Polar Codes for Classical, Private, and Quantum Communication *and Superactivation!*

(with Joseph M. Renes)

Mark M. Wilde

School of Computer Science
McGill University

In collaboration with
Saikat Guha

arXiv:1109.2591, arXiv:1109.5346

Second International Conference on Quantum Error Correction (QEC11),
University of Southern California, December 9, 2011

The Quantum Coding Problem

We have some idea of good rates for classical, private, and quantum communication over quantum channels
(*and in some cases, we know capacity*)

Quantum turbo codes and **quantum LDPC codes** are attempts at explicit constructions, but it seems difficult to prove that they are capacity-achieving.

Very little work on codes for classical or private communication

Polar codes are a promising code construction in the classical world, so why not explore their quantum generalization in these different contexts?

Result is a **near-explicit, capacity-achieving scheme** for these different contexts

Channel Polarization

Begin with a binary-input, classical-quantum channel:

$$W : x \rightarrow \rho_x$$

One channel parameter is **symmetric Holevo information:**

$$\begin{aligned} I(W) &\equiv I(X;B) \\ &= H((\rho_0 + \rho_1)/2) - H(\rho_0)/2 - H(\rho_1)/2 \end{aligned}$$

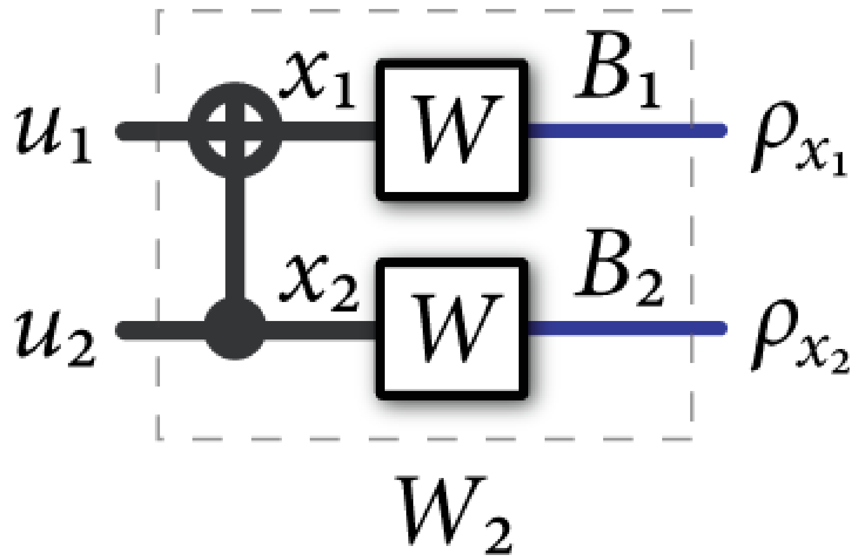
Evaluate *I*(*X*;*B*) with respect to

$$\frac{1}{2}(|0\rangle\langle 0|^X \otimes \rho_0^B + |1\rangle\langle 1|^X \otimes \rho_1^B)$$

Equal to <u>one</u> for *perfect channels* and <u>zero</u> for *useless channels*

Channel Polarization

Take two copies of this channel and perform encoding:



