

# Quantum Polarization of Qudit Channels

Ashutosh Goswami<sup>1</sup> Mehdi Mhalla<sup>2</sup> Valentin Savin<sup>3</sup>

<sup>1</sup> Univ. Grenoble Alpes, Grenoble INP, LIG, F-38000 Grenoble, France

<sup>2</sup> Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France

<sup>3</sup> Univ. Grenoble Alpes, CEA, LETI, F-38054 Grenoble, France

## Abstract

We provide a generalization of quantum polar codes to quantum channels with qudit-input, achieving the symmetric coherent information of the channel. Our scheme relies on a channel combining and splitting construction, where a two-qudit unitary randomly chosen from a unitary 2-design is used to combine two instances of a qudit-input channel. The inputs to the synthesized bad channels are frozen by sharing EPR pairs between the sender and the receiver, so our scheme is entanglement assisted. Using the fact that the generalized two-qudit Clifford group forms a unitary 2-design, we conclude that the channel combining operation can be chosen from this set. Moreover, we show that polarization also happens for a much smaller subset of two-qudit Cliffords, which is not a unitary 2-design. Finally, we show how to decode the proposed quantum polar codes on Pauli qudit channels.

## 1 Introduction

In classical information theory, polar codes are the first explicit construction provably achieving the symmetric capacity of any discrete memoryless channel [1]. The construction is based on the recursive application of a channel combining and splitting procedure. It first combines two instances of the transmission channel, using a controlled-NOT gate as channel combiner, and then splits the combined channel into two virtual channels, referred to as good and bad channels. Applied recursively  $n$  times, the above procedure yields  $N = 2^n$  virtual channels. These virtual channels exhibit a polarization property, in the sense that they tend to become either completely noisy or noiseless, as  $N$  goes to infinity. Polar coding consists of efficient encoding and decoding algorithms that take effective advantage of the channel polarization property.

Polar codes have been generalized to classical-quantum channels with binary and non-binary classical input in [2, 3]. For the transmission of quantum information over quantum channels with qubit-input, two approaches have been considered in the literature. The first approach is based on CSS-like constructions, which essentially exploit polarization in either amplitude or phase basis [4, 5, 6]. The second approach relies on a *purely quantum polarization* construction [7, 8], where the synthesized virtual channels tend to become either completely noisy or noiseless as quantum channels, not merely in one basis. This approach uses a randomized channel combining, employing a random two-qubit Clifford unitary as channel combiner.

In this work, we extend the work in [7] to the case of quantum channels with qudit-input. To the best of our knowledge, this is the first generalization of polar codes to qudit-input channels. First, we show that purely quantum polarization (in the sense of [7]) happens for any qudit-input quantum channel, using as channel combiner a random

two-qudit unitary, chosen from a unitary 2-design. Further, we provide a simple proof of the fact that the generalized two-qudit Clifford group forms a unitary 2-design, therefore the channel combining operation can be randomly chosen from this set. Moreover, when the qudit dimension  $d$  is a prime, we show that polarization happens for a subset of two-qudit Clifford unitaries containing only  $d^4 + d^2 - 2$  elements, which is not a unitary 2-design. Hence, unitary 2-designs are not necessary for the quantum polarization of qudit-input channels.

To exploit the above polarization property, the inputs to the synthesized noisy channels are frozen by presharing EPR pairs between the sender and the receiver. Hence, our polar coding scheme is entanglement assisted. Finally, we consider the case of Pauli qudit channels. Similarly to [7], we associate a *classical counterpart channel* to a Pauli qudit channel. Then, we show that a quantum polar code on a Pauli qudit channel yields a classical polar code on the classical counterpart channel. Hence, we show that Pauli errors can be identified by decoding the polar code on the classical counterpart channel, using classical polar decoding.

The paper is organized as follows. Section 2 provides the basic definitions needed for quantum polarization. Section 3 contains our main polarization results for qudit-input quantum channels. Section 4 discusses the decoding of our quantum polar codes on Pauli qudit channels.

## 2 Preliminaries

We consider  $d$ -dimensional quantum systems, referred to as qudits, where  $d \geq 2$  is fixed throughout the paper. We denote by  $\rho_A$  a quantum state (*i.e.*, density matrix) of a quantum system  $A$ . When no confusion is possible, we shall discard the quantum system from the notation. For a bipartite quantum state  $\rho_{AB}$ , we shall denote by  $\rho_B := \text{Tr}_A(\rho_{AB})$  the quantum state of the system  $B$ , obtained by tracing out the system  $A$ . The identity matrix is denoted by either  $\mathbb{1}$  or  $I$ , with the former notation used for quantum states, and the latter for quantum operators. Throughout the paper, logarithm is taken in base  $d$ .

**Definition 1** (von Neumann entropy). (a) The von Neumann entropy of a quantum state  $\rho$  is defined as

$$H(\rho) := -\text{Tr}(\rho \log \rho).$$

(b) The conditional von Neumann entropy of a bipartite quantum state  $\rho_{AB}$  is defined as

$$H(A|B)_{\rho_{AB}} = H(\rho_{AB}) - H(\rho_B).$$

**Definition 2** (Conditional sandwiched Rényi entropy of order 2). Let  $\rho_{AB}$  be a quantum state. Then,

$$\tilde{H}_2^\downarrow(A|B)_\rho := -\log \text{Tr} \left[ \rho_B^{-\frac{1}{2}} \rho_{AB} \rho_B^{-\frac{1}{2}} \rho_{AB} \right].$$

**Definition 3** (Petz-Rényi entropy of order  $\frac{1}{2}$ ). Let  $\rho_{AB}$  be a quantum state. Then,

$$H_{\frac{1}{2}}^\uparrow(A|B)_\rho := 2 \log \sup_{\sigma_B} \text{Tr} \left[ \rho_{AB}^{\frac{1}{2}} \sigma_B^{\frac{1}{2}} \right],$$

where the supremum is taken over all quantum states  $\sigma_B$ .

We consider quantum channels  $\mathcal{W}_{A' \rightarrow B}$ , with qudit input system  $A'$ , and output system  $B$  of arbitrary dimension. When no confusion is possible, we shall discard the channel input and output systems from the notation. An EPR pair on two-qudit systems  $A$  and  $A'$  is the quantum state  $\Phi_{AA'} := |\Phi_{AA'}\rangle \langle \Phi_{AA'}|$ , with  $|\Phi_{AA'}\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_{A'}$ . Given a quantum channel  $\mathcal{W}_{A' \rightarrow B}$ , we denote by  $\mathcal{W}(\Phi_{AA'}) := (I_A \otimes \mathcal{W})(\Phi_{AA'})$  the quantum state on the  $AB$  system obtained by applying  $\mathcal{W}$  on the  $A'$ -half of the EPR pair  $\Phi_{AA'}$ .

**Definition 4** (Symmetric coherent information). *Let  $\mathcal{W}_{A' \rightarrow B}$  be a channel with qudit input  $A'$  and output system  $B$  of arbitrary dimension. The symmetric coherent information of  $\mathcal{W}$  is defined as the coherent information of the channel for a uniformly distributed input, that is*

$$I(\mathcal{W}) := -H(A|B)_{\mathcal{W}(\Phi_{AA'})} \in [-1, 1].$$

We further introduce the following parameter of a quantum channel, which can be seen as the quantum counterpart of the classical Bhattacharyya parameter [7], and which we refer to as the ‘‘Rényi-Bhattacharyya’’ parameter.

**Definition 5** (Rényi-Bhattacharyya parameter). *Let  $\mathcal{W}_{A' \rightarrow B}$  be a channel with qudit input  $A'$  and output system  $B$  of arbitrary dimension. Then,*

$$R(\mathcal{W}) := d^{\frac{H_{\frac{1}{2}}^{\uparrow}(A|B)_{\mathcal{W}(\Phi_{AA'})}}}{2}} = d^{-\frac{\tilde{H}_{\frac{1}{2}}^{\downarrow}(A|E)_{\mathcal{W}^c(\Phi_{AA'})}}}{2}} \in \left[\frac{1}{d}, d\right],$$

where  $\mathcal{W}^c$  denotes the complementary channel associated with  $\mathcal{W}$  [9], and the equality  $H_{\frac{1}{2}}^{\uparrow}(A|B)_{\mathcal{W}(\Phi_{AA'})} = -\tilde{H}_{\frac{1}{2}}^{\downarrow}(A|E)_{\mathcal{W}^c(\Phi_{AA'})}$  follows from [10, Theorem 2].

