10-22-2012

Quantum polar codes for arbitrary channels

Mark M. Wilde
Université McGill

Joseph M. Renes
ETH Zürich

Recommended Citation
Wilde, M., & Renes, J. (2012). Quantum polar codes for arbitrary channels. *IEEE International Symposium on Information Theory - Proceedings*, 334-338. https://doi.org/10.1109/ISIT.2012.6284203

Quantum polar codes for arbitrary channels

Mark M. Wilde
School of Computer Science, McGill University
Montreal, Quebec, Canada

Joseph M. Renes
Institut für Theoretische Physik, ETH Zurich
Zürich, Switzerland

***Abstract*—We construct a new entanglement-assisted quantum polar coding scheme which achieves the symmetric coherent information rate by synthesizing "amplitude" and "phase" channels from a given, *arbitrary* quantum channel. We first demonstrate the coding scheme for arbitrary quantum channels with qubit inputs, and we show that quantum data can be reliably decoded by $O(N)$ rounds of coherent quantum successive cancellation, followed by N controlled-NOT gates (where N is the number of channel uses). We also find that the entanglement consumption rate of the code vanishes for *degradable* quantum channels. Finally, we extend the coding scheme to channels with multiple qubit inputs. This gives a near-explicit method for realizing one of the most striking phenomena in quantum information theory: the *superactivation effect*, whereby two quantum channels which individually have zero quantum capacity can have a non-zero quantum capacity when used together.**

Polar coding is a promising code construction for transmitting classical information over classical channels [1]. Arikan proved that polar codes achieve the symmetric capacity of any classical channel [1], with an encoding and decoding complexity that is $O(N\log N)$ where N is the number of channel uses. These codes exploit the channel polarization effect whereby a particular recursive encoding induces a set of virtual channels, such that a fraction of the virtual channels are perfect for data transmission while the other fraction are useless for this task. The fraction containing perfect virtual channels is equal to the channel's symmetric capacity.

In this paper, we offer a new quantum polar coding scheme strongly based on ideas of Renes and Boileau [2], who showed that quantum coding protocols can be constructed from two different protocols that protect classical information encoded into complementary observables. In particular, a protocol for reliably transmitting quantum data can be built from a protocol that reliably recovers classical information encoded into an "amplitude" observable and a protocol that reliably recovers "phase" information with the assistance of quantum side information (see Refs. [3], [4], [5], [6] for related ideas).

These ideas were used to construct a quantum polar coding scheme with an efficient decoder in [7], but only for a certain set of channels with essentially classical outputs. Following a different approach, Ref. [8] constructed quantum polar codes for degradable channels. Our new quantum polar coding scheme has several advantages over these previous schemes:

- The net rate of quantum communication is equal to the symmetric coherent information for an *arbitrary* quantum channel with qubit input.
- The decoder is *explicit*, and consists of $O(N)$ rounds of coherent quantum successive cancellation followed by N CNOT gates.
- The entanglement consumption rate vanishes for an *arbitrary* degradable channel with qubit input.

Following the multi-level coding method of Ref. [9], we show how to extend the coding scheme to channels with multiple qubit inputs. This gives an explicit code construction for the superactivation effect, in which two zero-capacity channels have a non-zero quantum capacity when used together [10] (in this sense, the channels *activate* each other).

I. Quantum Polar Coding Scheme

A. Classical-quantum channels for complementary variables

Consider a quantum channel $\mathcal{N}$ with a two-dimensional input system A' and a d-dimensional output system B. Let $U_{\mathcal{N}}^{A'\to BE}$ denote the isometric extension of this channel. Let $|z\rangle$ denote the computational or "amplitude" basis with $z\in\{0,1\}$, and let $|\widetilde{x}\rangle$ denote the conjugate, Hadamard, or "phase" basis with $\widetilde{x}\in\{+,-\}$ and $|\pm\rangle\equiv(|0\rangle\pm|1\rangle)/\sqrt{2}$.

Following Ref. [2], we consider building up a quantum communication protocol from two classical communication protocols that preserve classical information encoded into complementary variables. In this vein, two particular classical-quantum (cq) channels are important. First, consider the cq channel induced by sending an amplitude basis state over $\mathcal{N}$:

$$W_A : z\to\mathcal{N}^{A'\to B}\left(|z\rangle\langle z|\right)\equiv\phi_z^B, \tag{1}$$

where the classical input z is a binary variable and the notation W_A indicates that the classical information is encoded into the amplitude basis. We can regard this as the sender (Alice) modulating a standard signal $|0\rangle$ with X^z and transmitting the result to the receiver (Bob).

For the other cq channel, suppose that Alice instead transmits a binary variable x by modulating the signal with Z^x, a rephasing of the amplitude basis states. However, instead of applying this to $|0\rangle$, she modulates one half of an entangled qubit pair (ebit) shared with Bob. These qubits are in the state

$$|\Phi\rangle^{CA'}\equiv\frac{1}{\sqrt{2}}\sum_{z\in\{0,1\}}|z\rangle^C|z\rangle^{A'}=\frac{1}{\sqrt{2}}\sum_{\widetilde{x}\in\{+,-\}}|\widetilde{x}\rangle^C|\widetilde{x}\rangle^{A'},$$

with Alice holding A' and Bob C. The modulation yields

$$|\sigma_x\rangle^{BCE}=U_{\mathcal{N}}^{A'\to BE}\left(Z^x\right)^{A'}|\Phi\rangle^{A'C}, \tag{2}$$

$$=\tfrac{1}{\sqrt{2}}\sum_{z\in\{0,1\}}(-1)^{xz}|\phi_z\rangle^{BE}|z\rangle^C, \tag{3}$$

where $|\phi_z\rangle^{BE}$ is a purification of ϕ_z^B in (1). The resulting cq channel is then of the following form:

$$W_P : x \to \sigma_x^{BC}, \tag{4}$$

where the notation W_P indicates that the classical information is encoded into a phase variable. In contrast to W_A, the channel W_P is one in which the receiver has quantum side information (in the form of system C) that is helpful for decoding the transmitted phase information.[1]

Both cq channels in (1) and (4) arise in the error analysis of our quantum polar coding scheme, in the sense that its performance depends on the performance of constituent polar codes constructed for these cq channels. Moreover, the two channels are more closely related than they may initially appear. To see their relationship, consider the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} |\widetilde{x}\rangle^A |\sigma_x\rangle^{BCE} = \frac{1}{\sqrt{2}} \sum_{z\in\{0,1\}} |z\rangle^A |z\rangle^C |\phi_z\rangle^{BE}.$$

Measuring system A in the phase basis $|\widetilde{x}\rangle$ generates the W_P output state σ_x^{BE}, while measuring A in the amplitude basis generates the W_A output ϕ_z^B.

Another important channel is the cq channel W_E induced to the environment when inputting amplitude-encoded classical information: $W_E : z \to \mathrm{Tr}_B\{U_N^{A'\to BE}(|z\rangle\langle z|)\}$. We do not consider this channel for our quantum polar coding scheme or its error analysis, but we instead consider it in Section II when relating the quantum polar coding scheme of this paper to the previous one from Ref. [8].

