Generalized Perfect Codes for Symmetric Classical-Quantum Channels

Andreu Blasco Coll
Universitat Politècnica de Catalunya
andreu.blasco@upc.edu

Gonzalo Vazquez-Vilar
Universidad Carlos III de Madrid
gvazquez@ieee.org

Javier R. Fonollosa
Universitat Politècnica de Catalunya
javier.fonollosa@upc.edu

***Abstract*—We define a new family of codes for symmetric classical-quantum channels and establish their optimality. To this end, we extend the classical notion of generalized perfect and quasi-perfect codes to channels defined over some finite dimensional complex Hilbert output space. The resulting optimality conditions depend on the channel considered and on an auxiliary state defined on the output space of the channel. For certain 2-qubit classical-quantum channels, we show that codes based on a generalization of Bell states are quasi-perfect. Therefore, they feature the smallest error probability among all codes of the same blocklength and cardinality.**

I. Introduction

In the context of reliable communication, the ultimate goal of information theory is to characterize the best achievable performance of any transmission scheme and to establish the structure of codes and decoders attaining it. While information theory has not reached this goal in general, in certain regimes the best performance of a classical system is nowadays accurately characterized. Indeed, several code constructions attain the asymptotic channel capacity with vanishing error probability. For a finite blocklength, non-asymptotic bounds accurately describe the error probability of the best coding scheme for a certain range of transmission rates. Indeed, the performance of a code can even attain a converse bound with equality, thus proving its non-asymptotic optimality. For example, perfect and quasi-perfect binary codes attain the sphere-packing bound [1, Eq. (5.8.19)] in the binary symmetric channel (BSC). In particular, a binary code is said to be *perfect* if non-overlapping Hamming spheres of radius t centered on the codewords exactly fill out the space. Similarly, a *quasi-perfect* code is defined as a code in which Hamming spheres of radius t centered on the codewords are non-overlapping and Hamming spheres of radius $t+1$ cover the space, possibly with overlaps. The definition of perfect and quasi-perfect codes can be extended beyond binary alphabets. For classical channels, this notion was generalized in [2] using the hypothesis-testing bound [3, Th. 27]. The new definition depends on the channel considered and includes, e.g., maximum-distance separable (MDS) codes for erasure channels.

G. Vazquez-Vilar is also with the Gregorio Marañón Health Research Institute, Madrid, Spain. This work has been funded by the ERC grant 714161, by the AEI of Ministerio de Ciencia, Innovación y Universidades of Spain, TEC2016-75067-C4-2-R, TEC2016-78434-C3-3-R and RED2018-102668-T with ESF and Dept. d'Empresa i Coneixement de la Generalitat de Catalunya, 2017 SGR 578 AGAUR and 001-P-001644 QuantumCAT with ERDF.

In contrast to the classical setting, for classical-quantum channels much less is known about the structure of optimal codes. A lower bound to the error probability of any quantum code is [4, Th. 19] (see also [5, Sec. 4.6]). Optimizing the bound [4, Eq. (45)] over its free parameters for a fixed code yields the exact error probability for classical-quantum channels [6, Eq. (37)]. However, since this result is for a particular code, it does not yield insights on the structure of the best code. The analysis of good codes in terms of superadditivity of mutual information was studied in [7], [8].

In this work, we consider a relaxation of [4, Eq. (45)] which is independent of the codebook. We generalize the definition of perfect and quasi-perfect codes for symmetric classical-quantum channels. These codes, whenever they exist, are shown to attain the converse bound with equality and they are thus optimal. While these codes are rare, we characterize a family of codes based on the Bell states which are quasi-perfect for certain 2-qubit classical-quantum channels.

A. Notation

In the general case, a quantum state is described by a density operator ρ acting on some finite dimensional complex Hilbert space $\mathcal{H}$. Density operators are self-adjoint, positive semidefinite, and have unit trace. A measurement on a quantum system is a mapping from the state of the system ρ to a classical outcome $m \in \{1, \ldots, M\}$. A measurement is represented by a collection of positive self-adjoint operators $\{\Pi_1, \ldots, \Pi_M\}$ such that $\sum \Pi_m = \mathbb{1}$, where $\mathbb{1}$ is the identity operator. These operators form a *positive operator-valued measure (POVM)*. A POVM measurement $\{\Pi_1, \ldots, \Pi_M\}$ applied to ρ has outcome m with probability $\mathrm{Tr}(\rho\Pi_m)$. For self-adjoint operators A, B, the notation $A \geq B$ means that $A-B$ is positive semidefinite. Similarly $A \leq B$, $A > B$, and $A < B$ means that $A - B$ is negative semidefinite, positive definite and negative definite.

For a self-adjoint operator A with spectral decomposition $A = \sum_i \lambda_i E_i$, where $\{\lambda_i\}$ are the eigenvalues and $\{E_i\}$ are the orthogonal projections onto the corresponding eigenspaces, we define

$$\{A > 0\} \triangleq \sum_{i:\lambda_i>0} E_i. \tag{1}$$

This corresponds to the projector associated to the positive eigenspace of A. We shall also use $\{A \geq 0\} \triangleq \sum_{i:\lambda_i \geq 0} E_i$, $\{A < 0\} \triangleq \sum_{i:\lambda_i<0} E_i$ and $\{A \leq 0\} \triangleq \sum_{i:\lambda_i \leq 0} E_i$.

