Lower bounds on Q_B of E_p

Q_B = quantum capacity assisted by back classical communication

E_p = erasure channel with erasure prob p

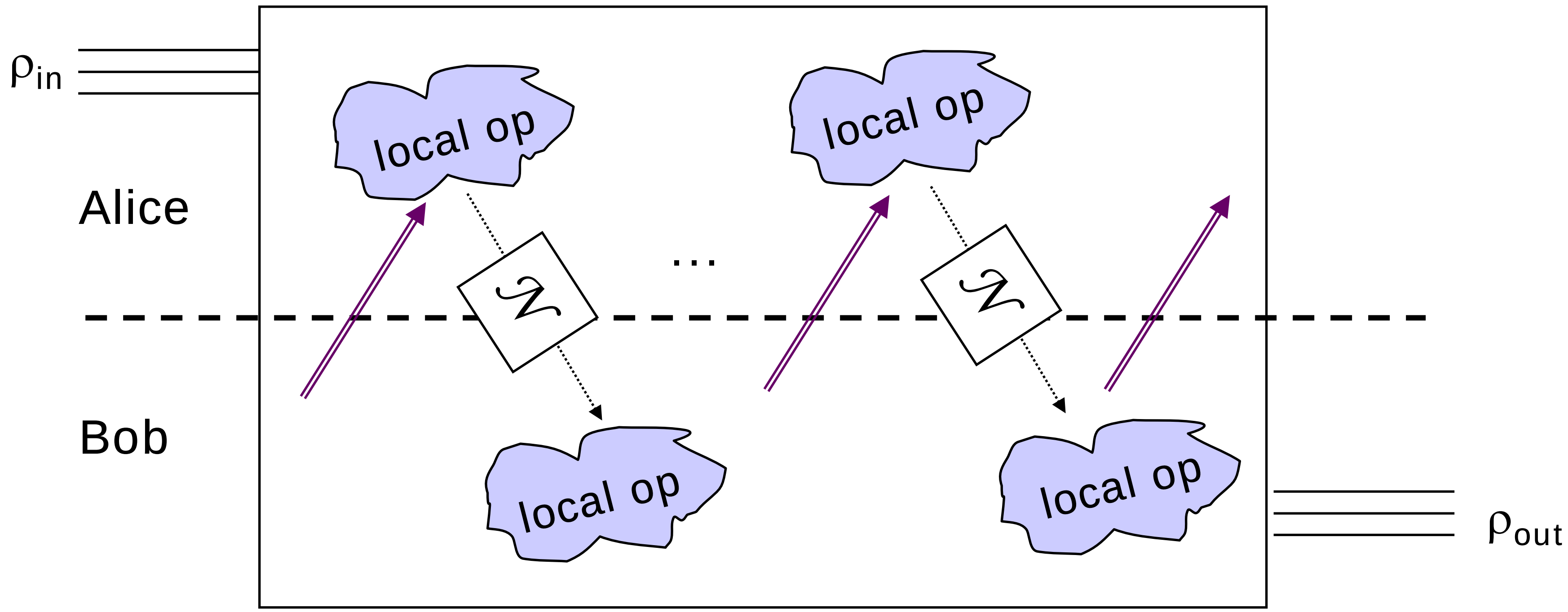
Debbie Leung[1] & Peter Shor[2]

