Polar codes for private classical communication

Mark M. Wilde

School of Computer Science
McGill University

In collaboration with
Joseph M. Renes (ETH)

arXiv:1203.5794

International Symposium on Information Theory and Applications (ISITA 2012),
Honolulu, HI, Wednesday, October 31, 2012

Quantum Wiretap Channel

A simple model for a quantum wiretap channel:

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

Each density operator above "lives" on the
tensor product Hilbert space
for the legitimate receiver *B* and the wiretapper *E*

Goal:

Use the above channel *many times* in order to achieve the **highest rate** of communication possible, such that

1) the **error probability** for the legitimate receiver is asymptotically negligible

2) the messages are **asymptotically indistinguishable** to the wiretapper.

Entropic Uncertainty Relation

Suppose that Alice, Bob, and Eve share a tripartite state:

Suppose further that Alice's system is a qubit

Alice could measure an observable X on her system and Bob's uncertainty about the result is quantified by $H(X|B)$

Alice could also measure a conjugate observable Z on her system and Eve's uncertainty about the result is quantified by $H(Z|E)$

The following uncertainty relation (*Renes and Boileau*) applies

$$H(X|B) + H(Z|E) \geq 1$$

Interpretation: If Bob can guess X, then Eve can't guess Z!

This is the basis of our scheme for private classical communication

Review of Polar Codes for Classical Communication

Classical-Quantum Channels

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

$$W : x \longrightarrow \rho_x$$

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*

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*

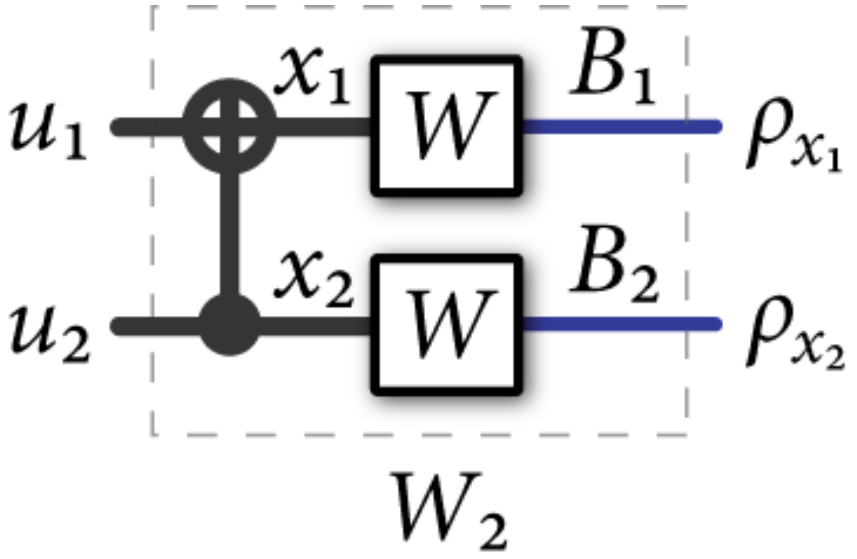
Generalizes classical fidelity (Bhattacharya parameter)

Channel Polarization

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

$$W : x \longrightarrow \rho_x$$

Take two copies of this channel and perform encoding:



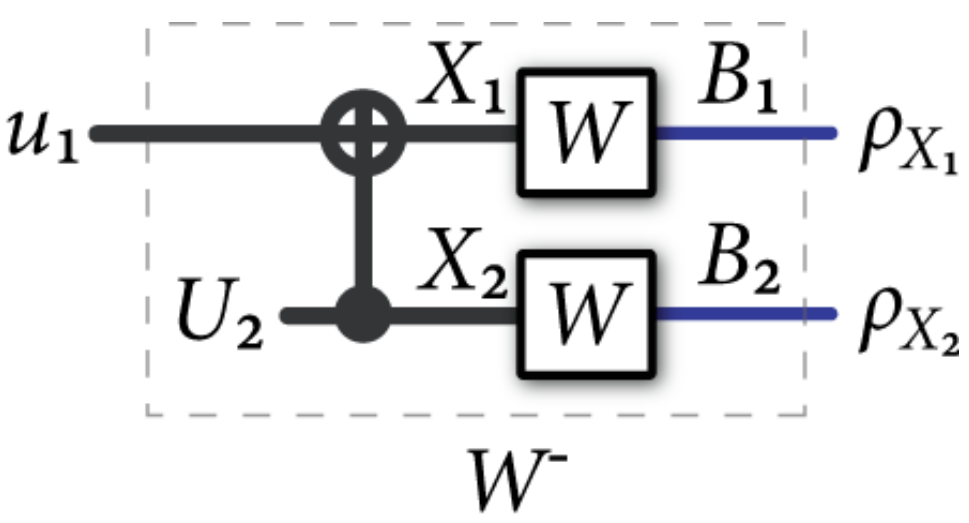
Observe that

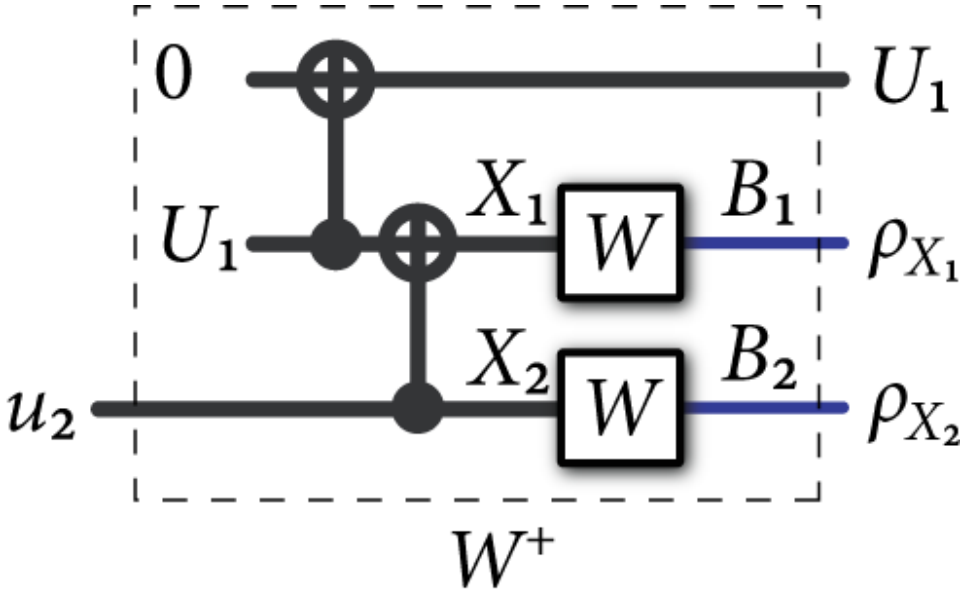
$$\begin{aligned} 2I(W) &= I(X_1X_2; B_1B_2) \\ &= I(U_1U_2; B_1B_2) \\ &= I(U_1; B_1B_2) + I(U_2; B_1B_2U_1) \end{aligned}$$

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.)

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

Polar Coding Scheme

Encoding circuit—same as Arikan's, though use fidelity for polar coding rule

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

Wilde and Guha, arXiv:1109.2591, Pranab Sen, Lemma 3 of arXiv:1109.0802

Polar Codes for Private Classical Communication

Towards Private Polar Codes

Use amplitude and phase coding ideas of Renes and Boileau

Suppose we're trying to code for a channel $\mathcal{N}^{A' \to B}$

Consider polar coding for a cq channel:

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

From before, we know that
there is a polar code for this channel with rate $I(Z;B)$

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1203.5794

Towards Private Polar Codes

Now, consider a cq phase channel with quantum side info.

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

where the state on *CA'* is the maximally entangled Bell state (just assuming for the moment that Bob has *C*)

This is a virtual channel!

We also know that there is a good polar encoder and decoder for this virtual channel with rate $I(X;BC)$

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1203.5794

Private Polar Codes

Build private polar codes from these 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, good for Phase: send information bits into these

Good for Amp, bad for Phase: send random bits into these

Bad for Amp, good for Phase: send ancilla bits 0 into these

Bad for Amp, bad for Phase: send shares of secret key bits into these

Wilde and Renes, arXiv:1203.5794

Security from Uncertainty Relation

Due to the entropic uncertainty relation:

$$H(X|B) + H(Z|E) \geq 1$$

the virtual channels which are **good in phase** for Bob
must be **bad in amplitude** for Eve.

This then implies security of our scheme (see paper for details)

Note: Our construction applies equally well
to classical wiretap channels because
these can be understood as quantum wiretap channels

Wilde and Renes, arXiv:1203.5794

Rates of Communication

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

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

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

$$I(Z;B) + I(X;BC) - 1 = I(Z;B) - I(Z;E)$$

(This is the rate of information bits minus the rate of secret key bits consumed)

We can show that the rate of secret key bits vanishes in the case of degraded quantum wiretap channels

Wilde and Renes, arXiv:1203.5794

Conclusion

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

Most important open problem:

Show how to make the decoder **efficient**
(progress in Renes, Dupuis, Renner (arXiv:1109.3195) for Pauli channels)

Other important problems:

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