II. System Model and Preliminaries

We consider the channel coding problem of transmitting M equiprobable messages over a one-shot classical-quantum channel $x \to W_x$, with $x \in \mathcal{X}$ and $W_x \in \mathcal{H}$. A channel code is defined as a mapping from the message set $\{1, \ldots, M\}$ into a set of M codewords $\mathcal{C} = \{x_1, \ldots, x_M\}$. For a source message m, the decoder receives the associated density operator W_{x_m} and must decide on the transmitted message.

With some abuse of notation, for a fix code, sometimes we shall write $W_m \triangleq W_{x_m}$. The minimum error probability for a code $\mathcal{C}$ is then given by

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) \triangleq \min_{\{\Pi_1,\ldots,\Pi_M\}} \left\{ 1 - \frac{1}{M} \sum_{m=1}^{M} \operatorname{Tr}\bigl(W_m \Pi_m\bigr) \right\}. \quad (2)$$

In contrast to the classical setting, in which (2) is minimized by the maximum likelihood decoder, the minimizer of (2) has no simple form in general:

Lemma 1 (Holevo-Yuen-Kennedy-Lax conditions): The decoder $\mathcal{P} \triangleq \{\Pi_1, \ldots, \Pi_M\}$ minimizes (2) if and only if, for each $m = 1, \ldots, M$,

$$\bigl(\Lambda(\mathcal{P}) - \tfrac{1}{M} W_m\bigr)\Pi_m \;=\; \Pi_m\bigl(\Lambda(\mathcal{P}) - \tfrac{1}{M} W_m\bigr) \;=\; 0, \quad (3)$$

$$\Lambda(\mathcal{P}) - \tfrac{1}{M} W_m \;\geq\; 0, \quad (4)$$

where

$$\Lambda(\mathcal{P}) \triangleq \frac{1}{M} \sum_{\ell=1}^{M} W_\ell \Pi_\ell = \frac{1}{M} \sum_{\ell=1}^{M} \Pi_\ell W_\ell \quad (5)$$

is required to be self-adjoint.

Proof: The theorem follows from [9, Th. 4.1, Eq. (4.8)] or [10, Th. I] after simplifying the optimality conditions. ■

A. Binary hypothesis testing

Let us consider a binary hypothesis test discriminating between the density operators ρ_0 and ρ_1 acting on $\mathcal{H}$. In order to distinguish between the two hypotheses we perform a measurement. We define a test measurement $\{T, \bar{T}\}$, such that T and $\bar{T} \triangleq \mathbb{1} - T$ are positive semidefinite. The test decides ρ_0 (resp. ρ_1) when the measurement outcome corresponding to T (resp. $\bar{T}$) occurs. The optimal trade-off between the type-I error –deciding ρ_1 when the true hypothesis is ρ_0– and the type-II error –deciding ρ_0 when the true hypothesis is ρ_1– is

$$\alpha_\beta(\rho_0 \| \rho_1) \triangleq \inf_{T: \operatorname{Tr}(\rho_1 T) \leq \beta} 1 - \operatorname{Tr}(\rho_0 T). \quad (6)$$

The form of the test minimizing (6) is given by the quantum Neyman-Pearson lemma, presented next.

Lemma 2 (Neyman-Pearson lemma): The best trade-off between type-I and type-II error probabilities is attained by tests of the form

$$T_{\mathrm{NP}} = \bigl\{\rho_0 - t\rho_1 > 0\bigr\} + \theta_t^0, \quad (7)$$

for some t and θ_t^0, and where $0 \leq \theta_t^0 \leq \bigl\{\rho_0 - t\rho_1 = 0\bigr\}$.

Proof: A slightly different formulation of this result is usually given in the literature. The statement included here can be found, e.g., in [11, Lem. 3]. ■

Then, for the values of t and θ^0 such that $\operatorname{Tr}(\rho_1 T_{\mathrm{NP}}) = \beta$, the resulting test T_{NP} in (7) minimizes (6).

B. Meta-converse bound

The error probability (2) of any code can be lower bounded by the error probability of a binary hypothesis test. Let P denote a (classical) distribution over the input alphabet $\mathcal{X}$ and define

$$PW \triangleq \sum_{x\in\mathcal{X}} P(x) \Bigl(|x\rangle\langle x| \otimes W_x\Bigr), \quad (8)$$

$$P \otimes \mu \triangleq \Bigl(\sum_{x\in\mathcal{X}} P(x)\, |x\rangle\langle x|\Bigr) \otimes \mu. \quad (9)$$

Theorem 1 (Meta-converse): Let $\mathcal{C}$ be any codebook of cardinality M for a channel $W_x \in \mathcal{H}$. Then,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) \geq \inf_P \sup_\mu \Bigl\{ \alpha_{\frac{1}{M}}\bigl(PW \,\|\, P \otimes \mu\bigr) \Bigr\}, \quad (10)$$

where the minimization is over (classical) input distributions P, and the maximization is over auxiliary states $\mu \in \mathcal{H}$.

