Coversheet

How to cite this publication:

Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz (2017). "Coherent-state constellations and polar codes for thermal Gaussian channels." PHYSICAL REVIEW A, 95, 062343.
https://doi.org/10.1103/PhysRevA.95.062343

Publication metadata

Coherent-state constellations and polar codes for thermal Gaussian channels

Felipe Lacerda,[1,2] Joseph M. Renes,[2] and Volkher B. Scholz[2,3]

[1]*Department of Computer Science, Aarhus University, 8200 Aarhus N, Denmark*
[2]*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*
[3]*Department of Physics, Ghent University, 9000 Gent, Belgium*

Optical communication channels are ultimately quantum mechanical in nature, and we must therefore look beyond classical information theory to determine their communication capacity as well as to find efficient encoding and decoding schemes of the highest rates. Thermal channels, which arise from linear coupling of the field to a thermal environment, are of particular practical relevance; their classical capacity has been recently established, but their quantum capacity remains unknown. While the capacity sets the ultimate limit on reliable communication rates, it does not promise that such rates are achievable by practical means. Here we construct efficiently encodable codes for thermal channels which achieve the classical capacity and the so-called Gaussian coherent information for transmission of classical and quantum information, respectively. Our codes are based on combining polar codes with a discretization of the channel input into a finite "constellation" of coherent states. Encoding of classical information can be done using linear optics.

I. INTRODUCTION

Optical communication channels such as glass fibers are the workhorses of state-of-the-art communication networks, and they are also of particular importance in quantum communication theory. First, in our quest to squeeze ever more data through existing communication infrastructure, we are gradually reaching the realm of quantum effects and hence need to consider their influence on data transmission. Second, optical channels are the most promising candidate to establish quantum links between distant locations and possibly a quantum internet. Hence developing communication schemes for such noisy quantum channels is of central importance in quantum information.

The quantum effects of noise in such electromagnetic systems are well modeled by linear coupling of the field modes to additional Bosonic fields by quadratic Hamiltonians. This leads to the class of Gaussian channels, the action of which can be described by linear operations in phase space [1,2]. Mixing of a single mode with thermal noise is a particularly relevant Gaussian channel, called the thermal channel. The ultimate capacity for transmitting classical information over thermal channels, and indeed any phase-insensitive channel, has been recently established in [3]. Less is rigorously established about their quantum capacity, but it is widely believed to be given by the regularized coherent information [2]. Restricting attention to Gaussian inputs, the most practically relevant case of states defined by their first and second moments, [1] showed that thermal states with ever larger mean photon number optimize the coherent information. For degradable channels, e.g., pure loss channels in which the thermal noise of the channel is at zero temperature, Gaussian inputs to the coherent information are in fact optimal, that is, they maximize the coherent information [4].

While capacity is an important property, it does not address the practical limitations of high-rate communication, such as the efficiency of encoding and decoding operations, or their implementability using linear optics. In this paper we construct explicit codes that achieve the classical capacity as well as (likewise explicit) quantum codes that achieve the Gaussian coherent information of thermal channels. On the way to the latter, we construct codes for private information transmission that also achieve the coherent information. All codes have efficient encoding operations and explicit decoders, though their decoding efficiency is unknown. In the case of transmitting classical information, private or not, the encoding operations require only the generation of coherent states. Superpositions of coherent states are used for transmission of quantum information.

Our code constructions are based on *discretizing* the optimal channel input to a finite "constellation," and then using a *polar code* on the induced channel. Both are concepts originating in classical information theory. Finite constellations of input signals have always been used for continuous-input classical channels, e.g., the additive white Gaussian noise channel (AWGN), and several particular constellations are known to achieve the AWGN capacity (see [5]). Meanwhile, polar codes are a recent breakthrough, the first explicitly constructed codes with efficient encoding and decoding that achieve the classical capacity of discrete-input channels [6]. Polar coding was adapted for classical communication over finite-dimensional quantum channels by Wilde and Guha [7] and for quantum communication by one of the authors [8].

We construct constellations for the thermal channel from AWGN constellations. The thermal input state can be viewed as a Gaussian-weighted mixture of coherent states, i.e., its Glauber-Sudarshan *P* function is a two-dimensional Gaussian. The optimal AWGN input is a one-dimensional Gaussian distribution, and we can therefore use AWGN constellations for the real and imaginary parts to give a finite constellation of coherent states. The difficulty is to show that the constellation achieves essentially the same rate as does the thermal input. After all, the discretized input only resembles the ideal Gaussian input in a very weak sense (specifically, in their lower-order moments), and it is not immediate that these limited similarities are enough to ensure similar rates. Luckily, Wu and Verdú [5] have recently established precisely this result for the AWGN, and we adapt this to the quantum case. Not having to very strictly emulate the optimal input state frees us considerably in designing coding protocols and should have

application to other settings, such as two-way protocols or quantum repeaters.

II. THERMAL CHANNELS

We consider single-mode thermal-noise channels [3], denoted $\mathcal{E}_{k,N_0}$, which describes an input mode interacting with a thermal state with mean photon number N_0 at a beamsplitter of transmittivity $k < 1$. The channel action can be described by the following transformation of the annihilation operators a and b of the input (signal) and auxiliary (ancilla) modes, respectively:

$$a \to a' = ka + \sqrt{1 - k^2}\,b, \tag{1a}$$

$$b \to b' = kb - \sqrt{1 - k^2}\,a, \tag{1b}$$

where the ancilla mode is initially in the thermal state with mean photon number N_0. Equivalently, defining $N_c = (1 - k^2)N_0$, $\mathcal{E}_{k,N_0}$ describes the composition of an attenuation channel ($N_0 = 0$ in $\mathcal{E}_{k,N_0}$) with coefficient $0 \leqslant k \leqslant 1$ and a channel adding Gaussian-distributed noise to each quadrature with identical variance $\sqrt{N_c}$ [9]. Indeed the case $k = 1$ requires the latter formulation; see [[9], Sec. IV].

For a fixed maximum input mean photon number N, the classical capacity $C(N)$ of the thermal-noise channel has been shown [3] to be the Holevo information of the channel, evaluated for a Gaussian ensemble of mean photon number N of coherent states.