We will also need the definitions of the generalized (qudit) Pauli and Clifford groups [11, 12], and unitary 2-designs [13].

**Definition 6** (Generalized Pauli Group). *(a) The Pauli operators  $X$  and  $Z$  for a qudit quantum system are defined as  $X = \sum_{j=0}^{d-1} |j\rangle \langle j \oplus 1|$ , and  $Z = \sum_{j=0}^{d-1} \omega^j |j\rangle \langle j|$ , where  $\oplus$  denotes the sum modulo  $d$ , and  $\omega = e^{\frac{2\pi i}{d}}$ .*

*(b) The generalized Pauli group on one qudit is defined as  $\mathcal{P}_d^1 := \{\omega^\lambda P_{r,s} \mid \lambda, r, s = 0, \dots, d-1\}$ , where  $P_{r,s} := X^r Z^s$ .*

*(c) The generalized Pauli group on  $n$  qudits is defined as  $\mathcal{P}_d^n := \mathcal{P}_d^1 \otimes \mathcal{P}_d^1 \otimes \dots \otimes \mathcal{P}_d^1$ .*

It is easily seen that  $X^d = Z^d = I$  and  $XZ = \omega ZX$ , hence  $\mathcal{P}_d^1$  is indeed a group. Applying the commutation relation  $XZ = \omega ZX$  appropriately many times, we have that

$$P_{r,s} P_{t,u} = \omega^{ru-st} P_{t,u} P_{r,s}. \quad (1)$$

**Definition 7** (Generalized Clifford Group). *The Clifford group  $\mathcal{C}_d^n$  is the unitary group on  $n$  qudits that takes  $\mathcal{P}_d^n$  to  $\mathcal{P}_d^n$  by conjugation.*

Let  $\mathcal{U}(d^n)$  be the set of unitary operators on  $n$  qudits, and  $\mathcal{W}_n$  be a quantum channel with  $n$ -qudit input. The twirling of  $\mathcal{W}_n$  with respect to  $\mathcal{U}(d^n)$  is defined as the quantum channel that maps a  $n$ -qudit quantum state  $\rho$  to  $\int U^\dagger \mathcal{W}_n(U\rho U^\dagger) U d\eta$ , where  $U \in \mathcal{U}(d^n)$  is randomly chosen according to the Haar measure  $\eta$ . The twirling of  $\mathcal{W}_n$  with respect to a finite subset  $\mathcal{U} \subset \mathcal{U}(d^n)$  is defined as the quantum channel acting as  $\rho \mapsto \frac{1}{|\mathcal{U}|} \sum_{U \in \mathcal{U}} U^\dagger \mathcal{W}_n(U\rho U^\dagger) U$ .

**Definition 8** (Unitary 2-Design). *A finite subset  $\mathcal{U} \subset \mathcal{U}(d^n)$  is said to form a unitary 2-design if it satisfies the following, for all  $n$ -qudit input quantum channels  $\mathcal{W}_n$ , and all  $n$ -qudit quantum states  $\rho$ :*

$$\frac{1}{|\mathcal{U}|} \sum_{U \in \mathcal{U}} U^\dagger \mathcal{W}_n(U\rho U^\dagger) U = \int U^\dagger \mathcal{W}_n(U\rho U^\dagger) U d\eta. \quad (2)$$

### 3 Quantum Polarization of Qudit Channels

#### 3.1 Main polarization results

Throughout this section  $\mathcal{W}_{A' \rightarrow B}$  denotes a quantum channel with qudit input, and arbitrary dimension output. Our quantum polarization scheme is based on the channel combining and splitting operations depicted in the following figure.

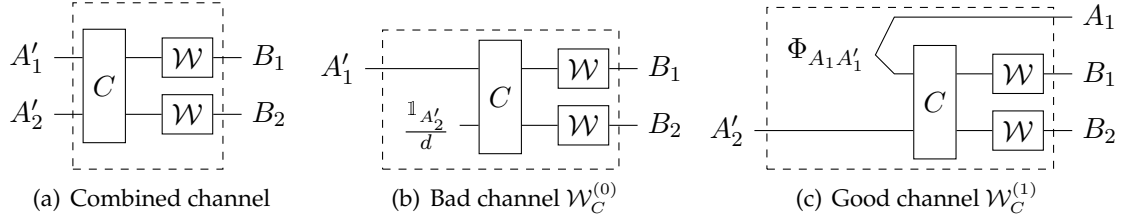


Figure 1: Channel combining and splitting. (a) combined channel: a two-qudit unitary  $C$  is applied on the two inputs. (b) bad channel: we input a totally mixed state into the second input. (c) good channel: we input half of an EPR pair into the first input, and the other half becomes the output  $A_1$ .

First, two instances of  $\mathcal{W}$  are combined, by entangling their inputs through a two-qudit unitary  $C$ . The combined channel is then split into one bad and one good channel. The bad channel  $\mathcal{W}_C^{(0)}$  is a channel from  $A'_1$  to  $B_1 B_2$  that acts as  $\mathcal{W}_C^{(0)}(\rho) = \mathcal{W}^{\otimes 2} \left( C(\rho \otimes \frac{\mathbb{1}_{A'_2}}{d})C^\dagger \right)$ , where  $\frac{\mathbb{1}_{A'_2}}{d}$  is the completely mixed state. The good channel  $\mathcal{W}_C^{(1)}$  is a channel from  $A'_2$  to  $A_1 B_1 B_2$  that acts as  $\mathcal{W}_C^{(1)}(\rho) = \mathcal{W}^{\otimes 2} \left( C(\Phi_{A_1 A'_1} \otimes \rho)C^\dagger \right)$ , where  $\Phi_{A_1 A'_1}$  is an EPR pair.

The polarization construction is obtained by recursively applying the above channel combining and splitting operations, while choosing  $C$  randomly from some finite set of unitaries, denoted by  $\mathcal{U} \subset \mathcal{U}(d^2)$ . To accommodate the random choice of  $C \in \mathcal{U}$ , a classical description of  $C$  is included as part of the output of the bad and good channels. Hence, for  $i = 0, 1$ , we define:

$$\mathcal{W}^{(i)}(\rho) = \frac{1}{|\mathcal{U}|} \sum_{C \in \mathcal{U}} |C\rangle\langle C| \otimes \mathcal{W}_C^{(i)}(\rho), \quad (3)$$

where  $\{|C\rangle\}_{C \in \mathcal{U}}$  is an orthogonal basis of some auxiliary system. Applying twice the transformation  $\mathcal{W} \mapsto (\mathcal{W}^{(0)}, \mathcal{W}^{(1)})$ , we get channels  $\mathcal{W}^{(i_1 i_2)} := (\mathcal{W}^{(i_1)})^{(i_2)}$ , where  $(i_1 i_2) \in \{00, 01, 10, 11\}$ . In general, after  $n$  levels of recursion, we obtain  $2^n$  channels:

$$\mathcal{W}^{(i_1 \dots i_n)} := \left( \mathcal{W}^{(i_1 \dots i_{n-1})} \right)^{(i_n)}, \quad \forall (i_1 \dots i_n) \in \{0, 1\}^n. \quad (4)$$

The quantum polarization theorem below states that the symmetric coherent information of the synthesized channels  $\mathcal{W}^{(i_1 \dots i_n)}$  polarizes, meaning that it goes to either  $-1$  or  $+1$  as  $n$  goes to infinity (except possibly for a vanishing fraction of channels), provided that  $\mathcal{U}$  is a unitary 2-design. The second theorem states that polarization also happens when  $\mathcal{U}$  is taken to be the generalized Clifford group on two qudits,  $\mathcal{C}_d^2$ , or some specific subset of it.