B. Channel Polarization

Two channel parameters that determine the performance of a cq channel $W : x \to \rho_x$ are the fidelity $F(W) \equiv \left\|\sqrt{\rho_0}\sqrt{\rho_1}\right\|_1^2$ and the symmetric Holevo information $I(W) \equiv H((\rho_0+\rho_1)/2) - [H(\rho_0)+H(\rho_1)]/2$ where $H(\sigma) \equiv -\mathrm{Tr}\{\sigma \log_2 \sigma\}$ is the von Neumann entropy. These parameters generalize the Bhattacharya parameter and the symmetric mutual information [1], respectively, and are related as $I(W) \approx 1 \Leftrightarrow F(W) \approx 0$ and $I(W) \approx 0 \Leftrightarrow F(W) \approx 1$ [11]. The channel W is near perfect when $I(W) \approx 1$ and near useless when $I(W) \approx 0$.

Ref. [11] demonstrated how to construct synthesized versions of W, by channel combining and splitting [1]. For blocksize N, the synthesized channels are of the following form:

$$W_N^{(i)} : u_i \to \rho_{(i),u_i}^{U_1^{i-1}B^N}, \tag{5}$$

where

$$\rho_{(i),u_i}^{U_1^{i-1}B^N} \equiv \sum_{u_1^{i-1}} \frac{1}{2^{i-1}} \left|u_1^{i-1}\right\rangle\left\langle u_1^{i-1}\right|^{U_1^{i-1}} \otimes \overline{\rho}_{u_1^i}^{B^N}, \tag{6}$$

$$\overline{\rho}_{u_1^i}^{B^N} \equiv \sum_{u_{i+1}^N} \frac{1}{2^{N-i}} \rho_{u^N G_N}^{B^N}, \qquad \rho_{x^N}^{B^N} \equiv \rho_{x_1}^{B_1} \otimes \cdots \otimes \rho_{x_N}^{B_N},$$

and G_N is Arikan's encoding circuit matrix built from classical CNOT and permutation gates. The interpretation of this channel is that it is the one "seen" by the input u_i if all of the previous bits u_1^{i-1} are available and if we consider all the future bits u_{i+1}^N as randomized. This motivates the development of a quantum successive cancellation decoder (QSCD) [11] that attempts to distinguish $u_i = 0$ from $u_i = 1$ by adaptively exploiting the results of previous measurements and quantum hypothesis tests for each bit decision.

The synthesized channels $W_N^{(i)}$ polarize, in the sense that some become nearly perfect for classical data transmission while others become nearly useless. To prove this result, one can model the channel splitting and combining process as a random birth process [1], [11], and one can demonstrate that the induced random birth processes corresponding to the channel parameters $I(W_N^{(i)})$ and $F(W_N^{(i)})$ are martingales that converge almost surely to zero-one valued random variables in the limit of many recursions. The following theorem characterizes the rate with which the channel polarization effect takes hold [11], and it is useful in proving statements about the performance of polar codes for cq channels:

Theorem 1: Given a binary input cq channel W and any $\beta < 1/2$, it holds that $\lim_{n\to\infty} \mathrm{Pr}_I\{\sqrt{F(W_{2^n}^{(I)})} < 2^{-2^{n\beta}}\} = I(W)$, where n indicates the level of recursion for the encoding, $W_{2^n}^{(I)}$ is a random variable characterizing the I^{th} split channel, and $F(W_{2^n}^{(I)})$ is the fidelity of that channel.

Assuming knowledge of the good and bad channels, one can then construct a coding scheme based on the channel polarization effect, by dividing the synthesized channels according to the following polar coding rule:

$$\mathcal{G}_N(W,\beta) \equiv \left\{ i \in [N] : \sqrt{F(W_N^{(i)})} < 2^{-N^\beta} \right\}, \tag{7}$$

and $\mathcal{B}_N(W,\beta) \equiv [N] \setminus \mathcal{G}_N(W,\beta)$, so that $\mathcal{G}_N(W,\beta)$ is the set of "good" channels and $\mathcal{B}_N(W,\beta)$ is the set of "bad" channels. The sender then transmits the information bits through the good channels and "frozen" bits through the bad ones. A helpful assumption for error analysis is that the frozen bits are chosen uniformly at random such that the sender and receiver both have access to these frozen bits. Ref. [11] provided an explicit construction of a QSCD that has an error probability equal to $o(2^{-N^\beta})$—let $\{\Lambda_{u_\mathcal{A}}^{(u_{\mathcal{A}^c})}\}$ denote the corresponding decoding POVM, with $u_\mathcal{A}$ the information bits and $u_{\mathcal{A}^c}$ the frozen bits.

For our quantum polar coding scheme, we exploit a coherent version of Arikan's encoder [1], meaning that the gates are quantum CNOTs and permutations (this is the same encoder as in Refs. [7], [8]). When sending amplitude-basis classical information through the encoder and channels, the effect is to induce synthesized channels $W_{A,N}^{(i)}$ as described above. Theorem 1 states that the fraction of amplitude-good channels (according to the criterion in (7)) is equal to $I(Z;B)_\phi$ where the Holevo information $I(Z;B)_\phi$ is evaluated with respect to the cq state $\phi^{ZB} = \frac{1}{2}\sum_{z\in\{0,1\}} |z\rangle\langle z|^Z \otimes \phi_z^B$, with ϕ_z^B defined in (1). It will be convenient to express this quantity as

[1]Operationally, this quantum side information becomes available to Bob after he coherently decodes the amplitude variable. It does *not* correspond operationally to a Bell state shared before communication begins.

$I(Z^A;B)_\psi$ using the state $|\psi\rangle$, where the Z^A indicates that system A is first measured in the amplitude basis.

As in [7], the same encoding operation leads to channel polarization for the phase channel W_P as well. Suppose Alice modulates her halves of the entangled pairs as before, but then inputs them to the coherent encoder before sending them via the channel to Bob. The result is

$$\frac{1}{\sqrt{2^N}} \sum_{z^N \in \{0,1\}^N} (-1)^{x^N \cdot z^N} \left|\phi_{z^N G_N}\right\rangle^{B^N E^N} \left|z^N\right\rangle^{C^N}, \quad (8)$$

whose $B^N C^N$ marginal state is simply $U_\mathcal{E}^{C^N} \sigma_{x^N G_N^T}^{B^N C^N} U_\mathcal{E}^{\dagger C^N}$, where $U_\mathcal{E}$ denotes the polar encoder. Here we have used the fact that the matrix corresponding to G_N is invertible. Thus, the coherent encoder also induces synthesized channels $W_{P,N}^{(i)}$ using the encoding matrix G_N^T instead of G_N, modulo the additional $U_\mathcal{E}$ acting on C^N. Note that the classical side information for the $W_{P,N}^{(i)}$ is different from that in (5) because the direction of all CNOT gates is flipped due to the transpose of G_N when acting on phase variables. The change in the direction of the CNOT gates means that the i^{th} synthesized phase channel $W_{P,N}^{(i)}$ is such that all of the *future* bits $x_N \cdots x_{i+1}$ are available to help in decoding bit x_i while all of the *previous* bits $x_{i-1} \cdots x_1$ are randomized. (This is the same as described in Ref. [7] for Pauli channels.)

For the channel in (4), the fraction of phase-good channels is approximately equal to $I(X;BC)_\sigma$, where the Holevo information $I(X;BC)_\sigma$ is with respect to a cq state of the form $\frac{1}{2}\sum_{x\in\{0,1\}} |x\rangle\langle x|^X \otimes \sigma_x^{BC}$, with σ_x^{BC} in (4). Again, we can formulate this using $|\psi\rangle$ as $I(X^A;BC)_\psi$, this time X^A indicating A is measured in the phase basis.