More precisely, we have the following. Let Z be a random variable over $\mathbb{C}$ with probability density $P_Z(z) = \psi_N(z)$ for

$$\psi_N(z) := (\pi N)^{-1} \exp(-|z|^2/N), \tag{2}$$

$|z\rangle$ the coherent state centered at $z \in \mathbb{C}$, and $\theta_z^B = \mathcal{E}_{k,N_0}^{A \to B}(|z\rangle\langle z|^A)$. Here A denotes the input mode and B the output mode. We denote by E the output ancilla mode, so that the joint output produced by the channel is the bipartite state θ_z^{BE}. The capacity can then be expressed as [3]

$$C(N) = I(Z : B)_\rho, \tag{3}$$

where ρ^{ZB} is the classical-quantum state corresponding to the ensemble $\{P_Z(z), \theta_z^B\}_{z \in \mathbb{C}}$, and $I(Z : B)_\rho$ is defined as

$$I(Z : B)_\rho = H(\rho^B) - \int_{\mathbb{C}} dz\, P_Z(z) H(\theta_z^B), \tag{4}$$

with $\rho^B = \int_{\mathbb{C}} dz\, P_Z(z) \theta_z^B$. Here $H(\rho)$ is the von Neumann entropy, $H(\rho) = -\operatorname{Tr}[\rho \ln \rho]$, and we use the natural logarithm throughout. The marginal state of the input is then just the thermal state τ_N having average photon number N: $\int_{\mathbb{C}} dz\, P_Z(z)|z\rangle\langle z| = \tau_N$, with

$$\tau_N := \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1}\right)^n |n\rangle\langle n|, \tag{5}$$

where $\{|n\rangle\}_{n=0}^{\infty}$ is the number basis. Observe that P_Z is the P function of the input state τ_N, while for given z the above description of the channel implies that the P function of the output θ_z^B in B is simply $P_{\theta_z^B}(w) = \psi_{N_c}(w - kz)$. Similarly, the output θ_z^E in the auxiliary mode has P function $P_{\theta_z^E}(w) = \psi_{k^2 N_0}(w + \sqrt{1 - k^2}\,z)$.

In establishing the formula for the classical capacity, [3] relies on random coding arguments. For the pure loss case ($N_0 = 0$), Guha and Wilde constructed polar codes for a constellation of two coherent states (binary phase-shift keying) [10] the optimal rate of which approaches the capacity in the limit of vanishing input mean photon number.

Compared to the case of classical data transmission, less is known about the best rate to transmit *quantum data*, which is set by the *quantum* capacity of the thermal noise channel (we refer the reader to the book [11] for the precise definitions and an introduction into these concepts). This is related to the fact that we currently do only have a limited understanding of quantum coding in the infinite-dimensional setting, especially when taking physical limitations such as precision restrictions into account. For example, Devetak's proof [12] that the coherent information and its regularization are achievable rates of quantum communication does not deal with infinite-dimensional channels. Although it seems straightforward to extend his method by suitably truncating the input and output spaces (as carried out for entanglement distillation in [[13], Appendix I]), this proof technique would lead to random codes involving superpositions of products of number states. These encodings are arguably very hard to realize experimentally.

It is thus interesting to determine possible rates of noiseless communication if we restrict to *Gaussian* encodings. Adding another simplification, namely, disregarding the fact that the coherent information needs to be regularized in order to give the ultimate quantum capacity of a channel, leads to single-letter Gaussian quantum capacity $Q_G^{(1)}$. This quantity is given by maximizing the coherent information over Gaussian input states,

$$Q_G^{(1)} = \max_\rho H(B)_\omega - H(E)_\omega, \tag{6}$$

where $\omega^{ABE} = V_{\mathcal{E}_{k,N_0}}^{A' \to BR}(\xi^{AA'})$ for $\xi^{AA'}$ is a purification of the Gaussian state ρ^A at the channel input and V is a Stinespring dilation of the channel. In [1], Holevo and Werner showed that this optimization problem can be solved explicitly in the case of the thermal noise channel, and that the unique maximizer is the state τ_N for $N \to \infty$. The corresponding output is given by $\tau_{N'}$ where $N' = k^2 N + N_c$. They also showed that $Q_G^{(1)}$ remains finite in this limit, that is, in the limit of infinite energy. This is in sharp contrast to the classical case, where the capacity is infinite in the absence of an energy bound. The difference between the classical and the quantum case may be argued for by the fact that the quantum uncertainty principle prevents us from arbitrary dense packing of quantum information, but a satisfactory analytic understanding of this point is still missing. In addition, a finite-energy bound is of course also of practical interest, even in the quantum-mechanical case, due to implementation limitations.

Nevertheless, the quantity (6) is a lower bound on the quantum capacity, because it is restricted to Gaussian inputs which are moreover not entangled in the case of multiple channel uses. Hence, the construction of communication schemes which achieve this rate is a necessary first step for advancing our understanding of the limitations of quantum communication via the thermal noise channel. Moreover, in the case of
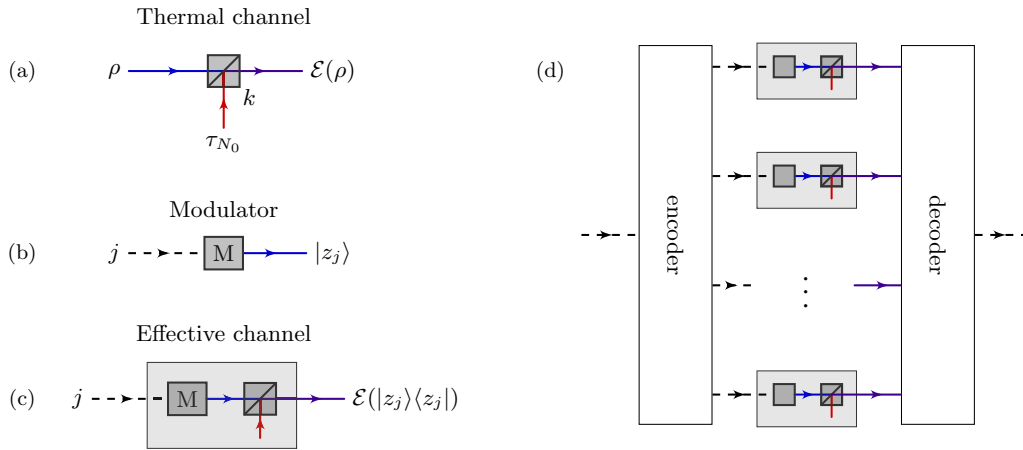
FIG. 1. (a) The thermal channel $\mathcal{E}$ mixes the input state ρ with the thermal state of mean photon number N_0 on a beamsplitter of transmittivity k. (b) The modulator taking classical input j to the jth coherent state $|z_j\rangle$ in the constellation. (c) The effective channel resulting from combining the modulator with the thermal channel. (d) The classical coding scheme using the effective channel. In the quantum scheme the encoder accepts a quantum state and the modulator must be able to output superpositions of constellation coherent states.