**Theorem 9.** Let  $\mathcal{U}$  be a unitary 2-design. For any qudit-input quantum channel  $\mathcal{W}$ , let  $\{\mathcal{W}^{(i_1 \dots i_n)} : (i_1 \dots i_n) \in \{0, 1\}^n\}$  be the set of channels defined in (4), with channel combining unitary  $C$  randomly chosen from  $\mathcal{U}$ . Then, for any  $\delta > 0$ ,

$$\lim_{n \rightarrow \infty} \frac{\#\{(i_1 \dots i_n) \in \{0, 1\}^n : I(\mathcal{W}^{(i_1 \dots i_n)}) \in (-1 + \delta, 1 - \delta)\}}{2^n} = 0$$

and furthermore,

$$\lim_{n \rightarrow \infty} \frac{\#\{(i_1, \dots, i_n) \in \{0, 1\}^n : I(\mathcal{W}^{(i_1, \dots, i_n)}) \geq 1 - \delta\}}{2^n} = \frac{I(\mathcal{W}) + 1}{2}$$

**Theorem 10.** (a) The generalized Clifford group on two qudits,  $\mathcal{C}_d^2$ , is a unitary 2-design. Thus, polarization happens when the channel combining unitary  $C$  is randomly chosen from  $\mathcal{C}_d^2$ .

(b) If  $d$  is prime, there exists a subset  $\mathcal{U} \subset \mathcal{C}_d^2$ , of size  $|\mathcal{U}| = d^4 + d^2 - 2$ , which is not a unitary 2-design, and such that polarization happens when the channel combining unitary  $C$  is randomly chosen from  $\mathcal{U}$ .

We note that part (a) of Theorem 10 may be inferred from Lemmas 1, 2 and 3 in [14]. We will give an alternative and more elementary proof in Section 3.3, by generalizing the proof from [13] to the qudit case.

### 3.2 Proof of Theorem 9 (quantum polarization)

To prove the polarization theorem, we essentially need three ingredients, as follows.

1. For any two-qudit unitary  $C$ , the total symmetric coherent information is preserved under channel combining and splitting, that is,  $I(\mathcal{W}_C^{(0)}) + I(\mathcal{W}_C^{(1)}) = 2I(\mathcal{W})$ . We omit the proof of this, as the proof given in [8, Lemma 10] for qubit-input channels remains valid in the qudit case, with minor adjustments.
2. The symmetric coherent information  $I(\mathcal{W})$  approaches  $\{-1, +1\}$  values if and only if the Rényi-Bhattacharyya parameter  $R(\mathcal{W})$  approaches  $\{d, 1/d\}$  values. This follows from Lemma 11, below.
3. Taking the good channel yields a guaranteed improvement of the average Rényi-Bhattacharyya parameter, in the sense of Lemma 12, below.

The proof of Theorem 9 then follows by using [8, Lemma 7], similar to the proof of quantum polarization for qubit-input channels in [8].

**Lemma 11.** Let  $\mathcal{W}_{A' \rightarrow B}$  be a channel with qudit input. Then,

1.  $R(\mathcal{W}) \leq \frac{1}{d} + \delta \Rightarrow I(\mathcal{W}) \geq 1 - \log(1 + d\delta)$ .
2.  $R(\mathcal{W}) \geq d - \delta \Rightarrow I(\mathcal{W}) \leq -1 + 2\sqrt{\frac{\delta}{d}} + \frac{\sqrt{d} + \sqrt{\delta}}{\sqrt{d}} h\left(\frac{\sqrt{\delta}}{\sqrt{d} + \sqrt{\delta}}\right)$ , where  $h(\cdot)$  denotes the binary entropy function.

*Proof.* We prove first 1). For  $\rho_{AB} = \mathcal{W}(\Phi_{AA'})$ , we have that

$$\frac{1}{d} + \delta \geq R(\mathcal{W}) = d^{\frac{H_1^{\frac{1}{2}}(A|B)_\rho}{2}} \geq d^{H(A|B)_\rho} = d^{-I(\mathcal{W})},$$

where we have used  $H_{\frac{1}{2}}^\uparrow(A|B)_\rho \geq H(A|B)_\rho$  for the second inequality, which follows from the monotonically decreasing property of the conditional Petz-Rényi entropy with respect to its order [15, Theorem 7]. Hence,  $I(\mathcal{W}) \geq 1 - \log(1 + d\delta)$ .

We now turn to point 2). We have that

$$\begin{aligned}
d - \delta &\leq R(\mathcal{W}) \leq R(\mathcal{W}) \\
&= \max_{\sigma_B} \text{Tr} \left[ \rho_{AB}^{\frac{1}{2}} \sigma_B^{\frac{1}{2}} \right]^2 \\
&= d \max_{\sigma_B} \text{Tr} \left[ \sqrt{\rho_{AB}} \sqrt{\frac{\mathbb{1}_A}{d} \otimes \sigma_B} \right]^2 \\
&\leq d \max_{\sigma_B} \left\| \sqrt{\rho_{AB}} \sqrt{\frac{\mathbb{1}_A}{d} \otimes \sigma_B} \right\|_1^2 \\
&= d \max_{\sigma_B} F \left( \rho_{AB}, \frac{\mathbb{1}_A}{d} \otimes \sigma_B \right)^2
\end{aligned} \tag{5}$$

Using the Fuchs-van de Graaf inequalities [16], we get that there exists a  $\sigma_B$  such that  $\frac{1}{2} \|\rho_{AB} - \frac{\mathbb{1}_A}{d} \otimes \sigma_B\|_1 \leq \sqrt{\frac{\delta}{d}}$ . We are now in a position to use the Alicki-Fannes-Winter [17, Lemma 2] inequality, which states that

$$|H(A|B)_\rho - 1| \leq 2\sqrt{\frac{\delta}{d}} + \frac{\sqrt{d} + \sqrt{\delta}}{\sqrt{d}} h \left( \frac{\sqrt{\delta}}{\sqrt{d} + \sqrt{\delta}} \right).$$

This concludes the proof of the lemma.  $\square$

**Lemma 12.** *Let  $\mathcal{W}_{A' \rightarrow B}$  be a channel with qudit input. Then,*

$$\mathbb{E}_C R \left( \mathcal{W}_C^{(1)} \right) = \frac{d}{d^2 + 1} (1 + R(\mathcal{W})^2) \leq R(\mathcal{W}),$$

where  $\mathbb{E}_C$  denotes the expectation operator,  $C$  is the channel combining unitary, chosen uniformly at random from a unitary 2-design  $\mathcal{U}$ . Moreover, equality happens if and only if  $R(\mathcal{W}) \in \{1/d, d\}$ .

