Security proof of continuous-variable quantum key distribution using three coherent states

Kamil Brádler and Christian Weedbrook

Phys. Rev. A **97**, 022310 — Published 6 February 2018

DOI: 10.1103/PhysRevA.97.022310

A SECURITY PROOF OF CONTINUOUS-VARIABLE QKD USING THREE COHERENT STATES

KAMIL BRÁDLER AND CHRISTIAN WEEDBROOK

Abstract. We introduce a new ternary quantum key distribution (QKD) protocol and asymptotic security proof based on three coherent states and homodyne detection. Previous work had considered the binary case of two coherent states and here we nontrivially extend this to three. Our motivation is to leverage the practical benefits of both discrete and continuous (Gaussian) encoding schemes creating a best-of-both-worlds approach; namely, the postprocessing of discrete encodings and the hardware benefits of continuous ones. We present a thorough and detailed security proof in the limit of infinite signal states which allows us to lower bound the secret key rate. We calculate this is in the context of collective eavesdropping attacks and reverse reconciliation postprocessing. Finally, we compare the ternary coherent state protocol to other well-known QKD schemes (and fundamental repeaterless limits) in terms of secret key rates and loss.

1. Introduction

Quantum key distribution (QKD) [1, 2], in principle, provides the most secure form of quantum safe cybersecurity, i.e., protection against a quantum computing attack. As opposed to post quantum cryptography [3], which is based on computationally secure mathematics, QKD exploits the laws of quantum physics to achieve, at least in theory, unbreakable codes. Since QKD was first suggested in 1984, many advances have taken place; from theoretical to proof-of-principle experiments to field tests and even the forming of companies.

Even though this seems like the end of the story there are still many advances being made in all of these areas. To this point, in this paper, we look at creating a best-of-both worlds approach to QKD by combining the beneficial practical aspects of the two main implementations of QKD: those using discrete variables (DVs) [1] and those using continuous variables (CVs) [4, 5]. To be more specific, we would like to use the simpler encoding and decoding methods from DV QKD but at the same time leverage the simpler and more affordable room temperature hardware components of CV QKD.

Recently, the ultimate (optimal) limit for a lossy bosonic channel was discovered and is given by the PLOB bound [6]. An interpretation of this result is that no QKD protocol can go beyond this bound without a quantum repeater. In terms of key rate as a function of channel loss (cf. for instance with Fig. 6 of [6]) this corresponds to a CV QKD Gaussian protocol with reverse reconciliation using a quantum memory at Alice's side and heterodyne at Bob's side [7]. In terms of implementations, below this optimal bound lies the single photon BB84 protocol [8]. Both of these two protocols are in terms of the ideal case, i.e., perfect sources and perfect detectors. However, when one considers the realistic version of these two (in the case of DV QKD this corresponds to the decoy state scheme [9, 10]), both become remarkably similar in terms of key rates as a function of loss; except for a slight advantage in key rates for CVs in the low-loss regime and a slight distance advantage in DVs for the high-loss regime. In this realistic scenario, both the DV and the CV QKD schemes sit below the PLOB bound. Ideally we would like to either: (1) find a (realistic) protocol above these two protocols or (2) have a protocol similar to these protocols in terms of key rates but one that leverages the practical benefits of both schemes.

(Kamil Brádler) Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada
(Christian Weedbrook, Kamil Brádler) CipherQ, 10 Dundas St E, Toronto, M5B 2G9, Canada
E-mail: kbradler@uottawa.ca.

With that in mind, we consider a protocol first introduced in 2009 by Zhao et al. [11] that uses binary-phase shift-keying (BPSK) of coherent states, $|\alpha\rangle$ and $|-\alpha\rangle$, along with homodyne detection. Unfortunately, as one can see, the performance of this protocol is below that of the realistic BB84 with decoy states and the realistic Gaussian modulation CV scheme. In this paper, we consider a ternary-phase shift-keying (TPSK) of coherent states, $|\alpha\rangle_i$ where $i = 0, 1, 2$, with homodyne detection. Here each of the three coherent states are phase shifted in phase space by 120°, cf. Fig. 1. One may ask the question, what is the motivation of going from two coherent states to three coherent states? Or perhaps why not go to more coherent states straightaway? In terms of the second question, this is easily answered by considering the Zhao et al. paper [11] and our results here. The extension to three states is challenging enough, while the extension to more than three states is a very hard problem if one wants a strong security proof like the one we have given here. In terms of the first question, there are two possible ways to answer this. One way is that we know that at some stage as one increases the number of coherent states there must be a point where it becomes a close approximation to the full Gaussian distribution. So there may be a point where one may not need the entire (continuum) Gaussian distribution. Another way is to consider the affect that decoy state BB84 QKD has on ideal single photon BB84 and draw inspiration from there. Specifically, by increasing the number of pulses from the ideal case of one to say three pulses gives a boost to both the key rate and distance [9, 10]. So perhaps we can consider increasing the number of discrete coherent states from two to three (and potentially higher) as a decoy-state-like extension of the BPSK-modulated CV QKD protocol.

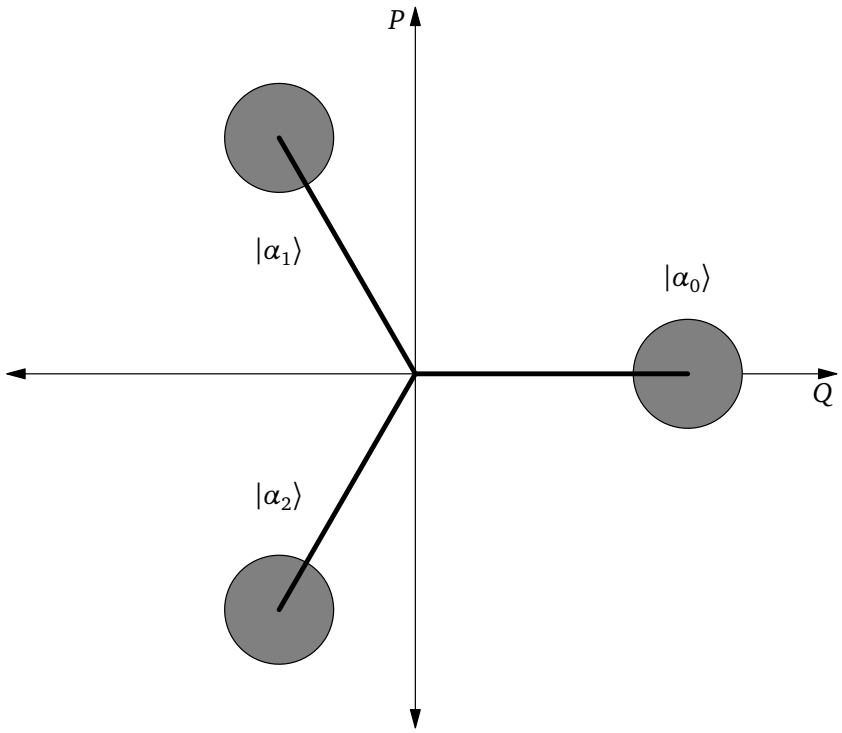

FIGURE 1. Phase space configurations of the ternary coherent state QKD protocol. Note that each subsequent coherent state is 120° from the other one. Alice's role is to continually and randomly choose from these three options and then send them to Bob who performs homodyne detection on the incoming states by randomly alternating between the Q and P quadratures. As is standard, the quantum channel is assumed to be monitored by the eavesdropper, Eve.

In this paper, we introduce and rigorously prove the asymptotic security of a new ternary QKD protocol based on three coherent states and homodyne detection. For completeness, we mention that other discrete encodings for CVs have also been considered [12–15]. In the papers by Leverrier and Grangier [12–14], they considered two different coherent state encodings (i.e., two and four) but in order to analyze the security they 'padded out' the states with decoy-like states that effectively resembled a Gaussian distribution from Eve's point of view. This is instigated in order to leverage previous Gaussian encoding security proofs. Finally, in [15] a multi letter phase-shift keying scheme was introduced, where an N number of coherent states can be used. However, the security proof only considered a lossy bosonic channel (i.e., no excess noise). In contrast, we consider a bosonic channel with arbitrary noise. Our results here allow for the significant reduction, compared to Gaussian modulation protocols, in classical post-processing, random-number generation, and classical-communication overheads. Furthermore, by keeping the benefits of CV hardware, our approach has the practical benefits of doing away with single-photon detectors that characterize DV QKD systems. Such detectors are only able to reach their promise of low-noise and high-efficiency only with the addition of cumbersome cryogenics.

Outline. This paper is structured as follows. We begin by giving more background on the relationship between discrete and Gaussian encodings. This is followed by a description of the steps of our ternary coherent state protocol. Our main result is presented next and consists of a simulation of a TPSK modulated lossy bosonic channel. We end with our conclusion.

Notation. In what follows, f' denotes $\frac{\mathrm{d}f}{\mathrm{d}z}$ and similarly for higher derivatives. Sometimes we explicitly mention a function's variable (typically $f = f(z)$). The symbol $\stackrel{\mathrm{df}}{=}$ stands for 'defined'. The von Neumann entropy of a density matrix ϖ_A is $H(A)_\varpi \equiv H(\varpi_A) \stackrel{\mathrm{df}}{=} -\mathrm{Tr}[\varpi_A \log \varpi_A]$ [16] and it becomes Shannon entropy for classical probability distributions (denoted by X, Y in this paper). We will intensively study the properties of $H(X)$ where $X = \vec{x} = (x_1, x_2, 1-x_1-x_2)$ and so a special name will be reserved for it – the ternary Shannon entropy:

$$h_3(\vec{x}) \stackrel{\mathrm{df}}{=} -x_1 \log x_1 - x_2 \log x_2 - (1-x_1-x_2)\log[1-x_1-x_2]. \tag{1}$$

The base of the logarithms is irrelevant but will be set to two throughout the paper. The classical-quantum conditional entropy (entropy conditioned on a classical variable) reads $H(A|Y) = \sum_y p(y) H(\varpi_A^y)$. For a classical variable $A = X$ the entropy becomes the standard Shannon conditional entropy $H(X|Y) = -\sum_y p(y) \sum_x p(x|y) \log p(x|y)$. Other entropic quantities used in the paper include the classical mutual information $I(X:Y) \stackrel{\mathrm{df}}{=} H(X) + H(Y) - H(XY) = H(Y) - H(Y|X)$. We will also use the quantum version of the mutual information where one of the registers is quantum and express it as $I(Y:E) = H(E|X) + I(X:E) - H(E|Y)$.

When we say a function f is increasing we mean non-decreasing ($f(x) \leq f(y)$ whenever $x \leq y$). Similarly, a decreasing function means a non-increasing function.

Conventions. We will use the convention of [11] for the quadrature operators. They are given by $Q = 1/\sqrt{2}(a + a^\dagger), P = 1/\sqrt{2}(a - a^\dagger)$ and so $\langle(\Delta Q)^2\rangle_\alpha = \langle(\Delta P)^2\rangle_\alpha = 1/2$ ($\hbar = 1$) and $\langle Q\rangle_\alpha = 1/\sqrt{2}(\alpha + \bar{\alpha})$ where $\alpha = r \exp[i\sigma]$. In our case we have $(\alpha_x)_{x=0,1,2}$ and $\sigma_0 = 0, \sigma_1 = 2\pi/3$ and $\sigma_2 = 4\pi/3$ and $r_i = r$ is a free parameter chosen by the legitimate participants to maximize the secret key rate.

A lossy bosonic channel is a Gaussian channel parametrized by has two quantitites. One of them is the transmittance $0 \leq \eta \leq 1$ and the other one the number of thermal photons representing the Gaussian excess noise. For the sake of comparison, we use the definition of excess noise from [11]:

$$\delta = \frac{\langle(\Delta Q)^2\rangle_{\varrho_B}}{\langle(\Delta Q)^2\rangle_{|0\rangle}} - 1 \tag{2}$$

given by Bob's measurement of ϱ_B. For the simulation scenario we also assume $\langle(\Delta Q)^2\rangle_{\varrho_B} = \langle(\Delta P)^2\rangle_{\varrho_B}$. A quantity called a "mixedness parameter" $\varepsilon_x \geq 0$ is upper bounded by Bob's second moments according to (65) of [11] and it is the main estimate of the state in Eve's possession. In our simulation scenario we may set[1], $\varepsilon \equiv \varepsilon_x$.

2. Discrete versus Gaussian encoding

The most studied QKD schemes are discrete-variable (DV) QKD [1, 2] and continuous-variable (CV) QKD [4] based on a Gaussian encoding. The DV QKD security analysis is very mature but the secret key rates are limited given the discrete nature of the encoding. Higher-dimensional DV QKD scheme have been analyzed [17] but yet to have graduated from the experimental point of view. Gaussian CV QKD offers much generous secret key rates together with a relatively simple experimental realization in terms of the state preparation and detection. But it has also its disadvantages. For instance, the classical postprocessing such as error-correction is computationally demanding and currently not very efficient. The aspiration of CV QKD based on a distribution of discrete signal states holds a promise of combining the best of both worlds.