Charles Bennett, Igor Devetak, Aram Harrow, Patrick Hayden, Andreas Winter

1: IQI, Caltech & IQC, UWaterloo
2: MIT

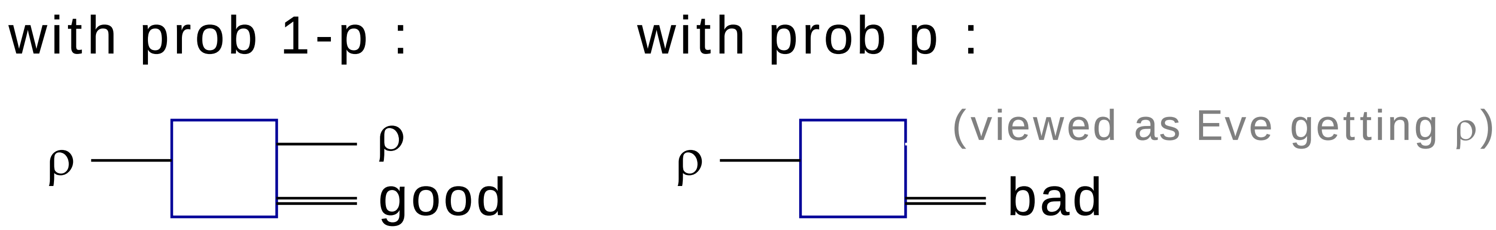
CRC, CFI, OIT, NSERC, CIAR
NSF

Q_B: Quantum capacity assisted by back classical communication



- Asymptotic ability to send quantum data: large # uses, high fidelity, entanglement preserving, unlimited local ops
- Unlimited back classical comm (quantity & # rounds)

E_p: Erasure channel with erasure prob p



Obvious "resource inequalities" (Devetak-Harrow-Winter)

SP: E_p + $cbit_{\leftarrow} \geq (1\text{-}p)$ ebit

Use E_p to send ebits (+ Bob telling Alice Good/Bad @ time)

CC: E_p + $cbit_{\leftarrow} \geq (1\text{-}p)\ cbit_{\rightarrow}$

Use E_p to send cbits (+ feedback)

Omit free $cbit_{\leftarrow}$ from now on ...

If you care, augment @ E_p with $cbit_{\leftarrow}$

Post-presentation editing:
$E_p \geq$ (1-2p) $\text{qbit}_{\rightarrow}$ w/o back comm

Previous slide:

SP: $E_p \geq$ (1-p) ebit

CC: $E_p \geq$ (1-p) $\text{cbit}_{\rightarrow}$

S $\subset$ {Bennett, DiVincenzo, Wootters, Smolin} - 95/96

Original protocol / lower bound for $Q_B(E_p)$

Using TP: 1 ebit + 2 $\text{cbit}_{\rightarrow} \geq$ 1 $\text{qbit}_{\rightarrow}$ (Teleportation)

$\therefore \quad E_p \geq (1\text{-}p)/3 \ \text{qbit}_{\rightarrow}$

Idea of the new protocol (coined by Harrow):
don't do anything you'll regret

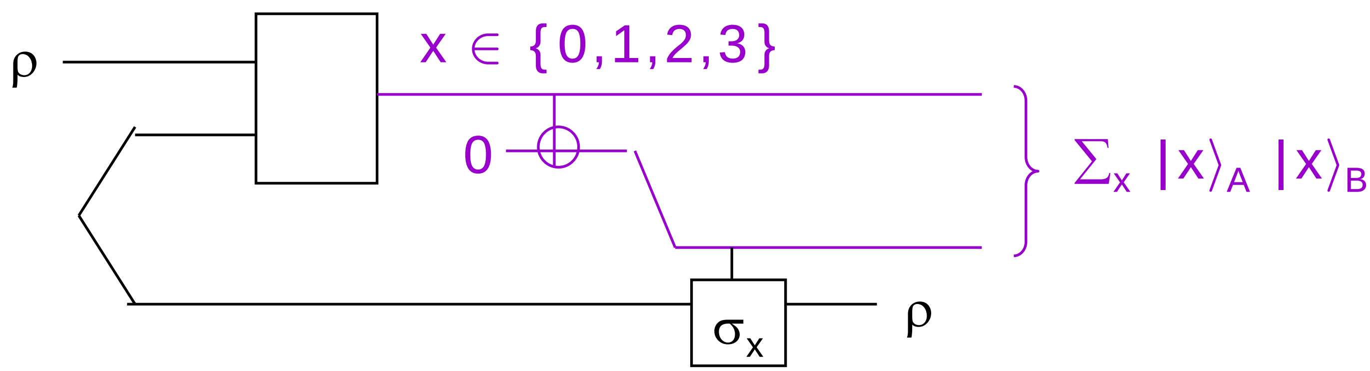
Regret what ?

cbit: $|x\rangle_A \rightarrow |x\rangle_E \otimes |x\rangle_B$ Harrow 03

cobit: $|x\rangle_A \rightarrow |x\rangle_A \otimes |x\rangle_B$ cf qbit: $|x\rangle_A \rightarrow |x\rangle_B$

e.g. TP^{co} : 1 ebit + 2 cobits $\geq$ 1 qbit + 2 ebits !