*Proof.* Let  $\mathcal{W}_{A' \rightarrow E}^c$  and  $(\mathcal{W}_C^{(1)})_{A'_2 \rightarrow E_1 E_2}^c$  be the complementary channel associated with  $\mathcal{W}_{A' \rightarrow B}$  and the good channel  $\mathcal{W}_{C_{A'_2 \rightarrow A_1 B_1 B_2}}^{(1)}$ , respectively. The complementary of the good channel acts as  $(\mathcal{W}_C^{(1)})^c(\rho) = (\mathcal{W}^c \otimes \mathcal{W}^c) \left( C \left( \frac{\mathbb{1}_{A'_1}}{d} \otimes \rho \right) C^\dagger \right)$  (see [8, Appendix A] for a proof). Therefore,  $R(\mathcal{W}_C^{(1)}) = d^{-\tilde{H}_2^\downarrow(A_2|E_1 E_2)_\rho}$ , where  $\rho_{A_2 E_1 E_2} = (\mathcal{W}_C^{(1)})^c(\Phi_{A_2 A'_2})$ . Note that  $\rho_{E_1 E_2} = \mathcal{W}^c \left( \frac{\mathbb{1}}{d} \right) \otimes \mathcal{W}^c \left( \frac{\mathbb{1}}{d} \right)$ , which is independent of  $C$ . To compute the expected value of  $R(\mathcal{W}_C^{(1)})$  with respect to  $C$ , we proceed as follows.

$$\begin{aligned}
\mathbb{E}_C d^{-\tilde{H}_2^\downarrow(A_2|E_1 E_2)_\rho} &= \mathbb{E}_C \text{Tr} \left[ \left( \rho_{E_1 E_2}^{-\frac{1}{4}} \rho_{A_2 E_1 E_2} \rho_{E_1 E_2}^{-\frac{1}{4}} \right)^2 \right] \\
&= \mathbb{E}_C \text{Tr} \left[ \left( \rho_{E_1 E_2}^{-\frac{1}{4}} (\mathcal{W}^c \otimes \mathcal{W}^c) \left( C \left( \frac{\mathbb{1}_{A'_1}}{d} \otimes \Phi_{A_2 A'_2} \right) C^\dagger \right) \rho_{E_1 E_2}^{-\frac{1}{4}} \right)^2 \right].
\end{aligned}$$

Note that this is basically the same calculation as in [18, Equation (3.32)] (there,  $U$  is chosen according to the Haar measure over the full unitary group, but all that is required

is a unitary 2-design). However, we will not make the simplifications after (3.44) and (3.45) in [18], but will instead keep all the terms. We therefore get  $\mathbb{E}_C d^{-\tilde{H}_2^\downarrow(A_2|E_1E_2)_\rho} = \alpha \text{Tr} \left[ \left( \frac{\mathbb{1}_{A_2}}{d} \right)^2 \right] + \beta \text{Tr} \left[ \left( \frac{\mathbb{1}_{A_1}}{d} \otimes \Phi_{A_2A_2'} \right)^2 \right] = \frac{1}{d}\alpha + \frac{1}{d}\beta$ , where  $\alpha = \frac{d^4}{d^4-1} - \frac{d^2}{d^4-1} d^{-\tilde{H}_2^\downarrow(A_1A_2|E_1E_2)_\omega}$ ,  $\beta = \frac{d^4}{d^4-1} d^{-\tilde{H}_2^\downarrow(A_1A_2|E_1E_2)_\omega} - \frac{d^2}{d^4-1}$ , and  $\omega_{A_1A_2E_1E_2} := (\mathcal{W}^c \otimes \mathcal{W}^c)(\Phi_{A_1A_1'} \otimes \Phi_{A_2A_2'})$ . Hence,

$$\begin{aligned} \mathbb{E}_C d^{-\tilde{H}_2^\downarrow(A_2|E_1E_2)_\rho} &= \frac{d}{d^2+1} + \frac{d}{d^2+1} d^{-\tilde{H}_2^\downarrow(A_1A_2|E_1E_2)_\omega} \\ &= \frac{d}{d^2+1} (1 + R(\mathcal{W})^2), \end{aligned}$$

where the second equality follows from  $d^{-\tilde{H}_2^\downarrow(A_1A_2|E_1E_2)_\omega} = R(\mathcal{W})^2$  using the fact that conditional sandwiched Rényi entropy of order 2 is additive with respect to tensor-product states. It is easily seen that the function  $f(R) = \frac{d}{d^2+1}(1 + R^2)$  is a convex function satisfying  $f(R) = R$  for  $R \in \{\frac{1}{d}, d\}$  and  $f(R) < R$  for  $R \in (\frac{1}{d}, d)$ .  $\square$

### 3.3 Proof of Theorem 10

*Proof of part (a).* It is shown in [13, Theorem 1] (see also [19]) that the Clifford group on  $n$ -qubits forms a unitary 2-design for any  $n \geq 1$ . Here, we generalize the proof from [13] to the qudit case, and for  $n = 2$ . We need to prove that the Clifford group  $\mathcal{C}_d^2$  satisfies the Definition 8. For this, it is sufficient to prove (2), with  $\mathcal{U} = \mathcal{C}_d^2$ , for two-qudit input quantum channels of the form  $\mathcal{W}_2(\rho) := A\rho B$  (since any quantum channel is a convex combination of quantum channels of this form).

We first consider the twirling of  $\mathcal{W}_2$  with respect to the Clifford group  $\mathcal{C}_d^2$ . Since the Pauli group  $\mathcal{P}_d^2$  is a normal subgroup of  $\mathcal{C}_d^2$ , we may choose a subset  $\bar{\mathcal{C}}_d^2 \subset \mathcal{C}_d^2$  containing one representative for each equivalence class in the quotient group  $\mathcal{C}_d^2/\mathcal{P}_d^2$ . Thus, any element of  $\mathcal{C}_d^2$  can be uniquely written as a product  $CP$ , where  $C \in \bar{\mathcal{C}}_d^2$ , and  $P \in \mathcal{P}_d^2$ . Therefore, in order to twirl  $\mathcal{W}_2$  with respect to  $\mathcal{C}_d^2$ , we may first twirl it with respect to  $\mathcal{P}_d^2$ , then twirl again the obtained channel with respect to  $\bar{\mathcal{C}}_d^2$ .

The elements of  $\mathcal{P}_d^2$  have the form  $\omega^\lambda P_{r,s} \otimes P_{r',s'}$ , with  $\lambda, r, s, r', s' = 0, \dots, d-1$ . Hence, twirling  $\mathcal{W}_2$  with respect to  $\mathcal{P}_d^2$  gives a quantum channel, denoted  $\mathcal{W}'_2$ , defined below

$$\begin{aligned} \mathcal{W}'_2(\rho) &:= \frac{1}{d^5} \sum_{\lambda, r, s, r', s'} (\omega^\lambda P_{r,s} \otimes P_{r',s'})^\dagger A (\omega^\lambda P_{r,s} \otimes P_{r',s'}) \rho (\omega^\lambda P_{r,s} \otimes P_{r',s'})^\dagger B (\omega^\lambda P_{r,s} \otimes P_{r',s'}), \\ &= \frac{1}{d^4} \sum_{r, s, r', s'} (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) A (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) B (P_{r,s} \otimes P_{r',s'}). \end{aligned} \quad (7)$$

The last equality from the above shows that it is actually enough to twirl  $\mathcal{W}_2$  with respect to the subset  $\bar{\mathcal{P}}_d^2 := \{P_{r,s} \otimes P_{r',s'} \mid r, s, r', s' = 0, \dots, d-1\}$ , obtained by omitting phase factors. Since  $\bar{\mathcal{P}}_d^2$  forms an operator basis (for two-qudit operators), we may write  $A = \sum_{r, s, r', s'} \alpha(r, s, r', s') P_{r,s} \otimes P_{r',s'}$ , and  $B = \sum_{r, s, r', s'} \beta(r, s, r', s') P_{r,s} \otimes P_{r',s'}$ . The following two lemmas are proven in Appendix A and Appendix B, respectively.

**Lemma 13.** *The quantum channel  $\mathcal{W}'_2$ , obtained by twirling  $\mathcal{W}_2$  with respect to  $\bar{\mathcal{P}}_d^2$ , is a Pauli channel satisfying the following*

$$\mathcal{W}'_2(\rho) = \sum_{r, s, r', s'} \gamma_{r, s, r', s'} (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger), \quad (8)$$

where  $\gamma_{r, s, r', s'} := \omega^{rs+r's'} \alpha(r, s, r', s') \beta(-r, -s, -r', -s')$  and  $-x$  denotes the additive inverse of  $x$  modulo  $d$ .



