Quantum Polar Coding

Joseph M. Renes, Frédéric Dupuis, and Renato Renner
Institute for Theoretical Physics
ETH Zurich, Switzerland

August 29, 2011

Abstract

Polar coding, introduced 2008 by Arıkan, is the first efficiently encodable and decodable coding scheme that provably achieves the Shannon bound for the rate of information transmission over classical discrete memoryless channels (in the asymptotic limit of large block sizes). Here we study the use of polar codes for the efficient coding and decoding of quantum information. Focusing on the case of qubit channels we construct a coding scheme which, using some pre-shared entanglement, asymptotically achieves a net transmission rate equal to the coherent information. Furthermore, for channels with sufficiently low noise level, no pre-shared entanglement is required.

Polar Codes in Classical Information Theory

Polar codes are a family of error-correcting codes recently introduced by Arıkan [Arı09] in the context of classical information theory. The main feature of polar codes is that, in the limit of large block sizes, they provably achieve the symmetric capacity of classical discrete memoryless channels (DMCs) [ŞTA09], while allowing for efficient encoding and decoding (in $O(n\log(n))$ steps where n is the block length). Since their invention, polar codes have attracted considerable interest in the classical information theory community and various improvements and generalizations have been suggested (see, for instance, [MT09] for efficient constructions of polar codes, [KŞU10] for bounds on their error probabilities, and [HUK09, Kor09] for their use for source coding).

The main idea underlying the construction of polar codes is *channel polarization*: out of n identical DMCs one creates a new set of n logical channels by prepending an encoder, and these logical channels have the property that they are either "good" (nearly noiseless) or "bad" (have nearly zero capacity). Furthermore, for large n, the fraction of good channels is very close to the symmetric capacity [1] of the original DMC. To encode information, the encoder simply fixes or "freezes" the input to the bad channels (to a value known to the decoder) and directs the information to be transmitted to the good channels. The communication rate achieved by the scheme therefore corresponds to the fraction of good channels and hence, in the limit of large n, approaches the symmetric capacity of the original DMC. For a detailed description of polar coding for classical channels, we refer to Appendix A.

Main Results

We introduce a quantum version of polar codes and show that these have the following properties when applied to Pauli channels $\mathcal{N}$:

[1] The symmetric capacity is the mutual information of the output of a channel given a uniform input.

- Both the encoding and decoding operations are efficient. More precisely, they have complexity $O(n \log(n))$, where n is the block length.
- In the limit of large block lengths, the net rate of quantum information transmission approaches the coherent information of the channel. To formulate this more precisely, we consider the task of distributing entanglement. Assume that sender and receiver can invoke a channel $\mathcal{N}$ n times and, in addition, have access to a reservoir of shared entanglement. Then polar coding with block length n can be used to generate a net amount of entanglement $\Delta\ell(n)$ (i.e., $\Delta\ell(n)$ is the total number of freshly generated ebits minus the number of consumed ebits) such that

$$\lim_{n\to\infty} \frac{\Delta\ell(n)}{n} = -H(A|B)_\Psi \ .$$

  Here $-H(A|B)_\Psi$ denotes the *coherent information*, defined by $-H(A|B)_\Psi := H(\Psi^B) - H(\Psi^{AB})$, where $H(\cdot)$ is the von Neumann entropy. It is evaluated for the state $\Psi^{AB} = (\mathcal{I}\otimes\mathcal{N})(|\Phi\rangle\langle\Phi|^{AB})$ obtained by sending the B-part of a maximally entangled qubit $|\Phi\rangle^{AB}$ through the channel $\mathcal{N}$.
- If the noise level of the channel is below a certain threshold (see Figure 3) then no pre-shared entanglement is required to achieve the coherent information of the channel using polar codes.
- In addition, we provide numerical evidence for the conjecture that, even for large noise levels of the channel, no initial entanglement is required.
- Our construction yields CSS codes.

Proof idea

The proof of the above statements is divided into several steps. Each of these is explained in detail in a separate section of the appendix.

- In Appendix B, we show that polar coding has the following important property. If the classical coding operation is applied coherently to n qubits in a fixed basis (referred to as the *amplitude* basis) then this is equivalent to applying the coding operation to (appropriately reordered) qubits in a conjugate basis (the *phase* basis). In other words, the encoder simultaneously encodes in the amplitude and in the phase basis.
- In Appendix C, we use the polarizing property of classical polar codes to infer that polarization occurs simultaneously in the amplitude and in the phase basis. As in the classical case, a coding scheme is then constructed by "freezing" the inputs to the "bad" channels while using the "good" ones for the actual information transmission. The complication arising in the quantum case is that each of the individual channels may be "good" for both the amplitude and phase bases, "bad" for both of them, or "good" for one basis and "bad" for the other. Only the "doubly good" channels are used to transmit quantum information. Since the amplitude and phase bases are conjugate to each other, the inputs to the "doubly bad" channels cannot be fixed to a classical value. Instead, we use one half of the preshared entanglement to "freeze" the inputs to these channels.
- In Appendix D, we describe the construction of the decoder. The construction is based on coherently combining the classical decoders applied to the amplitude and the phase basis. The full protocol for channel transmission is then described in Appendix E.
- In Appendix F, we analyze our quantum generalization of polar coding and show that its net rate approaches the coherent information of the channel. Finally, in Appendix G, we analyze the need for initial entanglement.

Outlook

We have adapted the results for classical polar codes to show that there likewise exist efficiently encodable and decodable qubit codes, which when entanglement-assisted, achieve a communication rate equal to the coherent information for Pauli channels. An immediate practical application of such codes is to quantum key distribution. Due to the CSS nature of the codes, using the well-known relationship between CSS coding and secret key generation [SP00], our protocol can be converted into a means for efficient, high-rate secret key generation, possibly assisted by preshared key.

Our results merely initiate the study of quantum polar codes, as many unanswered questions remain. Most immediately is the issue of entanglement assistance. We have been able to rigorously show that it is not always necessary, but one would like to know that it is never necessary, a conjecture supported by numerical evidence. Beyond this, one would also like to extend the results to non-Pauli qubit channels as well as to more general qudit channels.

References

[Arı09] E. Arıkan. Channel polarization: A method for constructing Capacity-Achieving codes for symmetric Binary-Input memoryless channels. *IEEE Transactions on Information Theory*, 55(7):3051–3073, July 2009.

[AT09] E. Arıkan and E. Telatar. On the rate of channel polarization. In *IEEE International Symposium on Information Theory 2009*, pages 1493–1495. IEEE, July 2009.

[HUK09] N. Hussami, R. Urbanke, and S. B Korada. Performance of polar codes for channel and source coding. In *IEEE International Symposium on Information Theory 2009*, pages 1488–1492. IEEE, July 2009.

[KŞU10] S. B Korada, E. Şaşoğlu, and R. Urbanke. Polar codes: Characterization of exponent, bounds, and constructions. *IEEE Transactions on Information Theory*, 56(12):6253–6264, December 2010.

[Kor09] S. B. Korada. *Polar codes for channel and source coding*. PhD thesis, EPFL, Lausanne, Switzerland, 2009.

[MT09] R. Mori and T. Tanka. In *IEEE International Symposium on Information Theory 2009*, pages 1496–1500. IEEE Press, July 2009.

[ŞTA09] E. Şaşoğlu, E. Telatar, and E. Arıkan. Polarization for arbitrary discrete memoryless channels. In *IEEE Information Theory Workshop 2009*, pages 144–148. IEEE, October 2009.

[SP00] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2):441, July 2000.