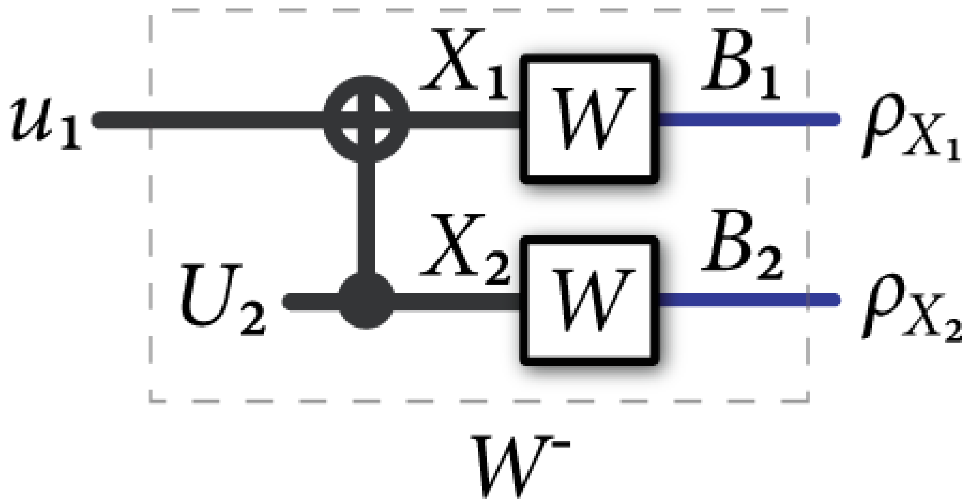
Observe that

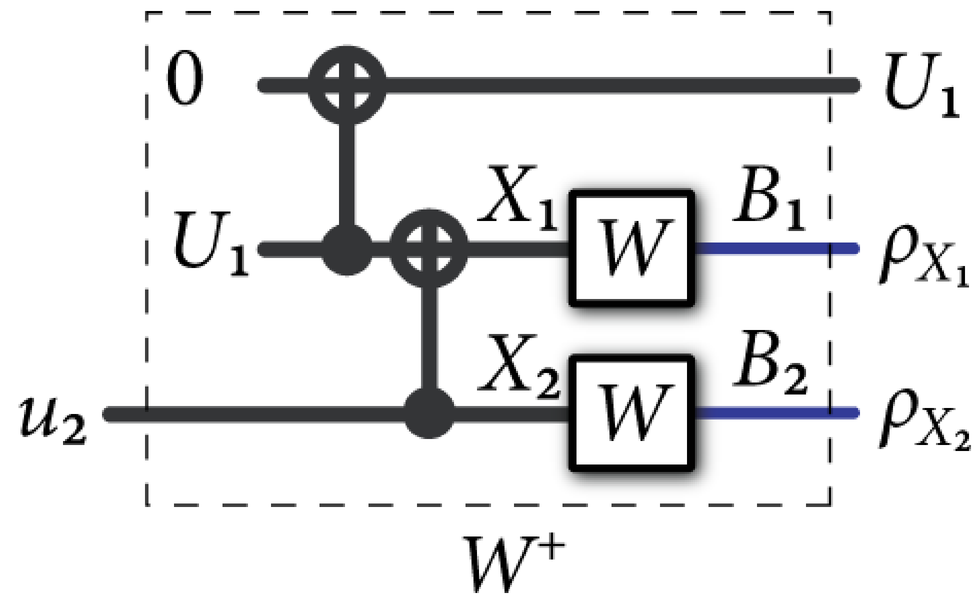
$$\begin{aligned} 2I(W) &= I(X_1X_2;B_1B_2) \\ &= I(U_1U_2;B_1B_2) \\ &= I(U_1;B_1B_2) + I(U_2;B_1B_2U_1) \end{aligned}$$

Channel Polarization (ctd.)

$$I(U_1; B_1 B_2) + I(U_2; B_1 B_2 U_1)$$

The chain rule suggests that we think about two different channels:



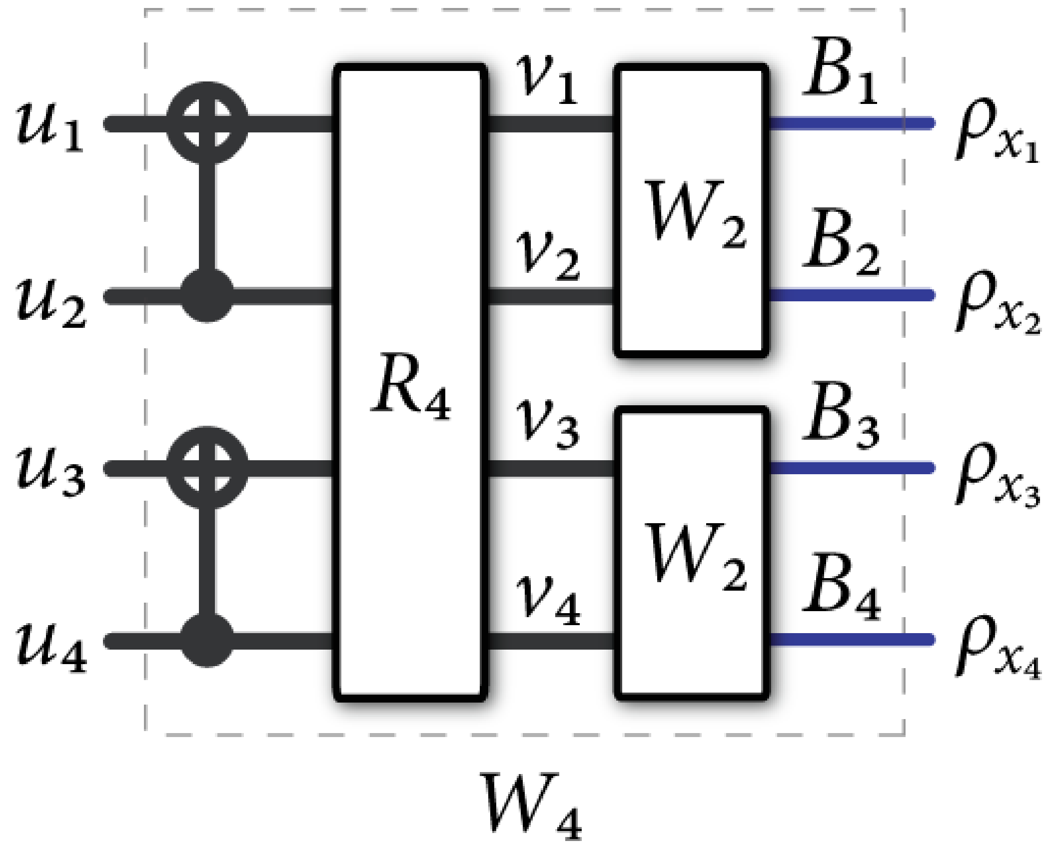


This is already hinting at how a decoder could operate!

Quantum Successive Cancellation:
Decode U_1 first with a quantum hypothesis test,
then use it as side information in a
quantum hypothesis test for decoding U_2

Channel Polarization (ctd.)

Continue this construction recursively:

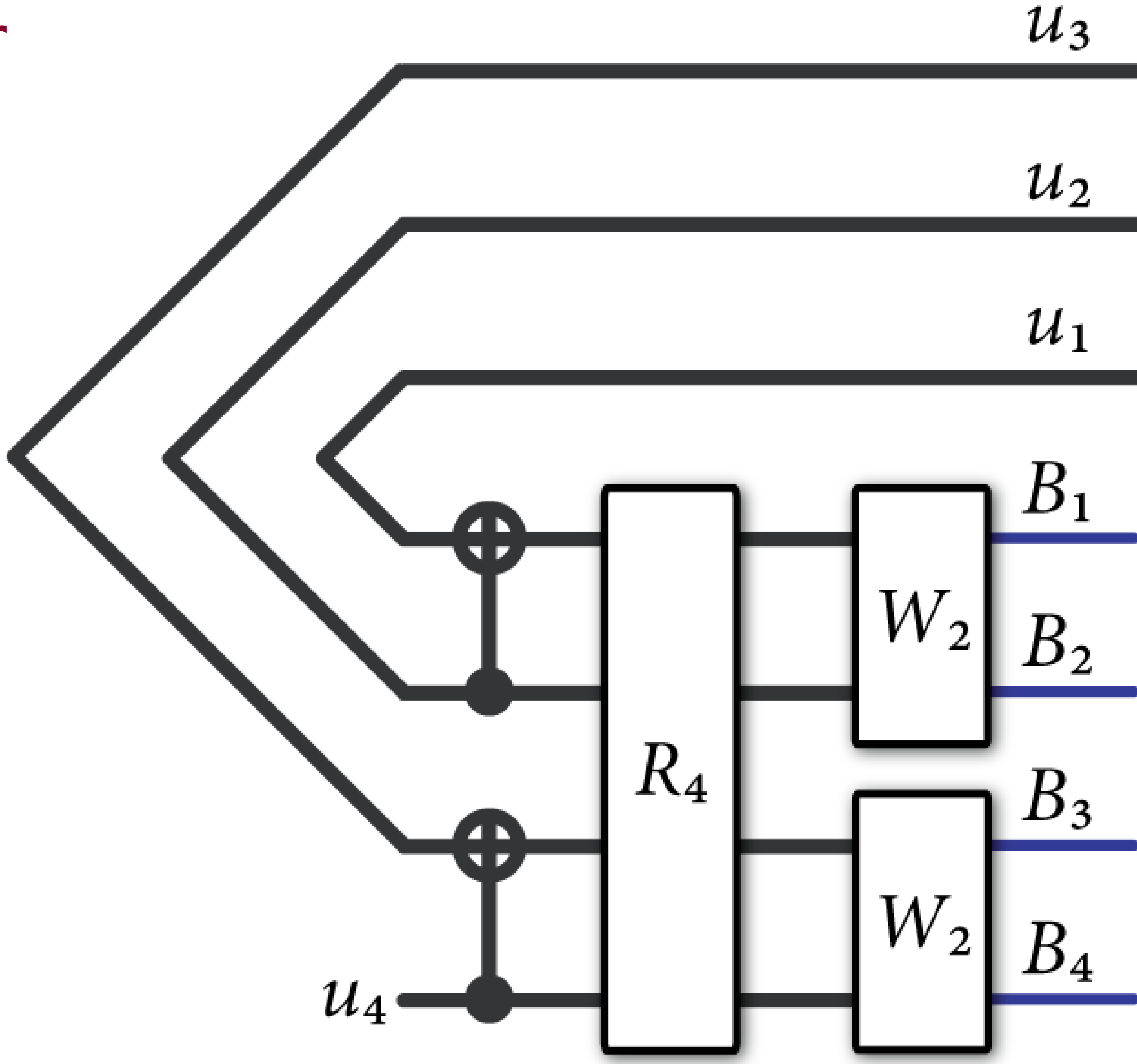


R_4 is an operation which places all of the odd indices first and even indices next

Continue with chain rule:

$$4I(W) = I(U_1; B_1^4) + I(U_2; B_1^4 U_1) + I(U_3; B_1^4 U_1^2) + I(U_4; B_1^4 U_1^3)$$

Quar oder



Channel Polarization (ctd.)

Can continue this recursive construction **many times**

Chain rule is now

$$N \cdot I(W) = \sum_{i=1}^{N} I(U_i; B_1^N \, U_1^{i-1})$$

Channel polarization occurs in the sense that

$$\frac{1}{N}\#\{i : I(U_i; B_1^N \, U_1^{i-1}) \approx 1\} \to I(W)$$

$$\frac{1}{N}\#\{i : I(U_i; B_1^N \, U_1^{i-1}) \approx 0\} \to 1 - I(W)$$

Can prove this result using martingale theory *à la* Arikan and quantum generalizations of Arikan's inequalities

Fidelity Channel Parameter

Fidelity characterizes **distinguishability** of two output states:

$$F(W) \equiv F(\rho_0, \rho_1)$$
$$= \| \sqrt{\rho_0} \sqrt{\rho_1} \|_1^2$$

$F(W) = 0$ if states are *perfectly distinguishable*

$F(W) = 1$ if states are *not distinguishable*

Generalizes classical fidelity (Bhattacharya parameter)

