Quantum polar codes for arbitrary channels

Mark M. Wilde

School of Computer Science
McGill University

In collaboration with
Joseph M. Renes (ETH)

arXiv:1201.2906

2012 International Symposium on Information Theory (ISIT 2012),
Boston, MA, USA Monday, July 2, 2012

The Quantum Coding Problem

We have some idea of good rates for
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.

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

Result is a **near-explicit, capacity-achieving scheme** for some quantum channels

Overview

Quantum codes from classical-quantum codes!

Using Arikan's code construction (encoder/decoder) directly would have suboptimal performance for general quantum channels...

Though, a generalization of the decoder to classical input, quantum output channels is helpful for us

First discuss polar codes for classical-quantum channels

Then discuss quantum polar codes from classical-quantum ones

Finally outline how quantum polar codes exhibit superactivation

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 one for *perfect channels* and zero 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)

Quantum Hypothesis Testing

Suppose someone else prepares ρ or σ with equal probability and then hands you the prepared system

Your task:

Perform a measurement to determine which state was prepared

Your measurement will be of the following form:

$$\{\Lambda_\rho, \Lambda_\sigma\} \quad \text{where} \quad \Lambda_\rho + \Lambda_\sigma = I$$

Error probability is then

$$p_{\text{err}} = \frac{1}{2}(\text{Tr}\{\Lambda_\rho \sigma\} + \text{Tr}\{\Lambda_\sigma \rho\})$$

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

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

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

Towards Quantum 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 coding for a cq channel:

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

Suppose there is a good decoding POVM $\{\Lambda_z\}$

$$\text{Tr}\{\Lambda_z \mathcal{N}(|z\rangle\langle z|)\} \geq 1-\epsilon$$

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1201.2906

Towards Quantum Polar Codes

Similarly, consider the 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*)

Suppose there is a good decoding POVM $\{\Gamma_x\}$

$$\mathrm{Tr}\{\Gamma_x \sigma_x^{BC}\} \geq 1 - \epsilon$$

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1201.2906

First Decoding Step

Initial state: $$\sum_z \sqrt{p(z)} |z\rangle^A |z\rangle^{A'}$$

State sent through channel: $$\sum_z \sqrt{p(z)} |z\rangle^A |\psi_z\rangle^{BE}$$

Coherent version of cq decoder: $$\sum_z \sqrt{\Lambda_z}^B \otimes |z\rangle^C$$

State after 1st decoding step:

$$\approx \sum_z \sqrt{p(z)} |z\rangle^A |\psi_z\rangle^{BE} |z\rangle^C$$

This approximation follows from performance of cq code

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1201.2906

Second Decoding Step

Rewrite the state using the Fourier basis:

$$\sum_z \sqrt{p(z)}|z\rangle^A|\psi_z\rangle^{BE}|z\rangle^C = \sum_x |\tilde{x}\rangle\langle\tilde{x}|^A \sum_z \sqrt{p(z)}|z\rangle^A|\psi_z\rangle^{BE}|z\rangle^C$$

$$= \sum_x |\tilde{x}\rangle^A \sum_z \langle\tilde{x}|z\rangle\sqrt{p(z)}|\psi_z\rangle^{BE}|z\rangle^C$$

$$= \frac{1}{\sqrt{d}}\sum_x |\tilde{x}\rangle^A (Z^{-x})^C \sum_z \sqrt{p(z)}|\psi_z\rangle^{BE}|z\rangle^C$$

Coherent version of cq phase decoder: $\sum_x \sqrt{\Gamma_x}^{BC} \otimes |\tilde{x}\rangle^D$

State after 2nd decoding step:

$$\approx \frac{1}{\sqrt{d}}\sum_x |\tilde{x}\rangle^A (Z^{-x})^C \sum_z \sqrt{p(z)}|\psi_z\rangle^{BE}|z\rangle^C|\tilde{x}\rangle^D$$

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1201.2906

Final Decoding Step

State after 2[nd] decoding step:

$$\approx \frac{1}{\sqrt{d}} \sum_x |\tilde{x}\rangle^A (Z^{-x})^C \sum_z \sqrt{p(z)} |\psi_z\rangle^{BE} |z\rangle^C |\tilde{x}\rangle^D$$