Proof:



Regret what ?

cbit: $|x\rangle_A \to |x\rangle_E \otimes |x\rangle_B$ Harrow 04

cobit: $|x\rangle_A \to |x\rangle_A \otimes |x\rangle_B$

e.g. TP^{co} : 1 ebit + 2 cobits $\geq$ 1 qbit + 2 ebits !

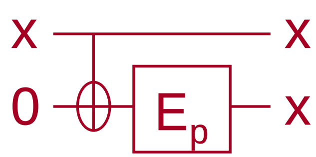
or TP^{co} : 2 cobits $\geq$ 1 qbit + 1 ebit

Also: SD: 2 cobits $\leq$ 1 qbit + 1 ebit

so 2 cobits = 1 qbit + 1 ebit

In hindsight … in teleportation protocol for previous lower bound of Q_B, should have exploited coherence in the classical comm generated by E_p

classical comm via E_p can be made coherent-conditioned-on-“Good”



But we don’t know which one is Good/Bad upfront …

Method 1:

Try using E_p to send x in TP as cobits.

If either is “Bad”, try sending again, now as a cbit.

$E_p \geq (1\text{-}p)^2$ cobit + (1-p) p cbit

Proof:

Prob	Cost	Yield
(1-p)	1 E_p	1 cobit
(1-p) p	2 E_p	1 cbit
(1-p) p^2	3 E_p	1 cbit
	...	

$\therefore$(1-p) (p + 2p + 3p^2 + ...) $E_p \geq$ (1-p) cobit + p cbit

Method 1:

Try using E_p to send x in TP as cobits.

If either is "Bad", try sending again, now as a cbit.

$E_p \geq (1\text{-}p)^2$ cobit + $(1\text{-}p)\, p$ cbit

If $p \geq ½$, rearrange using

2 cobits = ebit + qbit

1 ebit + 2 cbits $\geq$ 1 qbit

E_p + $\text{cbit}_{\leftarrow} \geq (1\text{-}p)$ ebits

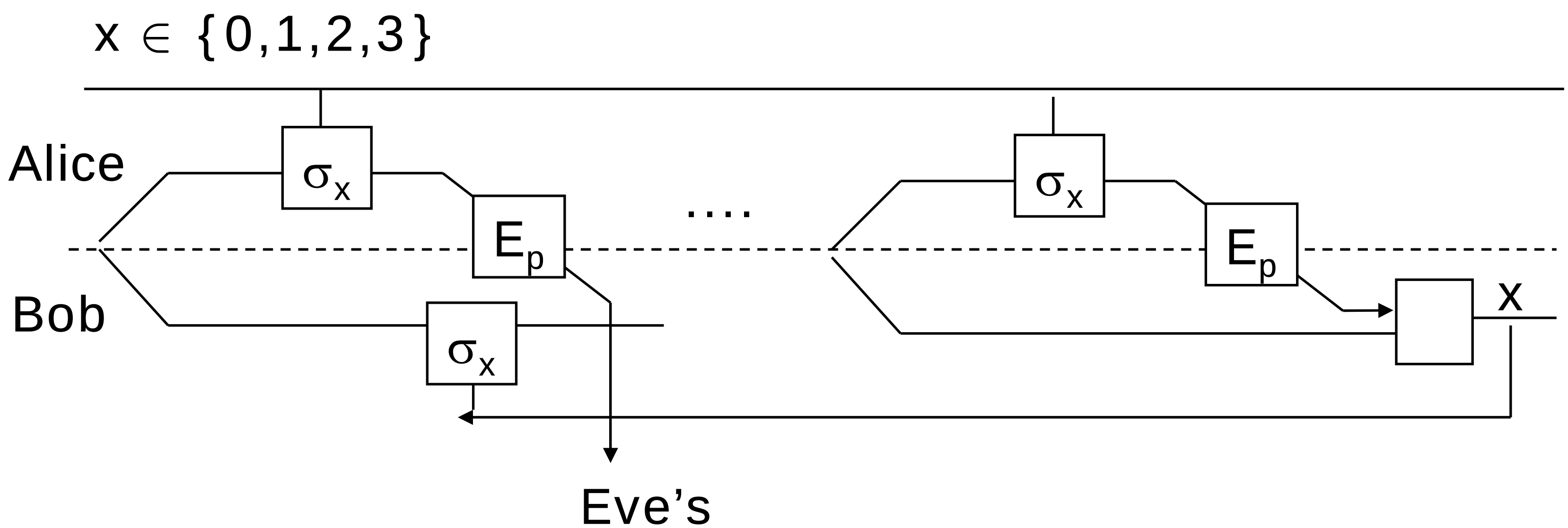
$$E_p \geq \frac{1-p}{1+2p}\ \text{qbit}_{\rightarrow}$$