**Lemma 14.** *The quantum channel obtained by twirling  $\mathcal{W}_2'$  with respect to  $\bar{\mathcal{C}}_d^2$ , is the quantum channel  $\mathcal{W}_2''$  acting as*

$$\mathcal{W}_2''(\rho) = \frac{\text{Tr}(AB)}{d^4} \mathbb{1} \otimes \mathbb{1} + \frac{d^2 \text{Tr}(A) \text{Tr}(B) - \text{Tr}(AB)}{d^2(d^4 - 1)} \left( \rho - \frac{1}{d^2} \mathbb{1} \otimes \mathbb{1} \right). \quad (9)$$

Now, the quantum channel  $\mathcal{W}_2''$  from (9) is the twirling of  $\mathcal{W}_2$  with respect to  $\mathcal{C}_d^2$ . To conclude that  $\mathcal{C}_d^2$  is a unitary 2-design, we need to show that twirling  $\mathcal{W}_2$  with respect to  $\mathcal{U}(d^2)$  yields the same channel, which follows from [20].

*Proof of part (b).* We will need the following two lemmas. The first is basically the same as [8, Lemma 14] and the proof can be easily generalized. The second is proven in Appendix C.

**Lemma 15.** *Consider  $C, C' \in \mathcal{C}_d^2$ , such that  $C' = C(C_1 \otimes C_2)$ , for some  $C_1, C_2 \in \mathcal{C}_d^1$ . Then,  $C'$  and  $C''$  yield the same Rényi-Bhattacharyya parameter for both good and bad channels, i.e., following equalities hold,*

- 1)  $R(\mathcal{W}_C^{(0)}) = R(\mathcal{W}_{C'}^{(0)})$ .
- 2)  $R(\mathcal{W}_C^{(1)}) = R(\mathcal{W}_{C'}^{(1)})$ .

**Lemma 16.** *If  $d$  is a prime number,  $|\mathcal{C}_d^1| = d^3(d^2 - 1)$  and  $|\mathcal{C}_d^2| = d^8(d^4 - 1)(d^2 - 1)$ .*

We are now in a position to prove the part (b) of the theorem. The group  $\mathcal{C}_d^2$  can be decomposed into left cosets with respect to the subgroup  $\mathcal{C}_d^1 \otimes \mathcal{C}_d^1 \subset \mathcal{C}_d^2$ . From Lemma 15, it follows that any two elements in the same left coset, when used as channel combiners, yield the same Rényi-Bhattacharyya parameter for both good and bad channels. Therefore, polarization also happens for any subset  $\mathcal{L} \subset \mathcal{C}_d^2$ , containing one representative of each left coset (since  $\mathbb{E}_{C \in \mathcal{L}} R(\mathcal{W}_C^{(1)}) = \mathbb{E}_{C \in \mathcal{C}_d^2} R(\mathcal{W}_C^{(1)})$ , thus the guaranteed improvement of the average Rényi-Bhattacharyya parameter, in the sense of Lemma 12, still holds when  $C$  is randomly chosen from  $\mathcal{L}$ ). Using Lemma 16, the number of cosets of  $\mathcal{C}_d^1 \otimes \mathcal{C}_d^1$  in  $\mathcal{C}_d^2$  is equal to  $\frac{|\mathcal{C}_d^2|}{|\mathcal{C}_d^1 \otimes \mathcal{C}_d^1|} = d^4 + d^2$ , therefore  $\mathcal{L}$  contains  $d^4 + d^2$  representatives, two of which may be chosen to be the identity ( $I$ ) and the swap ( $S$ ) operators. Since  $R(\mathcal{W}_I^{(1)}) = R(\mathcal{W}_S^{(1)}) = R(\mathcal{W}) \geq \mathbb{E}_{C \in \mathcal{L}} R(\mathcal{W}_C^{(1)})$ , we may further remove  $I$  and  $S$  from  $\mathcal{L}$ , thus getting a subset  $\mathcal{L}' := \mathcal{L} \setminus \{I, S\}$  containing  $d^4 + d^2 - 2$  elements, which still ensures polarization of qudit-input quantum channels. From [21, 22], we know that a set of unitaries in dimension  $\delta$  can only form a unitary 2-design if it has at least  $\delta^4 - 2\delta^2 + 2$  elements. As we consider a two-qudit system (dimension  $\delta = d^2$ ), a unitary 2-design would have at least  $d^8 - 2d^4 + 2$  two-qudit unitaries, which is clearly bigger than  $d^4 + d^2 - 2$ . Hence, the set  $\mathcal{L}'$  is not a unitary 2-design. This completes the proof of the part (b).  $\square$

One may try to further reduce the size of  $\mathcal{L}'$ , by considering the action of the swap gate  $S$ . Indeed, it can be seen that the two equalities from Lemma 15 also hold for two  $C, C' \in \mathcal{C}_d^2$ , such that  $C' = SC$  (see also [8, Lemma 15]). Hence, if both  $C$  and  $C'$  belong to  $\mathcal{L}'$ , one of them can be removed, while still ensuring polarization. Now, multiplying by  $S$  on the left induces a permutation on the left cosets of  $\mathcal{C}_d^1 \otimes \mathcal{C}_d^1$  in  $\mathcal{C}_d^2$ , which in turn induces a permutation  $\mathcal{L}' \xrightarrow{\sim} \mathcal{L}'$ . In the qubit case ( $d = 2$ ), this permutation has no fixed points, thus the size of  $\mathcal{L}'$  can be reduced by half. However, in general the above permutation may have fixed points. We provide such an example in Appendix D, where we show that for  $d = 5$ , there exist  $C \in \mathcal{C}_d^2$  and  $C_1, C_2 \in \mathcal{C}_d^1$ , such that  $SC = C(C_1 \otimes C_2)$ .



## 4 Quantum Polar codes on Pauli Qudit channels

In this section, we discuss the decoding of quantum polar codes on a Pauli qudit channel. We shall assume that all channel combining unitaries are Clifford unitaries.

A Pauli qudit channel  $\mathcal{W}$  is defined as the quantum channel that maps a qudit quantum state  $\rho$  to  $\sum_{r,s} a_{r,s} P_{r,s} \rho P_{r,s}^\dagger$ , where  $a_{r,s} \geq 0$  with  $\sum_{r,s} a_{r,s} = 1$ . Similar to [8, Definition 17], we associate a classical channel with  $\mathcal{W}$ , which is referred to as the classical counterpart of  $\mathcal{W}$ , and denoted by  $\mathcal{W}^\#$ . The classical counterpart  $\mathcal{W}^\#$  is a classical channel with input and output alphabet  $\bar{\mathcal{P}}_d^1 := \{P_{r,s} \mid r, s = 0, \dots, d-1\}$ , and transition probabilities  $\mathcal{W}^\#(P_{r,s} \mid P_{t,u}) = a_{v,w}$ , where  $v = r + t \pmod{d}$  and  $w = s + u \pmod{d}$ . Consider now the channel combining and splitting procedure on  $\mathcal{W}$ , where  $C \in \mathcal{C}_d^2$  is used to combine the two copies of  $\mathcal{W}$ . Let  $\Gamma_C : \bar{\mathcal{P}}_d^1 \otimes \bar{\mathcal{P}}_d^1 \mapsto \bar{\mathcal{P}}_d^1 \otimes \bar{\mathcal{P}}_d^1$  be the permutation induced by the conjugate action of  $C$ . We may define a channel combining and splitting procedure on the classical  $\mathcal{W}^\#$ , using  $\Gamma_C$  to combine the two copies of  $\mathcal{W}^\#$ . Similarly to [8], we may prove (but the proof is omitted here) that the Pauli qudit channel  $\mathcal{W}$  and its classical counterpart  $\mathcal{W}^\#$  *polarize simultaneously*, in the sense of [8, Proposition 20 and Corollary 21], under their respective channel combining and splitting procedure. As a consequence, to a quantum polar code on the Pauli qudit channel  $\mathcal{W}$ , we may associate a classical polar code on  $\mathcal{W}^\#$ , then exploit classical polar decoding in order to decode Pauli errors, as explained below (see also [8, Section 6]). Let  $\mathbf{P}$  denote the unitary corresponding to a quantum polar code of length  $N$  qudits (see also [8, Section 5]), and  $\mathbf{P}^\#$  the linear map corresponding to the classical polar code. To perform decoding, we first apply  $\mathbf{P}^\dagger$  on the  $N$ -qudit channel output, that is, the encoded quantum state corrupted by some Pauli error, say  $E \in (\bar{\mathcal{P}}_d^1)^{\otimes N}$  (we may omit phase factors). Hence, applying  $\mathbf{P}^\dagger$  brings it back to the original (un-encoded) state, which is however corrupted by a Pauli error  $E' \in (\bar{\mathcal{P}}_d^1)^{\otimes N}$ , such that  $\mathbf{P}^\#(E') = E$ . We are now in position to decode  $E'$ , provided that we have been given the errors corresponding to the noisy virtual channels. We know that the inputs to the noisy channels are halves of preshared EPR pairs. Hence, we may perform projective measurements on the preshared EPR pairs, with respect to the generalized Bell basis  $\{I \otimes P_{r,s} |\Phi_{AA'}\rangle \mid P_{r,s} \in \bar{\mathcal{P}}_d^1\}$ , which give us the errors, *i.e.*, the  $E'$  components, on the noisy virtual channels, as desired. Finally, we may decode the classical polar code to determine  $E'$ , and subsequently apply  $E'^\dagger$  to return the system to the original quantum state.