degradable channels such as pure loss, Wolf *et al.* have shown that Gaussian inputs are provably optimal among all inputs [4] (and moreover entangled inputs are not necessary [14]).

The first communication schemes which achieve the rate (6) were constructed by Harrington and Preskill for the case $k = 1$ in [15]. Their construction is not based on discretization, but rather embedding an appropriate number of qubits directly into the state space of a larger number of modes, using the method of [16]. The practicality of this method is, however, limited, even disregarding the nonexplicit nature of the code, as it ostensibly requires codewords which are superpositions of highly squeezed states.

Here, we construct new encoding schemes which are based on coherent states and are thus more feasible experimentally. As already explained in the introduction, our results are based on constellations, or discretizations of continuous input distributions.

III. NEW CODING SCHEMES

Any given constellation defines a mapping, or modulation, from a discrete set of m inputs (indexing the particular input state) to the coherent states in the constellation. Combining this mapping with the thermal channel then defines an "effective" discrete-input Bosonic-output channel, as depicted in Fig. 1.

The methods of polar coding can then be applied to this channel to yield a high-rate block code. As we show in the two subsequent sections, this results in classical codes with rates achieving the capacity $C(N)$ and quantum codes with rates achieving the Gaussian coherent information $Q_G^{(1)}$. The use of polar codes also ensures the encoding operation is efficient, though it is not known if efficient decoding is possible when the channel outputs noncommuting states.

In classical information theory, channel constellations are designed to emulate the optimizer of the channel mutual information, as this gives a means for showing that the overall coding scheme can approach the capacity. Here we take the same approach, and aim to emulate τ_N, the optimizer in both the Holevo information and coherent information.

As depicted in Fig. 2, several useful constellations are known for the AWGN. The equilattice is simply m equally spaced points with equal probability the variance of which matches that of the optimizer of the channel mutual information [17]. The quantile constellation chooses points based on the quantile (inverse of the cumulative distribution) [18], while the random walk is precisely the distribution of positions of a suitably rescaled random walk of length $(m - 1)$. Finally, the Gauss-Hermite constellation is based on Gauss-Hermite quadrature. This discretizes the Gaussian distribution to m points in $\mathbb{R}$ such that the first $2m - 1$ moments of the Gaussian
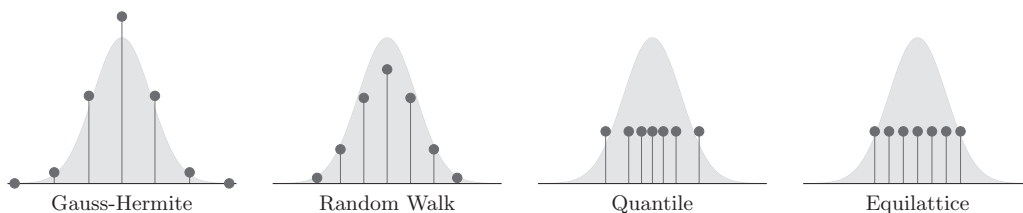

FIG. 2. Four constellations of $m = 7$ points which approximate a normally distributed random variable. The random-walk and equilattice constellations consist of equally spaced points, while the quantile and equilattice have equal probabilities. Gauss-Hermite quadrature has neither, but precisely reproduces the largest number of moments of the Gaussian distribution, the first $2m - 1$. The others have only the same mean and variance.
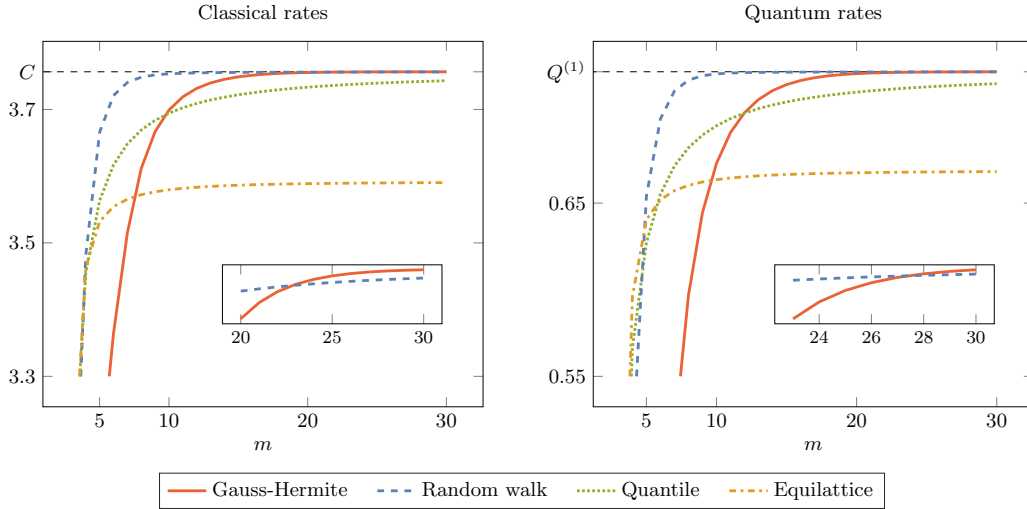
FIG. 3. Achievable rates for classical and quantum information transmission with increasing constellation size m, for the pure loss channel ($N_0 = 0$) with $k = 0.8$ and input state τ_N with $N = 7$. Although the Gauss-Hermite constellation (straight line) is optimal as $m \to \infty$, it is inferior for small m. For practical purposes, the random-walk constellation (dashed line) is best, rising very quickly to rates quite close to capacity.

are correctly reproduced. Indeed, Gauss-Hermite quadrature is optimal in that it reproduces the largest number of moments for fixed m. This constellation and the random walk were introduced in [5].

