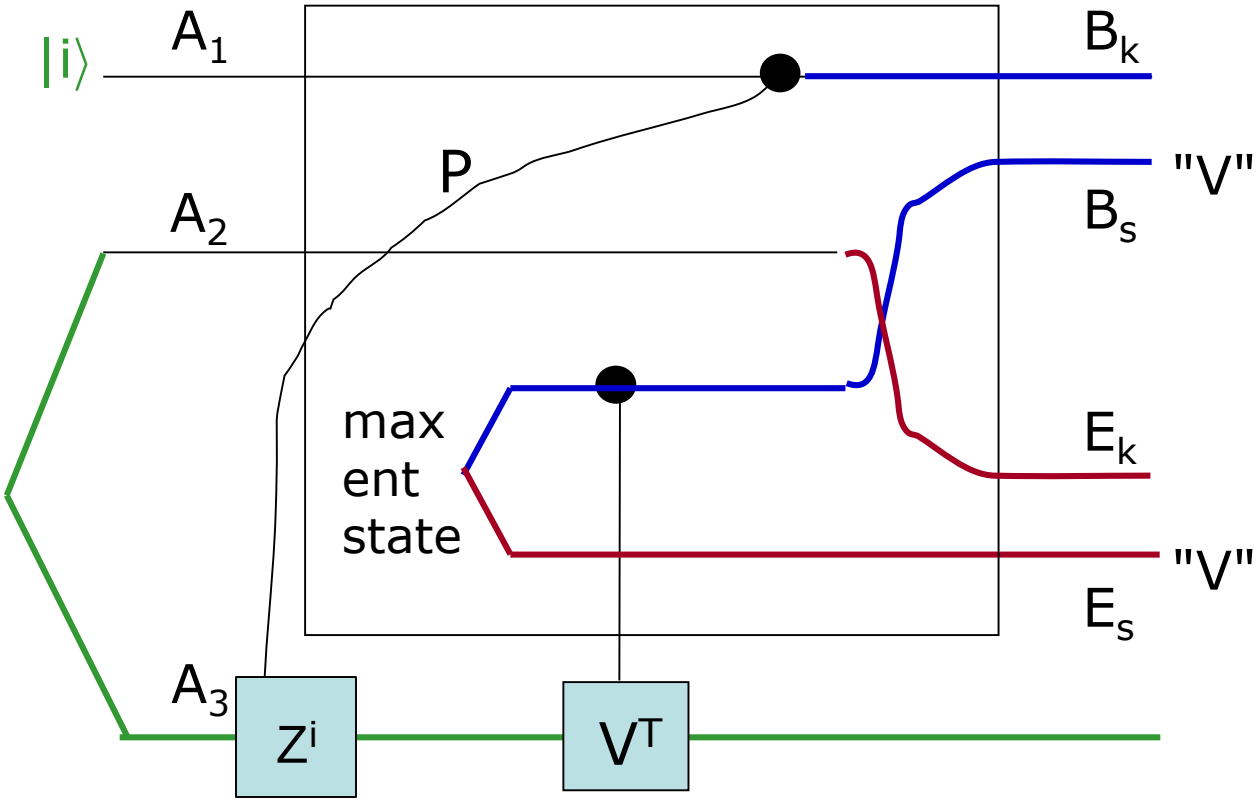
Why $P_0(N_d) = \log d$:

Let Alice's private message be $i \in \{1,2,\cdots,d\}$.
She inputs $|i\rangle$ into A_1, and half of a max ent state into A_2, holding the other half in A_3.



Why $P_0(N_d) = \log d$:

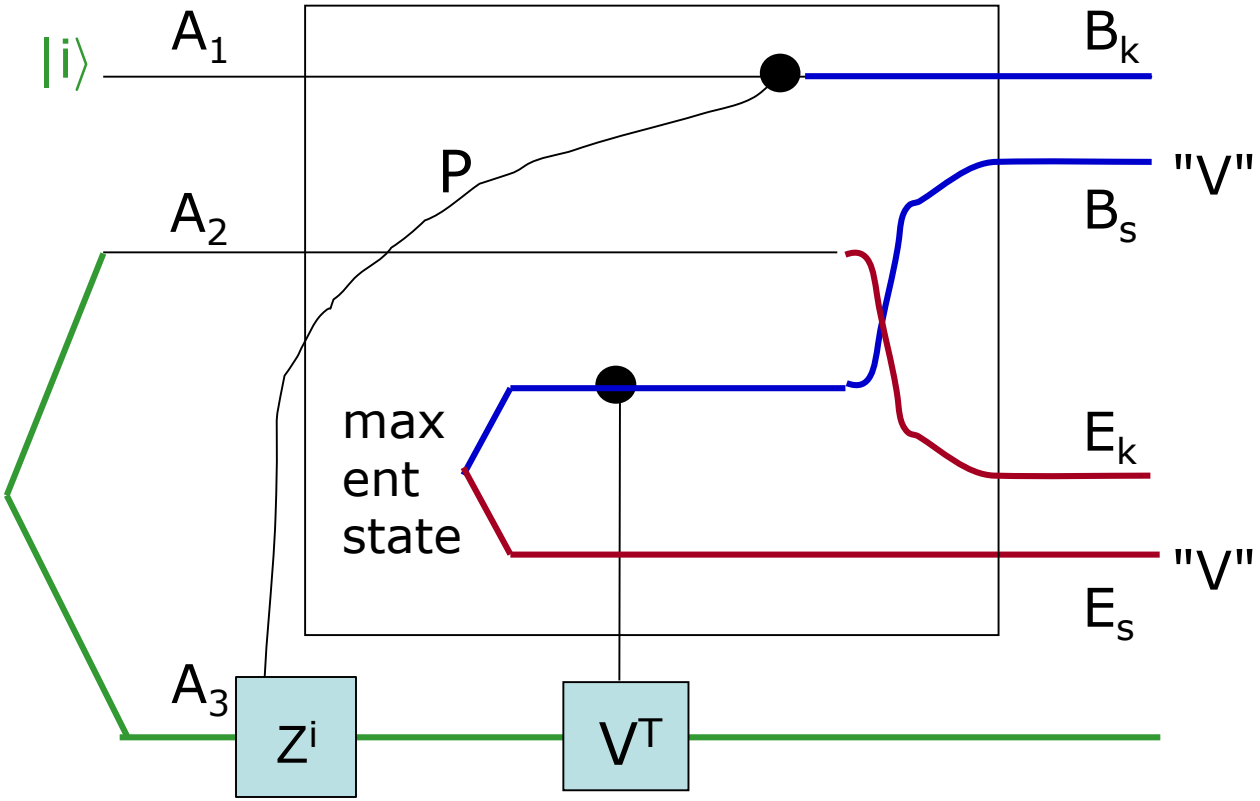
Let Alice's private message be $i \in \{1,2,\cdots,d\}$.
She inputs $|i\rangle$ into A_1, and half of a max ent state into A_2, holding the other half in A_3.



Why $P_0(N_d) = \log d$:

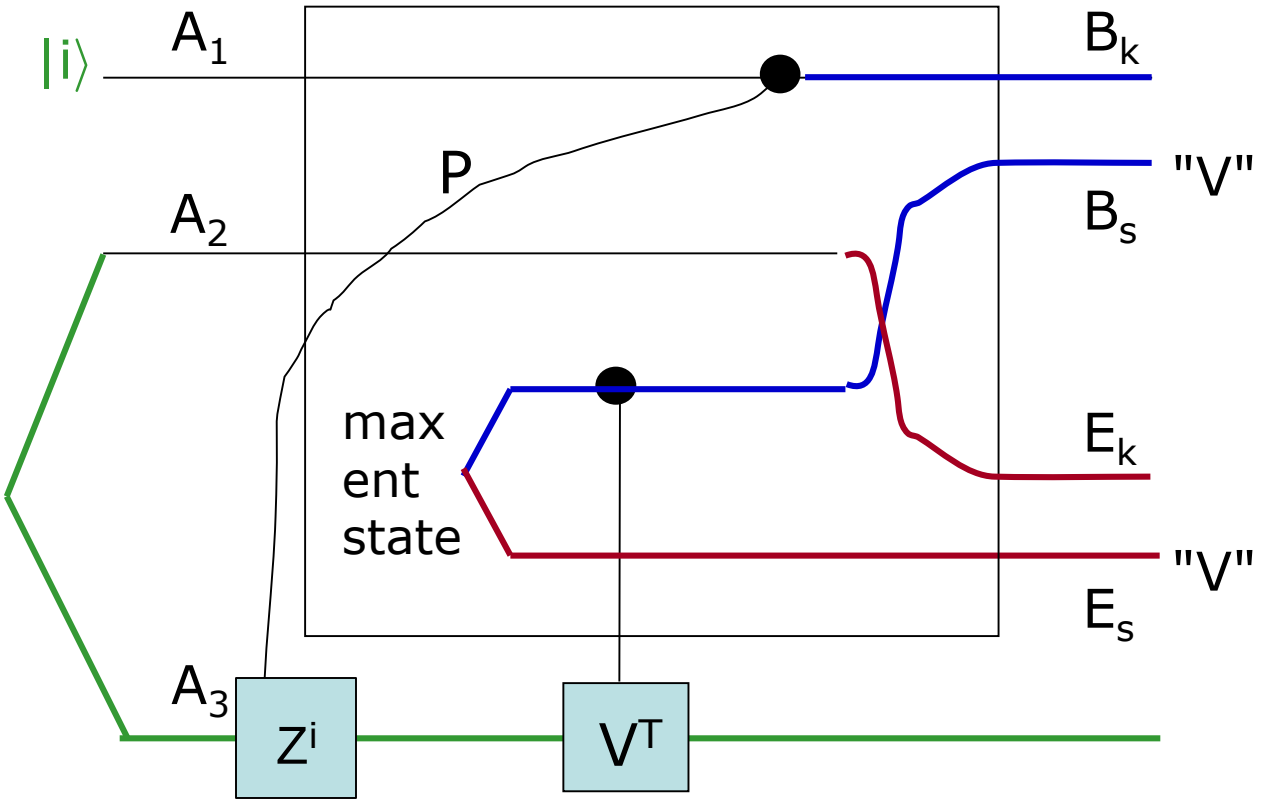
This an equivalent circuit in which E_k, E_s exist before i; they must be independent of i. So, $P_0(N) \geq \log d$.