## 5 Conclusion and perspectives

The goal of this work has been to generalize the purely quantum polarization construction to higher dimensional quantum systems. We have introduced the necessary definitions and worked out the proof of quantum polarization, assuming the channel combining unitary is randomized over (1) an unitary 2-design, (2) the two-qudit Clifford group, or (3) a smaller subset of two-qudit Cliffords. Using Clifford channel combining unitaries is important, as we showed it allows reducing the decoding problem to a classical polar code decoding, for qudit Pauli channels. However, we note that the reliability of the classical polar code decoding also depends on the speed of polarization [1]. We believe that fast polarization properties can also be generalized to the qudit case, although we leave this here as an open question.

## Acknowledgements

This research was supported in part by the ‘‘Investissements d’avenir’’ (ANR-15-IDEX-02) program of the French National Research Agency. Ashutosh Goswami acknowledges the European Union’s Horizon 2020 research and innovation programme, under the Marie Skłodowska Curie grant agreement No 754303.

## A Proof of Lemma 13

Recall that  $\bar{\mathcal{P}}_d^2 = \{P_{r,s} \otimes P_{r',s'} \mid r, s, r', s' = 0, \dots, d-1\}$  is the subset of two-qudit Pauli, without phase factors. Hence, twirling of  $\mathcal{W}_2$  with respect to  $\bar{\mathcal{P}}_d^2$  gives

$$\mathcal{W}'_2(\rho) = \frac{1}{d^4} \sum_{r,s,r',s'} (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) A (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) B (P_{r,s} \otimes P_{r',s'}) \quad (10)$$

Since  $\bar{\mathcal{P}}_d^2$  forms an operator basis, we may write

$$A = \sum_{r,s,r',s'} \alpha(r, s, r', s') P_{r,s} \otimes P_{r',s'}, \quad (11)$$

$$B = \sum_{r,s,r',s'} \beta(r, s, r', s') P_{r,s} \otimes P_{r',s'} \quad (12)$$

Substituting  $A$  and  $B$  in the above equation, we get

$$\mathcal{W}'_2(\rho) = \frac{1}{d^4} \sum_{t,u,t',u'} \sum_{v,w,v',w'} \alpha(t, u, t', u') \beta(v, w, v', w') \kappa, \quad (13)$$

$$\text{where } \kappa := \sum_{r,r',s,s'} (P_{r,s}^\dagger P_{t,u} P_{r,s}) \otimes (P_{r',s'}^\dagger P_{t',u'} P_{r',s'}) \rho (P_{r,s}^\dagger P_{v,w} P_{r,s}) \otimes (P_{r',s'}^\dagger P_{v',w'} P_{r',s'}). \quad (14)$$

From (1), we have that  $P_{t,u} P_{r,s} = \omega^{-ru+st} P_{r,s} P_{t,u}$ . Then, we may write

$$\kappa = k (P_{t,u} \otimes P_{t',u'}) \rho (P_{v,w} \otimes P_{v',w'}) \quad (15)$$

$$\text{with } k := \sum_{r,s} \omega^{-r(u+w)+s(v+t)} \sum_{r',s'} \omega^{-r'(u'+w')+s'(v'+t')}. \quad (16)$$

When  $u + w = v + t = 0 \pmod{d}$ , we have  $\sum_{r,s} \omega^{-r(u+w)+s(v+t)} = d^2$ . When either  $u + w \neq 0 \pmod{d}$  or  $t + w \neq 0 \pmod{d}$ , we have  $\sum_{r,s} \omega^{-r(u+w)+s(v+t)} = \frac{(\omega^{-d}-1)(\omega^d-1)}{(\omega^{-1}-1)(\omega-1)} = 0$ . Therefore,

$$k = \begin{cases} d^4, & \text{when } u + w = v + t = u' + w' = v' + t' = 0 \pmod{d} \\ 0, & \text{otherwise} \end{cases} \quad (17)$$

The condition  $u + w = v + t = 0 \pmod{d}$  implies that  $P_{t,u} P_{v,w} = X^t Z^u X^v Z^w = \omega^{-uv} I$ . Using  $t = -v \pmod{d}$ , we have that  $P_{v,w} = \omega^{tv} P_{t,u}^\dagger$ . Plugging  $\kappa$  into (13), we get

$$\mathcal{W}'_2(\rho) = \sum_{t,u,t',u'} \gamma_{t,u,t',u'} (P_{t,u} \otimes P_{t',u'}) \rho (P_{t,u}^\dagger \otimes P_{t',u'}^\dagger), \quad (18)$$

$$\text{where } \gamma_{t,u,t',u'} := \omega^{tu+t'u'} \alpha(t, u, t', u') \beta(-t, -u, -t', -u'). \quad (19)$$

Hence,  $\mathcal{W}'_2$  is a qudit Pauli channel, as desired.  $\square$

## B Proof of Lemma 14

Recall that  $\bar{\mathcal{C}}_d^2 \subset \mathcal{C}_d^2$  is a subset containing one representative for each equivalence class in the quotient group  $\mathcal{C}_d^2/\mathcal{P}_d^2$ . Twirling of  $\mathcal{W}'_2$  with respect to  $\bar{\mathcal{C}}_d^2$  gives

$$\mathcal{W}''_2(\rho) = \sum_{t,u,t',u'} \gamma_{t,u,t',u'} \frac{1}{|\bar{\mathcal{C}}_d^2|} \sum_{C \in \bar{\mathcal{C}}_d^2} C^\dagger (P_{t,u} \otimes P_{t',u'}) C \rho C^\dagger (P_{t,u}^\dagger \otimes P_{t',u'}^\dagger) C. \quad (20)$$

We know that the conjugate action of the entire set  $\bar{\mathcal{C}}_d^2$  maps any  $P_{t,u} \otimes P_{t',u'} \neq I \otimes I$  to all  $d^4 - 1$  two-qudit Paulis excluding  $I \otimes I$ , an equal number of times. In other words,  $P_{t,u} \otimes P_{t',u'} \neq I \otimes I$  gets mapped to a Pauli  $P_{r,s} \otimes P_{r',s'} \neq I \otimes I$ ,  $\frac{|\bar{\mathcal{C}}_d^2|}{d^4-1}$  times. Further,  $I \otimes I$  is always mapped to  $I \otimes I$ . Therefore, we have that

$$\mathcal{W}''_2(\rho) = \gamma_{0,0,0,0} \rho + \frac{1}{d^4-1} \gamma' \sum_{(r,s,r',s') \neq (0,0,0,0)} (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger), \quad (21)$$

$$\text{where } \gamma' := \sum_{(t,u,t',u') \neq (0,0,0,0)} \gamma_{t,u,t',u'}. \quad (22)$$

Using the following three identities, we can easily transform (21) into the form of (9).

1.  $\gamma_{0,0,0,0} = \frac{\text{Tr}(A)\text{Tr}(B)}{d^4}$ .
2.  $\sum_{t,u,t',u'} \gamma_{t,u,t',u'} = \frac{\text{Tr}(AB)}{d^2}$ .
3.  $\sum_{r,s,r',s'} (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) = d^2 I \otimes I$ .