Unlike a Gaussian encoding where the best adversary's strategy is known, the same is not true if the number of signal states is discrete. In fact, to the authors' knowledge, there exists only one paper dealing with the security of such a scheme without assuming nearly anything about the adversary's powers [11]. The security proof (and thus the corresponding secret key rate lower bound) is derived by assuming a collective attack and in the asymptotic scenario of an infinite code length. The collective attacks are not the most general eavesdropping scheme. However, it is widely believed that similarly to DV QKD or Gaussian CV QKD, a more general attack strategy does not bring any advantage. For the second point, an asymptotic analysis is not a realistic assumption but it is historically the first step after which a finite-key length analysis typically follows. The number of signal (coherent) states prepared by a sender in [11] is two and the receiver is allowed to measure only the first and second moments of whatever gets through the (unknown) quantum channel. Through a tour-de-force calculation, the authors essentially construct a statistical model of the adversary's quantum states compatible with the legitimate recipient's measurement and maximize the amount of information the adversary can in principle get, following a two-way public discussion. In this way, a secret key rate lower bound is derived.

The analysis is achieved by splitting the secret key rate for a reverse reconciliation protocol into three entropic quantities and upper/lower bounding them from the quantities available from the recipient's measurement. In this paper, we follow the same strategy but instead of two signals the communicating parties exchange three coherent signals. This may seems like a small iteration but the opposite is true. We get not only substantially better secret key rate lower bounds but also show the limitation of the approach. The latter point is worth elaborating on. The proof presented in [11] crucially relies on the monotonicity and concavity of the binary Shannon entropy as a function of the absolute value of the overlap of two pure states (not necessarily the signal states). For two signal states, these properties are trivial and they are not proved in [11, Eqs. (33), (34)]. The situation dramatically changes for three signal states. Essentially, the result of this paper is the proof that these two *crucial* properties hold for the ternary Shannon entropy, Eq. (1). Only then can the rest of the previous analysis be applied verbatim and that is precisely what we have done. Once these two properties are proven, the rest of the proof follows exactly as in [11] only with a few minor modifications which we will write explicitly.

There is a caveat, however. For two signal states, the binary Shannon entropy depends only on the absolute values of the overlap of the signal states. For three states, the ternary entropy depends on three possible overlaps and a certain phase. This wouldn't be a problem if we needed to study the entropy of the density matrix for the signal states only. After all, the participants are those who decide what symmetry (and a probability distribution) the signal states obey and that could greatly simplify the analysis. The

[1]The variables $\alpha, \delta, \varepsilon, \gamma$ used in this section should not be confused with those from Sec. A.

problem is that at one point of the previous analysis [11], the purified adversary's state (estimated from Bob's measurement) need not obey any such property and the state must be considered arbitrary. As it is discussed in the first remark of Section A.1, in the presence of more than one overlap, the studied function does not even satisfy the (suitably generalized) notion of monotonicity. This is not only surprising but it also affects the applicability of the approach of [11] that we follow here – unlike the case of two signal states, the proof strategy has its limits. Another consequence of our generalization is that unless a generic argument for monotonicity and concavity of the suitable generalized entropy function can be found (taking into account what we have just stated), it is most likely that a completely different approach is needed in order to study discrete CV QKD protocols and their rates for more than three signal states.

3. Description of Ternary Coherent State Protocol

Here we outline our ternary (three coherent state) QKD protocol. It goes as follows.

(1) Alice prepares one of three possible coherent states $|\alpha_i\rangle$ with probability $p_i = 1/3$, where $i = 0, 1, 2$. In Fig. 1, we have a schematic of the phase space depicting how the three coherent states are placed, i.e., sequentially separated by 120°. She then sends the randomly selected coherent state to the receiver, Bob, over an insecure quantum channel. It is assumed that this channel could be monitored by Eve. Alice repeats this step many times. Alice's choice for the ith signal (coherent state pulse) is recorded in the variable x_i. Specifically, the labeling goes as: $|\alpha_0\rangle$ is $x_i = 0$, $|\alpha_1\rangle$ is $x_i = 1$, and $|\alpha_2\rangle$ is $x_i = 2$.
(2) Bob, upon receiving a sequence of quantum states, randomly performs homodyne detection thereby randomly measuring the quadratures $Q(\phi)$ for $\phi = (\pi/2, -\pi/6, -5\pi/6)$ of each of the coherent states. A similar setup was used in [18] but tested on a specific eavesdropping strategy. Bob's measurement results are recorded in the variable y_i. Note that $Q(\pi/2) \equiv P$ in Fig. 1.
(3) After the transmission, the parties publicly announce the measurement quadratures. One of the quadratures, say $Q(-5pi/6)$, the measurement data is published which is used to determine the extent of the adversary's maliciousness. These data are subsequently discarded.
(4) The remaining data (which we denote as $\{\vec{x}, \vec{y}\}$) will be used for the final key generation. For the purpose of reverse reconciliation, Bob sends computes functions $u(\vec{y})$ and $w(\vec{y})$ and sends $u(\vec{y})$ over a public channel to Alice and keeps $w(\vec{y})$ which is a discrete proto-key (partially correlated with Alice's discrete variable $\{\vec{x}\}$.
(5) Classical post-processing procedures of error correction and privacy amplification are applied by Alice and Bob in order to extract the final shared secret-key. This final secret bit string is then used as a one-time pad in order to perfectly secure messages.

4. A secret key rate lower bound

In this section, we derive the lower secret key rate for the ternary protocol with respect to a lossy bosonic channel. Mathematically the main results needed for this lower bound (and which are rigorously proven in the Appendix) involve proving that monoticity and concavity both hold for the ternary Shannon entropy, Eq. (1). We begin by defining the lower bound of the secret key rate K followed by calculating the individual components of this bound which include Alice and Bob's mutual information and Eve's mutual information.

The secret key rate K is lower bounded as

$$K > I(X:Y) - \max_{\varrho_{ABE}} I(Y:E) \tag{3}$$

Eq. (3) has its origin in [19] where the one-way private quantum channel capacity was established. The lower bound also differs from [19] in several aspects. (i) The channel is a priori not known and is only partially estimated by the measurements of the legitimate participants. The ambiguity in its identification is an advantage for Eve – the optimization leads to the penalty on the amount of shared secret correlations as if Eve used the best eavesdropping channel compatible with the measurements. This translates into the

best channel purification ϱ_{ABE} held by Eve among all admissible ones in Eq. (3), see also Ref. [20]. (ii) Our key distribution protocol uses reverse reconciliation where the classical communication (exploited by Eve) is transmitted from Bob to Alice. This results in the appearance of the second term in (3) as opposed to [19, 20] dealing with direct reconciliation. (iii) Finally, given the reality of the explicit quantum private code described in Sec. 3, the RHS of (3) is a one-shot formula – a natural lower bound to a multi-letter secret key rate formula. A closely related expression for a secret key rate was derived in [21] while focusing solely on the security of QKD.

4.1. **A secret key rate lower bound for a Lossy Bosonic Channel.** The job here is to maximize the mutual information $I(Y:E)$ in order to find a lower bound on the secret key rate K. In an actual experiment, the classical probability distribution must be measured to be subsequently inserted to the relevant entropic quantities in (3). Following [11] we may simulate an actual link by a lossy bosonic channel. This is a realistic model for the atmospheric CV QKD with homodyne measurement. Note that the complementary channel is another lossy bosonic channel and it captures the effect of the environment or an adversary Eve. As is common for QKD, Eve is assumed to control the channel and take an advantage of the generated noise to hide her illicit behavior.

As we will see in Section A.1, unlike the BPSK case studied in [11] the entropic properties of the investigated density matrix depend not only on the mutual overlaps of the three signal states but also on the overall phase, see the expressions for d in Eq. (13) or (14b). In the simulation scenario for a lossy bosonic channel the phase can be computed as we will show now.

We will first consider the zero excess noise case $\delta = \frac{\langle(\Delta Q)^2\rangle_\alpha}{\langle(\Delta Q)^2\rangle_{|0\rangle}} - 1 = 0$ (a pure-loss bosonic channel). The estimated quantities become simpler as the recipient's detected states are pure coherent states and similarly for Eve. The parameter ε given by (65) in [11] is bounded from above by $U \equiv U_x = 0$ from (65). Hence $\varepsilon = 0$ and (66) together with (C17,C18) of [11] imply

$$|\langle\tilde{\beta}_i|\tilde{\beta}_j\rangle| = c_u = c_l = \kappa.$$

The RHS is given by $\kappa \equiv \kappa_{ij} = |\langle\sqrt{\eta}\alpha_i|\sqrt{\eta}\alpha_j\rangle|$. Inserting c_u, c_l into (70,71) in [11] we get

$$d_l = d_u = \frac{|\langle\alpha_i|\alpha_j\rangle|}{\kappa} \stackrel{\text{df}}{=} |\gamma_{ij}| \equiv |\gamma| = e^{-\frac{3}{2}(1-\eta)r^2}. \tag{4}$$

This quantity is the estimated overlap of the states going to the environment. As expected from the properties of a pure-loss bosonic channel it is the same quantity as κ with η substituted by $1-\eta$.

We can geometrically interpret the product of inner products in (13) (or its special case (14b)) if ψ_i are coherent states. Then the product

$$z_{01}z_{12}z_{20} = \langle\alpha_0|\alpha_1\rangle\langle\alpha_1|\alpha_2\rangle\langle\alpha_2|\alpha_0\rangle = e^{-\frac{1}{2}(c_{01}^2+c_{12}^2+c_{20}^2)}e^{-i2(A_{01}+A_{12}+A_{20})} \tag{5}$$

is written in terms of the sides c_{ij} and area $A_{012} \stackrel{\text{df}}{=} A_{01}+A_{12}+A_{20}$ of the triangle formed by the corresponding three points in phase space. This is the interpretation provided by Lemma 1.

We illustrate it on the symmetric case $c_{01} = c_{20} = c_{12} \equiv c$ of an equilateral triangle for $\delta = 0$, whose side squared is equal to $c^2 = 3r^2(1-\eta)$ found in (4). From the new triangle side we deduce, with the help of elementary geometry (essentially Heron's formula), the corresponding area:

$$A_{012} = \frac{1}{4}\left(4c_{01}^2c_{12}^2 - (c_{01}^2 + c_{12}^2 - c_{20}^2)^2\right)^{1/2}. \tag{6}$$

and consequently the phase: $\vartheta = 2A_{012} = r^2\frac{3\sqrt{3}}{2}(1-\eta)$.

How do we apply it to the $\delta > 0$ case? Here, the situation is slightly different. The effect of a lossy bosonic channel is not only shrinking of the phase space triangle but also increasing the states' variances – environment (Eve) and Bob do not receive a mixture of three pure states but rather of three mixed Gaussian states. Following the general procedure outlined in [11], where only the first and second moments are

measured, the overlaps of Eve's state figuring in our simulation scenario are bounded by (70) and (71) in [11]. In that case, neither $|\gamma|$ nor κ are overlaps of the corresponding pure coherent states. More precisely, since Bob measures only the first two moments, the authors of [11] introduced fiducial coherent states $|\overline{\beta}_i\rangle$ on Bob's side compatible with the measurement of the first moment. Then $\kappa = |\langle\overline{\beta}_i|\overline{\beta}_j\rangle|$ and as before $\kappa \equiv \kappa_{ij} = |\langle\sqrt{\eta}\alpha_i|\sqrt{\eta}\alpha_j\rangle|$ for the case of a lossy bosonic channel[2]. This provides the same interpretation for $|\gamma|$ (Eve's parameters estimated from Bob's measurement) and the phase is then determined according to Lemma 1.

The main object of study is a lower bound on the secret key rate, Eq. (3). Here we break down the lower bound for the simulated lossy bosonic channel. The central role is played by the ternary Shannon entropy, Eq. (1), where $x_k = t_k + 1/3$ and t_k is given by (18).

Eve's and Alice's Mutual Information, $I(X:E)$. Closely following [11, Sec. IV. B], to get a secret key lower bound, the first quantity to estimate is $I(X:E) < I(X:QE) = h_3(\vec{x}(Z))$ for x_k restricted to $p_k = 1/3$ and $\langle\Psi^i_{EQ}|\Psi^j_{EQ}\rangle = Z_{ij} = Z\exp[i\tilde{\tau}_{ij}]$, $Z > 0$. As explained in the remark on p. 12, the restriction to $|Z_{ij}| = Z$ is a necessary step for the proof strategy following [11] to go through. Then, from (18), we get the explicit form of x_k:

$$x_1 = \frac{1}{3}\Big(1 + 2Z\cos\frac{\vartheta}{3}\Big), \tag{7a}$$

$$x_{2,3} = \frac{1}{3}\Big(1 - Z\Big(\cos\frac{\vartheta}{3} \mp \sqrt{3}\sin\frac{\vartheta}{3}\Big)\Big). \tag{7b}$$

Denoting $f \equiv f_{ij} = F(\varrho^i_E, \varrho^j_E)$ to be the fidelity of $\varrho^{i(j)}_E = \mathrm{Tr}_Q[\Psi^{i(j)}_{EQ}]$ we get

$$h_3(\vec{x}(Z,\vartheta)) \le h_3(\vec{x}(f,\vartheta)) \le h_3\Big(\vec{x}((1-\tilde{\varepsilon}_0)^{1/2}(1-\tilde{\varepsilon}_1)^{1/2}|\gamma|,\vartheta)\Big) \tag{8}$$

where $0 \le \tilde{\varepsilon}_i \le \varepsilon$. The second inequality follows from the proof of monotonicity, Theorem 10, as a special case $p_k = 1/3$.