Lemma 2 of Ref. [2] outlines an important relationship between the Holevo information of the phase channel to Bob and the Holevo information of the amplitude channel to Eve, which for our case reduces to $I\left(X^A;BC\right)_\psi = 1 - I\left(Z^A;E\right)_\psi$. This relationship already suggests that channels which are phase-good for Bob should be amplitude-bad for Eve and that channels which are amplitude-good for Eve should be phase-bad for Bob, allowing us in Section II to relate the present quantum polar coding scheme to that from Ref. [8].

C. Coding scheme

We divide the synthesized cq amplitude channels $W_{A,N}^{(i)}$ into sets $\mathcal{G}_N(W_A,\beta)$ and $\mathcal{B}_N(W_A,\beta)$ according to (7), and similarly, we divide the synthesized cq phase channels $W_{P,N}^{(i)}$ into sets $\mathcal{G}_N(W_P,\beta)$ and $\mathcal{B}_N(W_P,\beta)$, where $\beta < 1/2$. The synthesized channels correspond to particular inputs to the encoding operation, and thus the set of all inputs divides into four groups: those that are good for both the amplitude and phase variable, those that are good for amplitude and bad for phase, bad for amplitude and good for phase, and those that are bad for both variables. We establish notation for these channels as follows:

$$\mathcal{A} \equiv \mathcal{G}_N(W_A,\beta) \cap \mathcal{G}_N(W_P,\beta),$$
$$\mathcal{X} \equiv \mathcal{G}_N(W_A,\beta) \cap \mathcal{B}_N(W_P,\beta),$$
$$\mathcal{Z} \equiv \mathcal{B}_N(W_A,\beta) \cap \mathcal{G}_N(W_P,\beta),$$
$$\mathcal{B} \equiv \mathcal{B}_N(W_A,\beta) \cap \mathcal{B}_N(W_P,\beta).$$

Our quantum polar coding scheme has the sender transmit information qubits through the inputs in $\mathcal{A}$, frozen bits in the phase basis through the inputs in $\mathcal{X}$, frozen bits in the amplitude basis through the inputs in $\mathcal{Z}$, and halves of ebits [12] through the inputs in $\mathcal{B}$ (we can think of these in some sense as being frozen simultaneously in both the amplitude and phase basis). It is straightforward to prove (see Appendix A) that the net rate [12] of quantum communication $(|\mathcal{A}| - |\mathcal{B}|)/N$ is equal to the coherent information $I(A\rangle B) \equiv H(B) - H(AB)$ by observing that the fraction of amplitude-good channels is $I\left(Z^A;B\right)_\psi$, the fraction of phase-good channels is $I\left(X^A;BC\right)_\psi$, and exploiting the relation $I\left(X^A;BC\right)_\psi = 1 - I\left(Z^A;E\right)_\psi$.

D. Error Analysis

We now demonstrate that this coding scheme works well. The sender and receiver begin with the following state:

$$|\Psi_0\rangle = N_0 \sum_{u_\mathcal{A}, u_\mathcal{B}} |u_\mathcal{A}\rangle |u_\mathcal{A}\rangle |u_\mathcal{Z}\rangle |\widetilde{u}_\mathcal{X}\rangle |u_\mathcal{B}\rangle \otimes |u_\mathcal{B}\rangle,$$

where Alice possesses the first five registers, Bob the last one,[2] and $N_0 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}$. We also assume for now that the bits in $u_\mathcal{Z}$ and $u_\mathcal{X}$ are chosen uniformly at random and are known to both the sender and receiver. Note that the 4^{th} register is expressed in the phase basis; the amplitude basis instead gives

$$|\Psi_0\rangle = N_1 \sum_{u_\mathcal{A}, u_\mathcal{B}, v_\mathcal{X}} (-1)^{u_\mathcal{X} \cdot v_\mathcal{X}} |u_\mathcal{A}\rangle |u_\mathcal{A}\rangle |u_\mathcal{Z}\rangle |v_\mathcal{X}\rangle |u_\mathcal{B}\rangle \otimes |u_\mathcal{B}\rangle,$$

where $N_1 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}$. The sender then feeds the middle four registers through the polar encoder and channel, leading to a state of the following form:

$$|\Psi_1\rangle = N_1 \sum_{u_\mathcal{A}, u_\mathcal{B}, v_\mathcal{X}} (-1)^{u_\mathcal{X} \cdot v_\mathcal{X}} |u_\mathcal{A}\rangle \otimes \left|\phi_{u_\mathcal{A}, u_\mathcal{Z}, v_\mathcal{X}, u_\mathcal{B}}\right\rangle^{B^N E^N} |u_\mathcal{B}\rangle,$$

where $\left|\phi_{u_\mathcal{A}, u_\mathcal{Z}, v_\mathcal{X}, u_\mathcal{B}}\right\rangle^{B^N E^N} \equiv U_\mathcal{N}^{\otimes N} U_\mathcal{E} |u_\mathcal{A}\rangle |u_\mathcal{Z}\rangle |v_\mathcal{X}\rangle |u_\mathcal{B}\rangle$ (abusing notation, the encoding operation G_N is left implicit).

Observe that, conditioned on amplitude measurements of $|u_\mathcal{A}\rangle$ and $|u_\mathcal{B}\rangle$, the B^N subsystem is identical to the polar-encoded output of W_A. Thus, the first step of the decoder is the following coherent implementation of the QSCD for W_A as in (1):

$$\sum_{u_\mathcal{A}, u_\mathcal{B}, v_\mathcal{X}} \sqrt{\Lambda_{u_\mathcal{A}, v_\mathcal{X}}^{(u_\mathcal{B}, u_\mathcal{Z})}} \otimes |u_\mathcal{A}\rangle |v_\mathcal{X}\rangle \otimes |u_\mathcal{B}\rangle |u_\mathcal{B}\rangle \langle u_\mathcal{B}| \otimes |u_\mathcal{Z}\rangle. \quad (9)$$

The idea here is that the decoder is coherently recovering the bits in $u_\mathcal{A}$ and $v_\mathcal{X}$ while using those in $u_\mathcal{Z}$ and $u_\mathcal{B}$ as classical and quantum side information, respectively. After doing so, the

[2] In quantum information theory the tensor product symbol is often used implicitly. Our convention is to leave it implicit for systems belonging to the same party and use it explicitly to denote a division between two parties.

resulting state is $o(2^{-N^{\beta}})$-close in expected trace distance to the following ideal state (see Appendix B):

$$|\Psi_2\rangle = N_1 \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}}} (-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}} |u_{\mathcal{A}}\rangle |\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^N E^N} \otimes |u_{\mathcal{A}}\rangle |v_{\mathcal{X}}\rangle |u_{\mathcal{B}}\rangle |u_{\mathcal{B}}\rangle |u_{\mathcal{Z}}\rangle .$$

The expectation is with respect to the uniformly random choice of $u_{\mathcal{X}}$. Thus, Bob has coherently recovered the bits $u_{\mathcal{A}}$ and $v_{\mathcal{X}}$ with the decoder in (9), while making a second coherent and incoherent copy of the bits $u_{\mathcal{B}}$ and $u_{\mathcal{Z}}$, respectively.