Proof: The result corresponds to [4, Eq. (46)] specialized to the classical-quantum setting. See also [5, Sec. 4.6]. ■

III. Quasi-Perfect Codes

For $t \in \mathbb{R}$, $t \geq 0$ and $\mu \in \mathcal{H}$, we define

$$\mathcal{E}_x(t,\mu) \triangleq \bigl\{W_x - t\mu \geq 0\bigr\}, \quad (11)$$

$$F_x(t,\mu) \triangleq \operatorname{Tr}\bigl(W_x \mathcal{E}_x(t,\mu)\bigr), \quad (12)$$

$$G_x(t,\mu) \triangleq \operatorname{Tr}\bigl(\mu\, \mathcal{E}_x(t,\mu)\bigr), \quad (13)$$

and we consider the following family of symmetric channels.

Definition 1: A channel $\{W_x\}$ is *symmetric* with respect to $\mu \in \mathcal{H}$ if $F_x(t,\mu)$ does not depend on $x \in \mathcal{X}$, i.e,

$$F_x(t,\mu) = F(t,\mu), \quad \forall x \in \mathcal{X},\ t \in \mathbb{R}. \quad (14)$$

Using (14), it can be shown that $G_x(t,\mu) = G(t,\mu)$ does not depend on x for any channel symmetric with respect to μ. Similarly to (11)-(13), we define

$$\mathcal{E}_x^\bullet(t,\mu) \triangleq \bigl\{W_x - t\mu > 0\bigr\}, \quad (15)$$

$$F_x^\bullet(t,\mu) \triangleq \operatorname{Tr}\bigl(W_x \mathcal{E}_x^\bullet(t,\mu)\bigr), \quad (16)$$

$$G_x^\bullet(t,\mu) \triangleq \operatorname{Tr}\bigl(\mu\, \mathcal{E}_x^\bullet(t,\mu)\bigr), \quad (17)$$

and, for a symmetric channel, $F_\bullet(\cdot) \triangleq F_x^\bullet(\cdot)$, $G_\bullet(\cdot) \triangleq G_x^\bullet(\cdot)$.

Definition 2: A code $\mathcal{C}$ is *perfect* for a classical-quantum channel $\{W_x\}$, if there exists a scalar t and a state $\mu \in \mathcal{H}$ such that the projectors $\bigl\{\mathcal{E}_x(t,\mu)\bigr\}_{x\in\mathcal{C}}$ are orthogonal to each other and $\sum_{x\in\mathcal{C}} \mathcal{E}_x(t,\mu) = \mathbb{1}$. More generally, a code is *quasi-perfect* if there exists t and $\mu \in \mathcal{H}$ such that the projectors $\bigl\{\mathcal{E}_x^\bullet(t,\mu)\bigr\}_{x\in\mathcal{C}}$ are orthogonal to each other and $\sum_{x\in\mathcal{C}} \mathcal{E}_x(t,\mu) \geq \mathbb{1}$.

The next result yields an alternative expression for the error probability of perfect and quasi-perfect codes.

Theorem 2 (Error probability of quasi-perfect codes): Let $\mathcal{C}$ be perfect or quasi-perfect according to Definition 2 with parameters t, μ, and let the channel $\{W_x\}$ be symmetric with respect to μ according to Definition 1. Then,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - F_\bullet(t,\mu) + t\bigl(G_\bullet(t,\mu) - |\mathcal{C}|^{-1}\bigr), \quad (18)$$

where $|\mathcal{C}|$ denotes the cardinality of the code $\mathcal{C}$.

Proof: Let the decoder $\mathcal{P} = \{\Pi_1, \dots, \Pi_M\}$ satisfy

$$\Pi_m = \mathcal{E}^{\bullet}_{x_m}(t,\mu) + \Pi_m \mathcal{E}^{\circ}_{x_m}(t,\mu), \quad m = 1, \dots, M, \tag{19}$$

where $\mathcal{E}^{\circ}_x(t,\mu) \triangleq \bigl\{W_x - t\mu = 0\bigr\}$. We next show that this decoder satisfies the Holevo-Yuen-Kennedy-Lax conditions from Lemma 1 and therefore it minimizes (2). To this end, we define an orthogonal basis $\{E_i\}$ such that

$$\mathcal{E}^{\bullet}_x(t,\mu) = \sum_{i \in \mathcal{I}(x)} E_i, \quad \text{for all } x \in \mathcal{C}. \tag{20}$$