Let Alice's private message be $i \in \{1,2,\cdots,d\}$.
She inputs $|i\rangle$ into A_1, and half of a max ent state into A_2, holding the other half in A_3.

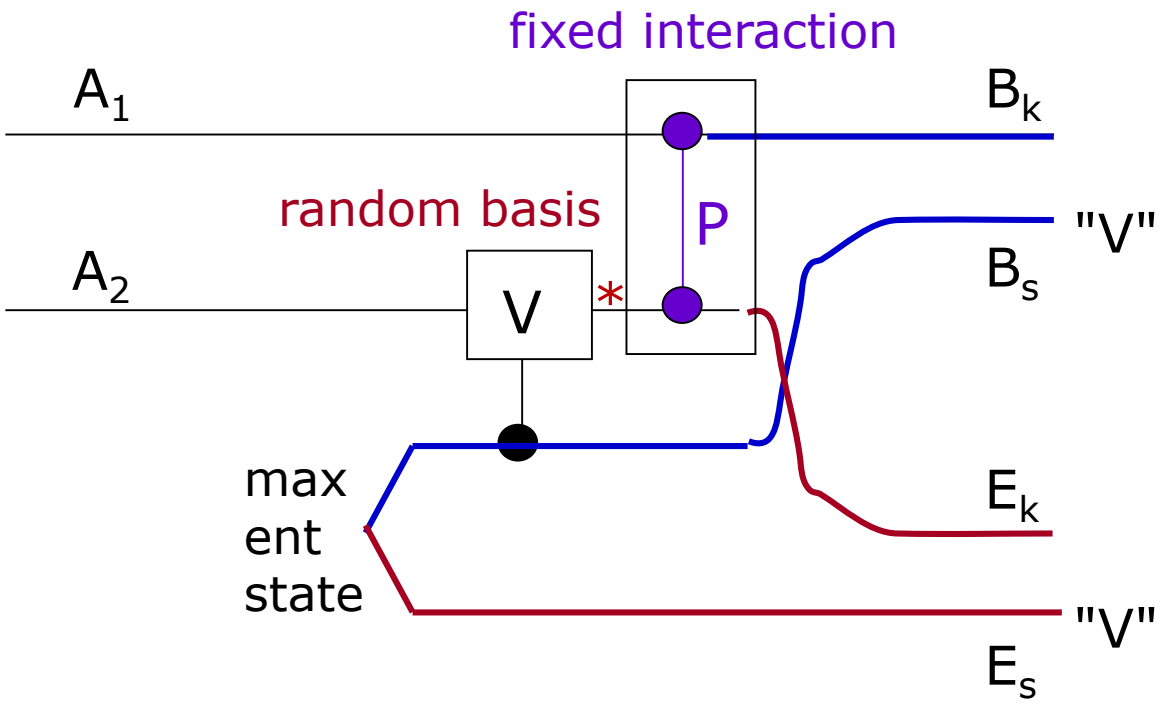


Turning privacy to coherence?

Note: B_k entangled with A_3 which is entangled with E_k – this method cannot be tweaked to create entanglement between Alice and Bob.



Intuition for small quantum capacity



B_k, E_k almost certainly very very entangled.