When restricted to the simulation scenario of a lossy bosonic channel, the parameter ϑ is a phase whose value we determine with the help of Lemma 1. Before doing so, recall that for $\delta = 0$ the lossy bosonic channel merely "shrinks" the triangle representing the mixture of three coherent states in phase space and the shrinking factor is $1-\eta$ for Eve's system (see (4)). Consequently, ϱ^i_E are pure and Eq. (4) can be interpreted as the modulus of their overlap.

Eve's Entropy conditioned on Alice's variable X, $H(E|X)$. The next expression used for the secret key estimation is the conditional entropy $H(E|X)$. It is upper bounded by [11]

$$\frac{1}{3}\sum_x (1+V_x)\log[1+V_x] - V_x\log V_x,$$

where $V_x = \big(\langle(\Delta Q)^2\rangle_{\varrho_B}\langle(\Delta P)^2\rangle_{\varrho_B}\big)^{1/2} - 1/2$. In the case of a lossy bosonic channel we find $V_x = \delta/2$.

Eve's Entropy conditioned on Bob's measurement outcome Y, $H(E|Y)$. The third expression needed to be evaluated from the secret key lower bound is $H(E|Y)$ in (62) from [11]. In order to do so we have to generalize the conditional probability distribution related to the action of a lossy bosonic channel. We cannot simply take the derived expressions in [11] since for three and more signal states the states cannot all be aligned with a real line in phase space. Instead, we introduce

$$p(y|x) = \frac{1}{\pi(1+\delta)}\exp\Big[-\frac{|y-\sqrt{\eta}\alpha_x|^2}{\delta+1}\Big] = \frac{1}{\pi(1+\delta)}\exp\Big[-\frac{|y|^2+\eta r^2 - 2|y|r\sqrt{\eta}\cos[\phi-\sigma_x]}{\delta+1}\Big],$$

[2]An insight provided by Saikat Guha.

where $y = |y|\exp[i\phi]$ and $\alpha_x = r\exp[i\sigma_x]$. For three signal states we take the values of $\sigma_{0,1,2}$ introduced in Section 3. To simulate the channel we further use $p(x|y) = \frac{1}{3}p(y|x)/p(y)$ together with

$$p(y) = \sum_{x=0,1,2} p(y|x)p(x) = \frac{1}{3}\frac{1}{\pi(1+\delta)}\sum_{x=0,1,2}\exp\Big[-\frac{|y-\sqrt{\eta}\alpha_x|^2}{\delta+1}\Big].$$

Hence, for example,

$$p(0|y) = \frac{\exp\Big[-\frac{|y-\sqrt{\eta}\alpha_0|^2}{\delta+1}\Big]}{\sum_{x=0,1,2}\exp\Big[-\frac{|y-\sqrt{\eta}\alpha_x|^2}{\delta+1}\Big]}.$$

A straightforward generalization of the derivation of Eqs. (56) and (57) in [11] allows us to lower bound $H(E|Y)$.

Alice's and Bob's Mutual Information, $I(X:Y)$. The final component is the classical mutual information $I(X:Y) = H(X) - H(X|Y)$ calculated with the help of $p(x|y)$ and $p(y)$ defined above.

Final Secret Key Rate Lower Bound for a Lossy Bosonic Channel. Now we have all the ingredients we need to find the actual secret key rate lower bound. It is expression (72) given in [11], adapted to the TPSK encoding. It can be written as

$$\begin{aligned} K > & \underbrace{\log 3 - \int_0^\infty \mathrm{d}|y||y| \int_0^{2\pi} \mathrm{d}\phi\, p(y) \sum_{x=0,1,2} p(x|y)\log[p(x|y)]}_{I(X:Y)} \\ & - \underbrace{\big((1+\delta/2)\log[1+\delta/2] - \delta/2\log[\delta/2]\big)}_{H(E|X)} - \max_{0\le\tilde{\varepsilon}\le\varepsilon}\Bigg[\underbrace{h_3\big(\vec{x}((1-\tilde{\varepsilon})|\gamma|,\vartheta)\big)}_{H(X:E)} \\ & \left.\begin{aligned} & - \int_0^\infty \mathrm{d}|y||y| \int_0^{2\pi} \mathrm{d}\phi\, p(y) h_3(\vec{x}(|\gamma|,\vartheta,p(0|y),p(1|y))) \\ & + \sum_{x=0,1}\Bigg[\Big(\frac{\tilde{\varepsilon}}{3}\frac{1+|\gamma|}{1-|\gamma|}\Big)^{1/2}\Bigg(\int_0^\infty \mathrm{d}|y||y| \int_0^{2\pi} \mathrm{d}\phi\, p(y)\frac{h_3^2\big(\vec{x}(|\gamma|,\vartheta,p(0|y),p(1|y))\big)}{p(x|y)}\Bigg)^{1/2}\Bigg] \\ & + \frac{\tilde{\varepsilon}}{1-|\gamma|} h_3\big(\vec{x}(|\gamma|,\vartheta,1/3,1/3)\big) \end{aligned}\right\} - H(E|Y). \end{aligned} \tag{9}$$

For ease of sight we identified the *origin* of the summands by the expressions in the braces. The main technical result of this paper – the proofs of monotonicity and concavity of the ternary Shannon entropy – participate in the derivation of $H(E|Y)$. The reasoning is nearly a verbatim copy of Section IV.C and the Appendices A and C of [11] implying the conditional entropy to be a lower bound on the secret key rate K.

In Fig. 2 we present the main result of our analysis (applied to a simulated lossy bosonic channel). We plot the secret key lower bound, Eq. (9), for several values of the excess noise parameter. Compared to [11], we find better lower bounds as expected from the use of three signals states but also much better threshold values where the rate is zero. It therefore supports the idea that to approach the high rates given by a continuous Gaussian encoding, one would need only a reasonably small number of signal states. This cannot, strictly speaking, be correct for the vicinity of $\eta = 1$. It is known that the ultimate upper bound for the two-way secret key rate at the presence of zero excess noise is equal to $K = -\log[1-\eta]$ [6], a quantity diverging for $\eta \to 1$. Clearly, for any finite number of discrete signal states d, the maximal secret key rate for $\eta = 1$ is $\log d$ like in our case $d = 3$. Ref. [6] also provided an achievable bound (actually a lower bound based on [7]) by taking into account the input energy constraint. This is depicted in Fig. 2

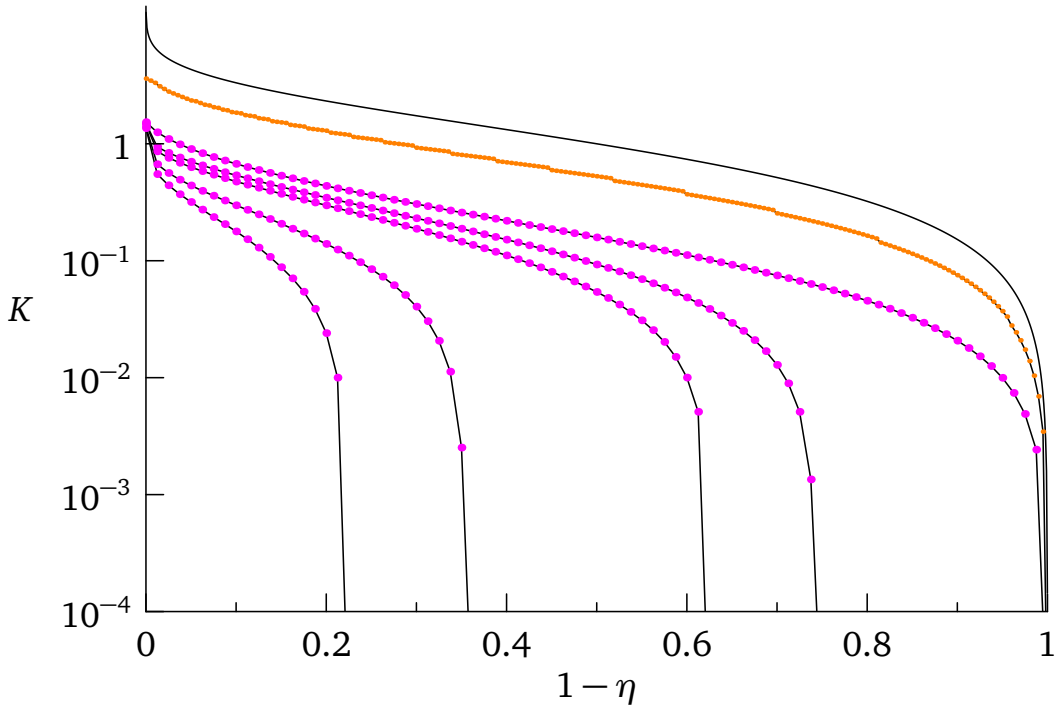

FIGURE 2. Secret key rates as functions of loss $1-\eta$ for several values of the channel excess noise $\delta = (0, 0.0004, 0.001, 0.005, 0.01)$ (the pink dots). The black curve is the ultimate achievable bound without an energy constraint for $\delta = 0$. The orange curve is an achievable bound for $\delta = 0$ taking into account the input energy constraint [6]. All curves are functions of the channel loss.

as the orange dotted curve for $\delta = 0$. The 'stairs' on this curve are the consequence of a different optimal energy (input state overlap leading to a different input energy constraint) shown in Fig. 3.

An important fact to realize is that even though we have only proved monotonicity and concavity of h_3 for $0 \leq \vartheta \leq \pi/2 \Leftrightarrow \varepsilon \leq 0$ (for ε given by (17e)), it does not affect the secret key rate lower bound. The optimal input energy falls inside the region $\varepsilon \leq 0$. The situation is also depicted in Fig. 3.

5. Differences in an actual QKD experiment

The real-world scenario introduces further complications. The channel may not be lossy bosonic (it may not even be described by a stationary process for the duration of the experiment but we will avoid this type of complications). For a stationary channel and in the asymptotic scenario the participants collect enough statistics to reconstruct the channel to estimate the conditional probability distributions $p(y|x)$ and $p(y)$ arbitrarily well. The same applies to the BPSK analysis from [11] but as we already alluded to, there is more degrees of freedom in the ternary case. There are in total three overlaps in the form of three real parameters for a general triple of coherent pure states and in addition there is a phase. In the simulation scenario of a lossy bosonic channel the overlaps if chosen symmetrically by Alice (our assumption) and the phase can be subsequently calculated as done in the previous section[3] But in for an actual experiment we

[3]Note that similarly to [11] we not only calculate the entropy of the input density matrix but also of other, say intermediate, density matrices in order to lower bound the secret key rate. Even there the three real parameters coincide (they can't be interpreted as overlaps, though, see below Eq. (6)) and the phase can be calculated for a lossy bosonic channel.

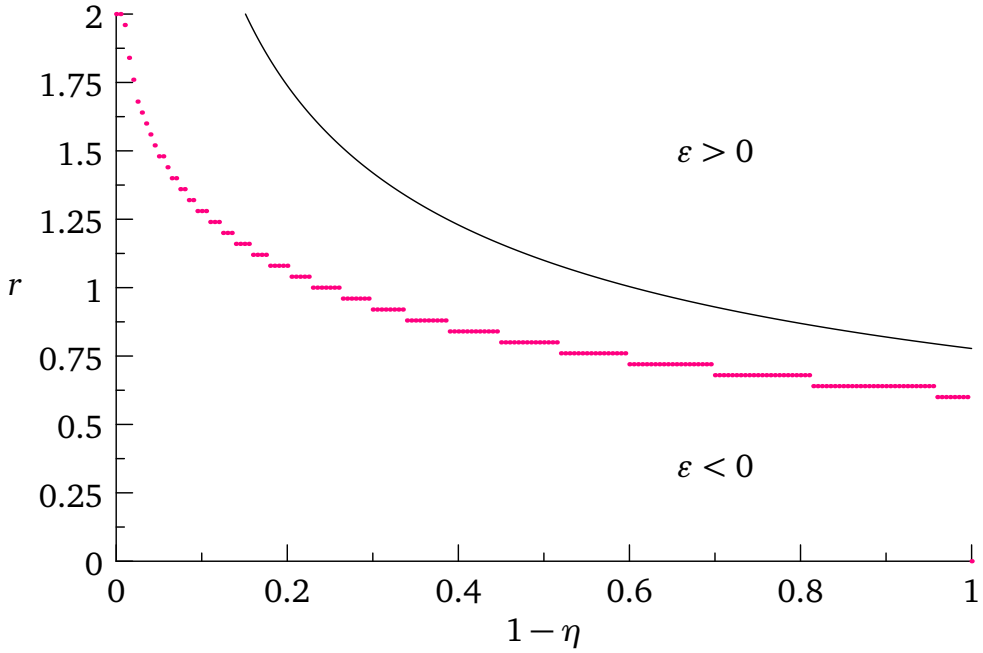

FIGURE 3. The red dots depict the optimizing overlaps r for $\delta = 0$. The black curve is a boundary $\varepsilon = 0$ of (17e) ($\vartheta = \pi/2$) given by $r^2 \frac{3\sqrt{3}}{2}\eta = \pi/2$ (see below Eq. (6)) below which the proofs of monotonicity and concavity exist ($\varepsilon \leq 0$).

can only assume the symmetry of a density matrices directly prepared by Alice. The states where Eve can in principle intervene has no a priori symmetry which translates into their entropy to be dependent on three plus one free parameters. As it turns out (see the discussion in Sec. A.1), the key property of monotonicity of the ternary Shannon entropy does not hold in general and the strategy to lower bound the secret key rate from [11] must be abandoned.