Here, $\mathcal{I}(x)$ denotes the set of basis indexes belonging to the decoding region of the codeword $x \in \mathcal{C}$. This decomposition is guaranteed to exist since $\mathcal{C}$ being perfect or quasi-perfect implies that the projectors $\bigl\{\mathcal{E}^{\bullet}_x(t,\mu)\bigr\}_{x\in\mathcal{C}}$ are orthogonal to each other (see Definition 2). We also define the set

$$\mathcal{I}_0 \triangleq \Bigl\{ i \,|\, i \notin \bigcup\nolimits_{x\in\mathcal{C}} \mathcal{I}(x) \Bigr\} \tag{21}$$

of indexes not assigned to any codeword. The basis $\{E_i\}$ jointly diagonalizes the projectors $\bigl\{\mathcal{E}^{\bullet}_x(t,\mu)\bigr\}_{x\in\mathcal{C}}$. Indeed,

$$\begin{aligned}\Lambda(\mathcal{P}) &= \frac{1}{M}\sum_{\ell=1}^{M} W_\ell \Pi_\ell &(22)\\ &= \frac{1}{M}\sum_{\ell=1}^{M} W_\ell \left(\mathcal{E}^{\bullet}_{x_\ell}(t,\mu) + \Pi_\ell \mathcal{E}^{\circ}_{x_\ell}(t,\mu)\right) &(23)\\ &= \frac{1}{M}\sum_{\ell=1}^{M} \sum_{i\in\mathcal{I}(x_\ell)} W_\ell E_i + \frac{t}{M}\mu \sum_{i\in\mathcal{I}_0} E_i, &(24)\end{aligned}$$

where (24) follows from (20) and (21), since the indicator of the subspace $\mathcal{E}^{\circ}_{x_m}(t,\mu) = \bigl\{W_m - t\mu = 0\bigr\}$ implies that $W_m \mathcal{E}^{\circ}_{x_m}(t,\mu) = t\mu \mathcal{E}^{\circ}_{x_m}(t,\mu)$. Therefore, using (24), yields

$$\begin{aligned}&\left(\Lambda(\mathcal{P}) - \frac{1}{M}W_m\right)\Pi_m\\ &= \frac{1}{M}\sum_{\ell=1}^{M} \sum_{i\in\mathcal{I}(x_\ell)} W_\ell E_i \Pi_m + \frac{t\mu}{M}\sum_{i\in\mathcal{I}_0} E_i\Pi_m - \frac{1}{M}W_m\Pi_m &(25)\\ &= \frac{1}{M}\sum_{i\in\mathcal{I}(x_m)} W_m E_i + \frac{t\mu}{M}\sum_{i\in\mathcal{I}_0} E_i \Pi_m\\ &\quad - \frac{1}{M}\sum_{i\in\mathcal{I}(x_m)} W_m E_i - \frac{t}{M}\mu\sum_{i\in\mathcal{I}_0} E_i\Pi_m = 0, &(26)\end{aligned}$$

where in (26) we used (19), $E_i \Pi_m = 0$ for any $i \in \mathcal{I}(x_\ell)$, $\ell \neq m$, and the fact that $\mathcal{E}^{\circ}_{x_m}(t,\mu) = \bigl\{W_{x_m} - t\mu = 0\bigr\}$ implies $W_m \mathcal{E}^{\circ}_{x_m}(t,\mu) = t\mu\mathcal{E}^{\circ}_{x_m}(t,\mu)$. Following analogous steps we show that $\Pi_m\left(\Lambda(\mathcal{P}^\star) - \frac{1}{M}W_m\right) = 0$ and hence we conclude that (3) is satisfied.

On the other hand, using (24), since $\sum_i E_i = \mathbb{1}$, we obtain

$$\begin{aligned}&\Lambda(\mathcal{P}^\star) - \frac{1}{M}W_m\\ &= \frac{1}{M}\sum_{\ell\neq m}\sum_{i\in\mathcal{I}(x_\ell)} W_\ell E_i + \frac{t}{M}\mu\sum_{i\in\mathcal{I}_0} E_i - \frac{1}{M}\sum_{i\notin\mathcal{I}(x_m)} W_m E_i. &(27)\end{aligned}$$

For $i \in \mathcal{I}(x_\ell)$, using the definition of the projector $\mathcal{E}^{\bullet}_x(t,\mu)$, we have that $W_\ell E_i > t\mu E_i$ according to (20). Similarly, for $i \notin \mathcal{I}(x_m)$, it follows that $W_m E_i \leq t\mu E_i$. Then, from (27), we conclude that $\Lambda(\mathcal{P}^\star) - \frac{1}{M}W_m$ is lower bounded by

$$\frac{1}{M}\sum_{\ell\neq m}\sum_{i\in\mathcal{I}(x_\ell)} t\mu E_i + \frac{t}{M}\mu\sum_{i\in\mathcal{I}_0} E_i - \frac{1}{M}\sum_{i\notin\mathcal{I}(x_m)} t\mu E_i = 0, \tag{28}$$

and therefore (4) holds.