As noted in [5], the equilattice has a minimal gap to capacity of roughly 0.25 bits, while the gap closes in the $m \to \infty$ limit for the quantile, random walk, and Gauss-Hermite constellations. The latter closes exponentially in m in the asymptotic limit, but only polynomially in the other two cases. Nonetheless, the capacity of the random-walk constellation is already quite close to the optimal value even for modest m, while the Gauss-Hermite constellation only becomes optimal for larger m. We observe the same behavior for the thermal channel, as depicted in Fig. 3.

IV. COHERENT-STATE CONSTELLATIONS

For the thermal channel we can apply any of these constellations in phase space, to the P function of τ_N. As described above, this is a circularly symmetric complex Gaussian, and we use the AWGN constellations to mimic the real and imaginary parts separately. Specifically, the constellation is described by the distribution $Q_{N,m}(z)$, supported on m^2 points, such that

$$\frac{N}{2} Q_{N,m}\left[\sqrt{\frac{N}{2}}(x + iy)\right] = P_{X_m}(x)P_{X_m}(y), \qquad (7)$$

where P_{X_m} is one of the four constellations considered in [5]. In terms of random variables, $Z_m = \sqrt{\frac{N}{2}}(X_m + iX'_m)$, where X_m and X'_m are independent realizations of the given constellation. The factor $\sqrt{N}$ ensures that the resulting P function has variance N, while the $1/\sqrt{2}$ factor takes care of the conversion from two real variables to one complex variable.

Define the associated ensemble

$$\rho^{ZA}_{N,m} = \{Q_{N,m}(z), |z\rangle\langle z|\}_{z \in \mathbb{C}}. \qquad (8)$$

As for the classical Gaussian channel, for $m \geqslant 2$ the first two moments of $\rho^A_{N,m}$ match those of the thermal state τ_N.

Now we sketch how to upper bound the gap between the coherent information and the rate of the polar code applied to the induced discretized channel. A simpler version of the same argument yields the analogous result for the classical capacity.

Let us denote the target rate without using modulation as R, and the associated rate using the modulation with m points R_m. The former is the coherent information of the channel, while the latter is the same entropic expression, but evaluated for the input state given by the discretization scheme. The coherent information may be written as $R = I(Z : B) - I(Z : E)$ for P_Z as in Eq. (2), and R_m is the same expression, evaluated with $Z \sim Q_{N,m}$. Here E is the output of the channel to the environment. This follows because θ^{BE}_z, the state of BE given the input $Z = z$ (or $Z_m = z$), is pure and hence $H(B|Z) + B(E|Z) = 0$.

We would like to find an upper bound on $\Delta = R - R_m$, which can be written as $\Delta = \Delta_B - \Delta_E$ for $\Delta_B = I(Z : B) - I(Z_m : B_m)$ and similarly for Δ_E. Here, B_m is the channel output for the input Z_m. Clearly, we need not consider Δ_E for the problem of classical information transmission. These quantities can be written as relative entropies. More specifically, let ρ^{ZBE} and $\rho^{Z_m B_m E_m}_m$ be ensembles of the state θ^{BE}_z with distributions ψ_N as in Eq. (2) and $Q_{N,m}$ as in Eq. (7), respectively. Then

$$\Delta_B := I(Z : B) - I(Z_m : B_m) = D\left(\rho^{B_m}_m \big\| \rho^B\right), \qquad (9a)$$

$$\Delta_E := I(Z : E) - I(Z_m : E_m) = D\left(\rho^{E_m}_m \big\| \rho^E\right), \qquad (9b)$$

where the relative entropy is defined as $D(\rho\|\sigma) = \text{Tr}[\rho(\ln\rho - \ln\sigma)]$.

To see this, consider the claim for Δ_B; the following argument will also work for Δ_E. Expanding out the mutual information, we obtain $\Delta_B = H(B) - H(B|Z) - H(B_m) + H(B_m|Z_m)$. Since P functions of the output states θ^B_z are all identical up to translation, it follows that their entropies are also

identical, and therefore $H(B|Z) = H(B_m|Z_m)$. This leaves $\Delta_B = H(B) - H(B_m)$. Using the form of the relative entropy, it is apparent that the claim is equivalent to the statement $\mathrm{Tr}[\rho_m^{B_m} \ln \rho^B] = \mathrm{Tr}[\rho^B \ln \rho^B]$. Since the channel is Gaussian, ρ^B is a zero-mean Gaussian state, equivalent up to symplectic unitary conjugation to a tensor product of thermal states [1,2]. It follows that $\ln \rho^B$ is a second-order polynomial $q(r,r^\dagger)$ of the output creation and annihilation operators r and $r^\dagger$. We thus have

$$\mathrm{Tr}\left[\rho^B \ln \rho^B\right] = \mathrm{Tr}[\mathcal{E}_{k,N_0}^{A \to B}(\rho^A)q(r,r^\dagger)] \quad (10a)$$

$$= \mathrm{Tr}\left\{\rho^A \mathcal{E}_{k,N_0}^{A \to B\dagger}[q(r,r^\dagger)]\right\} \quad (10b)$$

$$= \mathrm{Tr}[\rho^A p(a,a^\dagger)], \quad (10c)$$

where $\mathcal{E}_{k,N_0}^\dagger$ is the channel adjoint and, since the channel is Gaussian, $p(a,a^\dagger)$ is a second-degree polynomial in the input creation and annihilation operators. Similarly, we have $\mathrm{Tr}[\rho_m^{B_m} \ln \rho^B] = \mathrm{Tr}[\rho_m^A p(a,a^\dagger)]$. Finally, since the first two moments of ρ_m^A match those of ρ^A, this also holds for the outputs ρ_m^B and ρ^B, and we indeed have $\mathrm{Tr}[\rho_m^{B_m} \ln \rho^B] = \mathrm{Tr}[\rho^B \ln \rho^B]$.