The next step in the process is to make coherent use of the W_P decoder. For this to be useful, however, we must show that encoded versions of $|\sigma_x\rangle^{BCE}$, as in (8), are present in $|\Psi_2\rangle$. To see this, first observe that we can write

$$|\Psi_2\rangle = N_2 \sum_{\substack{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},\\ x_{\mathcal{A}},x_{\mathcal{B}}}} (-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}+x_{\mathcal{A}}\cdot u_{\mathcal{A}}+x_{\mathcal{B}}\cdot u_{\mathcal{B}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^N E^N} |u_{\mathcal{A}}\rangle |v_{\mathcal{X}}\rangle |u_{\mathcal{B}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle |u_{\mathcal{Z}}\rangle ,$$

where $N_2 \equiv 1/\sqrt{2^{2|\mathcal{A}|+2|\mathcal{B}|+|\mathcal{X}|}}$, by expressing the first register and the second $|u_{\mathcal{B}}\rangle$ register in the phase basis. This is nearly the expression we are looking for, as all the desired phase factors are present, except one corresponding to $|u_{\mathcal{Z}}\rangle$.

As $u_{\mathcal{Z}}$ is chosen at random, we can describe it quantum-mechanically as arising from part of an entangled state. The other part is shared by Alice and an inaccessible reference. Including this purification degree of freedom, $|\Psi_2\rangle$ becomes

$$|\Psi_2'\rangle = N_3 \sum_{\substack{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},\\ u_{\mathcal{Z}},x_{\mathcal{A}},x_{\mathcal{B}}}} (-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}+x_{\mathcal{A}}\cdot u_{\mathcal{A}}+x_{\mathcal{B}}\cdot u_{\mathcal{B}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^N E^N} |u_{\mathcal{A}}\rangle |v_{\mathcal{X}}\rangle |u_{\mathcal{B}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle |u_{\mathcal{Z}}\rangle \otimes |u_{\mathcal{Z}}\rangle ,$$

where $N_3 = N_2/\sqrt{2^{|\mathcal{Z}|}}$. Again utilizing the phase basis gives

$$|\Psi_2'\rangle = N_3 \sum_{\substack{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},u_{\mathcal{Z}},\\ x_{\mathcal{A}},x_{\mathcal{B}},x_{\mathcal{Z}}}} (-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}+x_{\mathcal{A}}\cdot u_{\mathcal{A}}+x_{\mathcal{B}}\cdot u_{\mathcal{B}}+x_{\mathcal{Z}}\cdot u_{\mathcal{Z}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^N E^N} |u_{\mathcal{A}}\rangle |v_{\mathcal{X}}\rangle |u_{\mathcal{B}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle |u_{\mathcal{Z}}\rangle \otimes |\widetilde{x}_{\mathcal{Z}}\rangle .$$

Thus, $|\Psi_2'\rangle$ is a superposition of polar encoded states as in (8) and therefore the phase decoder will be useful to the receiver. In particular, Bob can first apply $U_{\mathcal{E}}^{\dagger C^N}$ and then apply

$$\sum_{x_{\mathcal{A}},x_{\mathcal{Z}},x_{\mathcal{B}}} \sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}}} \otimes |\widetilde{x}_{\mathcal{A}}\rangle |\widetilde{x}_{\mathcal{Z}}\rangle |\widetilde{u}_{\mathcal{X}}\rangle \otimes |\widetilde{x}_{\mathcal{B}}\rangle \langle \widetilde{x}_{\mathcal{B}}|$$

to coherently extract the values of $x_{\mathcal{A}}$ and $x_{\mathcal{Z}}$ using the frozen bits $x_{\mathcal{B}}$ and $u_{\mathcal{X}}$. He then applies $U_{\mathcal{E}}^{C^N}$ to restore the C^N registers to their previous form. As with the amplitude decoding step, the closeness of the output of this process to the ideal output is governed by the error probability of the W_P decoder (see Appendix B). To express the ideal output succinctly, we first make the assignments

$$|\Phi_{\mathcal{A}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{A}|}}} \sum_{u_{\mathcal{A}}} |u_{\mathcal{A}}\rangle |u_{\mathcal{A}}\rangle , \ |\Phi_{\mathcal{Z}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{Z}|}}} \sum_{v_{\mathcal{Z}}} |v_{\mathcal{Z}}\rangle |v_{\mathcal{Z}}\rangle ,$$

$$|\Phi_{\mathcal{X}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{X}|}}} \sum_{v_{\mathcal{X}}} |v_{\mathcal{X}}\rangle |v_{\mathcal{X}}\rangle , \ |\Phi_{\mathcal{B}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{B}|}}} \sum_{u_{\mathcal{B}}} |u_{\mathcal{B}}\rangle |u_{\mathcal{B}}\rangle .$$

Rewriting phase terms with Pauli operators, we then have that the actual output of this step of the decoder is $o(2^{-N^{\beta}})$-close in expected trace distance to the following ideal state:

$$|\Psi_3\rangle = N_4 \sum_{x_{\mathcal{A}},x_{\mathcal{B}},x_{\mathcal{Z}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\widetilde{x}_{\mathcal{A}}\rangle |\widetilde{x}_{\mathcal{Z}}\rangle |\widetilde{u}_{\mathcal{X}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle Z^{x_{\mathcal{A}},x_{\mathcal{Z}},u_{\mathcal{X}},x_{\mathcal{B}}} U_N^{\otimes N} U_{\mathcal{E}} |\Phi_{\mathcal{A}}\rangle |\Phi_{\mathcal{Z}}\rangle |\Phi_{\mathcal{X}}\rangle |\Phi_{\mathcal{B}}\rangle \otimes |\widetilde{x}_{\mathcal{Z}}\rangle ,$$

where $N_4 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{Z}|}}$. Here $Z^{x_{\mathcal{A}},x_{\mathcal{Z}},u_{\mathcal{X}},x_{\mathcal{B}}}$ is shorthand for $Z^{x_{\mathcal{A}}} \otimes Z^{x_{\mathcal{Z}}} \otimes Z^{u_{\mathcal{X}}} \otimes Z^{x_{\mathcal{B}}}$, which acts on the second qubits in the entangled pairs, while the encoding and channel unitaries act on the first.

The final step in the decoding process is to remove the phase operator $Z^{x_{\mathcal{A}},x_{\mathcal{Z}},v_{\mathcal{X}},x_{\mathcal{B}}}$ by controlled operations from the registers $|\widetilde{x}_{\mathcal{A}}\rangle |\widetilde{x}_{\mathcal{Z}}\rangle |\widetilde{u}_{\mathcal{X}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle$ to the second qubits in the entangled pairs. This phase-basis controlled phase operation is equivalent to N CNOT operations from the latter systems to the former and results in

$$N_0 \sum_{x_{\mathcal{A}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\widetilde{x}_{\mathcal{A}}\rangle U_N^{\otimes N} U_{\mathcal{E}} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle \sum_{x_{\mathcal{B}}} |u_{\mathcal{X}}\rangle |\widetilde{x}_{\mathcal{B}}\rangle ,$$

with Bob sharing $1/\sqrt{2^{|\mathcal{Z}|}} \sum_{x_{\mathcal{Z}}} |\widetilde{x}_{\mathcal{Z}}\rangle \otimes |\widetilde{x}_{\mathcal{Z}}\rangle$ with the inaccessible reference. Thus the sender and receiver generate $|A|$ ebits with fidelity $o(2^{-N^{\beta}})$ at the end of the protocol.

Remark 2: The above scheme performs well with respect to a uniformly random choice of the bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$, in the sense that the expectation of the fidelity is high. Though, we can invoke Markov's inequality to demonstrate that a large fraction of the possible codes have good performance.