As the decoder $\mathcal{P} = \{\Pi_1, \dots, \Pi_M\}$ satisfies the conditions from Lemma 1, it minimizes (2). Using (2) and (5), we obtain

$$\begin{aligned}\mathsf{P}_{\mathrm{e}}(\mathcal{C}) &= 1 - \mathrm{Tr}\bigl(\Lambda(\mathcal{P}^\star)\bigr) &(29)\\ &= 1 - \frac{1}{M}\sum_{m=1}^{M} F^{\bullet}_{x_m}(t,\mu) - \frac{t}{M}\sum_{i\in\mathcal{I}_0}\mathrm{Tr}\bigl(\mu E_i\bigr), &(30)\end{aligned}$$

where in the second step we used (24), (20) and (16). We now combine $\sum_i \mathrm{Tr}\bigl(\mu E_i\bigr) = 1$, (17) and (21) to obtain

$$\sum_{i\in\mathcal{I}_0}\mathrm{Tr}\bigl(\mu E_i\bigr) + \sum_{m=1}^{M} G^{\bullet}_{x_m}(t,\mu) = 1. \tag{31}$$

Multiplying both sides by $1/M$, noting that for a symmetric channel $G_\bullet(t,\mu) = G^{\bullet}_x(t,\mu)$ does not depend on x, it yields

$$\frac{1}{M}\sum_{i\in\mathcal{I}_0}\mathrm{Tr}\bigl(\mu E_i\bigr) = \frac{1}{M} - G_\bullet(t,\mu). \tag{32}$$

Then, substituting (32) in (30), and using $F_\bullet(t,\mu) = F^{\bullet}_x(t,\mu)$ and $M = |\mathcal{C}|$, we obtain the desired result. ■

We next show that perfect and quasi-perfect codes attain the meta-converse (10) with equality. This result is based on the following auxiliary lemmas.

Lemma 3: For any binary hypothesis test discriminating between the quantum states ρ_0 and ρ_1, it follows that

$$\begin{aligned}\alpha_\beta(\rho_0\|\rho_1) = \sup_{t'\geq 0}\Bigl\{&\mathrm{Tr}\bigl(\rho_0\{\rho_0 - t'\rho_1 \leq 0\}\bigr)\\ &+ t'\bigl(\mathrm{Tr}\bigl(\rho_1\{\rho_0 - t'\rho_1 > 0\}\bigr) - \beta\bigr)\Bigr\}. &(33)\end{aligned}$$

Proof: The proof follows closely that of [6, Lem. 2]. ■

Lemma 4: Let $\rho_0 = PW$ and $\rho_1 = P\otimes\mu$ be defined in (8) and (9), respectively. Then, the optimal trade-off (6) satisfies

$$\alpha_\beta\bigl(PW \,\|\, P\otimes\mu\bigr) = \inf_{\substack{\{\beta_x\}:\\ \beta=\sum_x P(x)\beta_x}} \sum_{x\in\mathcal{X}} P(x)\alpha_{\beta_x}\bigl(W_x \,\|\, \mu\bigr). \tag{34}$$

Proof: The proof is an extension of that of [12, Lem. 25] to the classical-quantum setting. ■

Lemma 3 provides an alternative characterization of the optimal trade-off (6). Lemma 4 asserts that, for a binary hypothesis test between classical-quantum distributions, it is possible to express the optimal type-I error as a convex combination of that of disjoint sub-tests provided that the type-II error is optimally distributed among them. Combining Theorem 2 and Lemmas 3 and 4 we next show that perfect and quasi-perfect codes attain the meta-converse with equality.

Theorem 3 (Quasi-perfect codes attain the meta-converse): Let $\mathcal{C}$ be quasi-perfect with parameters t, μ, and let the channel W_x be symmetric with respect to μ. Then, for $M = |\mathcal{C}|$,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = \inf_{P} \sup_{\mu'} \alpha_{\frac{1}{M}}\bigl(PW \,\|\, P \otimes \mu'\bigr) \tag{35}$$

$$= \alpha_{\frac{1}{M}}\bigl(W_x \,\|\, \mu\bigr). \tag{36}$$

Proof: According to Theorem 1, the right-hand side of (35) is a lower bound to the error probability of any code. Then, to prove (35), it suffices to show that the error probability of $\mathcal{C}$ coincides with this lower bound. Using Theorem 1 and Lemma 4, fixing the auxiliary state μ to that from Definition 2, we obtain

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) \geq \inf_{\substack{\{P(x),\beta_x\}:\\ \sum_x P(x)\beta_x = \frac{1}{M}}} \sum_{x\in\mathcal{X}} P(x)\alpha_{\beta_x}\bigl(W_x \,\|\, \mu\bigr). \tag{37}$$

Now, according to Lemma 3, letting $t' = t$, and using the definitions of $F_x^{\bullet}(t,\mu)$ and $G_x^{\bullet}(t,\mu)$, it follows that

$$\alpha_{\beta_x}\bigl(W_x \,\|\, \mu\bigr) \geq 1 - F_x^{\bullet}(t,\mu) + t\bigl(G_x^{\bullet}(t,\mu) - \beta_x\bigr) \tag{38}$$

$$= 1 - F_{\bullet}(t,\mu) + t\bigl(G_{\bullet}(t,\mu) - \beta_x\bigr), \tag{39}$$

where in the last step we used that for symmetric channels with respect to μ, $F_{\bullet}(t,\mu) = F_x^{\bullet}(t,\mu)$ and $G_{\bullet}(t,\mu) = G_x^{\bullet}(t,\mu)$.