How do we overcome this problem here? If the parameters measured by Bob indicate that the incoming states are not symmetrically distributed, the participants assume the closest symmetric distribution that gives Eve the biggest advantage. One could be tempted to take the smallest of the three overlaps and create a symmetric distribution based on it. However, as the example in [22, p. 10] shows, the entropy of such a density matrix does not necessarily becomes smaller thus indicating *more* distinguishable quantum states. So a better strategy to introduce a single overlap is called for and it will necessarily reduce the secret key rate. But only this is the situation for which we can follow the proof in [11] once the monotonicity and concavity of the ternary Shannon entropy is proven. The worst case scenario happens if Bob detects only two states, that is, if the channel is so disruptive that it managed to merge two signal states to one quantum state. In that case the secret key rate would be zero and it would probably be better to switch to BPSK.

How do we recover the other free parameter, namely the angle? Similarly to the lossy bosonic case, a triple of fiducial coherent states $(|\overline{\beta}_i\rangle)_{i=0,1,2}$ with the same absolute value of the overlap is introduced. We assume that the triple properly bounds the entropies as described in the previous paragraph, so that the advantage is given to Eve resulting in the key rate reduction. Then we followed the procedure of phase calculation described below Eq. (6) following Lemma 1. This is the right phase for the fiducial triple of pure coherent states.

6. Conclusion

In conclusion, we introduced and rigorously proved the asymptotic security of a new ternary QKD protocol based on three coherent states and homodyne detection. The motivation for introducing such a protocol is to extract a best-of-both-world's approach to QKD in terms of the encoding and decoding of discrete variable schemes along with the practical hardware of continuous variable schemes. There is, however, the downside that the security proof is very challenging compared to the results for Gaussian modulated continuous-variable QKD protocols. We overcame this challenge by mathematically proving that two crucial properties, monotonicity and concavity, hold for the ternary Shannon entropy. This allowed us to evaluated a lower bound to the secret key rate in the collective attack scenario.

Other interesting avenues of research could include considering a four-state extension (if possible, or perhaps using a different method), determining what number of signal states are enough to tend close to the full Gaussian distribution and also a thorough finite-key analysis. This is a lively area of research for many classes of bosonic channels where the lossy bosonic channel is an important subclass [6, 23]. A measurement-device-independent (MDI)-QKD [24–26] version of our scheme presented here would also be interesting as a way of ruling out side channel attacks.

Acknowledgement

We would like to thank Saikat Guha for helpful discussions. The authors acknowledge support from the U.S. Office of Naval Research (ONR). This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-17-1-0083. The authors thank Saikat Guha for valuable comments and discussions.

Appendix A. Full Details of Main result

A.1. **Properties of ternary density matrix.** In this section, we give the calculations needed to prove the main results. To begin with, let

$$\varpi = p_0|\psi_0\rangle\langle\psi_0| + p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2| \tag{10}$$

be a rank-three density operator where $p_0 + p_1 + p_2 = 1$. The state ϖ takes on a different meaning depending on where it is used. It can be an input density matrix a sender prepares in a lab in which case $p_k = 1/3$ and ψ_k are the signal (coherent) states with a chosen symmetry. Or, it can be Eve's conditioned state based on Bob's measurement. In that case, p_k are arbitrary conditional probabilities $p_k(x|y)$ and ψ_k are pure states with no obvious symmetry properties [11].

Following the Cayley-Hamilton theorem, one finds the coefficients of the characteristic polynomial

$$\det[\varpi - x\,\mathrm{id}] = f(x) = ax^3 + bx^2 + cx + d = 0, \tag{11}$$

where

$$a = 1, \tag{12a}$$

$$b = -\mathrm{Tr}[\varpi] = -1, \tag{12b}$$

$$c = \frac{1}{2}((\mathrm{Tr}[\varpi])^2 - \mathrm{Tr}[\varpi^2]) = \frac{1}{2}(1 - \mathrm{Tr}[\varpi^2]), \tag{12c}$$

$$d = -\frac{1}{6}((\mathrm{Tr}[\varpi])^3 - 3\,\mathrm{Tr}[\varpi]\,\mathrm{Tr}[\varpi^2] + 2\,\mathrm{Tr}[\varpi^3]) = -\frac{1}{6}(1 - 3\,\mathrm{Tr}[\varpi^2] + 2\,\mathrm{Tr}[\varpi^3]). \tag{12d}$$

The last two coefficient become

$$c = \frac{1}{2}(1 - p_0^2 - p_1^2 - p_2^2 - 2p_0p_1|z_{01}|^2 - 2p_1p_2|z_{12}|^2 - 2p_0p_2|z_{02}|^2), \tag{13a}$$

$$d = \frac{1}{6}\Big(-1 + 3\left(p_0^2 + p_1^2 + p_2^2 + 2p_0p_1|z_{01}|^2 + 2p_0p_2|z_{02}|^2 + 2p_1p_2|z_{12}|^2\right)$$

$$-2\big(p_0^3+p_1^3+p_2^3+3(p_0^2p_1+p_0p_1^2)|z_{01}|^2+3(p_0^2p_2+p_0p_2^2)|z_{02}|^2+3(p_1^2p_2+p_1p_2^2)|z_{12}|^2$$
$$+3p_0p_1p_2(z_{01}z_{12}z_{20}+c.c)\big)\Big). \tag{13b}$$

Note that ϖ in all its roles in the security proof if always a sum of rank-one operators. Hence the trace quantities in Eqs. (12) are easy to find. An additional check was performed by calculating the quartic term

$$\frac{1}{24}\big((\mathrm{Tr}[\varpi])^4-6(\mathrm{Tr}[\varpi])^2\,\mathrm{Tr}[\varpi^2]+3(\mathrm{Tr}[\varpi^2])^2+8\,\mathrm{Tr}[\varpi]\,\mathrm{Tr}[\varpi^3]-6\,\mathrm{Tr}[\varpi^4]\big)$$

and was found to be zero as it should be.

We set the overlaps to be $\langle\psi_i|\psi_j\rangle=z_{ij}=|z|\exp[i\tau_{ij}]$ and get

$$c=\frac{1}{2}\big(1-p_0^2-p_1^2-p_2^2-|z|^2(2p_0p_1+2p_1p_2+2p_0p_2)\big), \tag{14a}$$
$$d=\frac{1}{6}\Big(-1+3\big(p_0^2+p_1^2+p_2^2+2|z|^2(p_0p_1+p_0p_2+p_1p_2)\big)$$
$$-2\big(p_0^3+p_1^3+p_2^3+3(p_0^2p_1+p_0p_1^2)|z|^2+3(p_0^2p_2+p_0p_2^2)|z|^2+3(p_1^2p_2+p_1p_2^2)|z|^2$$
$$+6|z|^3p_0p_1p_2\cos\vartheta\big)\Big), \tag{14b}$$

where $\vartheta=\tau_{01}+\tau_{12}+\tau_{20}$. The absolute value $|z|$ and the angle $0\le\vartheta\le\pi$ are not independent and we will revisit the relation below Eq. (18) (see also Lemma 1).

Remark. It may seem that by setting $|z_{ij}|=|z|,\forall i,j$ we limit ourselves to a special case of ϖ. This is indeed true. Quite surprisingly, however, it is the most general case for which one of the studied properties (monotonicity) actually holds. It turns out that the multivariable function studied in this paper, the ternary Shannon entropy (Eq. (1)), is not monotone decreasing unless $|z_{ij}|=|z|,\forall i,j$ in which case it reduces to the standard single-variable problem. What does it mean for a multivariable function to be monotone increasing/decreasing? This question is closely related to the existence of sets that cannot be totally ordered (totality means that either $x\le y$ or $y\ge x$ holds). An example is $\mathbb{R}^n$ for $n>1$ which is only a partially ordered set. To this end, one defines the componentwise order [27] of two n-tuples $(x_1,\ldots,x_n)\le(y_1,\ldots,y_n)$ iff $x_i\le y_i,\forall i$. A monotone increasing or decreasing function $f:\mathbb{R}^n\mapsto\mathbb{R}^m$ then satisfies $f(x_1,\ldots,x_n)\le f(x_1,\ldots,x_n)$ and $f(x_1,\ldots,x_n)\ge f(x_1,\ldots,x_n)$, respectively. The lack of this property (namely not decreasing) means that the strategy outlined in [11] we follow here is simply not applicable.

Coefficients, Eqs. (14), are used to get the eigenvalues of ϖ. Following [28] (or Wikipedia for a quick summary) we form

$$\Delta_0=b^2-3ac=1-3c, \tag{15a}$$
$$\Delta_1=2b^3-9abc+27a^2d=-2+9c+27d \tag{15b}$$

and define

$$p=-\frac{\Delta_0}{3}=\alpha+\beta z^2, \tag{16a}$$
$$q=\frac{\Delta_1}{27}=\gamma+\delta z^2+\varepsilon z^3. \tag{16b}$$

They are the coefficients of a reduced cubic t^3+pt+q the general cubic polynomial $f(x)$ can be converted to. The coefficients of p,q from Eqs. 16 are given by

$$\alpha=\frac{1}{6}(1-3p_0^2-3p_1^2-3p_2^2)\le 0, \tag{17a}$$
$$\beta=-(p_0p_1+p_0p_2+p_1p_2)\le 0, \tag{17b}$$

$$\gamma = \frac{1}{27}(-2+9p_0^2-9p_0^3+9p_1^2-9p_1^3+9p_2^2-9p_2^3)$$
$$= \frac{1}{27}(3p_1-1)(3p_2-1)(3p_1+3p_2-2) \lesseqgtr 0, \tag{17c}$$
$$\delta = \frac{1}{27}\big(18(p_0p_1+p_0p_2+p_1p_2)-27(p_0^2p_1+p_0p_1^2+p_0^2p_2+p_1^2p_2+p_0p_2^2+p_1p_2^2)\big) \leq 0, \tag{17d}$$
$$\varepsilon = -2p_0p_1p_2\cos\vartheta \lesseqgtr 0, \tag{17e}$$

where we also summarized some basic properties based on $0 \leq p_i \leq 1, \sum_i p_i = 1$. Then, the three roots (the eigenvalues of ϖ) are $x_k = t_k - b/(3a) = t_k + 1/3$ where

$$t_k = 2\sqrt{-\frac{p}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{3}{2}\frac{q}{p}\sqrt{-\frac{3}{p}}\right)-\frac{2k\pi}{3}\right). \tag{18}$$

It is known [28] that

$$t_0 + t_1 + t_2 = 0, \tag{19}$$
$$t_0 \geq t_1 \geq t_2 \tag{20}$$

hold. Hence $x_0 + x_1 + x_2 = 1$ as we expect from $\mathrm{Tr}[\varpi] = 1$ but $x_2 \geq 0$ is not satisfied for all $|z|$ and ϑ. For example, if $\psi_1 = e^{i\varphi_1}\psi_0, \psi_2 = e^{i\varphi_2}\psi_0$ then $|z| = 1$ and $\vartheta = \tau_{01} + \tau_{12} + \tau_{20} = 0$. In general, it turns out that $x_2 \geq 0$ is equivalent to $q \leq \frac{1}{27} + \frac{p}{3}$ which provides a bound on ϑ given $|z|$. Indeed, for $|z| = 1$ the only possibility is $\vartheta = 0$.

Something much stronger can be said about the phases if ψ_i are actual coherent states (either the signal states or the fiducial states we mentioned in the main text).

Lemma 1. *The phase* $\mathrm{Arg}[\langle\alpha_i|\alpha_j\rangle]$ *of an inner product of two coherent states* $|\alpha_i\rangle$ *and* $|\alpha_j\rangle$ *is a function of* $|\langle\alpha_i|\alpha_j\rangle|$.