*Proof of identity 1)* We have that  $\gamma_{0,0,0,0} = \alpha(0,0,0,0)\beta(0,0,0,0)$ . Also,

$$\text{Tr}(P_{r,s}) = \begin{cases} d, & \text{when } P_{r,s} = I \\ 0, & \text{otherwise} \end{cases}$$

Using (11) and (12), we get  $\text{Tr}(A) = \alpha(0,0,0,0)d^2$  and  $\text{Tr}(B) = \beta(0,0,0,0)d^2$ . Hence,  $\gamma_{0,0,0,0} = \frac{\text{Tr}(A)\text{Tr}(B)}{d^4}$ .

*Proof of identity 2)* We have,

$$\begin{aligned} \text{Tr}(AB) &= \sum_{t,u,t',u'} \sum_{v,w,v',w'} \alpha(t,u,t',u') \beta(v,w,v',w') \text{Tr}(P_{t,u} P_{v,w}) \text{Tr}(P_{t',u'} P_{v',w'}) \\ &= \sum_{t,u,t',u'} d^2 \omega^{tu+t'u'} \alpha(t,u,t',u') \beta(-t,-u,-t',-u') \\ &= d^2 \sum_{t,u,t',u'} \gamma_{t,u,t',u'}. \end{aligned}$$

*Proof of identity 3)* Let  $\rho = \sum_{r,s,r',s'} \rho_{r,s,r',s'} P_{r,s} \otimes P_{r',s'}$ . Since  $\rho$  is a density matrix, we have

$\rho_{0,0,0,0} = \frac{\text{Tr}(\rho)}{d^2} = \frac{1}{d^2}$ . Hence,

$$\begin{aligned}
\sum_{r,s,r',s'} (P_{r,s} \otimes P_{r',s'}) \rho (P_{r,s}^\dagger \otimes P_{r',s'}^\dagger) &= \sum_{r,s,r',s'} \sum_{t,u,t',u'} \rho_{t,u,t',u'} (P_{r,s} P_{t,u} P_{r,s}^\dagger) \otimes (P_{r',s'} P_{t',u'} P_{r',s'}^\dagger) \\
&= \sum_{t,u,t',u'} \rho_{t,u,t',u'} \left( \sum_{r,s,r',s'} \omega^{-st+ru} \omega^{-s't'+r'u'} \right) P_{t,u} \otimes P_{t',u'} \\
&= d^4 \rho_{0,0,0,0} I \otimes I \\
&= d^2 I \otimes I.
\end{aligned}$$

We get (9) from (21) by using the above identities, while also substituting the notation  $\mathbb{1}$  for the identity matrix  $I$ , as it denotes a quantum state here.  $\square$

## C Proof of Lemma 16

Consider the one-qudit Clifford group  $\mathcal{C}_d^1$ . We count first the permutations generated by  $\mathcal{C}_d^1$  on  $\bar{\mathcal{P}}_d^1 := \{P_{r,s} | r, s = 0, \dots, d-1\}$ , and later we will accommodate the phase factors. Any Clifford  $C \in \mathcal{C}_d^1$  is uniquely determined by its conjugate action on the generators of the Pauli group,  $X$  and  $Z$ . Suppose that  $C$  maps  $X \mapsto P_{r,s}$  and  $Z \mapsto P_{t,u}$  via its conjugate action, where  $P_{r,s}, P_{t,u} \neq I$ . On the one hand, since commutation relations are preserved under unitary conjugation,  $P_{r,s}$  and  $P_{t,u}$  must satisfy  $P_{r,s} P_{t,u} = \omega P_{t,u} P_{r,s}$ . On the other hand, from (1), we have that  $P_{r,s} P_{t,u} = \omega^{ru-st} P_{t,u} P_{r,s}$ . Therefore,  $r, u, s, t$  must be such that  $ru - st = 1 \pmod{d}$ . We fix  $r, s$  and solve for  $t, u$ . Since  $P_{r,s} \neq I$ , it follows that either  $r$  or  $s$  is non-zero. Without loss of generality, we may assume that  $r \neq 0$ . Since  $d$  is a prime number,  $r$  is invertible under multiplication modulo  $d$ . Therefore, for any  $t \in \{0, \dots, d-1\}$ , there exists a unique  $u := r^{-1}(1 + st) \pmod{d}$ , satisfying  $ru - st = 1$ . Hence, there are exactly  $d$  choices for the  $t, u$  pair. Since we have  $d^2 - 1$  choices for the  $r, s$  pair, it follows that there are  $d(d^2 - 1)$  pairs of Paulis,  $P_{r,s}$  and  $P_{t,u}$ , such that  $P_{r,s} P_{t,u} = \omega P_{t,u} P_{r,s}$ . Taking into account the phase factors,  $\omega^\lambda, \lambda \in \{0, \dots, d-1\}$ , it follows that  $\mathcal{C}_d^1$  has  $d^3(d^2 - 1)$  elements.

We now count the number of elements in  $\mathcal{C}_d^2$ . The two-qudit Pauli group  $\mathcal{P}_d^2$  is generated by a set of four Paulis  $I \otimes X, I \otimes Z, X \otimes I$  and  $Z \otimes I$ , and any Clifford  $C \in \mathcal{C}_d^2$  is uniquely determined by its conjugate action on these four generators. The commutation relations between the four generators are illustrated in Fig. 2. Consider a mapping

$$\begin{array}{cc}
I \otimes X & X \otimes I \\
| & | \\
I \otimes Z & Z \otimes I
\end{array}$$

Figure 2: Connected Paulis satisfy  $AB = \omega BA$ , with  $A$  is the Pauli on the top row, and  $B$  the Pauli on the bottom row. Paulis that are not connected commute.

$I \otimes X \mapsto A, I \otimes Z \mapsto B, X \otimes I \mapsto A', Z \otimes I \mapsto B'$ , where  $A, B, A', B' \in \bar{\mathcal{P}}_d^2$ , that preserves all the commutation relations between generators. Pauli  $I \otimes X$  can be mapped to any two-qudit Pauli  $A \neq I \otimes I$ , so there are  $d^4 - 1$  choices for  $A$ . It is not very difficult to see that for any  $A \neq I \otimes I$  there are  $d^3$  choices for  $B$  such that  $AB = \omega BA$ . Further, there are  $d(d^2 - 1)$  pairs of two-qudit Paulis  $A'$  and  $B'$ , which commute with both  $A$  and  $B$ , and satisfy  $A'B' = \omega B'A'$ . Therefore, we have  $d^4(d^4 - 1)(d^2 - 1)$  possible permutations on  $\bar{\mathcal{P}}_d^2$ , which satisfy all the commutation relations. Taking into account the phase factors, it follows that  $\mathcal{C}_d^2$  has  $d^8(d^4 - 1)(d^2 - 1)$  elements.  $\square$

## D Example of left coset fixed by the swap gate

We consider  $d = 5$ . Let  $C_1 = I$  be the identity, and  $C'_2 \in \mathcal{C}_d^1$  be such that it maps  $X \mapsto X^4$  and  $Z \mapsto Z^4$ , via conjugation. Since  $X^4 Z^4 = \omega Z^4 X^4$ ,  $C'_2$  is indeed a one-qudit Clifford. We define  $C_2 = C'_2 X^2 Z^2$ . Further, let  $C \in \mathcal{C}_d^2$ , such that its conjugate action generates the following permutation on the generators of  $\mathcal{P}_d^2$ ,

$$\begin{aligned} I \otimes X &\mapsto X^4 Z \otimes X Z^4, \\ I \otimes Z &\mapsto X Z \otimes X^4 Z^4, \\ X \otimes I &\mapsto X^4 Z \otimes X^4 Z, \\ Z \otimes I &\mapsto X Z \otimes X Z. \end{aligned}$$

Using (1), it is easily seen that the above permutation preserves all the commutation relations between the generators. Now, the conjugate actions of  $SC$  and  $C(C_1 \otimes C_2)$  generate the same permutation on  $\mathcal{P}_d^2$ . Therefore,  $SC = C(C_1 \otimes C_2)$ .