Then, using (39) in (37), we obtain

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) \geq \inf_{\substack{\{P(x),\beta_x\}:\\ \sum_x P(x)\beta_x = \frac{1}{M}}} \Bigl(1 - F_{\bullet}(t,\mu) + t\Bigl(G_{\bullet}(t,\mu) - \textstyle\sum_x P(x)\beta_x\Bigr)\Bigr) \tag{40}$$

which, upon using the constraint $\sum_x P(x)\beta_x = \frac{1}{M}$ coincides with the error probability of the quasi-perfect codes (18) given in Theorem 2. We conclude that the meta-converse bound (35) is tight for quasi-perfect codes. Moreover, since (18) coincides with the lower bound (39) when $\beta_x = \frac{1}{M}$, then (36) follows. ■

IV. 2-Qubit Classical-Quantum Channels and Bell Codes

We consider a 2-qubit pure-state channel with output

$$|\varphi_x\rangle \equiv \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,, \tag{41}$$

for an input $x = (\alpha,\beta,\gamma,\delta) \in \mathbb{C}^4$ such that $\alpha,\beta,\gamma,\delta$ satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

We define the codebook $\mathcal{C} = \{x_1,\ldots,x_M\}$, $M = 2P \geq 4$, such that the channel output is given by

$$|\varphi_{x_m}\rangle = \begin{cases} \frac{1}{\sqrt{2}}\bigl(|00\rangle + e^{j\phi_p}\,|11\rangle\bigr), & m = 2p-1,\\ \frac{1}{\sqrt{2}}\bigl(|01\rangle + e^{j\phi_p}\,|10\rangle\bigr), & m = 2p, \end{cases} \tag{42}$$

where $\phi_p = 2\pi(p-1)/P$, and $p = 1,\ldots,P$.

We refer to this family of codes as *Bell codes*, since they follow from a generalization of the Bell states [13].

A. Pure 2-qubit classical-quantum channel

Bell codes are quasi-perfect for the ideal pure 2-qubit classical-quantum channel $W_x = |\varphi_x\rangle\langle\varphi_x|$, as shown next.

Proposition 1: Let $\mu_0 = \frac{1}{4}\mathbb{1}_4$. Then, the 2-quit classical-quantum channel $W_x = |\varphi_x\rangle\langle\varphi_x|$ is symmetric with respect to μ_0 and the Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = \alpha_{\frac{1}{M}}\bigl(W_x \,\|\, \mu_0\bigr) = 1 - \frac{4}{M}. \tag{43}$$

Proof: Let ρ_B be the density matrix observed by the decoder. For $M \geq 4$ it follows that

$$\rho_B = \frac{1}{M}\sum_{m=1}^{M} W_m = \frac{1}{M}\sum_{m=1}^{M} |\varphi_m\rangle\langle\varphi_m| = \frac{1}{4}\mathbb{1}_4. \tag{44}$$

We consider the decoder $\mathcal{P} = \{\Pi_1,\ldots,\Pi_M\}$ where

$$\Pi_i = \frac{1}{M}\rho_B^{-\frac{1}{2}} W_i \rho_B^{-\frac{1}{2}} = \frac{4}{M}W_i. \tag{45}$$

1) Decoder optimality: One can check that $\Pi_m \geq 0$ and that $\sum_{m=1}^{M}\Pi_m = \mathbb{1}_4$. Moreover,

$$\Lambda(\mathcal{P}) \triangleq \frac{1}{M}\sum_{m=1}^{M} W_m\Pi_m = \frac{4}{M^2}\sum_{m=1}^{M} W_m W_m = \frac{1}{M}\mathbb{1}_4. \tag{46}$$

We next show that this decoder satisfies the conditions from Lemma 1. First, we note that

$$\Lambda(\mathcal{P})\Pi_m = \frac{4}{M^2}W_m, \tag{47}$$

which upon substitution in (3) shows that this condition holds. The condition (4) is satisfied since, for an arbitrary unit norm vector $|\psi\rangle$,

$$\frac{\langle\psi|\,\Lambda(\mathcal{P})\,|\psi\rangle}{\frac{1}{M}\langle\psi|\,W_m\,|\psi\rangle} = \frac{\langle\psi|\psi\rangle}{|\,\langle\psi|\varphi_{x_m}\rangle\,|^2} \geq \frac{1}{\langle\varphi_{x_m}|\varphi_{x_m}\rangle} = 1, \tag{48}$$

where the second step follows from the Cauchy-Schwarz inequality. As (48) implies $\langle\psi|\,(\Lambda(\mathcal{P}) - \frac{1}{M}W_m)\,|\psi\rangle \geq 0$ for an arbitrary $|\psi\rangle$, then (4) follows. We conclude that $\mathcal{P} = \{\Pi_1,\ldots,\Pi_M\}$ minimizes the error probability for $\mathcal{C}$.