Proof. Using elementary trigonometry we write

$$\langle\alpha_i|\alpha_j\rangle = e^{-\frac{1}{2}(r_i^2+r_j^2-2r_ir_j\cos[\sigma_j-\sigma_i])}e^{-i2r_ir_j\sin[\sigma_j-\sigma_i]} = e^{-\frac{1}{2}c_{ij}^2}e^{-i2A_{ij}}, \tag{21}$$

where c_{ij} a side of triangle opposite to the angle $\tau_{ji} = \sigma_j - \sigma_i$ between the sides r_i and r_j and A_{ij} is the triangle area (it is oriented since $A_{ij} = -A_{ji}$). But knowing r_i, r_j, c_{ij}, we can easily calculate the area of the triangle and hence the phase $\mathrm{Arg}\,[\langle\alpha_i|\alpha_j\rangle] = -2A_{ij} = 2A_{ji}$. Hence the phase is much more constrained if ψ_i are coherent states. ∎

This trivial statement (we could also use the relation between sin and cos to get the phase) has interesting consequences we exploited in Eq. (5).

A.2. **Monotonocity of the ternary Shannon entropy.** The following result will be a useful tool in the course of our analysis.

Theorem 2 (Descartes' rule of signs [29, 30])**.** *Let* $p(x) = \sum_{m=0}^{s} a_{n-m}x^{n-m}$ *be a real polynomial of order* n *where* $s \leq n$ *and* $a_{n-m} \neq 0$*. Then the number of positive real zeros (including multiplicities) is equal to* $V - 2k$ *where* $k \geq 0$ *and* V *is the number of sign variations of* a_{n-m} *starting from* a_n*.*

Lemma 3. *Let* $\varepsilon \leq 0$*. Then* $q(z)$ *in* (16a) *is monotone-decreasing and concave in* $z \in (0,1)$ *for all* p_k*. It has a single positive root* $z^{\#} \in (0,1)$ *iff* $\gamma > 0$ *in which case* $q(z) \geq 0$ *for* $z \in (0, z^{\#})$*.*

Proof. The monotonicity of q follows from

$$q' = 2\delta z + 3\varepsilon z^2,$$

since $\delta, \varepsilon \leq 0$. Because of Theorem 2 (or just by inspection), there is no positive root of $q(z)$ for $\gamma < 0$ again following from $\delta, \varepsilon \leq 0$. There is one positive root for $\gamma > 0$ and it has to lie in the interval $(0,1]$ since $q(0) = \gamma > 0$ and

$$q(1) = \gamma + \delta + \varepsilon \leq \gamma + \delta = -\frac{2}{27} + 2p_0p_1p_2 \leq 0$$

valid for all p_k. ■

Remark. Even more straightforward is to show $p < 0$ in $z \in (0,1)$ (follows from Eqs. (16a), (17a) and (17b) by considering $(p_0+p_1+p_2)^2 = 1$). The equality $p = 0$ is achieved for $z = 0$ and $p_0 = p_1 = p_2 = 1/3$ but in order to have future expressions well-defined we will consider the open interval $z \in (0,1)$ throughout this work. Similarly, we find $p' \leq 0$.

It is useful to know the generic behavior of the central piece of the cubic solutions, Eq. (18). That is uncovered in the following lemma.

Lemma 4. *Let $\varepsilon \leq 0$ and*

$$g(z) = \frac{3}{2}\frac{q}{p}\sqrt{-\frac{3}{p}}. \tag{22}$$

Then $|g(z)| \leq 1$, $g(z) \propto -q(z)$ and $g' \lesseqgtr 0$ for $z \in (0,1)$.

Proof. The bound $|g(z)| \leq 1$ follows from the cubic equation discriminant

$$\frac{q^2}{4} + \frac{p^3}{27} \leq 0, \tag{23}$$

where the inequality is always true for the case of three real roots of a cubic equation [28]. This, on the other hand, must be true since ϖ is a density matrix. Eq. (22) can be both positive and negative with its sign always opposite to that of $q(z)$. This is because $\frac{1}{p}\sqrt{-\frac{3}{p}} < 0$ for $z \in (0,1)$ following from Lemma 3. A related useful fact is that for $\gamma < 0$ we get $g(z) > 0$ for $z \in (0,1)$. Finally, by writing

$$g' = \frac{3\sqrt{3}}{4}\frac{2pq' - 3p'q}{p^2\sqrt{-p}} \tag{24}$$

and noticing that the denominator is nonnegative we only need to study the behavior of $\nu_1(z) = 2pq' - 3p'q$. First, we find a zero root due to $\nu_1(z) = -2z\left(-2\alpha\delta + 3\beta\gamma - 3z\alpha\varepsilon + z^2\beta\delta\right)$. The quadratic equation $-2\alpha\delta + 3\beta\gamma - 3z\alpha\varepsilon + z^2\beta\delta = 0$ yields two other real roots and, in general, they both may lie in the interval $(0,1)$. Only when $\gamma \geq 0$, one of the roots is negative. ■

Lemma 5. *Let $\tau(z,n) = \sqrt{-p}\cos\frac{h}{n}$ and $n \in \mathbb{Z}_{>1}$ such that $p, p' < 0$, $0 \leq h \leq \pi$ in $z \in (0,1)$ and $h' > 0$ in $\mathcal{J} \subset (0,1)$. Then $\frac{\mathrm{d}\tau(z,n)}{\mathrm{d}z} > \frac{\mathrm{d}\tau(z,2)}{\mathrm{d}z}$ in $\mathcal{J}$.*

Proof. We find

$$\frac{\mathrm{d}\tau(z,n)}{\mathrm{d}z} = \frac{2ph'\sin\frac{h}{n} - np'\cos\frac{h}{n}}{2n\sqrt{-p}}. \tag{25}$$

The denominator is positive for $z \in (0,1)$ but there are two competing expressions in the numerator. The first summand is negative, the second one is nonnegative and so the overall sign may be hard to infer. The inequality follows by observing that the nonnegative summand in the numerator of (25) remains constant as n increases while the negative one is divided by n and so its overall contribution diminishes. Finally, $\sin\frac{h}{n}$ and $\cos\frac{h}{n}$ do not change their sign with a growing $n \geq 2$ and, conveniently, $\sin\frac{h}{n} > \sin\frac{h}{n+1}$ holds together with $\cos\frac{h}{n} < \cos\frac{h}{n+1}$ for $n \geq 2$ as illustrated in Fig. 4. ■

Proposition 6. *The function t_0 is monotone-increasing in $z \in (0,1)$ for $\varepsilon \leq 0$.*

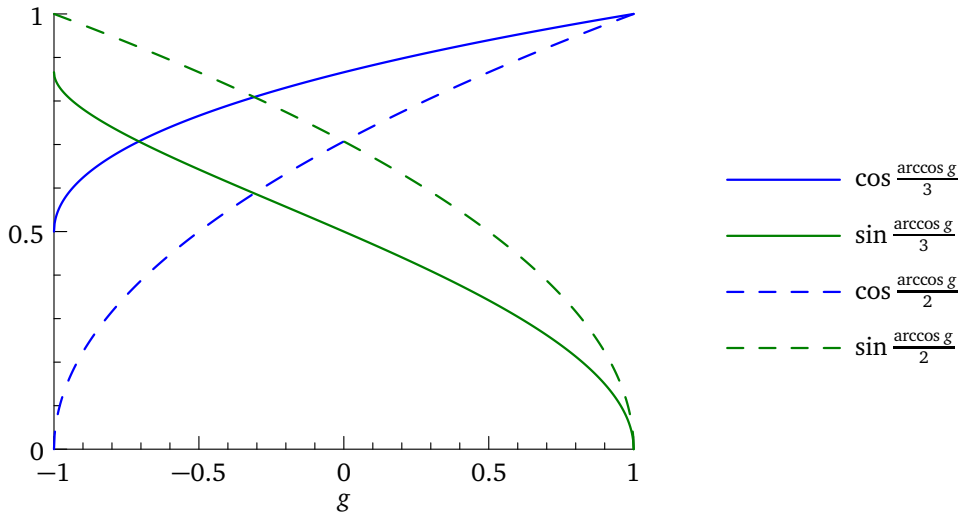

FIGURE 4. Properties of some trigonometric functions.

Proof. From (18) we get

$$t_0' = \frac{2}{3}\frac{\sqrt{-p(z)}g'(z)\sin\left(\frac{1}{3}\arccos\left(g(z)\right)\right)}{\sqrt{1-g(z)^2}} - \frac{p'(z)\cos\left(\frac{1}{3}\arccos\left(g(z)\right)\right)}{\sqrt{-p(z)}}. \tag{26}$$

Both denominators are non-negative (check zero). Since $|g(z)| \leq 1$ and $\mathrm{ran}\,[\arccos] = [0,\pi]$, both trigonometric functions are nonnegative. So the second summand (without the minus) is always negative due to $p' \leq 0$. The overall expression is thus positive whenever $g' \geq 0$. But from Lemma 4 we know that $g' < 0$ can occur as well so let us assume that for the rest of the proof. For $h \overset{\mathrm{df}}{=} \arccos g$ we first observe

$$h' = -\frac{g'}{\sqrt{1-g^2}} \tag{27}$$

and so $h' > 0$. We now summon Lemma 5 and for it to be useful we show $\frac{\mathrm{d}\tau(z,2)}{\mathrm{d}z} \geq 0$. The case $n = 2$ is special since we can use the half-angle formula $\cos\frac{h}{2} = \sqrt{\frac{1+\cos h}{2}}$ (valid for $-\pi \leq h \leq \pi$) to be inserted into $\tau(z,2) = \sqrt{-p}\cos\frac{h}{2}$ and we get

$$\frac{\mathrm{d}\tau(z,2)}{\mathrm{d}z} = \frac{ph'\sin h - p'(1+\cos h)}{2\sqrt{-2p(1+\cos h)}} = \frac{-pg' - p'(1+g)}{2\sqrt{-2p(1+g)}} = -\frac{(p(1+g))'}{2\sqrt{-2p(1+g)}} \geq 0. \tag{28}$$

The inequality $(p(1+g))' \leq 0$ follows from $p(1+g)$ being monotone-decreasing since both p and $pg \approx q\sqrt{-3/p}$ are monotone-decreasing (from Lemma 3 we know that for $\varepsilon \leq 0$ the function $q \lesseqgtr 0$ is monotone-decreasing and $\sqrt{-3/p}$ as well and because $\min_{p_k,z}[\sqrt{-3/p}] = 3$ then $\sqrt{-3/p}$ merely "stretches" q). A sum of decreasing functions is decreasing which concludes the proof since according to Lemma 5 we have

$$t_0'\frac{\sqrt{3}}{2} \equiv \frac{\mathrm{d}\tau(z,3)}{\mathrm{d}z} > \frac{\mathrm{d}\tau(z,2)}{\mathrm{d}z} \geq 0.$$

■

Proposition 7. *The function t_2 is monotone-decreasing in $z \in (0,1)$ for $\varepsilon \leq 0$.*

Proof. Considering t_k in (18) as functions of p and q, it is known [28] that $t_2(p,q) = -t_0(p,-q)$. The mapping $q \mapsto -q$ changes the sign of g (and so of g' as well, see (22) and (24)). The proof of Proposition 6 then goes through in the same way as for $t_0(p,-q)$ since the trigonometric functions in (26) remain non-negative for $-g$ and the proof "covers" both cases $g' \geq 0$ and $g' < 0$. Hence, $t_0'(p,-q) > 0$ and we conclude that $t_2' < 0$. ∎

Corollary 8. *The function $t_0 + t_1$ is monotone-increasing in $z \in (0,1)$ for $\varepsilon \leq 0$.*

Proof. From Eq. (19) we find $t_0 + t_1 = -t_2$ and because t_2 is monotone-decreasing, its negative is monotone-increasing. ∎

Remark. Notice that we do not claim anything about the monotonocity of t_1 and indeed it in general does not hold.

Definition 1 ([31])**.** A function is called Schur-concave iff it is concave and symmetric.

Definition 2. Let $\vec{u}$ be an ℓ-tuple for a non-increasingly ordered sequence $u_0 \geq \ldots \geq u_{\ell-1}$ denoted as $u_k^{\downarrow}$ where $u_k \geq 0$. We say that $\vec{u}$ is majorized by $\vec{v}$ (written as $\vec{u} \prec \vec{v}$) iff

$$\sum_{k=0}^{m-1} u_k^{\downarrow} \leq \sum_{k=0}^{m-1} v_k^{\downarrow}, \tag{29}$$

$$\sum_{k=0}^{\ell-1} u_k = \sum_{k=0}^{\ell-1} v_k \tag{30}$$

is satisfied for $0 \leq m \leq \ell - 1$.