As the relative entropy is non-negative, we immediately have $\Delta_E \geqslant 0$, and we need only an upper bound for Δ_B. A convenient choice is the χ^2 distance, given by $\chi^2(\rho,\sigma) = \mathrm{Tr}[(\rho\sigma^{-1/2})^2] - 1$, since $D(\rho\|\sigma) \leqslant \chi^2(\rho,\sigma)$ [19,20].

In [5] Wu and Verdú obtain a bound on the χ^2 distance between the optimal output state and the discretized version for the case of the AWGN. They relate $\chi^2(P_{Y_m}, P_Y)$ directly to the moments of X_m, specifically the moments of the Hermite polynomials of X_m. (These all vanish for standard normal X, save the zeroth-order polynomial.) Indeed, they show the following slightly more general statement [[5], Sec. V.A]. First denote the AWGN with signal-to-noise ratio s by W_s; it has the action $W_s(X) = \sqrt{s}X + G$, where G is a normally distributed random variable with unit variance. Then for $X \sim \mathsf{N}(0,1)$, X' an arbitrary random variable with density $P_{X'}$, and $Y = W_s(X)$ and $Y' = W_s(X')$,

$$1 + \chi^2(P_{Y'}, P_Y) = \sum_{k=0}^{\infty} \frac{1}{k!}\left(\frac{s}{1+s}\right)^k |\mathbb{E}[H_k(X')]|^2. \quad (11)$$

We can use their result to bound $\chi^2(\rho_m^{B_m}, \rho^B)$. In particular, with $Q_{N,m}[\sqrt{\frac{N}{2}}(x+iy)]$ as in Eq. (7), $s = k^2 N/(\sqrt{N'(N'+1)} - k^2 N)$, and $Y_m = W_s(X_m)$,

$$\Delta_B \leqslant \left[1 + \chi^2\left(P_{Y_m}, P_Y\right)\right]^2 - 1. \quad (12)$$

This bound is a consequence of the χ^2 upper bound on the relative entropy described above, and finding tractable expressions for quantum and classical χ^2 quantities relies on the fact that the second argument to the relative entropy is a thermal state or a Gaussian probability distribution, respectively. The inequality (12) is an instance of a more general statement relating the quantum and classical χ^2 quantities in this setting for general factorizable P functions. The proof involves somewhat intricate Gaussian integration and is given in the Appendix.

Hence, per ([5], Sec. VII), using the quantile or random-walk constellations will lead to Δ_B decaying as the inverse of

the number of points in the coherent-state constellation m^2, while the Gauss-Hermite quadrature leads to $\Delta_B \leqslant O(e^{-cm})$ for $c = 2 \ln \frac{1+s}{s}$. Using the above expression for s, one obtains $c \approx 2\frac{1-k^2}{k^2} \frac{N_0}{N}$ for $N \gg N_0$. If we wish to increase N but fix the gap to capacity or coherent information, this implies that the number of constellation points must scale linearly with N.

V. POLAR CODES FOR THE THERMAL CHANNEL

The polar code construction can be used for classical, private classical, and quantum coding. Here we provide only the essential details for the present case and will not attempt to provide a background on polar coding. One could also appeal to other capacity-achieving schemes for the task of transmitting classical information, e.g., spatially coupled low-density parity-check codes [21] (after showing these work for channels with quantum output), but no explicit quantum coding schemes besides polar codes are known to achieve the coherent information. Common to all our coding scenarios is a truncation of the *output* space to finite dimensions, as described at the end of Sec. II. This ensures that we may apply existing results on the construction and properties of polar codes. It appears that all the necessary statements also hold for channels with infinite-dimensional outputs, but we have not shown this definitively.

A. Classical coding

Wilde and Guha [7] show how to construct polar codes to transmit classical information over channels with binary classical input and finite-dimensional quantum output. Recently, one of the present authors extended the construction to arbitrary input alphabets [22]. Here, the modulator selects a coherent-state input for the Bosonic Gaussian channel, but the choice of which input to make is classical. Both [7] and [22] only considered the case of uniformly random channel input (befitting the equilattice or quantile constellations), but this restriction can be lifted by the construction of Honda and Yamamoto [23] (using modified polarization statements found in [24]), so as to apply to random-walk or Gauss-Hermite constellations.

Thus, a rate of $I(Z_m : B_m)$ is achievable. Both [7] and [22] appeal to Arikan's original encoder, hence encoding is efficient. The quantum version of the successive cancellation decoder is likewise explicit, but its implementation complexity is unknown.

B. Private coding

For private coding, the task is not only to transmit information reliably but also to hide it from an eavesdropper. Codes to do so are constructed by Renes and Wilde in [25], where it is shown that the "naive" wiretap rate $I(Z_m : B_m) - I(Z_m : E_m)$ is achievable. Generally, the code requires secret-key assistance at nonzero rate, but not if the channel is degradable [4], e.g., for pure loss ($N_0 = 0$).

Crucial to the construction is the observation that the channels to the legitimate receiver Bob and to the eavesdropper Eve are related by an entropic uncertainty relation. Eve's information about the actual classical message must be small

if the code is constructed so that it could send complementary "phase" information to Bob. The construction in [25] is again for uniform channel inputs, but can be extended as just described above. The uncertainty principle argument is unaffected by having nonuniform channel inputs.

C. Quantum coding

For quantum coding, we proceed as in the case of private coding, except we use the channels to send quantum states. Now we regard the modulator as mapping the kth basis state of an m^2-dimensional quantum system to the kth coherent state in the constellation. Since this mapping is not unitary, the coherent information of the modulator composed with $\mathcal{E}_{k,N_0}$ is lower than that of $\mathcal{E}_{k,N_0}$ itself. This implies that we cannot employ the method of Devetak [12] to upgrade a private code to a quantum code (at least, not at the same rate).