Also serves as an **upper bound** on error probability in a **quantum hypothesis test** that attempts to distinguish ρ_0 from ρ_1:

$$P_e \leq \frac{\sqrt{F(W)}}{2}$$

Relation between Channel Parameters

Fidelity and **symmetric Holevo information** are related

$I(W) \approx 1$ iff $F(W) \approx 0$ and

$I(W) \approx 0$ iff $F(W) \approx 1$

The following bounds make this precise

$$I(W) \geq \log_2\left(\frac{2}{1+\sqrt{F(W)}}\right)$$

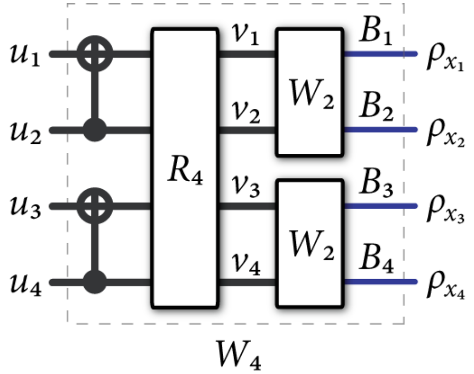
$$I(W) \leq \sqrt{1-F(W)}$$

Proved using results from Holevo quant-ph/9907087 and Roga *et al*. 1004.4782

Can prove things about fidelity and they imply results about SHI

Channel Polarization

Recall **recursive channel construction**



Let $W_N^{(i)}$ be the i^{th} channel in n^{th} recursion level ($N = 2^n$)

Can prove that fidelities and Holevo informations *move away from the center*, helping polarization

$$I(W_{2N}^{(2i-1)}) \leq I(W_N^{(i)}) \leq I(W_{2N}^{(2i)})$$

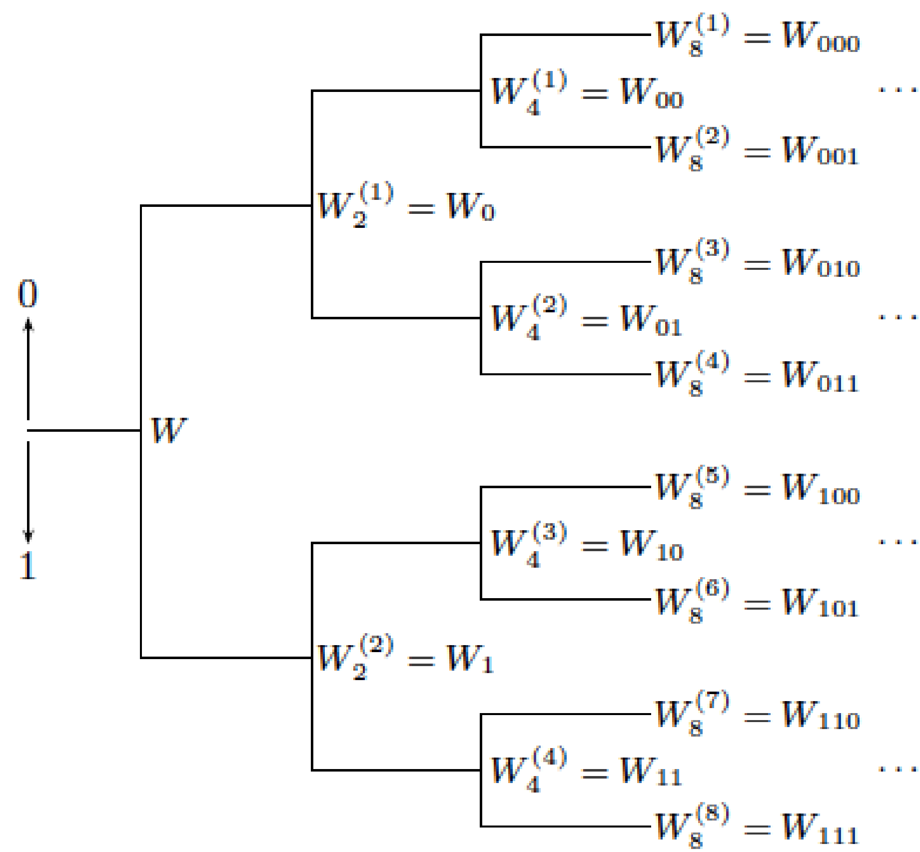
$$\sqrt{F(W_{2N}^{(2i-1)})} \geq \sqrt{F(W_N^{(i)})} \geq \sqrt{F(W_{2N}^{(2i)})}$$