Theorem 9 ([31], Karamata [32])**.** *If a function $f(u)$ is concave then $f(\vec{u}) \stackrel{\text{df}}{=} \sum_k f(u_k)$ is Schur-concave and*

$$\vec{u} \prec \vec{v} \Rightarrow f(\vec{u}) \geq f(\vec{v}). \tag{31}$$

Remark. The function $f(u) = -u \log u$ is concave in $u \in (0,1)$ and therefore the Shannon entropy $S(\vec{u}) \stackrel{\text{df}}{=} -\sum_{k=0}^{K} u_k \log u_k$ is a Schur-concave function. For $K = 2$, we obtain the ternary Shannon entropy $h_3(\vec{u})$, Eq. (1).

Theorem 10. *The von Neumann entropy $H(\varpi)$ of density matrix* (10) *is a monotone-decreasing function of the overlap z as introduced in* (14)*, for all p_k and for all $0 \leq \vartheta \leq \pi/2$ corresponding to $\varepsilon \leq 0$ in* (17e)*.*

Proof. The eigenvalues of ϖ are $x_0 \geq x_1 \geq x_2$ and satisfy $\sum_k x_k = 1$. From the discussion below Eq. (19) we know when $x_2 \geq 0$ holds and so $(x_k)_{k=0,1,2}$ is a probability distribution. We will identify $\vec{u} = \vec{x}(z_1)$ and $\vec{v} = \vec{x}(z_2)$ where $0 < z_1 \leq z_2 < 1$. Then, Proposition 6 and Corollary 8 imply (29). Since $\sum_{k=0}^{2} u_k = \sum_{k=0}^{2} v_k = 1$ holds (so (30) is satisfied) we may write $\vec{u} \prec \vec{v}$. Following Theorem 9 we obtain $h_3(\vec{u}) \geq h_3(\vec{v})$ and $H(\varpi) \equiv h_3$ concludes the proof. ∎

A.3. **Concavity of the ternary Shannon entropy.** We now turn our attention to the concavity proof. We start by a proving the convexity of t_0 in (18) in z. To that end, we set $\tau(z,n) = \sqrt{-p}\cos\frac{h}{n}$ as in Lemma 5 and study the properties of its second derivative

$$\frac{\mathrm{d}^2\tau(z,n)}{\mathrm{d}z^2} = \frac{1}{4(-p)^{3/2}}\left(\cos\frac{h}{n}\,\frac{-4p^2h'^2 + n^2(2pp'' - p'^2)}{n^2} + \sin\frac{h}{n}\,\frac{-4p(ph')'}{n}\right). \tag{32}$$

To show $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2} \geq 0$ we have to separately investigate several different cases. We will need a couple of auxiliary results.

The proof of concavity will be presented for $\varepsilon \leq 0$. The next lemma is the only exception where ε is arbitrary.

Lemma 11. *We find*

$$\frac{-4p^2h'^2+n^2(2pp''-p'^2)}{n^2}\geq 0$$

for p in (16a)*, $h=\arccos g$ for g given by* (22) *and $n=3$.*

Proof. Using (22) in (27) the inequality becomes

$$27(3qp'-2pq')^2-9(4p^3+27q^2)(2pp''-p'^2)=(\alpha+\beta z^2)\,\nu_4(z)\leq 0, \tag{33}$$

where

$$\nu_4(z)=\beta(4\alpha^3+27\gamma^2)+z^2(8\alpha^2\beta^2+12\alpha\delta^2+18\beta\gamma\delta)+36z^3\alpha\delta\varepsilon+z^4\big(\alpha(4\beta^3+27\varepsilon^2)+3\beta\delta^2\big). \tag{34}$$

Since $\alpha+\beta z^2\equiv p\leq 0$ we have to show that $\nu_4(z)$ is nonnegative for $z\in(0,1)$. Theorem 2 reveals a lot of information about ν_4 through its coefficients. Depending on the sign of ε we find from (17)

monomial degree	*sign for* $\varepsilon<0$	*sign for* $\varepsilon>0$
4	+	+
3	−	+
2	±	±
0	+	+

No matter what the signs of $8\alpha^2\beta^2+12\alpha\delta^2+18\beta\gamma\delta$ and ε are there are always two sign changes. Hence $\nu_4(z)$ has two or none positive roots (for $\varepsilon=0$ the second row from the top is missing but still there can be two or none positive roots). Let's first assume $\varepsilon=-2p_0p_1p_2$ (its minimal value given by $\vartheta=0$). In this case we observe

$$\nu_4(1)=4\alpha^3\beta+8\alpha^2\beta^2+\alpha\big(4\beta^3+3(2\delta+3\varepsilon)^2\big)+3\beta(3\gamma+\delta)^2=0.$$

Since $\nu_4'(1)=0$ as well and $\nu_4''(1)=4\big(4\alpha^2\beta^2+3\alpha(4\beta^3+2\delta^2+18\delta\varepsilon+27\varepsilon^2)+9\beta\delta(\gamma+\delta)\big)\geq 0$ the point $z=1$ is a proper local minimum. The expression ν_4' is a cubic polynomial. Hence it has three roots: one of them is always zero and the greatest one always equals one (the one we found previously). The third root can be both positive or negative and whatever its position is we want to make sure that $\nu_4\geq 0$ in the interval $(0,1)$. Recall that according Theorem 2 there must be another positive root of ν_4. At first sight it seems impossible because if the third root of ν_4' is negative then the segment of ν_4 in $(0,1)$ must be decreasing ($\nu_4(0)=\beta(4\alpha^3+27\gamma^2)\geq 0$). Even if the third root of ν_4' lies in $(0,1)$ it can be either a *positive* local maximum or a stationary point. This is because we showed that $z=1$ is a local minimum, ν_4' has only three roots and again because of $\nu_4(0)\geq 0$. So where is the remaining positive root? The only possibility is that $z=1$ is a double root. Indeed, by calculating the discriminant [28] of ν_4 we find it to be equal to zero. This means that at least two roots coincide. Hence $\nu_4\geq 0$ holds for $\varepsilon=-2p_0p_1p_2$.

For $0<\vartheta\leq\pi/2$ the coefficients of the monomials of order 3 and 4 in (34) clearly increase and hence no new root can appear in the interval $(0,1)$. For $\pi/2<\vartheta\leq\pi$, the monomial order 4 coefficient decreases but $\varepsilon^2\propto\cos^2\vartheta$ is a symmetric function and we have seen that $\nu_4(z)$ had no positive root even when $\varepsilon<0$. But now $\varepsilon>0$ and so again there is no positive root which concludes the proof. ∎

Remark. The claim holds for any $n\geq 3$ but we do not make use of it.

Lemma 12. *The function $(pg')'(z)$ has a single positive root z^* whenever $\gamma(z)\geq 0$ and $(pg')'(z)\leq 0$ for $z\in(0,z^*)$.*

Proof. We calculate

$$(pg')'=\frac{3\sqrt{3}}{8}\frac{q(9p'^2-6pp'')+4p(-2p'q'+pq'')}{\sqrt{-p}p^2}. \tag{35}$$

The position of the positive roots is unaffected by the numerical prefactors or by the denominator. Hence, we rewrite only the numerator $\nu_2(z) = q(9p'^2 - 6pp'') + 4p(-2p'q' + pq'')$ in terms of Eqs. (16a) and (16b):

$$\nu_2(z) = -12\alpha\beta\varepsilon z^3 + \left(24\beta^2\gamma - 28\alpha\beta\delta\right)z^2 + 24\alpha^2\varepsilon z + 8\alpha^2\delta - 12\alpha\beta\gamma. \tag{36}$$

Given $\alpha, \beta, \delta, \varepsilon \leq 0$ and $\gamma > 0$ there is only one sign change if $8\alpha^2\delta - 12\alpha\beta\gamma \leq 0$. This is indeed satisfied for $\gamma > 0$. The observation

$$\lim_{z\to+\infty}[(pg')'] = +\infty$$

concludes the proof. ∎

Remark. In fact, we can refine the previous lemma by calculating

$$\lim_{z\to 0}[(pg')'] = -\frac{3}{2}\sqrt{3}\left(-\frac{1}{\alpha}\right)^{3/2}(2\alpha\delta - 3\beta\gamma) \leq 0$$

and expressing $\nu_2(z)$ with the help of (17) and $\sum_i p_i = 1$ as

$$\nu_2(1) = \frac{8}{9}\left(p_0^4 + 2p_0^3(-1+p_1) + (-1+p_1)^2p_1^2 + p_0p_1(-1-p_1+2p_1^2) + p_0^2(1-p_1+3p_1^2)\right) \geq 0. \tag{37}$$

Therefore, $z^* \in (0,1)$. The minimum on the RHS is achieved for $p_0 = p_1 = p_2 = 1/3$.

Lemma 13. *The function $(ph')'(z)$ has a single positive root for $z \in (0,1)$ whenever $\gamma \geq 0$ and for all $\varepsilon \leq 0$.*

Proof. We write

$$(ph')' = -\frac{gpg' + (1-g^2)(pg')'}{(1-g^2)^{3/2}} \tag{38}$$

and after inserting Eqs. (24), (22) and

$$g''(z) = \frac{3\sqrt{3}\left(4p(pq'' - 3p'q') + 3q(5p'^2 - 2pp'')\right)}{8(-p)^{-3/2}p^5} \tag{39}$$

we get an expression whose numerator reads

$$\nu_5 = -81q^3p'' + 54q^2\left(p'q' + pq''\right) + q\left(-12p^3p'' + 18p^2p'^2 - 54pq'^2\right) + 8p^4q'' - 16p^3p'q' \tag{40}$$

and whose denominator is negative in $(0,1)$. By inserting Eqs. (16) we get a daunting polynomial of degree seven:

$$\begin{aligned}\nu_5 = {} & z^7\left(-24\alpha\beta^3\varepsilon - 162\alpha\varepsilon^3 - 54\beta\delta^2\varepsilon\right) + z^6\left(-56\alpha\beta^3\delta - 378\alpha\delta\varepsilon^2 + 48\beta^4\gamma + 324\beta\gamma\varepsilon^2 - 54\beta\delta^3\right)\\ & + z^5\left(324\beta\gamma\delta\varepsilon - 324\alpha\delta^2\varepsilon\right) + z^4\left(-96\alpha^2\beta^2\delta + 72\alpha\beta^3\gamma + 162\alpha\gamma\varepsilon^2 - 108\alpha\delta^3 - 54\beta\gamma\delta^2\right)\\ & + z^3\left(72\alpha^3\beta\varepsilon + 216\alpha\gamma\delta\varepsilon + 162\beta\gamma^2\varepsilon\right) + z^2\left(-24\alpha^3\beta\delta - 162\beta\gamma^2\delta\right) + z\left(48\alpha^4\varepsilon + 324\alpha\gamma^2\varepsilon\right)\\ & + 16\alpha^4\delta - 24\alpha^3\beta\gamma + 108\alpha\gamma^2\delta - 162\beta\gamma^3.\end{aligned} \tag{41}$$

Let us first assume $\varepsilon = -2p_0p_1p_2$ which is the minimal value given by $\vartheta = 0$. Then, there is an inflection point at $z = 1$: $\nu_5'(1) = \nu_5''(1) = 0$. This indicates a triple root (corroborated by the zero discriminant indicating multiple roots) and so

$$\nu_5 = f_4(z-1)^3, \tag{42}$$

where $f_4 = \sum_{i=0}^4 a_i z^i$. By comparing the coefficients with (41) we deduce the coefficient a_i and get

$$\begin{aligned}f_4 = {} & -6z^4\varepsilon\left(4\alpha\beta^3 + 27\alpha\varepsilon^2 + 9\beta\delta^2\right)\\ & + 2z^3\left(-4\alpha\beta^3(7\delta+9\varepsilon) - 27\alpha\varepsilon^2(7\delta+9\varepsilon) + 24\beta^4\gamma - 27\beta(-6\gamma\varepsilon^2 + \delta^3 + 3\delta^2\varepsilon)\right)\\ & - 6z^2(4\alpha^3 + 27\gamma^2)(\alpha(4\delta+6\varepsilon) - \beta(6\gamma+\delta))\\ & - 6z(4\alpha^3 + 27\gamma^2)(2\alpha(\delta+\varepsilon) - 3\beta\gamma)\end{aligned}$$

$$-2(4\alpha^3+27\gamma^2)(2\alpha\delta-3\beta\gamma). \tag{43}$$

With the help of the following table

monomial degree	*sign*
4	−
3	?
2	+
1	+
0	+

Theorem 2 reveals that there is only one positive root. Note that the degree three coefficient of (43) seems too complicated to analytically deduce its sign but our ignorance does not affect the number of sign variations. Now we show that by for any $\varepsilon \leq 0$ the single root shifts and the inflection disappears. We inspect the coefficients of (41) where ε appears. Considering $\gamma \geq 0$, the ones accompanying the monomials z, z^3 and z^5 satisfy

$$48\alpha^4\varepsilon + 324\alpha\gamma^2\varepsilon \leq 0, \tag{44a}$$

$$72\alpha^3\beta\varepsilon + 216\alpha\gamma\delta\varepsilon + 162\beta\gamma^2\varepsilon \leq 0, \tag{44b}$$

$$324\beta\gamma\delta\varepsilon - 324\alpha\delta^2\varepsilon \leq 0. \tag{44c}$$