Remark 3: The first step of the decoder is identical to the first step of the decoder from Ref. [8]. Though, the second step above is an improvement over the second step in Ref. [8] because it is an explicit coherent QSCD, rather than an inexplicit controlled-decoupling unitary. Additionally, the decoder's complexity is equivalent to $O(N)$ quantum hypothesis tests and other unitaries resulting from the polar decompositions of $\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v_{\mathcal{X}}}$ and $\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}}$, but it remains unclear how to implement these efficiently.

II. Zero e-bit rate for degradable channels

We can now prove that the entanglement consumption rate of our quantum polar coding scheme vanishes for an arbitrary degradable quantum channel. We provide a brief summary of the proof (see Appendix C for more detail). Consider the following entropic uncertainty principle [3]: $H(X^A|B)_{\rho}+H(Z^A|E)_{\rho} \geq 1$, where the conditional entropies are with respect to the phase and amplitude observables X and Z measured with respect to a tripartite state ρ^{ABE} with A being a qubit system. Using this and the fact that $H(X^A)+H(Z^A) = 2$ for our case, we can prove the following uncertainty relation for the i^{th} synthesized channels $W_{P,N}^{(i)}$ and $W_{E,N}^{(i)}$: $I(W_{P,N}^{(i)}) + I(W_{E,N}^{(i)}) \leq 1$, which is reminiscent of the relation $I(X;BC) = 1 - I(Z;E)$ mentioned previously. The above uncertainty relation then implies the following one: $2\sqrt{F(W_{P,N}^{(i)})} + \sqrt{F(W_{E,N}^{(i)})} \geq 1$. This in turn implies that the phase-good channels to Bob are amplitude-"very bad" channels to Eve. From degradability, we also know that the doubly-bad channels in $\mathcal{B}$ are amplitude-bad channels to Eve. These two observations imply that the phase-good channels to Bob, the doubly-bad channels to Bob, and amplitude-good channels to Eve are disjoint sets. Furthermore, we know from Theorem 1 that the sum rate of the phase-good channels to Bob and the amplitude-good channels to Eve is equal to $I(X;BC) + I(Z;E) = 1 - I(Z;E) + I(Z;E) = 1$ as $N \to \infty$, implying that the rate of the doubly-bad channel set $\mathcal{B}$ (the entanglement consumption rate) approaches zero in the same limit. This same argument implies that the entanglement consumption rate for the quantum polar codes in Ref. [8] vanishes for degradable quantum channels because the rate of the phase-good channels to Bob is a lower bound on the rate of the amplitude-"very bad" channels to Eve.

III. Superactivation

Our quantum polar coding scheme can be adapted to realize the superactivation effect, in which two zero-capacity quantum channels can *activate* each other when used jointly, such that the joint channel has a non-zero quantum capacity [10]. Recall that the channels from Ref. [10] are a four-dimensional PPT channel and a four-dimensional 50% erasure channel. Each of these have zero quantum capacity, but the joint tensor-product channel has non-zero capacity.[3]

We now discuss how to realize a quantum polar coding scheme for the joint channel. Observe that the input space of the joint channel is 16-dimensional and thus has a decomposition as a tensor product of four qubit-input spaces: $\mathbb{C}^4 \otimes \mathbb{C}^4 \simeq \mathbb{C}^{16} \simeq \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Thus, we can exploit a slightly modified version of our qubit polar coding scheme. The idea is for Alice and Bob to employ a quantum polar code for each qubit-input space in the tensor factor (this is similar to the idea in Ref. [9]). There are amplitude and phase variables for each of these qubit input spaces. Let $Z_1, \ldots, Z_4$ denote the amplitude variables and let $X_1, \ldots, X_4$ denote the phase variables. Bob's decoder is such that he coherently decodes Z_1, uses it as quantum side information (QSI) to decode Z_2, uses both Z_1 and Z_2 as QSI to decode Z_3, and then uses all of $Z_1, \ldots, Z_3$ to help decode Z_4. With all of the amplitude variables decoded, Bob then uses these as QSI to decode X_1, and continues successively until he coherently decodes X_4. At the end he performs controlled phase gates to recover entanglement established with Alice.

We now calculate the total rate of this scheme. For the first qubit space in the tensor factor, the channels split up into four types depending on whether they are good/bad for amplitude/phase. Using the formula (10) in Appendix A, the net quantum data rate for the first tensor factor is equal to $I(Z_1;B) + I(X_1;BZ_1Z_2Z_3Z_4) - 1$. (The formula is slightly different here because Bob decodes the phase variable X_1 with all of the amplitude variables as QSI.) For the second qubit space in the tensor factor, the net quantum data rate is $I(Z_2;BZ_1) + I(X_2;BZ_1Z_2Z_3Z_4X_1) - 1$. We can similarly determine the respective net quantum data rates for the third and fourth qubit spaces as$I(Z_3;BZ_1Z_2) + I(X_3;BZ_1Z_2Z_3Z_4X_1X_2) - 1$, $I(Z_4;BZ_1Z_2Z_3) + I(X_4;BZ_1Z_2Z_3Z_4X_1X_2X_3) - 1$. Summing all these rates together with the chain rule and using the fact that any two amplitude and/or phase variables are independent whenever $i \neq j$, we obtain the overall net quantum data rate: $I(Z_1Z_2Z_3Z_4;B) + I(X_1X_2X_3X_4;BZ_1Z_2Z_3Z_4) - 4$, which is equal to the coherent information of the joint channel (by applying the same Lemma 2 of Ref. [2]). The fact that our quantum polar code can achieve the symmetric coherent information rate then proves that superactivation occurs, given that Smith and Yard already showed that this rate is non-zero for the channels mentioned above [10].

[3]We are speaking of *catalytic* superactivation. A catalytic protocol uses entanglement assistance, but the figure of merit is the net rate of quantum communication—the total quantum communication rate minus the entanglement consumption rate. Note that the catalytic quantum capacity is equal to zero if the standard quantum capacity is zero. Thus, the superactivation effect that we speak of in this section is for the catalytic quantum capacity.

IV. Conclusion

Our quantum polar coding scheme has two benefits over the work in Refs. [8], [7]: it achieves the symmetric coherent information rate for an arbitrary quantum channel and its entanglement consumption rate vanishes for an arbitrary degradable channel. Though, we should clarify that the analysis here actually implies that the scheme from Ref. [8] has the above two properties. A further benefit over the scheme from Ref. [8] is that the decoder here is explicitly realized as $O(N)$ rounds of coherent quantum successive cancellation, followed by $O(N)$ controlled-phase gates. Finally, we outlined how the scheme here can exhibit the superactivation effect. We acknowledge discussions with F. Dupuis, S. Guha, and G. Smith.

References

[1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[2] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Physical Review A*, vol. 78, p. 032335, September 2008.

[3] ——, "Conjectured strong complementary information tradeoff," *Phys. Rev. Lett.*, vol. 103, p. 020402, July 2009.

[4] J.-C. Boileau and J. M. Renes, "Optimal state merging without decoupling," in *Theory of Quantum Comp., Comm., and Crypt.*, ser. Lecture Notes in Computer Science, vol. 5906, 2009, pp. 76–84.

[5] J. M. Renes, "Approximate quantum error correction via complementary observables," March 2010, arXiv:1003.1150.

[6] ——, "Duality of privacy amplification against quantum adversaries and data compression with quantum side information," *Proceedings of the Royal Society A*, vol. 467, no. 2130, pp. 1604–1623, 2011.