Proved using generalizations of Arikan's results in 0807.3917

Arikan's Martingale Argument

Recall $W_N^{(i)}$ is the i^{th} channel in n^{th} recursion level $(N = 2^n)$

Represent *i* as a binary number and think of *i* as being generated by a **random birth process**



$F(W_N^{(i)})$ is a **martingale** and converges to a {0,1}-valued random variable w/ $\Pr\{F(W_N^{(i)}) = 0\} = I(W)$

Polar Coding Scheme

Send information bits through the good channels

Send frozen (ancilla) bits through the bad channels

Quantum Successive Cancellation Decoder
performs quantum hypothesis tests
to make decisions on the information bits

Key tool in the proof that this scheme works
is Pranab Sen's "**non-commutative union bound**":

$$1 - \mathrm{Tr}\{\Pi_N \cdots \Pi_1 \rho \Pi_1 \cdots \Pi_N\} \leq 2\sqrt{\sum_{i=1}^{N} \mathrm{Tr}\{(I - \Pi_i)\rho\}}$$

This leads to a near-explicit capacity-achieving scheme

Pranab Sen, Lemma 3 of arXiv:1109.0802

Polar Codes for Private Comm.

A simple model for a quantum wiretap channel:

$$x \longrightarrow \rho_x^{BE}$$

Channel to Bob:

$$W : x \longrightarrow \rho_x^B$$

Channel to Eve:

$$W^* : x \longrightarrow \rho_x^E$$

Private capacity of a degradable quantum wiretap channel is

$$I(W) - I(W^*)$$

These codes build on work of Mahdavifar and Vardy arXiv:1007.3568

Polar Codes for Private Comm. (Ctd.)

Channels polarize in four different ways:
(*and this leads to a coding scheme*)

Good for Bob, good for Eve: send random bits into these

Good for Bob, bad for Eve: send information bits into these

Bad for Bob, good for Eve: send halves of secret key bits into these

Bad for Bob, bad for Eve: send ancilla bits into these

If channel is **degradable with classical environment**,
then this scheme provably achieves
the **wiretap capacity** of the channel
(*using the same quantum successive cancellation decoder*)

Rate of secret key required goes to zero in the asymptotic limit

Wilde and Guha, arXiv:1109:5346

Quantum Polar Codes

Idea is to **"run the wiretap code in superposition,"**
à la Devetak's proof of the achievability of coherent information

Use a coherent version of the same encoder,
where CNOT gates are with respect to some orthonormal basis

This induces a wiretap channel,
when considering the isometric extension
of the original quantum channel