Instead, we employ a scheme based on one-way entanglement distillation, combining it with teleportation to enable transmission of arbitrary states [26]. Recall that in entanglement distillation Alice and Bob use local operations and classical communication to transform many copies of a bipartite mixed state into a number of maximally entangled states. The mixed state in question is that obtained by Alice transmitting the state in Eq. (8) through the channel to Bob, while keeping its purification. Abusing notation and denoting by $Q_{N,m}(j)$ the probability of the jth coherent state $|z_j\rangle$, the state at the input to the channel can be written

$$|\xi\rangle^{A'A} = \sum_{j=1}^{m^2} \sqrt{Q_{N,m}(j)} |b_j\rangle^{A'} |z_j\rangle^A, \qquad (13)$$

where the $|b_j\rangle$ are an orthonormal basis for an m^2-dimensional space A'. Here we are interested in using stabilizer codes for entanglement distillation, where Alice makes stabilizer measurements on A' and sends the outcomes (the syndrome) to Bob. Bob then uses this side information to execute a decoding operation on his system. By choosing a suitable stabilizer code, Alice and Bob end up with copies of a maximally entangled state. As shown in [8,24], by using a polar code the scheme has rate equal to $I(Z_m : B) - I(Z_m : E)$ which approaches $Q_G^{(1)}(\mathcal{E}_{k,N_0})$ as $m \to \infty$. The former construction is simpler, yet may require entanglement assistance, while the latter is somewhat more complicated but does not require entanglement assistance. In either case Alice's stabilizer measurements can be done efficiently, since the requisite quantum circuit is just the polar coding circuit.

This scheme can be converted into a quantum code involving no classical communication as follows. Consider a particular syndrome, selected in advance and known to Bob (since the final state is entangled, the distribution of syndromes is essentially uniform). Instead of preparing many copies of the state $|\xi\rangle^{A'A}$ and making the stabilizer measurement, Alice could just create the bipartite state that results when the given syndrome is observed. After receiving the channel output Bob proceeds with his decoding operation. By the properties of stabilizer codes, each logical codeword will correspond to a superposition of tensor products of coherent states. The catch in this construction is that we no longer have any guarantee that the codewords are efficiently constructable except by

the tedious protocol of performing the procedure above and keeping the state only when the desired syndrome is obtained.

VI. CONCLUSIONS AND OUTLOOK

We have constructed three classes of codes for the thermal noise channel, all based on concatenation of polar coding with suitable discretizations of the channel into a constellation of input coherent states. For transmitting classical information, this leads to explicit codes with efficiently implementable encoders that achieve the single letter channel capacity if restricted to Gaussian inputs. Moreover, the encoder need only prepare products of coherent states. For transmitting classical information privately, our codes naively achieve the unoptimized wiretap rate $I(Z : B) - I(Z : E)$, but this could presumably be improved by preprocessing exactly as in the classical wiretap scenario.

In the fully quantum case, we have shown how to employ a one-way entanglement distillation scheme in order to send quantum information at a rate given by the Gaussian coherent information. Alice's operations are efficiently implementable in this scheme, but it is not clear how to efficiently generate the corresponding quantum codewords for use in a standard error-correction scenario. From a more technical perspective, this construction provides a rigorous proof taking the subtleties of the infinite-dimensional setting into account that the Gaussian coherent information is a lower bound on the quantum capacity of the thermal channel and equal to it for pure loss.

While our results thus provide explicit and efficiently implementable encodings, the question of how to construct efficient and experimentally realizable decoders is still wide open. Although an explicit decoder is known for classical information transmission, the successive cancellation decoder of [7], it is not known how to implement it efficiently for noncommuting channel outputs. Moreover, recent results by Winter and coworkers even suggest that, while Gaussian encodings are sufficient to achieve the capacity, Gaussian decoders seem not to be sufficient [27]. This again shows that much further work is needed to understand the limitations of data transmission through Gaussian quantum channels.

APPENDIX: THE RELATIVE ENTROPY UPPER BOUND

Equation 12 follows from Eq. (9a), the upper bound $D(\rho||\sigma) \leqslant \chi^2(\rho,\sigma)$, and the following.

Lemma 1. Let $X \sim \mathsf{N}(0,1)$ and X_1', X_2' be arbitrary real random variables with densities $P_{X_1'}$ and $P_{X_2'}$. For $Z = \sqrt{\frac{N}{2}}(X_1' + iX_2')$ with density $Q(z)$ and arbitrary $N > 0$, define $\rho = \int_{\mathbb{C}} dz\, Q(z)\theta_z$. Then, with $Y = W_s(X)$ and $Y_j' = W_s(X_j')$, $N' = k^2 N + N_c$, and $s = k^2 N/(\sqrt{N'(N'+1)} - k^2 N)$,

$$1 + \chi^2(\rho, \tau_{N'}) = [1 + \chi^2(P_{Y_1'}, P_Y)]\,[1 + \chi^2(P_{Y_2'}, P_Y)].$$

We prove Lemma 1 by establishing two intermediate results which give explicit expressions for the classical and quantum χ^2 quantities. First, define the real Gaussian density

$$\varphi_s(x) := \frac{1}{\sqrt{2\pi s}} \exp\left[-\frac{x^2}{2s}\right], \qquad (A1)$$

for $x \in \mathbb{R}$ and $s > 0$; recall that the corresponding complex density ψ_s is defined in Eq. (2). Observe that $\varphi_s(x) = \frac{1}{\sqrt{s}}\varphi_1(\frac{x}{\sqrt{s}})$ and $\psi_s(x + iy) = \varphi_{s/2}(x)\varphi_{s/2}(y)$. We will make use of the following Gaussian integral formula. For A an arbitrary $n \times n$ complex matrix with positive definite Hermitian part, i.e., $\frac{1}{2}(A + A^\dagger) \geqslant 0$, and arbitrary $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$ we have [[28], Eq. 3.18]

$$\int_{\mathbb{C}^n} d\mathbf{w}\; e^{-\bar{\mathbf{w}}^T A \mathbf{w} + \bar{\mathbf{u}}^T \mathbf{w} + \bar{\mathbf{w}}^T \mathbf{v}} = \pi^n \det A^{-1} e^{\bar{\mathbf{u}}^T A^{-1} \mathbf{v}}. \qquad (A2)$$