[7] J. M. Renes, F. Dupuis, and R. Renner, "Efficient quantum polar coding," September 2011, arXiv:1109.3195.

[8] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," September 2011, arXiv:1109.5346.

[9] E. Sasoglu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," *2009 IEEE Information Theory Workshop*, pp. 144–148, 2009, arXiv:0908.0302.

[10] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, pp. 1812–1815, September 2008.

[11] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," September 2011, arXiv:1109.2591.

[12] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, Oct. 2006.

APPENDIX A

We now calculate the rate of the set $\mathcal{A}$ (the rate of information qubits that Alice and Bob should be able to establish with our quantum polar coding scheme). From basic set theory, we know that

$$\begin{aligned}|\mathcal{A}| &= |\mathcal{G}_N(W_A,\beta)\cap\mathcal{G}_N(W_P,\beta)| \\ &= |\mathcal{G}_N(W_A,\beta)| + |\mathcal{G}_N(W_P,\beta)| - |\mathcal{G}_N(W_A,\beta)\cup\mathcal{G}_N(W_P,\beta)|\,.\end{aligned}$$

Given the polarization results for the cq amplitude and phase channels, we know that $\lim_{N\to\infty}\frac{1}{N}|\mathcal{G}_N(W_A,\beta)| = I(Z;B)$ and $\lim_{N\to\infty}\frac{1}{N}|\mathcal{G}_N(W_P,\beta)| = I(X;BC)$. Also, consider that

$$\begin{aligned}|\mathcal{G}_N(W_A,\beta)\cup\mathcal{G}_N(W_P,\beta)| &= |[N]\ \setminus\ (\mathcal{G}_N(W_A,\beta)\cup\mathcal{G}_N(W_P,\beta))^c| \\ &= |[N]\ \setminus\ (\mathcal{B}_N(W_A,\beta)\cap\mathcal{B}_N(W_P,\beta))| \\ &= N - |\mathcal{B}|\,.\end{aligned}$$

Thus, the rate of $\mathcal{A}$ is equal to

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}|\mathcal{A}| &= I(Z;B) + I(X;BC) - 1 + \lim_{N\to\infty}\frac{1}{N}|\mathcal{B}| \\ &= I(Z;B) + I(X;BC) - H(Z) + \lim_{N\to\infty}\frac{1}{N}|\mathcal{B}| \\ &= I(A\rangle B) + \lim_{N\to\infty}\frac{1}{N}|\mathcal{B}|\,.\end{aligned}\tag{10}$$

where the second equality exploits the fact that $H(Z) = 1$ for a uniformly random bit and the third exploits Lemma 2 of Renes and Boileau [2]. Thus, the net rate of information qubits generated by this quantum polar coding scheme is equal to the symmetric coherent information:

$$\lim_{N\to\infty}\frac{|\mathcal{A}| - |\mathcal{B}|}{N} = I(A\rangle B)\,.$$

APPENDIX B

We rigorously prove some of the statements in Section I-D. The ideal state after the first step of the decoder is

$$\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}}\sum_{u''_{\mathcal{A}},u''_{\mathcal{B}},v''_{\mathcal{X}}}(-1)^{u_{\mathcal{X}}\cdot v''_{\mathcal{X}}}|u''_{\mathcal{A}}\rangle\left|\phi_{u''_{\mathcal{A}},u_{\mathcal{Z}},v''_{\mathcal{X}},u''_{\mathcal{B}}}\right\rangle^{B^NE^N}|u''_{\mathcal{A}}\rangle|v''_{\mathcal{X}}\rangle|u''_{\mathcal{B}}\rangle|u''_{\mathcal{B}}\rangle|u_{\mathcal{Z}}\rangle\,.$$

The actual state is

$$\begin{aligned}&\left(\sum_{u'_{\mathcal{A}},u'_{\mathcal{B}},v'_{\mathcal{X}}}\sqrt{\Lambda^{(u'_{\mathcal{B}},u_{\mathcal{Z}})}_{u'_{\mathcal{A}},v'_{\mathcal{X}}}}\otimes|u'_{\mathcal{A}}\rangle|v'_{\mathcal{X}}\rangle\otimes|u'_{\mathcal{B}}\rangle|u'_{\mathcal{B}}\rangle\langle u'_{\mathcal{B}}|\otimes|u_{\mathcal{Z}}\rangle\right)\times \\ &\quad\left(\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}}}(-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}}|u_{\mathcal{A}}\rangle|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}|u_{\mathcal{B}}\rangle\right) \\ &= \left(\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}}\sum_{\substack{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},\\u'_{\mathcal{A}},v'_{\mathcal{X}}}}(-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}}|u_{\mathcal{A}}\rangle\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u'_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}|u'_{\mathcal{A}}\rangle|v'_{\mathcal{X}}\rangle|u_{\mathcal{B}}\rangle|u_{\mathcal{B}}\rangle|u_{\mathcal{Z}}\rangle\right)\end{aligned}$$

The overlap between the above two states is equal to

$$\begin{aligned}&\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}\sum_{\substack{u''_{\mathcal{A}},u''_{\mathcal{B}},v''_{\mathcal{X}},\\u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},\\u'_{\mathcal{A}},v'_{\mathcal{X}}}}(-1)^{u_{\mathcal{X}}\cdot(v''_{\mathcal{X}}+v_{\mathcal{X}})}\langle u''_{\mathcal{A}}|u_{\mathcal{A}}\rangle\langle\phi_{u''_{\mathcal{A}},u_{\mathcal{Z}},v''_{\mathcal{X}},u''_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u'_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N} \\ &\qquad\times\langle u'_{\mathcal{A}}|u''_{\mathcal{A}}\rangle\langle v'_{\mathcal{X}}|v''_{\mathcal{X}}\rangle\langle u_{\mathcal{B}}|u''_{\mathcal{B}}\rangle\langle u_{\mathcal{B}}|u''_{\mathcal{B}}\rangle\langle u_{\mathcal{Z}}|u_{\mathcal{Z}}\rangle \\ &= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}}}(-1)^{u_{\mathcal{X}}\cdot(v'_{\mathcal{X}}+v_{\mathcal{X}})}\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\end{aligned}$$

Taking the expectation of the fidelity over the uniformly random choice of the ancilla bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$ then gives

$$\begin{aligned}
&\mathbb{E}_{U_{\mathcal{X}},U_{\mathcal{Z}}}\left\{\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}}}(-1)^{U_{\mathcal{X}}\cdot\left(v'_{\mathcal{X}}+v_{\mathcal{X}}\right)}\langle\phi_{u_{\mathcal{A}},U_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},U_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},U_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\right\}\\
&=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\frac{1}{2^{|\mathcal{X}|}}\sum_{u_{\mathcal{X}},u_{\mathcal{Z}}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}}}(-1)^{u_{\mathcal{X}}\cdot\left(v'_{\mathcal{X}}+v_{\mathcal{X}}\right)}\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\\
&=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}},u_{\mathcal{Z}}}\left[\frac{1}{2^{|\mathcal{X}|}}\sum_{u_{\mathcal{X}}}(-1)^{u_{\mathcal{X}}\cdot\left(v'_{\mathcal{X}}+v_{\mathcal{X}}\right)}\right]\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\\
&=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}},u_{\mathcal{Z}}}\delta_{v'_{\mathcal{X}},v_{\mathcal{X}}}\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\\
&=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},u_{\mathcal{Z}}}\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}|\sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v_{\mathcal{X}}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\\
&\geq\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},u_{\mathcal{Z}}}\langle\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}|\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v_{\mathcal{X}}}|\phi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\rangle^{B^NE^N}\\
&\geq 1-o(2^{-N^{\beta}}),
\end{aligned}$$

where the last inequality follows from the good performance of the quantum successive cancellation decoder for the cq amplitude channels (see Proposition 4 of Ref. [11]).