Method 2:

Staying “coherent” in the presence of uncertainty

SD via E_p : 1 ebit + $E_p \geq$ (1-p) 2 cobits

Proof:



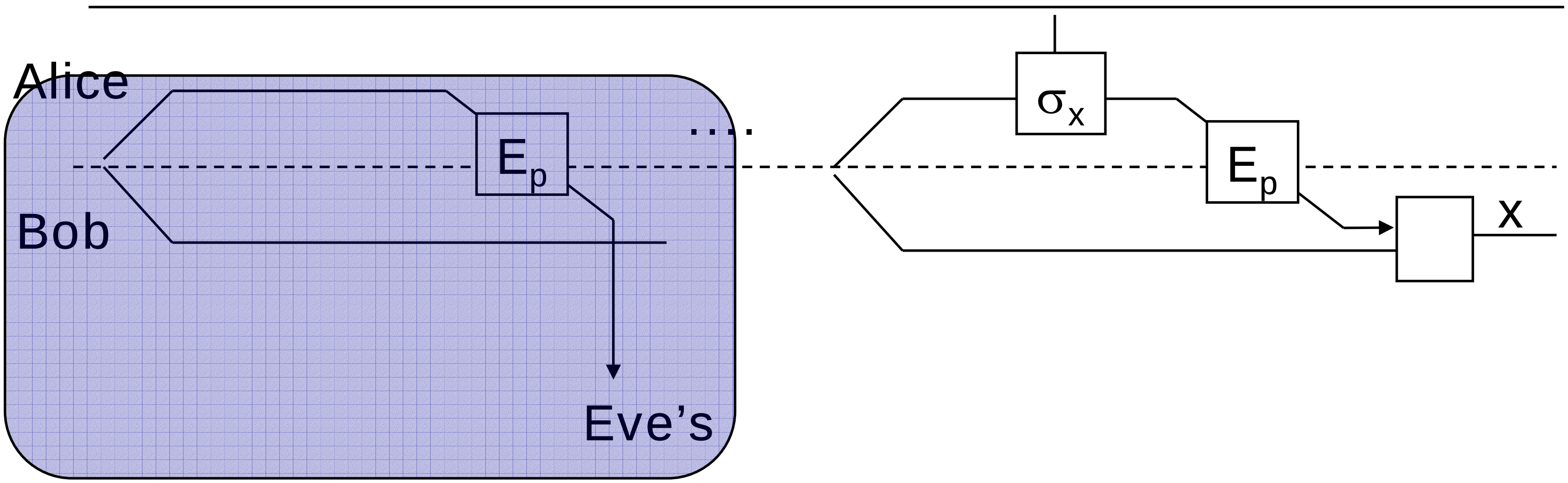
Method 2:

Staying "coherent" in the presence of uncertainty

SD via E_p : 1 ebit + $E_p \geq (1\text{-}p)$ 2 cobits

Proof:

$x \in \{0,1,2,3\}$



Just an ebit between Bob and Eve

Method 2:

Staying "coherent" in the presence of uncertainty

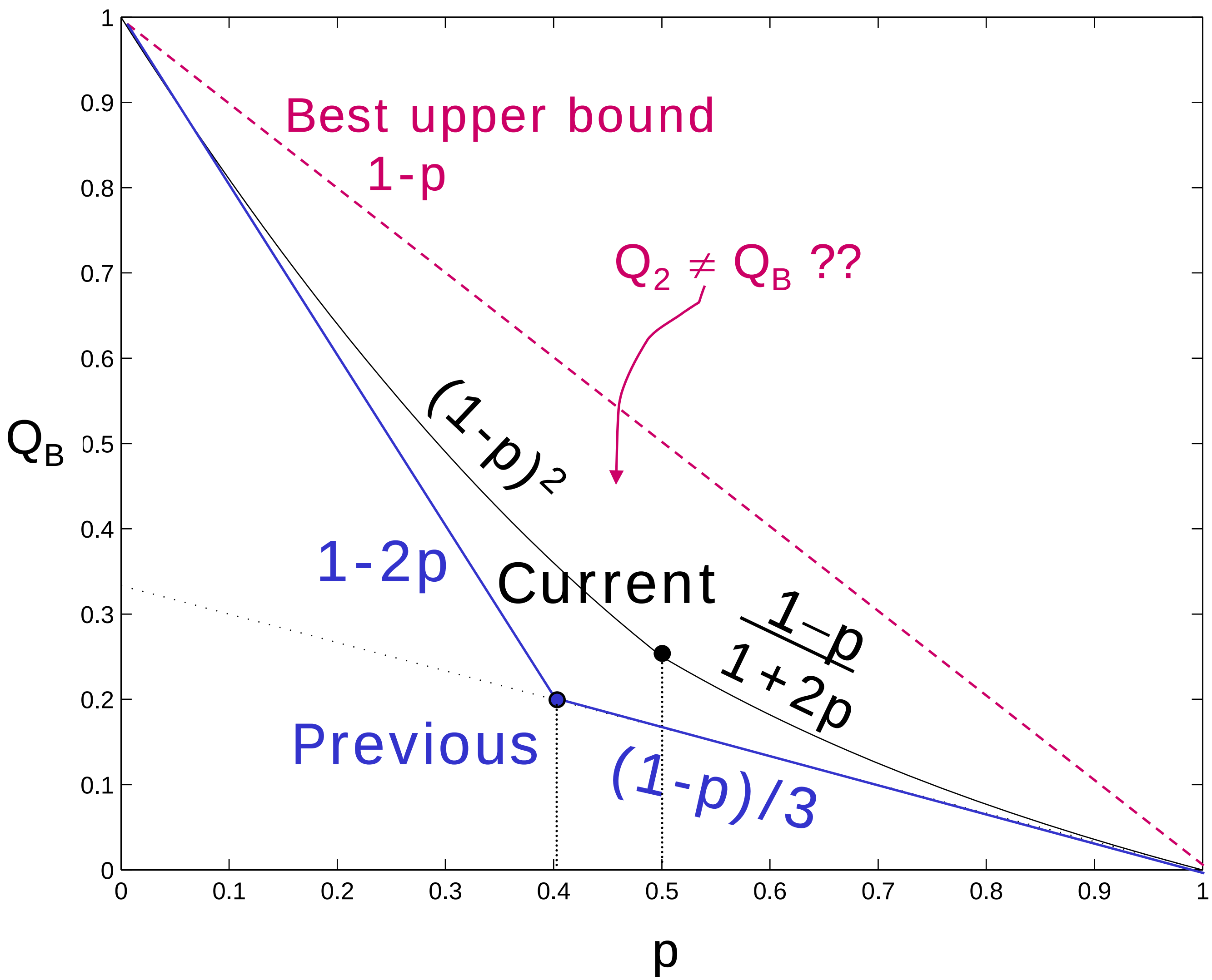
SD via E_p : 1 ebit + $E_p \geq$ (1-p) 2 cobits

$$TP^{co}: \ 1 \text{ ebit} + \frac{1 \text{ ebit} + E_p}{1-p} \geq 1 \text{ qbit}_{\rightarrow} + 2 \text{ ebits}$$

rearranging, and using SP: $E_p \geq$ (1-p) ebits

$$\boxed{E_p \geq (1-p)^2 \text{ qbit}_{\rightarrow}}$$

Summary of lower bounds for Q_B (E_p):



Further work

- Simple generalization:
  - Phase erasure/mixed erasure channels
  - dimension > 2
  - remote state preparation

- Current method as secret sharing schemes.
  - generalization gives worse results.
  -