Now we give the expression for the relevant classical χ^2 quantity, $\chi^2(P_{Y'}, P_Y)$ with an arbitrary input X'. To this end define, for $s \geqslant 0$ and $x, x' \in \mathbb{R}$,

$$K_s(x,x') := \frac{1+s}{\sqrt{1+2s}} \exp\left\{-\frac{s}{2(1+2s)}[s(x-x')^2 - 2xx']\right\}. \qquad (A3)$$

Lemma 2. For random variables $X, X', Y,$ and Y' as in Eq. (11),

$$1 + \chi^2(P_{Y'}, P_Y) = \int_{\mathbb{R}^2} dx\; dx'\, P_{X'}(x)P_{X'}(x')K_s(x,x'). \qquad (A4)$$

Proof. First observe that $P_Y(y) = \varphi_{1+s}(y)$, while

$$P_{Y'}(y) = \int_{\mathbb{R}} dx\; P_{X'}(x)\varphi_1(y - \sqrt{s}x). \qquad (A5)$$

Computing $1 + \chi^2(P_{Y'}, P_Y)$, we find

$$1 + \chi^2(P_{Y'}, P_Y) = \int_{\mathbb{R}} dy\, \frac{P_{Y'}(y)^2}{P_Y(y)} \qquad (A6)$$

$$= \int_{\mathbb{R}} dx \int_{\mathbb{R}} dx'\, P_{X_m}(x)P_{X'}(x')I_s(x,x'), \qquad (A7)$$

where

$$I_s(x,x') = \int_{\mathbb{R}} dy\, \varphi_{1+s}(y)^{-1}\varphi_1(y - \sqrt{s}x)\varphi_1(y - \sqrt{s}x'). \qquad (A8)$$

This is a simple Gaussian integral, and using Eq. (A2) we find $I_s(x,x') = K_s(x,x')$. ∎

Next we turn to the expression for the quantum χ^2 quantity.

Lemma 3. Let ρ be a state with positive P function (a probability density P). For any $N > 0$,

$$1 + \chi^2(\rho, \tau_N) = \int_{\mathbb{C}^2} dz\; dz'\, P(z)\, P(z')\, C_N(z,z'), \qquad (A9)$$

where, for $t_N = \sqrt{\frac{N+1}{N}}$,

$$C_N(z,z') := (N+1)\exp[-|z|^2 - |z'|^2 + t_n(z\bar{z}' + \bar{z}z')].$$

Proof. Computing the trace in the number basis, we get

$$1 + \chi^2(\rho, \tau_N) = \sum_{n=0}^{\infty} \langle n|\, \rho\, \tau_N^{-1/2}\rho\, \tau_N^{-1/2}\, |n\rangle$$

$$= (N+1)\sum_{n,n'=0}^{\infty} t_N^n t_N^{n'} \langle n|\,\rho\,|n'\rangle\,\langle n'|\,\rho\,|n\rangle$$

$$= (N+1)\sum_{n,n'=0}^{\infty} t_N^n t_N^{n'} \int_{\mathbb{C}} dz'\, P(z')\,\langle n'|z'\rangle\,\langle z'|n\rangle$$

$$= \int_{\mathbb{C}^2} dz\; dz'\, P(z)P(z')S_N(z,z'),$$

where

$$S_N(z,z') = (N+1)\sum_{n,n'=0}^{\infty} t_N^n t_N^{n'}\,\langle n|z\rangle\,\langle z|n'\rangle\,\langle n'|z'\rangle\,\langle z'|n\rangle.$$

Computing $S_N(z,z')$, we find

$$\frac{S_N(z,z')}{N+1} = \sum_{n,n'=0}^{\infty} t_N^n t_N^{n'} e^{-|z|^2}\frac{z^n \bar{z}^{n'}}{\sqrt{n!}\sqrt{n'!}} e^{-|z'|^2}\frac{z'^{n'}\bar{z}'^n}{\sqrt{n'!}\sqrt{n!}}$$

$$= e^{-|z|^2 - |z'|^2} \sum_{n=0}^{\infty} \frac{1}{n!}(t_N z\bar{z}')^n \sum_{n'=0}^{\infty} \frac{1}{n'!}(t_N z'\bar{z})^{n'}$$

$$= \frac{C_N(z,z')}{N+1}.$$

This completes the proof. ∎

With these two intermediate results, we are ready to establish Lemma 1.

Proof of Lemma 1. Using the form of θ_z as described in Sec. II, it is apparent that the P function of ρ is simply

$$P_\rho(w) = \int_{\mathbb{C}} dz\, Q(z)\psi_{N_c}(w - kz). \qquad (A10)$$

Now applying Lemma 3 with number parameter N', we have

$$1 + \chi^2(\rho, \tau_{N'}) = \int_{\mathbb{C}^2} dz\; dz'\, Q(z)\, Q(z')R_{N'}(z,z'), \qquad (A11)$$

where $R_{N'}(z,z')$ is just

$$\int_{\mathbb{C}^2} dw\; dw'\, \psi_{N_c}(w - kz)\psi_{N_c}(w' - kz')C_{N'}(w,w').$$

Recalling Eq. (2) and using $A_N = \begin{pmatrix} 1 & t_N \\ t_N & 1 \end{pmatrix}$ to express the argument to the exponential in $C_{N'}(w,w')$ in matrix form, we

obtain a Gaussian integral for $R_{N'}(z,z')$:

$$R_{N'}(z,z') = \frac{N'+1}{\pi^2 N_c^2} e^{-\frac{k^2}{N_c}(|z|^2+|z'|^2)} \int_{\mathbb{C}^2} d\mathbf{w} \, \exp\left[-\bar{\mathbf{w}}^T A_{N'} \mathbf{w} - \frac{1}{N_c}\bar{\mathbf{w}}^T \mathbf{w} + \frac{k}{N_c}(\bar{\mathbf{z}}^T \mathbf{w} + \bar{\mathbf{w}}^T \mathbf{z})\right]. \tag{A12}$$