Bob performs controlled-phase gates on *C* and *D*:

$$\frac{1}{\sqrt{d}} \sum_x |\tilde{x}\rangle^A \sum_z \sqrt{p(z)} |\psi_z\rangle^{BE} |z\rangle^C |\tilde{x}\rangle^D$$

Rewrite this state as

$$\frac{1}{\sqrt{d}} \sum_x |\tilde{x}\rangle^A |\tilde{x}\rangle^D \otimes \sum_z \sqrt{p(z)} |\psi_z\rangle^{BE} |z\rangle^C$$

Decoding successful! (b/c maximal ent. shared between *A* and *D*)

Renes and Boileau, PRA 78, 032335 (2008), Wilde and Renes, arXiv:1201.2906

Quantum Polar Codes

Use amplitude and phase encoding ideas of Renes

Build quantum polar codes from cq channels:

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

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

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, arXiv:1201.2906

Construction (Ctd.)

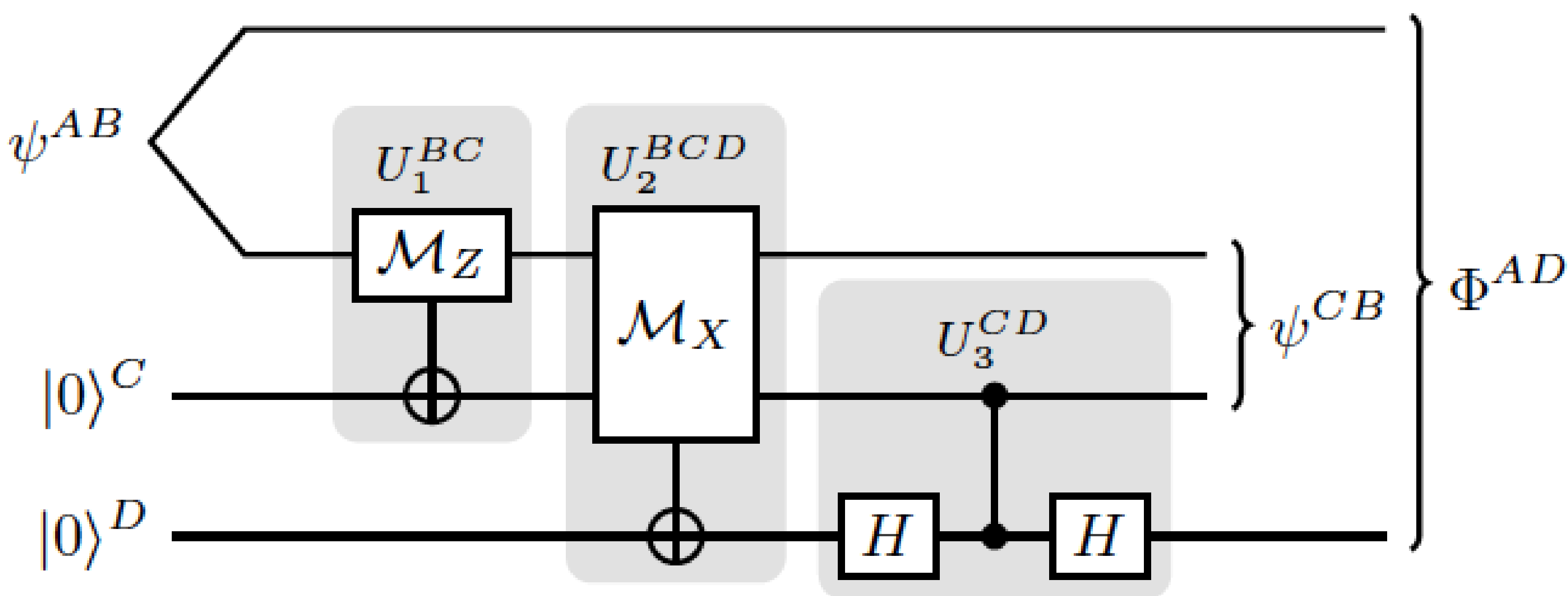
$N \cdot I(Z;B)$ channels **good for Amplitude**

$N \cdot I(X;BC)$ 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, arXiv:1201.2906

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, arXiv:1201.2906

Conclusion

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