Polar Codes for Classical, Private, and Quantum Communication

Mark M. Wilde
School of Computer Science
McGill University

Saikat Guha
Raytheon BBN Technologies


Quantum Information Processing 2012,
Montreal, Quebec, December 13, 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:

\[
W : x \rightarrow \rho_x
\]

Take two copies of this channel and perform encoding:

\[
\begin{align*}
W : u_1 x_1 &\rightarrow \rho_{x_1} \\
W : u_2 x_2 &\rightarrow \rho_{x_2}
\end{align*}
\]

Observe that

\[
2I(W) = I(X_1X_2; B_1B_2) = I(U_1U_2; B_1B_2) = I(U_1; B_1B_2) + I(U_2; B_1B_2U_1)
\]
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:

\[
\begin{align*}
R_4 \text{ is an operation which places all of the odd indices first} \\
\text{and even indices next}
\end{align*}
\]

Continue with chain rule:

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

\[ \frac{1}{N} \# \{ i : I(U_i; B_1^N U_1^{i-1}) \approx 1 \} \rightarrow I(W) \]

\[ \frac{1}{N} \# \{ i : I(U_i; B_1^N U_1^{i-1}) \approx 0 \} \rightarrow 1 - I(W) \]

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

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

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:

\[ x \rightarrow \rho^B_x \]

Channel to Bob:

\[ W : x \rightarrow \rho^B_x \]

Channel to Eve:

\[ W^* : x \rightarrow \rho^E_x \]

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 $|+\rangle$ 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 $|0\rangle$ 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*
Conclusion

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

**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