Here $\mathbf{z} = (z,z')$ and similarly for $\mathbf{w}$. The integrand has the form $e^{-\bar{\mathbf{w}}^T A \mathbf{w} + \bar{\mathbf{u}}^T \mathbf{w} + \bar{\mathbf{w}}^T \mathbf{v}}$ where $A = A_{N'} + \mathbb{1}/N_c$ and $\mathbf{u} = \mathbf{v} = k/N_c \mathbf{z}$. Applying Eq. (A2) to Eq. (A12), we obtain

$$R_{N'}(z,z') = \frac{N'+1}{N_c^2} \det(A^{-1}) \exp\left[\frac{k^2}{N_c} \bar{\mathbf{z}}^T \left(\frac{1}{N_c} A^{-1} - \mathbb{1}\right)\mathbf{z}\right] \tag{A13}$$

$$= \frac{N'(N'+1)}{N'+2N'N_c - N_c^2} \exp\left[-k^2 \frac{(N'-N_c)(|z|^2+|z'|^2) - \sqrt{N'(N'+1)}(z\bar{z}'+\bar{z}z')}{N'+2N'N_c - N_c^2}\right]. \tag{A14}$$

To simplify this expression, let $c = N' - N_c$ and $d = \sqrt{N'(N'+1)}$; these are the prefactors of the first and second terms in the argument of the exponential, absent the denominator. Observe that the denominator itself is simply $d^2 - c^2$. Now notice that s as defined in the statement of the lemma is such that $s/(1+s) = c/d$. By direct substitution it is easy to show that the prefactor of the exponential in Eq. (A14) simplifies to

$$\frac{N'(N'+1)}{N'+2N'N_c - N_c^2} = \frac{(1+s)^2}{1+2s}. \tag{A15}$$

Therefore,

$$R_{N'}(z,z') = \frac{(1+s)^2}{1+2s} \exp\left\{-\frac{k^2}{c}\frac{s}{1+2s}[s(|z|^2+|z'|^2) - (1+s)(z\bar{z}'+\bar{z}z')]\right\}. \tag{A16}$$

As $c = k^2 N$, we obtain

$$R_{N'}\left(\sqrt{\frac{N}{2}}z, \sqrt{\frac{N}{2}}z'\right) = \frac{(1+s)^2}{1+2s} \exp\left\{-\frac{s}{2(1+2s)}[s(|z|^2+|z'|^2) - (1+s)(z\bar{z}'+\bar{z}z')]\right\}, \tag{A17}$$

and thus, finally,

$$R_{N'}\left(\sqrt{\frac{N}{2}}(x+iy), \sqrt{\frac{N}{2}}(x'+iy')\right) = K_s(x,x')K_s(y,y'). \tag{A18}$$

Returning to Eq. (A11) and changing variables $z \to \sqrt{\frac{N}{2}}(x+iy)$ yields

$$1 + \chi^2(\rho,\tau_{N'}) = \left[\int_{\mathbb{R}} dx \, dx' \, P_{X_1'}(x) P_{X_1'}(x') K_s(x,x')\right]\left[\int_{\mathbb{R}} dx \, dx' \, P_{X_2'}(x) P_{X_2'}(x') K_s(x,x')\right]. \tag{A19}$$

Appealing to Lemma 2 completes the proof. ∎

[1] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[2] J. Eisert and M. M. Wolf, in *Quantum Information with Continuous Variables of Atoms and Light*, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College, London, 2007), pp. 23–42.

[3] V. Giovannetti, R. García-Patrón, N. Cerf, and A. Holevo, Nat. Photonics **8**, 796 (2014).

[4] M. M. Wolf, D. Pérez-García, and G. Giedke, Phys. Rev. Lett. **98**, 130501 (2007).

[5] Y. Wu and S. Verdú, in *Proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2010* (IEEE, Piscataway, NJ, 2010), p. 620.

[6] E. Arikan, IEEE Trans. Inf. Theory **55**, 3051 (2009).

[7] M. M. Wilde and S. Guha, IEEE Trans. Inf. Theory **59**, 1175 (2013).

[8] J. M. Renes, F. Dupuis, and R. Renner, Phys. Rev. Lett. **109**, 050504 (2012).

[9] A. S. Holevo, Problems of Information Transmission **43**, 1 (2007).

[10] S. Guha and M. M. Wilde, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT), 2012* (IEEE, Piscataway, NJ, 2012), pp. 546–550.

[11] M. M. Wilde, *Quantum Information Theory* (Cambridge University, Cambridge, England, 2016).

[12] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).

[13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, arXiv:1510.08863v4.

[14] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).

[15] J. Harrington and J. Preskill, Phys. Rev. A **64**, 062301 (2001).

[16] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).

[17] G. Ungerboeck, IEEE Trans. Inf. Theory **28**, 55 (1982).

[18] F.-W. Sun and H. van Tilborg, IEEE Trans. Inf. Theory **39**, 1714 (1993).

[19] M. Ruskai and F. Stillinger, J. Phys. A **23**, 2421 (1990).

[20] K. Temme, M. Kastoryano, M. Ruskai, M. Wolf, and F. Verstraete, J. Math. Phys. **51**, 122201 (2010).

[21] S. Kudekar, T. Richardson, and R. Urbanke, IEEE Trans. Inf. Theory **59**, 7761 (2013).

[22] R. Nasser and J. M. Renes, arXiv:1701.03397 [cs.IT] (2017).

[23] J. Honda and H. Yamamoto, IEEE Trans. Inf. Theory **59**, 7829 (2013).

[24] J. Renes, D. Sutter, F. Dupuis, and R. Renner, IEEE Trans. Inf. Theory **61**, 6395 (2015).

[25] J. M. Renes and M. M. Wilde, IEEE Trans. Inf. Theory **60**, 3090 (2014).

[26] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[27] A. Winter, Hiding information with linear optics against classical adversaries, lecture given at the Secure Communication via Quantum Channels conference, Center for Interdisciplinary Research, Bielefeld, Germany, 2017 (unpublished).

[28] A. Altland and B. Simons, *Condensed Matter Field Theory*, 2nd ed. (Cambridge University, Cambridge, England, 2010).