Hence an increase of ε from its minimal values to any $\varepsilon \leq 0$ will not add a new root in $(0,1)$. Similarly for the z^7 coefficient $\varepsilon(-24\alpha\beta^3 - 162\alpha\varepsilon^2 - 54\beta\delta^2)$ which, due to

$$-24\alpha\beta^3 - 162\alpha\varepsilon^2 - 54\beta\delta^2 \geq 0 \tag{45}$$

(valid only for the minimal ε), is an increasing function of $\varepsilon \leq 0$. This is because $\alpha \leq 0$ and so (45) is a decreasing function of $\varepsilon \leq 0$ ((45) can become negative). Even if (45) does not change the sign, the z^7 coefficient will always be greater than the one with the minimal ε because the overall multiplication by $\varepsilon \leq 0$ swaps the sign (and so the order). Finally, the z^4 and z^6 coefficients contain negative factors accompanying ε^2 (recall $\alpha, \beta, \delta \leq 0$ and $\gamma \geq 0$ by assumption). Hence, as ε^2 decreases, it effectively increases the coefficients of z^4 and z^6. We can conclude that no new root for $z \in (0,1)$ appears for $\varepsilon \leq 0$. ■

Proposition 14. *The following relations hold:*

$$q \geq 0 \overset{\text{Lemma 4}}{\Longleftrightarrow} g \leq 0 \overset{\text{(i)}}{\Longrightarrow} (pg')' \leq 0$$
$$\Big\Downarrow \text{(ii)}$$
$$(ph')' \geq 0$$

Proof.
(i) The sought after implication can be reformulated in the language of Lemma 3 and 12 as $z^{\#} \leq z^*$ since $q \geq 0$ in $(0, z^{\#})$ and $(pg')' \leq 0$ in $(0, z^*)$. We proceed by setting $q = 0$ and, conveniently, the numerator of (35) simplifies to

$$\nu_2(z)\big|_{q=0} \propto -2p'q' + pq'' = 6\beta\varepsilon z^3 + 6\beta\delta z^2 - 6\alpha\varepsilon z - 2\alpha\delta. \tag{46}$$

We ignored the factor $4p$ as it does not affect the position of the roots for $q = 0$. In principle we just need to compare the position of the roots for the polynomials q and $\nu_2(z)|_{q=0}$. However, they are both cubic polynomials and the roots' form is too complicated to determine their relation. It follows from Lemma 3, Lemma 12 and the previous remark that the polynomials intersect at a single point in the interval $(z^{\#}, z^*) \subset (0,1)$ and, in addition, the position of the intersection point above or below the x axis informs us about the relation of the two roots. It would not be very helpful to set $q = \nu_2(z)|_{q=0}$ and solve for z, though. It again

leads to a cubic equation and we face a similar problem as before. The trick we will use is the following transformation:

$$q(z) \mapsto \tilde{q}(z) = -6\beta q = -6\beta\gamma - 6\beta\delta z^2 - 6\beta\varepsilon z^3. \tag{47}$$

The new function $\tilde{q}(z)$ has the same properties as $q(z)$ uncovered in Lemma 4 (the minus sign reverses the negative sign of β). By setting $\tilde{q} = \nu_2(z)|_{q=0}$ we obtain another cubic equation

$$\tilde{\mu}(z) = 2\mu(z) = 2\big(6\beta\varepsilon z^3 + 6\beta\delta z^2 - 3\alpha\varepsilon z - \alpha\delta + 3\beta\gamma\big) = 0. \tag{48}$$

Its (single) root in $(0,1)$ reveals where $\tilde{q}$ and $\nu_2(z)|_{q=0}$ intersect but that also means that by comparing the roots' position of μ (or $\tilde{\mu}$) with $\nu_2(z)|_{q=0}$ in the interval $(0,1)$ we learn whether $\tilde{q}$ and $\nu_2(z)|_{q=0}$ intersected above or below the x axis. So by setting $\mu(z) = \nu_2(z)|_{q=0}$ we crucially get a linear equation whose solution reads

$$z_\ell = \frac{-\alpha\delta - 3\beta\gamma}{3\alpha\varepsilon}. \tag{49}$$

By inserting it back to $\nu_2(z)|_{q=0}$ we get

$$\nu_2(z_\ell)|_{q=0} = \frac{2\beta\left(\alpha^3(27\gamma\varepsilon^2 + 2\delta^3) + 9\alpha^2\beta\gamma\delta^2 - 27\beta^3\gamma^3\right)}{9\alpha^3\varepsilon^2}. \tag{50}$$

It remains to show $\nu_2(z_\ell)|_{q=0} \leq 0$ in order to prove $z^\# \leq z^*$. Since $\alpha, \beta \leq 0$ it suffices to show that $\nu_3(z) = \alpha^3\left(27\gamma\varepsilon^2 + 2\delta^3\right) + 9\alpha^2\beta\gamma\delta^2 - 27\beta^3\gamma^3 \leq 0$. Using (17) and $\sum_i p_i = 1$ we find $\nu_3(z) \overset{\text{df}}{=} \frac{1}{27} f_1 f_2$ where

$$f_1 = \left(p_0 + 2p_0^3 + 3p_0^2(-1+p_1) - 3p_0p_1^2 + p_1(-1+3p_1-2p_1^2)\right)^2, \tag{51a}$$

$$\begin{aligned} f_2 = {} & 4p_0^6 + 12p_0^5(-1+p_1) + p_0^4(13 - 27p_1 + 24p_1^2) + p_0^3(-6 + 20p_1 - 42p_1^2 + 28p_1^3) \\ & + p_0^2(1 - 5p_1 + 24p_1^2 - 42p_1^3 + 24p_1^4) + p_1^2(1 - 3p_1 + 2p_1^2)^2 + p_0p_1^2(-5 + 20p_1 - 27p_1^2 + 12p_1^3). \end{aligned} \tag{51b}$$

Since $f_1 \geq 0$, we have to show $f_2 \leq 0$. We reduced the problem to a task analytically solvable by Mathematica. Indeed, we find $\max[f_2] = 0$ subject to $\gamma \geq 0$ and $0 \leq z_\ell \leq 1$. The first inequality is a necessary condition for the initial assumption $q \geq 0$ in $z \in (0, z^\#)$ via Lemma 3. Achieving the maximum implies $\nu_3 = 0$ which in turn implies $\nu_2(z_\ell)|_{q=0} = 0$ (from (50)) and so $\mu(z_\ell) = 0$ (see above (49)). This finally leads to $\nu_2(z_\ell)|_{q=0} = \tilde{q}(z_\ell) = 0 = q(z_\ell)$ and so $z_\ell^\# = z_\ell^*$ which concludes the proof.

(ii) Assuming $\gamma \geq 0$ as a necessary condition to the current case of interest $q \geq 0$ ($g \leq 0$) for $z \in (0, z^\#)$ (see Lemma 3 and 4) we find $\nu_5(0) = 2(4\alpha^3 + 27\gamma^2)(2\alpha\delta - 3\beta\gamma) \leq 0$ (the different sign in the bottom of the table on page 19 is due to f_4 being multiplied by $(z-1)^3$) and so $(ph')'(0) \geq 0$. This is because $(ph')' \propto -\nu_5$. We also notice that $(ph')' \geq 0$ for $g = 0$. This follows from Eq. (38) implying that in this case $(ph')' = -(pg')'$. But from item (i) of the current lemma we know that $(pg')' \leq 0$ for $g \leq 0$. Inevitably, the only positive root of $(ph')'$ occurs for $g \geq 0$, that is, as long as $g \leq 0$ we get $(ph')' \geq 0$ as we wanted to show. ■

Remark. Note that $(ph')'(0) \geq 0$ does not contradict $g'(0) = 0$ we found in Lemma 4. This could be hastily concluded by looking at Eq. (27). But it is true only if $g' = 0$ and $\sqrt{1-g^2} \neq 0$. In many cases it is found, however, that for $z = 0$ one gets $g' = \sqrt{1-g^2} = 0$ and $\lim_{z\to 0^+} h' \neq 0$.

Lemma 15. *Let* $h = \arccos g$ *and* $(ph')' \leq 0$. *Then*

$$\cos\frac{h}{2}\,\frac{-4p^2h'^2 + 3^2(2pp'' - p'^2)}{4\times 3^2(-p)^{3/2}} + \sin\frac{h}{2}\,\frac{-p(ph')'}{3(-p)^{3/2}} \geq 0 \tag{52}$$

whenever $g \geq 0$ *and for all* $\varepsilon \leq 0$.

Remark. The expression resembles part of Eq. (32). However, notice $n = 2$ in the trigonometric functions and $n = 3$ elsewhere.

Proof. Given $\tau(z,n)=\sqrt{-p}\cos\frac{\arccos g}{n}$, a straightforward calculation reveals

$$\frac{\mathrm{d}^2\tau(z,n)}{\mathrm{d}z^2}$$
$$=\cos\frac{\arccos g}{n}\,\frac{4p^2g'^2+n^2(-1+g^2)(2pp''-p'^2)}{4n^2(1-g^2)\sqrt{-p}p}+\sin\frac{\arccos g}{n}\,\frac{-pgg'^2+(-1+g^2)(pg')'}{n\sqrt{1-g^2}(1-g^2)\sqrt{-p}}. \tag{53}$$

We set $n=2$ in the trigonometric functions and $n=3$ elsewhere at which point (53) becomes the studied expression (Eq. (52)) by virtue of (27). We multiply both summands by $p\sqrt{-p}(1-g^2)\le 0$ and use $\cos\frac{x}{2}=\sqrt{\frac{1+\cos x}{2}}$ $(-\pi\le x\le\pi)$ and $\sin\frac{x}{2}=\sqrt{\frac{1-\cos x}{2}}$ $(0\le x\le 2\pi)$. We got the reverse inequality to prove

$$\kappa=\frac{4}{9}p^2g'^2(1-2g)+(-1+g^2)\Big((1+g)(2pp''-p'^2)+\frac{4}{3}p(pg')'\Big)\le 0. \tag{54}$$

For this purpose, we use Eq. (22) and deduce

$$\kappa=\frac{1}{p^2}\left(-\nu_4+f_3\frac{1}{2}\sqrt{\frac{3}{-p}}\right), \tag{55}$$

where ν_4 is given by (34) and

$$f_3(q)=-27q^2q''+q(-6pp'^2+18q'^2)-4p^2(pq''-2p'q'). \tag{56}$$

Since in Lemma 11 we proved $\nu_4>0$ we only have to show $f_3\le 0$ for $\kappa\le 0$ to hold. The inequality $f_3\le 0$ does not hold in general, however. That is not a problem as long as we show that it holds for $(ph')'\le 0$. First we assume $\gamma\ge 0$. By contrapositive of Proposition 14 (ii) we know

$$(ph')'\le 0\Rightarrow g\ge 0\Leftrightarrow q\le 0. \tag{57}$$

Hence we need to show $q\le 0\Rightarrow f_3\le 0$. For $q=0$ the function f_3 becomes $-4p^2(pq''-2p'q')$ which is proportional to $\nu_2(z_\ell)|_{q=0}$ (see (46)). Its relation to q was studied in Proposition 14 and we found $\nu_2(z_\ell)|_{q=0}=q(z_\ell)=0$ for z_ℓ given by (49). Therefore, $f_3(0)$=0. Then, as demanded in (57), for any $q<0$ we get $f_3(q)<0$ since Eq. (56) is an increasing function of q. This follows from $q''=6\varepsilon z\le 0$ (valid for $\varepsilon\le 0$) and $-6pp'^2+18q'^2\ge 0$ by looking at Eqs. (16) and (17). For $\gamma<0$ we know from Lemma 4 that $g>0$ $(q<0)$ always holds independently on the sign of $(ph')'$. Therefore $f_3<0$ and the proof goes as outlined above. ∎

Proposition 16. *The function t_0 is convex in $z\in(0,1)$.*

Proof. The function t_0 is proportional to $\tau(z,3)=\sqrt{-p}\cos\frac{\arccos g}{3}$ and so we will focus on proving $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2}\ge 0$ given by (32) for $n=3$. In Lemma 11 we presented a proof of nonnegativity of a fraction multiplying $\cos\frac{\arccos g}{3}$. Both $\cos\frac{\arccos g}{3}\ge 0$ and $\sin\frac{\arccos g}{3}\ge 0$ for $|g(z)|\le 1$ and so $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2}\ge 0$ holds whenever $(ph')'\ge 0$. For the rest of the proof assume $(ph')'<0$. We will construct a lower bound on $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2}$ and show it to be nonnegative. To this end, we summon the inequalities $\sin\frac{h}{n}>\sin\frac{h}{n+1}$ and $\cos\frac{h}{n}<\cos\frac{h}{n+1}$ (valid for $n\ge 2$ and visible in Fig. 4 for $n=2,3$) and substitute $\sin\frac{h}{3}$ and $\cos\frac{h}{3}$ by $\sin\frac{h}{2}$ and $\cos\frac{h}{2}$, respectively. This is a lower bound on $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2}$ and the quantity was proved to be nonnegative in Lemma 15. This concludes the proof. ∎

Remark. The fact that $g\not<0$ for $(ph')'\le 0$ is crucial. First of all, it is not clear how to prove the validity of $\frac{\mathrm{d}^2\tau(z,3)}{\mathrm{d}z^2}\ge 0$ given by (32) for $(ph')'\le 0$. But even the only manageable lower bound, Eq. (52), is in some cases not good enough (i.e., non-negative) for $g<0$ and $(ph')'\le 0$.