We can prove similarly that the phase decoder works well with a uniformly random choice of the bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$. Observe that a uniformly random choice of the bits $u_{\mathcal{Z}}$ induces a uniform distribution of the bits $x_{\mathcal{Z}}$. A similar error analysis as above then works for this case. Consider the ideal state:

$$\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}}}|\widetilde{x}_{\mathcal{A}}\rangle\, Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\,|\widetilde{x}_{\mathcal{A}}\rangle\,|\widetilde{x}_{\mathcal{Z}}\rangle\,|\widetilde{u}_{\mathcal{X}}\rangle\,|\widetilde{x}_{\mathcal{B}}\rangle\,,$$

and the actual state:

$$\begin{aligned}
&U_{\mathcal{E}}^{C^N}\left(\sum_{x'_{\mathcal{A}},x'_{\mathcal{Z}},x'_{\mathcal{B}}}\sqrt{\Gamma^{(x'_{\mathcal{B}},u_{\mathcal{X}})}_{x'_{\mathcal{A}},x'_{\mathcal{Z}}}}\otimes|\widetilde{x}'_{\mathcal{A}}\rangle\,|\widetilde{x}'_{\mathcal{Z}}\rangle\,|\widetilde{u}_{\mathcal{X}}\rangle\otimes|\widetilde{x}'_{\mathcal{B}}\rangle\,\langle\widetilde{x}'_{\mathcal{B}}|\right)U_{\mathcal{E}}^{\dagger C^N}\left(\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}}}|\widetilde{x}_{\mathcal{A}}\rangle\, Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\,|\widetilde{x}_{\mathcal{B}}\rangle\right)\\
&=\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}}\sum_{x'_{\mathcal{A}},x'_{\mathcal{Z}},x'_{\mathcal{B}},x_{\mathcal{A}}}|\widetilde{x}_{\mathcal{A}}\rangle\,U_{\mathcal{E}}^{C^N}\sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x'_{\mathcal{A}},x'_{\mathcal{Z}}}}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\,|\widetilde{x}_{\mathcal{B}}\rangle\,|\widetilde{x}'_{\mathcal{A}}\rangle\,|\widetilde{x}'_{\mathcal{Z}}\rangle\,|\widetilde{u}_{\mathcal{X}}\rangle\,.
\end{aligned}$$

Now consider the overlap between the above two states:

$$\begin{aligned}
&\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}}\sum_{x''_{\mathcal{A}},x''_{\mathcal{B}}}\sum_{x'_{\mathcal{A}},x'_{\mathcal{Z}},x'_{\mathcal{B}},x_{\mathcal{A}}}\langle\widetilde{x}''_{\mathcal{A}}|\widetilde{x}_{\mathcal{A}}\rangle\times\\
&\langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}|\,U_{\mathcal{E}}^{\dagger A'^N}U_{\mathcal{N}}^{\dagger}Z^{-x''_{\mathcal{A}},-u_{\mathcal{X}},-x''_{\mathcal{B}},-x_{\mathcal{Z}}}U_{\mathcal{E}}^{C^N}\sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x'_{\mathcal{A}},x'_{\mathcal{Z}}}}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\times\\
&\qquad\langle\widetilde{x}''_{\mathcal{A}}|\widetilde{x}'_{\mathcal{A}}\rangle\,\langle\widetilde{x}_{\mathcal{Z}}|\widetilde{x}'_{\mathcal{Z}}\rangle\,\langle\widetilde{u}_{\mathcal{X}}|\widetilde{u}_{\mathcal{X}}\rangle\,\langle\widetilde{x}''_{\mathcal{B}}|\widetilde{x}_{\mathcal{B}}\rangle\\
&=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}}}\langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}|\,U_{\mathcal{E}}^{\dagger A'^N}U_{\mathcal{N}}^{\dagger}Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}}U_{\mathcal{E}}^{C^N}\sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}}}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\\
&\geq\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}}}\langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}|\,U_{\mathcal{E}}^{\dagger A'^N}U_{\mathcal{N}}^{\dagger}Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}}U_{\mathcal{E}}^{C^N}\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle
\end{aligned}$$

Taking the expectation of this term over a uniformly random choice of $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$ (which implies a uniformly random choice of $x_{\mathcal{Z}}$) gives the following quantity:

$$\mathbb{E}_{U_{\mathcal{X}},X_{\mathcal{Z}}}\left\{\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}}}\langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}|\,U_{\mathcal{E}}^{\dagger A'^N}U_{\mathcal{N}}^{\dagger}Z^{-x_{\mathcal{A}},-U_{\mathcal{X}},-x_{\mathcal{B}},-X_{\mathcal{Z}}}U_{\mathcal{E}}^{C^N}\Gamma_{x_{\mathcal{A}},X_{\mathcal{Z}}}^{(x_{\mathcal{B}},U_{\mathcal{X}})}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},U_{\mathcal{X}},x_{\mathcal{B}},X_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\right\}$$

$$=\frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}}\sum_{x_{\mathcal{A}},x_{\mathcal{B}},u_{\mathcal{X}},x_{\mathcal{Z}}}\langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}|\,U_{\mathcal{E}}^{\dagger A'^N}U_{\mathcal{N}}^{\dagger}Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}}U_{\mathcal{E}}^{C^N}\Gamma_{x_{\mathcal{A}},x_{\mathcal{Z}}}^{(x_{\mathcal{B}},u_{\mathcal{X}})}U_{\mathcal{E}}^{\dagger C^N}Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}}U_{\mathcal{N}}U_{\mathcal{E}}^{A'^N}\,|\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle$$

$$\geq 1-o(2^{-N^{\beta}}),$$

where the last inequality again follows from the performance of the quantum successive cancellation decoder for the phase channels.

APPENDIX C

This appendix provides a detailed proof that the entanglement consumption rate of our quantum polar codes vanishes whenever the quantum channel is degradable. Consider a state of the following form:

$$\frac{1}{\sqrt{2^N}}\sum_{z^N}\left|z^N\right\rangle^{A^N}\left|\phi_{z^N G_N}\right\rangle^{B^N E^N}\left|z^N\right\rangle^{C^N}.$$

We can represent the registers $A_1\cdots A_{i-1}$ in the amplitude basis and the registers $A_{i+1}\cdots A_N$ in the phase basis as follows:

$$\frac{1}{\sqrt{2^{2N-i}}}\sum_{z^N,x_{i+1}^N}\left|z_1^{i-1}\right\rangle^{A_1^{i-1}}\left|z_i\right\rangle^{A_i}\left|\widetilde{x}_{i+1}^N\right\rangle^{A_{i+1}^N}\left|\phi_{z^N G_N}\right\rangle^{B^N E^N}\left(Z^{x_{i+1}^N}\right)^{C_{i+1}^N}\left|z^N\right\rangle^{C^N}.$$