2) Symmetry of the channel with respect to μ_0: We need to prove that $F_x(t,\mu_0) = \langle\varphi_x|\,\mathcal{E}_x(t,\mu_0)\,|\varphi_x\rangle$ is independent of x. We recall the definition of $\mathcal{E}_x(t,\mu_0)$ from (11),

$$\mathcal{E}_x(t,\mu_0) = \bigl\{|\varphi_x\rangle\langle\varphi_x| - t\mu_0 \geq 0\bigr\}, \tag{49}$$

and we shall prove that

$$\mathcal{E}_x(t,\mu_0) = \begin{cases} \mathbb{1}_4, & t < 0,\\ |\varphi_x\rangle\langle\varphi_x|\,, & 0 \leq t \leq t_0,\\ 0, & t > t_0, \end{cases} \tag{50}$$

for some $t_0 \geq 0$ independent of x. Then, using (50), we obtain

$$F_x(t,\mu_0) = \langle\varphi_x|\,\mathcal{E}_x(t,\mu_0)\,|\varphi_x\rangle = \begin{cases} 1, & t \leq t_0\\ 0, & t > t_0. \end{cases} \tag{51}$$

Since $F_x(t,\mu_0) = F(t,\mu_0)$ does not depend on x, we conclude that the channel is symmetric with respect to μ_0.

It remains to show that (50) holds. The identity for $t < 0$ follows trivially since both $|\varphi_x\rangle\langle\varphi_x| \geq 0$ and $\mu_0 \geq 0$. For $t \geq 0$, we obtain the eigenvector associated to the largest eigenvalue of $|\varphi_x\rangle\langle\varphi_x| - t\mu_0$. To this end, we consider an arbitrary unit-norm vector $|v\rangle$. The largest eigenvalue of $|\varphi_x\rangle\langle\varphi_x| - t\mu_0$ is given by

$$\max_v \langle v| \big(|\varphi_x\rangle\langle\varphi_x| - t\mu_0 \big) |v\rangle = \max_v \Big\{ \langle v|\varphi_x\rangle^2 - \frac{t}{4}\langle v|v\rangle \Big\} = 1 - \frac{t}{4} \tag{52}$$

where we used that $\langle v|\varphi_x\rangle^2$ is maximized over v for $v = \varphi_x$. The eigenvalue (52) is negative for $t > t_0 = 4$ and non-negative otherwise. Then, we obtain that $F_x(t, \mu_0) = 0$, for $t > 4$. For $0 \leq t \leq 4$, it can be shown that (52) is the only non-negative eigenvalue, and so we obtain (50).

3) $\mathcal{C}$ is quasi-perfect with respect to μ_0: Comparing (46) with μ_0 defined in the statement of Proposition 1, it follows that

$$\mu_0 = \frac{1}{c_0}\Lambda(\mathcal{P}) = \frac{1}{Mc_0}\sum_{m=1}^{M} W_m \Pi_m, \tag{53}$$

where $c_0 = \frac{4}{M}$ is a normalizing constant and where $\mathcal{P}$ satisfies the optimality conditions. For $t = Mc_0 = 4$, from the previous equation we conclude that $\frac{1}{M}W_m - \Lambda(\mathcal{P}) = \frac{1}{M}W_m - \frac{t}{M}\mu_0$ is negative semidefine. Hence, $\mathcal{E}_{x_m}(t,\mu_0) \triangleq \big\{W_m - t\mu_0 \geq 0\big\} = \big\{W_m - t\mu_0 = 0\big\} = \mathcal{E}^{\circ}_{x_m}(t,\mu_0)$ is the null eigenspace of $\frac{1}{M}W_m - \Lambda(\mathcal{P})$. This also implies that $\mathcal{E}^{\bullet}_{x_m}(t,\mu_0) = 0$, hence $\big\{\mathcal{E}^{\bullet}_x(t,\mu)\big\}_{x\in\mathcal{C}}$ are orthogonal to each other.

For this choice of t and μ_0, $\Lambda(\mathcal{P}) - \frac{1}{M}W_m = 0$, which corresponds to the fulfillment of (48) with equality. This implies $|\psi\rangle = |\varphi_{x_i}\rangle$ and $\mathcal{E}_{x_m}(t,\mu_0) = |\varphi_{x_m}\rangle\langle\varphi_{x_m}|$. Then, we conclude that $\sum_{x\in\mathcal{C}} \mathcal{E}_x(t,\mu) = \frac{M}{4}\mathbb{1}_4 \geq \mathbb{1}_4$.

4) Error probability: From Theorem 3 we conclude that $\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big)$. Moreover, using the optimal decoder $\mathcal{P}$, we obtain $\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - \frac{1}{M}\sum_{i=1}^{M}\mathrm{Tr}\big(W_i\Pi_i\big) = 1 - \frac{4}{M}$, where in the last step we used (46). ■

B. Classical-quantum erasure channel

We consider the classical-quantum channel (41) observed after a quantum erasure channel, defined as

$$\mathcal{N}^{E}_{A\to B}(\rho_A) = (1-\epsilon)\mathcal{I}_{A\to B}(\rho_A) + \epsilon|e\rangle\langle e|_B.$$

where the Isometric channel $\mathcal{I}_{A\to B}(\rho_A) = I_{A\to B}\rho_A I^{\dagger}_{A\to B}$ is defined using the isometry

$$I_{A\to B} = \begin{bmatrix} & \mathbb{1}_4 & \\ 0 & \dots & 0 \end{bmatrix} \tag{54}$$

as unique Kraus operator and since $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle, |e\rangle\}$ form an orthonormal basis in $\mathcal{H}_B$. The combined classical-quantum channel is then $W_x = \mathcal{N}^{E}_{A\to B}\big(|\varphi_x\rangle\langle\varphi_x|_A\big)$.