Good for Bob, good for Eve: send |+> states into these

Good for Bob, bad for Eve: send information qubits into these

Bad for Bob, good for Eve: send halves of ebits into these

Bad for Bob, bad for Eve: send ancilla qubits |0> into these

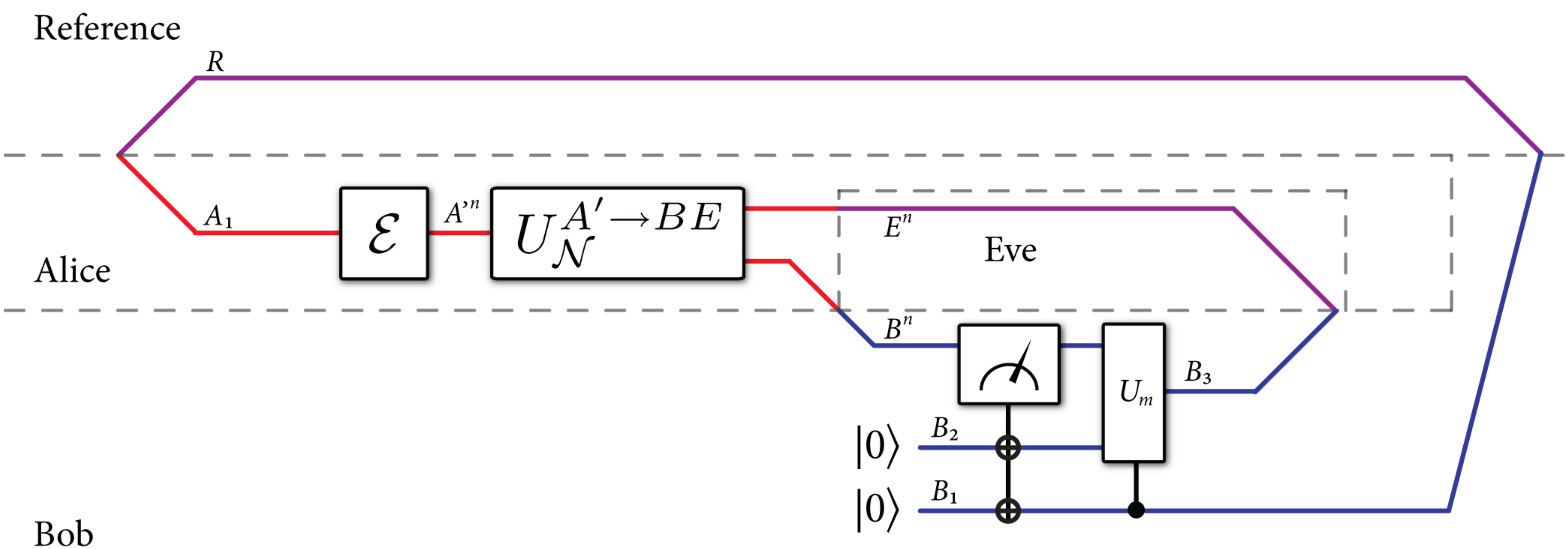
Quantum Polar Codes (ctd.)

Decoder consists of two steps (similar to Devetak):

1) A coherent version of the quantum successive cancellation decoder

2) Controlled decoupling unitary

The **reliability** and the **security** of the quantum wiretap code guarantee that this decoder recovers the transmitted quantum information reliably



Wilde and Guha, arXiv:1109:5346

New and Improved Construction

Use amplitude and phase encoding ideas of Renes

Build quantum polar codes from cq channels:

$$W_A : z \rightarrow \mathcal{N}^{A' \rightarrow B} \left(|z\rangle \langle z| \right)$$

$$W_P : x \rightarrow \left(Z^x \right)^C U_{\mathcal{N}}^{A' \rightarrow BE} |\Phi\rangle^{CA'}$$

Good for Amp, bad for Phase: send |+> states into these

Good for Amp, good for Phase: send information qubits into these

Bad for Amp, bad for Phase: send halves of ebits into these

Bad for Amp, good for Phase: send ancilla qubits |0> into these

Wilde and Renes, (missed out on 1111.1111---will try for 1212.1212)

Construction (Ctd.)