## References

- [1] Erdal Arıkan. “Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels”. In: *IEEE Transactions on Information Theory* 55.7 (July 2009), pp. 3051–3073. DOI: [10.1109/TIT.2009.2021379](https://doi.org/10.1109/TIT.2009.2021379). arXiv: [0807.3917](https://arxiv.org/abs/0807.3917).
- [2] Mark M. Wilde and Saikat Guha. “Polar Codes for Classical-Quantum Channels”. In: *IEEE Transactions on Information Theory* 59.2 (Feb. 2013), pp. 1175–1187. DOI: [10.1109/TIT.2012.2218792](https://doi.org/10.1109/TIT.2012.2218792). arXiv: [1109.2591](https://arxiv.org/abs/1109.2591).
- [3] Rajai Nasser and Joseph M. Renes. “Polar codes for arbitrary classical-quantum channels and arbitrary cq-MACs”. In: *IEEE Transactions on Information Theory* 64.11 (Nov. 2018), pp. 7424–7442. DOI: <https://doi.org/10.1109/TIT.2018.2869460>. arXiv: [1701.03397](https://arxiv.org/abs/1701.03397).
- [4] Joseph M. Renes, Frédéric Dupuis, and Renato Renner. “Efficient Polar Coding of Quantum Information”. In: *Physical Review Letters* 109 (5 Aug. 2012), p. 050504. DOI: [10.1103/PhysRevLett.109.050504](https://doi.org/10.1103/PhysRevLett.109.050504). arXiv: [1109.3195](https://arxiv.org/abs/1109.3195).
- [5] Mark M. Wilde and Saikat Guha. “Polar Codes for Degradable Quantum Channels”. In: *IEEE Transactions on Information Theory* 59.7 (July 2013), pp. 4718–4729. DOI: [10.1109/TIT.2013.2250575](https://doi.org/10.1109/TIT.2013.2250575). arXiv: [1109.5346](https://arxiv.org/abs/1109.5346).
- [6] Joseph M. Renes and Mark M. Wilde. “Polar Codes for Private and Quantum Communication Over Arbitrary Channels”. In: *IEEE Transactions on Information Theory* 60.6 (June 2014), pp. 3090–3103. DOI: [10.1109/TIT.2014.2314463](https://doi.org/10.1109/TIT.2014.2314463). arXiv: [1212.2537](https://arxiv.org/abs/1212.2537).
- [7] Frédéric Dupuis, Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. “Purely Quantum Polar Codes”. In: *2019 IEEE Information Theory Workshop (ITW)* (Aug. 2019). DOI: [10.1109/ITW44776.2019.8989387](https://doi.org/10.1109/ITW44776.2019.8989387).
- [8] Frédéric Dupuis, Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. “Polarization of Quantum Channels using Clifford-based Channel Combining”. In: *IEEE Transactions on Information Theory* 67.5 (2021), pp. 2857–2877. DOI: [10.1109/TIT.2021.3063093](https://doi.org/10.1109/TIT.2021.3063093). arXiv: [1904.04713](https://arxiv.org/abs/1904.04713).

- [9] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. Cambridge University Press. DOI: [10.1017/9781316809976.001](https://doi.org/10.1017/9781316809976.001). arXiv: [1106.1445](https://arxiv.org/abs/1106.1445).
- [10] Marco Tomamichel, Mario Berta, and Masahito Hayashi. “Relating different quantum generalizations of the conditional Rényi entropy”. In: *Journal of Mathematical Physics* 55.8, 082206 (2014). DOI: [10.1063/1.4892761](https://doi.org/10.1063/1.4892761). arXiv: [1311.3887](https://arxiv.org/abs/1311.3887).
- [11] Daniel Gottesman. “Fault-Tolerant Quantum Computation with Higher-Dimensional Systems”. In: *Chaos, Solitons and Fractals* 10.10 (Sept. 1999), pp. 1749–1758. DOI: [https://doi.org/10.1016/S0960-0779\(98\)00218-5](https://doi.org/10.1016/S0960-0779(98)00218-5). arXiv: [quant-ph/9802007](https://arxiv.org/abs/quant-ph/9802007).
- [12] Vlad Gheorghiu. “Standard form of qudit stabilizer groups”. In: *Physics Letters A* 378.5–6 (Jan. 2014), pp. 505–509. DOI: <https://doi.org/10.1016/j.physleta.2013.12.009>. arXiv: [1101.1519](https://arxiv.org/abs/1101.1519).
- [13] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. “Exact and approximate unitary 2-designs and their application to fidelity estimation”. In: *Physical Review A* 80.1 (July 2009), p. 012304. DOI: <https://doi.org/10.1103/PhysRevA.80.012304>. arXiv: [quant-ph/0606161](https://arxiv.org/abs/quant-ph/0606161).
- [14] Zak Webb. “The Clifford group forms a unitary 3-design”. In: *Quantum Information and Computation* 16 (2016), pp. 1379–1400. DOI: [10.26421/QIC16.15-16-8](https://doi.org/10.26421/QIC16.15-16-8). arXiv: [1510.02769](https://arxiv.org/abs/1510.02769).
- [15] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. “On quantum Rényi entropies: a new generalization and some properties”. In: *Journal of Mathematical Physics* 54.12, 122203 (2013). DOI: [10.1063/1.4838856](https://doi.org/10.1063/1.4838856). arXiv: [1306.3142](https://arxiv.org/abs/1306.3142).
- [16] Christopher A. Fuchs and Jeroen van de Graaf. “Cryptographic distinguishability measures for quantum-mechanical states”. In: *IEEE Transactions on Information Theory* 45.4 (1999), pp. 1216–1227. DOI: [10.1109/18.761271](https://doi.org/10.1109/18.761271). arXiv: [quant-ph/9712042](https://arxiv.org/abs/quant-ph/9712042).
- [17] Andreas Winter. “Tight Uniform Continuity Bounds for Quantum Entropies: Conditional Entropy, Relative Entropy Distance and Energy Constraints”. In: *Communications in Mathematical Physics* 347 (Oct. 2016), 291–313. DOI: <https://doi.org/10.1007/s00220-016-2609-8>. arXiv: [1507.07775](https://arxiv.org/abs/1507.07775).
- [18] Frédéric Dupuis. “The decoupling approach to quantum information theory”. PhD thesis. Université de Montréal, 2009. arXiv: [1004.1641](https://arxiv.org/abs/1004.1641).
- [19] Olivia Di Matteo. “A short introduction to unitary 2-designs”. eprint: [https://glassnotes.github.io/OliviaDiMatteo\\_Unitary2Designs.pdf](https://glassnotes.github.io/OliviaDiMatteo_Unitary2Designs.pdf).
- [20] Joseph Emerson, Robert Alicki, and Karol Życzkowski. “Scalable noise estimation with random unitary operators”. In: *Journal of Optics B: Quantum and Semiclassical Optics* 7.10 (Sept. 2005). DOI: <https://doi.org/10.1088/1464-4266/7/10/021>. arXiv: [quant-ph/0503243](https://arxiv.org/abs/quant-ph/0503243).
- [21] David Gross, Koenraad Audenaert, and Jens Eisert. “Evenly distributed unitaries: On the structure of unitary designs”. In: *Journal of Mathematical Physics* 48.5 (Feb. 2007), p. 052104. DOI: <https://doi.org/10.1063/1.2716992>. arXiv: [quant-ph/0611002](https://arxiv.org/abs/quant-ph/0611002).
- [22] Aidan Roy and A. J. Scott. “Unitary designs and codes”. In: *Designs, Codes and Cryptography* 53.5 (Apr. 2009), pp. 13–31. DOI: <https://doi.org/10.1007/s10623-009-9290-2>. arXiv: [0809.3813](https://arxiv.org/abs/0809.3813).