Then measuring the systems $A_1\cdots A_{i-1}$ in the amplitude basis and the systems $A_{i+1}\cdots A_N$ in the phase basis (we can think of this just as dephasing these systems in the respective bases) leads to a state which can generate the outputs of the i^{th} phase channel to Bob $W_{P,N}^{(i)}$ and the i^{th} amplitude channel to Eve $W_{P,N}^{(i)}$. Denote this state by ψ_i, and call the various measurement outputs systems $Z_1\cdots Z_{i-1}$ and $X_{i+1}\cdots X_N$ in order to indicate that they are classical. Then ψ_i is a tripartite state on $A_i|B^N C^N X_{i+1}^N|E^N Z_1^{i-1}$ is a tripartite state (where the vertical bars indicate the divisions of the parties), to which we can apply the following uncertainty relation proved in Ref. [3]:

$$H\left(X^{A_i}|B^N C^N X_{i+1}^N\right)_{\psi_i}+H\left(Z^{A_i}|E^N Z_1^{i-1}\right)_{\psi_i}\geq 1.$$

Combining this with $H\left(X^{A_i}\right)+H\left(Z^{A_i}\right)=2$ (which holds because X^{A_i} and Z^{A_i} are uniform random bits) gives

$$I\left(X^{A_i};B^N C^N X_{i+1}^N\right)_{\psi_i}+I\left(Z^{A_i};E^N Z_1^{i-1}\right)_{\psi_i}\leq 1,$$

or equivalently,

$$I(W_{P,N}^{(i)})+I(W_{E,N}^{(i)})\leq 1. \tag{11}$$

Note that in the limit $N\to\infty$, the channels polarize, so that the channels which are good in phase for Bob are bad in amplitude for Eve, and the ones which are good in amplitude for Eve are bad in phase for Bob. This demonstrates that our quantum polar coding scheme given here is asymptotically equivalent to the scheme of Wilde and Guha [8] in the limit of many recursions of the encoding after the channel polarization effect takes hold.

The above uncertainty relation is helpful in proving a different one about the synthesized channels' fidelities, that will in turn help us prove the statement about the entanglement consumption rate. Exploiting the following inequality (see Proposition 1 of Ref. [11])

$$I\left(W\right)\geq\log_2\left(\frac{2}{1+\sqrt{F\left(W\right)}}\right), \tag{12}$$

we can show that

$$2\sqrt{F\left(W_{P,N}^{(i)}\right)}+\sqrt{F\left(W_{E,N}^{(i)}\right)}\geq 1, \tag{13}$$

$$\sqrt{F\left(W_{P,N}^{(i)}\right)}+2\sqrt{F\left(W_{E,N}^{(i)}\right)}\geq 1.$$

Consider that the inequality in (12) above is equivalent to $\sqrt{F\left(W\right)}\geq 2^{1-I(W)}-1$. We then have

$$\sqrt{F\left(W_{P,N}^{(i)}\right)}\quad\geq\quad 2^{1-I\left(W_{P,N}^{(i)}\right)}-1\quad\geq\quad 2^{I\left(W_{E,N}^{(i)}\right)}-1\quad\geq\quad\frac{2}{1+\sqrt{F\left(W_{E,N}^{(i)}\right)}}-1,$$

where we used the uncertainty relation in (11) in the second inequality and we again applied (12) for the third inequality. Rewriting this, we obtain

$$\left(1+\sqrt{F\left(W_{E,N}^{(i)}\right)}\right)\sqrt{F\left(W_{P,N}^{(i)}\right)} \geq 2-\left(1+\sqrt{F\left(W_{E,N}^{(i)}\right)}\right),$$

which gives

$$2\sqrt{F\left(W_{P,N}^{(i)}\right)}+\sqrt{F\left(W_{E,N}^{(i)}\right)} \geq 1.$$

(We used the fact that the fidelity is less than one.) Proceeding in the symmetric way gives the other fidelity uncertainty relation in (13).

We can now argue that the entanglement consumption rate should be zero in the limit whenever the channel is a degradable quantum channel. We do this by a modification of the argument in Ref. [8]. Consider the set of channels $\mathcal{B}$ which are doubly bad for amplitude and phase. Also, consider the channels which are amplitude-good for Eve:

$$\mathcal{G}_N\left(W_E,\beta\right) \equiv \left\{i \in [N] : \sqrt{F(W_{E,N}^{(i)})} < 2^{-N^\beta}\right\}$$

and those which are phase-good for Bob: $\mathcal{G}_N\left(W_P,\beta\right)$. We prove now that these sets are disjoint and thus the sum of them must be smaller than N (the total number of channel uses). First consider that

$$\mathcal{B} \cap \mathcal{G}_N\left(W_P,\beta\right) = \emptyset$$

by the definition of the set $\mathcal{B}$. Now consider that

$$2\cdot 2^{-N^\beta} \geq 2\cdot\sqrt{F(W_{P,N}^{(i)})} \geq 1-\sqrt{F(W_{E,N}^{(i)})},$$

implying that

$$\sqrt{F(W_{E,N}^{(i)})} \geq 1-2\cdot 2^{-N^\beta},$$

whenever $2^{-N^\beta} \geq \sqrt{F(W_{P,N}^{(i)})}$. Thus, all of the channels that are phase-good for Bob are amplitude-“very bad” for Eve. So the following relation holds for large enough N:

$$\mathcal{G}_N\left(W_P,\beta\right) \cap \mathcal{G}_N\left(W_E,\beta\right) = \emptyset.$$

The relation $\mathcal{B} \cap \mathcal{G}_N\left(W_E,\beta\right) = \emptyset$ holds for degradable channels because

$$\begin{aligned}
&\mathcal{B} \cap \mathcal{G}_N\left(W_E,\beta\right) \\
&= \left(\mathcal{B}_N\left(W_A,\beta\right) \cap \mathcal{B}_N\left(W_P,\beta\right)\right) \cap \mathcal{G}_N\left(W_E,\beta\right) \\
&\subseteq \left(\mathcal{B}_N\left(W_E,\beta\right) \cap \mathcal{B}_N\left(W_P,\beta\right)\right) \cap \mathcal{G}_N\left(W_E,\beta\right) \\
&= \emptyset.
\end{aligned}$$

The second line follows from the definition and the third follows from the degradability condition (all the channels that are bad in amplitude for Bob are also bad in amplitude for Eve due to the existence of a degrading map under which the fidelity can only increase—see Lemma 3 of Ref. [8]). Thus, all of these sets are disjoint and it follows that

$$\frac{1}{N}\left(\left|\mathcal{G}_N\left(W_E,\beta\right)\right| + \left|\mathcal{G}_N\left(W_P,\beta\right)\right| + \left|\mathcal{B}\right|\right) \leq 1.$$

Finally, we know from Theorem 1 that the rates of the sets $\mathcal{G}_N\left(W_E,\beta\right)$ and $\mathcal{G}_N\left(W_P,\beta\right)$ in the asymptotic limit are

$$\begin{aligned}
\lim_{N\to\infty}\frac{1}{N}\left|\mathcal{G}_N\left(W_E,\beta\right)\right| &= I\left(Z^A;E\right)_\psi, \\
\lim_{N\to\infty}\frac{1}{N}\left|\mathcal{G}_N\left(W_P,\beta\right)\right| &= I\left(X^A;BC\right)_\psi = 1-I\left(Z^A;E\right)_\psi,
\end{aligned}$$

so that the rate of $\mathcal{B}$ must be zero in the asymptotic limit:

$$\lim_{N\to\infty}\frac{1}{N}\left|\mathcal{B}\right| = 0.$$