The Bell codes defined in (42) with channel output $W_m = \mathcal{N}^{E}_{A\to B}\big(|\varphi_{x_m}\rangle\langle\varphi_{x_m}|_A\big)$, $m = 1, \dots, M$, are quasi-perfect for the classical-quantum erasure channel.

Proposition 2: Let

$$\mu_0 = \frac{1}{4-3\epsilon}\begin{bmatrix} & & & 0 \\ & (1-\epsilon)\mathbb{1}_4 & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & \epsilon \end{bmatrix}. \tag{55}$$

Then, the 2-quit classical-quantum erasure channel is symmetric with respect to μ_0 and the Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{1}{M}(4 - 3\epsilon). \tag{56}$$

Proof: The proof follows the lines of that of Proposition 1 and it is omitted due to space constraints. ■

C. Classical-quantum depolarizing channel

Consider the 2-qubit classical-quantum channel in (41) observed after a quantum depolarizing channel, defined as

$$\mathcal{N}^{D}_{A\to B}(\rho_A) = p\frac{1}{4}\mathbb{1}_4 + (1-p)\rho_A,$$

The combined classical-quantum channel is thus $W_x = \mathcal{N}^{D}_{A\to B}\big(|\varphi_x\rangle\langle\varphi_x|_A\big)$. Using the Bell code defined in (42), the channel output is given by $W_m = \mathcal{N}^{D}_{A\to B}\big(|\varphi_{x_m}\rangle\langle\varphi_{x_m}|_A\big)$, $m = 1, \dots, M$.

Proposition 3: Let $\mu_0 = \frac{1}{4}\mathbb{1}_4$. Then, the 2-qubit classical-quantum depolarizing channel is symmetric with respect to μ_0 and the Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{1}{M}(4 - 3p). \tag{57}$$

Proof: The proof follows the lines of that of Proposition 1 and it is omitted due to space constraints. ■

V. Discussion

We introduced the notion of perfect and quasi-perfect codes for symmetric classical-quantum channels. Theorem 2 provides an expression of the error probability of these codes, which is then used in Theorem 3 to prove that quasi-perfect codes achieve the converse bound [4, Eq. (46)]. These codes, whenever they exist, are thus optimal in the sense that they achieve the smallest error probability among all codes of the same blocklength and cardinality.

Using the framework presented, we established that a family of codes based on a generalization of Bell states, that we name Bell codes, are quasi-perfect for the pure 2-qubit classical-quantum channel. Indeed, this is true even for a pure 2-qubit classical-quantum channel affected by quantum erasures or by depolarization. For these channels, we have thus established the error probability and structure of the best coding scheme.

Establishing the existence of generalized perfect and quasi-perfect codes given certain system parameters is a difficult problem, even for simple classical channels. For instance, [14] studies their existence for the BSC channel and [15] shows that MDS codes, which are generalized quasi-perfect for the q-ary erasure channel [2, Sec. IV], only exist for blocklengths $n \leq q+1$. Proving the existence of these codes for classical-quantum channels of practical interest is an unexplored line of research.

References

[1] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, Inc., 1968.

[2] G. Vazquez-Vilar, A. Guillén i Fàbregas, and S. Verdú, "The error probability of generalized perfect codes via the meta-converse," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5705–5717, Sep. 2019.

[3] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[4] W. Matthews and S. Wehner, "Finite blocklength converse bounds for quantum channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7317–7329, 2014.

[5] M. Hayashi, *Quantum Information: An Introduction*. Springer, 2006.

[6] G. Vazquez-Vilar, "Multiple quantum hypothesis testing expressions and classical-quantum channel converse bounds," in *2016 IEEE Int. Symp. on Inf. Theory*, Barcelona, Spain, July 2016.

[7] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "A demonstration of superadditivity in the classical capacity of a quantum channel," *Phys. Lett. A*, 1997.

[8] ——, "Quantum channels showing superadditivity in classical capacity," *Phys. Rev. A*, vol. 58, pp. 146–158, Jul 1998.

[9] A. S. Holevo, "Statistical decision theory for quantum systems," *J. Multivariate Anal. 3*, vol. 3, no. 4, pp. 337–394, 1973.

[10] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 125–134, Mar 1975.

[11] A. Jenčová, "Quantum hypothesis testing and sufficient subalgebras," *Lett. Math. Phys.*, vol. 93, no. 1, pp. 15–27, 2010.

[12] Y. Polyanskiy, "Saddle point in the minimax converse for channel coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2576–2595, May 2013.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[14] T. Etzion and B. Mounits, "Quasi-perfect codes with small distance," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3938–3946, Nov 2005.

[15] G. Seroussi and R. M. Roth, "On MDS extensions of generalized Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 32, no. 3, pp. 349–354, May 1986.