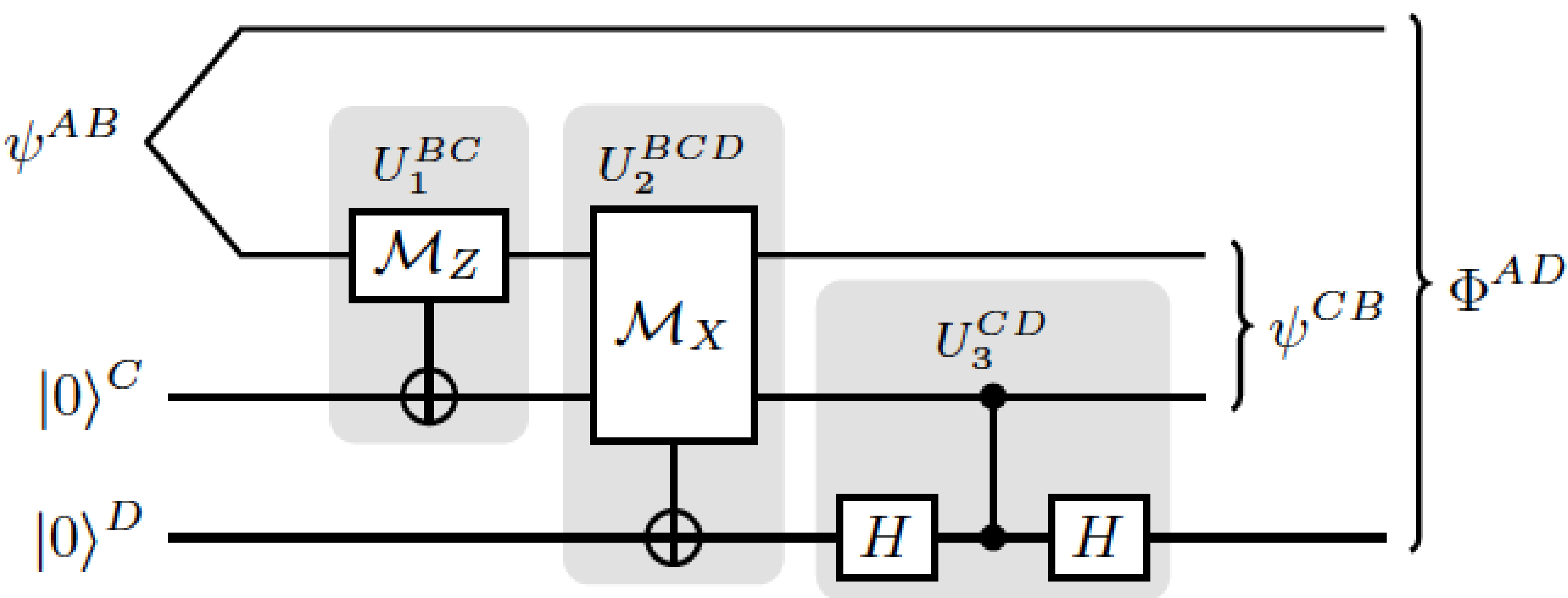
$N \bullet I(Z;B)$ channels **good for Amplitude**

$N \bullet I(X;BC)$ channels **good for Phase**

Can show that **net rate** of quantum communication is

$$I(Z;B) + I(X;BC) - 1 = I(A\rangle B)$$

Decoder operates coherently



Wilde and Renes, (missed out on 1111.1111---will try for 1212.1212)

Superactivation with near-explicit codes

Get near explicit codes for **superactivation** as a bonus!

Example of channels found by Smith and Yard
each have **4-dimensional inputs**,
Giving a **16-dimensional** input space for joint channel

Factor this as a tensor product of **4 qubit input spaces**,
and then apply a slightly modified version
of the amplitude and phase construction

Coherently decode the amplitude and phase variables in the order:

Z1,
Z2 | Z1,
Z3 | Z1 Z2,
Z4 | Z1 Z2 Z3,
X1 | Z1 Z2 Z3 Z4,
X2 | Z1 Z2 Z3 Z4 X1,
X3 | Z1 Z2 Z3 Z4 X1 X2,
X4 | Z1 Z2 Z3 Z4 X1 X2 X3,

Wilde and Renes, (missed out on 1111.1111---will try for 1212.1212)

Conclusion

Polar coding gives a
near-explicit, capacity-achieving scheme
for classical, private, and quantum communication

Even gives a near-explicit scheme for **superactivation**

Most important open problem:

Show how to make the decoder **efficient**
(progress in Renes *et al*. arXiv:1109.3195 for Pauli channels)

Other important problems:

1) Which channels are the good ones?
2) Extend to other scenarios