Corollary 17. *The function t_2 is concave in $z\in(0,1)$.*

Proof. Similarly to Proposition 7 we will make use of $t_2(p,q) = -t_0(p,-q)$. The mapping $q \mapsto -q$ changes the sign of g, g' and h' (see Eqs. (22), (24) and (27)). Looking at Eq. (32), we notice that for $n \geq 2$ the sign of the trigonometric functions remains unaffected (see Fig. 4 for $n = 2, 3$). Similarly for the expression from Lemma 11 coming from (32). The sign change of q also swaps the sign of $(ph')'$ in (32). This is because $(ph')' = p'h' + ph''$ together with

$$h'' = -\frac{g g'^2 + (1-g^2)g''}{(1-g^2)^{3/2}}$$

taking into account that g'' changes the sign upon $q \mapsto -q$. But both cases ($(ph')' \geq 0$ and $(ph')' < 0$) have been separately investigated in Proposition 16. So we conclude $t_0''(p,-q) \geq 0$ and so $t_2''(p,q) \leq 0$. ∎

Lemma 18. *Let $(u_i)_{i=0}^2$ be a probability distribution function and h_3 the ternary Shannon entropy defined in* (1). *Then h_3 is concave in $(0,1) \times (0,1) \subset \mathbb{R}^2$ and for a fixed $u_2 \in (0,1)$ the function h_3 is monotone increasing (decreasing) for $u_1 < (1-u_2)/2$ ($u_1 > (1-u_2)/2$).*

Proof. The Hessian matrix

$$\mathsf{H}(h_3(\vec{u})) = \begin{bmatrix} -\frac{1}{1-u_1-u_2} - \frac{1}{u_1} & -\frac{1}{1-u_1-u_2} \\ -\frac{1}{1-u_1-u_2} & -\frac{1}{1-u_1-u_2} - \frac{1}{u_2} \end{bmatrix} \tag{58}$$

is negative definite since $\operatorname{Tr}\mathsf{H} < 0$ and $\det\mathsf{H} = 1/(u_0u_1) + 1/(u_0u_2) + 1/(u_1u_2) > 0$. The concavity of h_3 follows from the positivity of the characteristic polynomial throughout the interval $(u_0, u_1) \in (0,1) \times (0,1)$. We now fix the value of u_2 and the equation $\partial h_3/\partial u_1 = 0$ is satisfied for $u_1 = (1-u_2)/2$. Thanks to the previously proved concavity, it is a local maximum for every $u_2 \in (0,1)$ and thus $(1-u_2)/2$ defines a one-parameter family of local maxima for h_3. ∎

Remark. Due to the symmetry between u_2 and u_1 in (1) we may fix u_1 and get a family of local maxima given by $-2u_2 + 1$. The global maximum of h_3 at $(u_2, u_1) = (1/3, 1/3)$ lies in the intersection of $(1-u_2)/2$ and $-2u_2 + 1$. The situation is illustrated in Fig. 5.

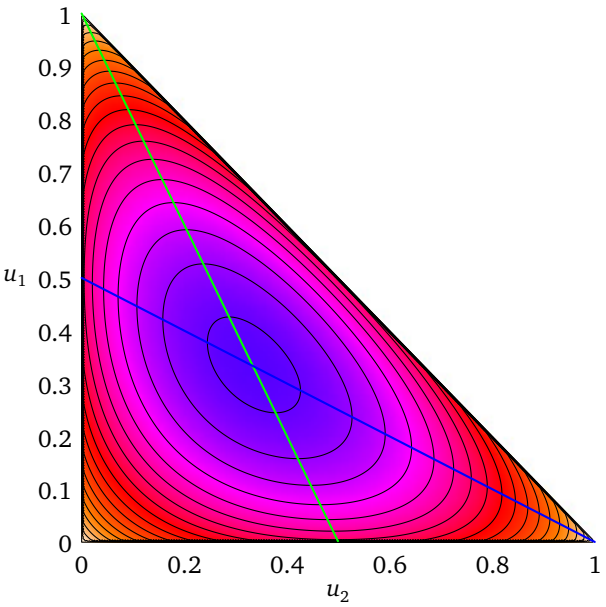

FIGURE 5. The ternary Shannon entropy Eq. (1) is shown. The blue line depicts $u_1 = (1-u_2)/2$ while the green one is the plot of $u_1 = -2u_2 + 1$.

Theorem 19. *The von Neumann entropy $H(\varpi)$ of density matrix* (10) *is a concave function of the overlap z as introduced in* (14)*, for all p_k and for all $0 \leq \vartheta \leq \pi/2$ corresponding to $\varepsilon \leq 0$ in* (17e)*.*

Proof. The von Neumann entropy $H(\varpi)$ is given by $h_3(\vec{x}(z))$ in (1) where $x_k = t_k + 1/3$ come from Eq. (18). Taking into account $\sum_{i=0}^{2} x_i = 1$ we get $\vec{x} : \mathbb{R} \mapsto \mathbb{R}^2$ and the investigated expression $\frac{\mathrm{d}^2 h_3}{\mathrm{d}z^2}$ will be written using the following notation: We define

$$\mathsf{x}' = \begin{bmatrix} x_1' \\ x_2' \end{bmatrix} \tag{59a}$$

$$\mathsf{x}'' = \begin{bmatrix} x_1'' \\ x_2'' \end{bmatrix} \tag{59b}$$

and

$$\mathsf{h}_3' = \begin{bmatrix} \frac{\partial h_3}{\partial x_1} \\ \frac{\partial h_3}{\partial x_2} \end{bmatrix}. \tag{60}$$

Using the chain rule, the second derivative can be succinctly expressed as

$$\frac{\mathrm{d}^2 h_3}{\mathrm{d}z^2} = (\mathsf{x}')^\top \mathsf{H}(h_3(\vec{x}))\mathsf{x}' + (\mathsf{h}_3')^\top \mathsf{x}'', \tag{61}$$

where $\top$ denotes transposition and the dot (matrix) product is implied. Hessian Eq. (58) is negative definite according to Lemma 18 and so the first summand is negative for any x'. In order for the second summand to be nonpositive as well, one possibility is when either the functions x_1 and x_2 are concave and the two components of h_3 nondecreasing or x_1, x_2 convex and h_3 entry-wise nonincreasing. We proved $x_2'' \leq 0$ in Corollary 17 but said nothing about the concavity of x_1. As a matter of fact, it is incomparably more difficult to prove $x_1'' \leq 0$ in spite of the overwhelming numerical evidence. The same numerics suggests that there is a whole class of input probabilities p_k for which $x_1'' = 0$. So no 'simple' bounds like those leading to Proposition 16 exist. But there is a third possibility of how to make the second summand in (61) negative and it is the combination of the two previous cases. We know that $x_0'' \geq 0$ from Proposition 16 and $x_2'' \leq 0$ from Corollary 17. The second summand (61) will be negative if we take x_0 instead of x_1 in Eqs. (59) and (60) and show $\frac{\partial h_3}{\partial x_0} \leq 0$ and $\frac{\partial h_3}{\partial x_2} \geq 0$. Note that the Hessian remains negative definite:

$$\mathsf{H}(h_3(\vec{x})) = \begin{bmatrix} -\frac{1}{1-x_0-x_2} - \frac{1}{x_0} & -\frac{1}{1-x_0-x_2} \\ -\frac{1}{1-x_0-x_2} & -\frac{1}{1-x_0-x_2} - \frac{1}{x_2} \end{bmatrix}. \tag{62}$$

Hence, in spite of the components of x' to have different signs (see Propositions 6 and 7), the summand is negative. Also note that we are proving the properties of the same ternary entropy (1) since it is equivalent to

$$h_3(\vec{x}(z)) = -x_0 \log x_0 - x_2 \log x_2 - (1 - x_0 - x_2) \log [1 - x_0 - x_2]. \tag{63}$$

Lemma 18 informs us that $\frac{\partial h_3}{\partial x_2} \geq 0$ and $x_2'' \leq 0$ together with $\frac{\partial h_3}{\partial x_0} \leq 0$ and $x_0'' \geq 0$ is satisfied in the domain's subset delimited by the blue line ($x_0 \geq (1 - x_2)/2$) and the green line ($x_0 \leq -2x_2 + 1$) depicted in Fig. 5 if instead of u_2, u_1 we have x_2, x_0 (resulting in the same figure). But it turns out that this is precisely the range of $\vec{x}$ represented by x_0, x_2. To this end, consider the basic property of the cubic roots [28] $t_0 \geq t_1 \geq t_2$ that becomes $x_0 \geq x_1 \geq x_2 \geq 0$ for the eigenvalues of ϖ. First, using $x_0 \geq x_1$ we write

$$\begin{aligned} x_0 &\geq \frac{x_0 + x_1}{2} \\ &= \frac{x_0 + x_1 + x_2 - x_2}{2} \\ &= \frac{1 - x_2}{2}, \end{aligned} \tag{64}$$

where in the second row we used the normalization condition $\sum_i x_i = 1$. The last equality leads to one of the desired bounds. For the second bound we start with $x_1 \geq x_2$ to write

$$\begin{aligned} x_0 &\leq x_0 - x_2 + x_1 \\ &= -2x_2 + x_0 + x_1 + x_2 \\ &= -2x_2 + 1, \end{aligned} \tag{65}$$

where the last line provides the other inequality we were looking for. Hence $(\mathsf{h}_3')^\top \mathsf{x}'' \leq 0$ resulting in $\frac{\mathrm{d}^2 h_3}{\mathrm{d}z^2} \leq 0$. ■

References

[1] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301, 2009.

[2] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8:595, 2014.

[3] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. *National Institute of Standards and Technology Internal Report 8105*, 2016.

[4] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621, 2012.

[5] Eleni Diamanti and Anthony Leverrier. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy*, 17(9):6072–6092, 2015.

[6] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, 2017.

[7] Raúl García-Patrón, Stefano Pirandola, Seth Lloyd, and Jeffrey H. Shapiro. Reverse coherent information. *Physical Review Letters*, 102:210501, 2009.

[8] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security. *Journal of Cryptology*, 18:133, 2005.

[9] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, 2005.

[10] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94:230503, 2005.

[11] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307, 2009.

[12] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102:180504, 2009.

[13] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum key distribution protocols with a discrete modulation. *arXiv:1002.4083*, 2010.

[14] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Physical Review A*, 83:042312, 2011.

[15] Denis Sych and Gerd Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12:053019, 2010.

[16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[17] Kamil Brádler, Mohammad Mirhosseini, Robert Fickler, Anne Broadbent, and Robert Boyd. Finite-key security analysis for multilevel quantum key distribution. *New Journal of Physics*, 18(7):073030, 2016.
[18] Ryo Namiki and Takuya Hirano. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Physical Review A*, 74(3):032302, 2006.
[19] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *Information Theory, IEEE Transactions on*, 51(1):44–55, 2005.
[20] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. 461(2053):207–235, 2005.
[21] Barbara Kraus, Cyril Branciard, and Renato Renner. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Physical Review A*, 75(1):012316, 2007.
[22] Richard Jozsa and Jürgen Schlienz. Distinguishability of states and von Neumann entropy. *Physical Review A*, 62(1):012301, 2000.
[23] Riccardo Laurenza, Samuel L Braunstein, and Stefano Pirandola. Finite-resource teleportation stretching for continuous-variable systems. *arXiv preprint arXiv:1706.06065*, 2017.
[24] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108:130502, 2012.
[25] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108:130503, 2012.
[26] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L Braunstein, Seth Lloyd, Tobias Gehring, Christian S Jacobsen, and Ulrik L Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9(6):397–402, 2015.
[27] Sudhir Ghorpade and Balmohan Vishnu Limaye. *A course in multivariable calculus and analysis*. Springer, 2010.
[28] B L van der Waerden. *Algebra Vol. 1*. 7th edition, 1970.
[29] Bruce Meserve. *Fundamental concepts of algebra*. Dover, 1982.
[30] Peter Henrici. *Applied and computational complex analysis. Volume I*. Wiley-Interscience, 1974.
[31] A Wayne Roberts and Dale Varberg. *Convex functions*, volume 57. Academic Press, 1974.
[32] Jovan Karamata. Sur une inégalité relative aux fonctions convexes. *Publications de l'Institut mathematique*, 1(1):145–147, 1932.