scientific reports

Check for updates

OPEN

Combating errors in quantum communication: an integrated approach

Rajni Bala✉, Sooryansh Asthana & V. Ravishankar

Near-term quantum communication protocols suffer inevitably from channel noises, whose alleviation has been mostly attempted with resources such as multiparty entanglement or sophisticated experimental techniques. Generation of multiparty higher dimensional entanglement is not easy. This calls for exploring realistic solutions which are implementable with current devices. Motivated particularly by the difficulty in generation of multiparty entangled states, in this paper, we have investigated error-free information transfer with minimal requirements. For this, we have proposed a new information encoding scheme for communication purposes. The encoding scheme is based on the fact that most noisy channels leave some quantities invariant. Armed with this fact, we encode information in these invariants. These invariants are functions of expectation values of operators. This information passes through the noisy channel unchanged. Pertinently, this approach is not in conflict with other existing error correction schemes. In fact, we have shown how standard quantum error-correcting codes emerge if suitable restrictions are imposed on the choices of logical basis states. As applications, for illustration, we propose a quantum key distribution protocol and an error-immune information transfer protocol.

The last three decades have witnessed a burgeoning interest in study of quantum communication, quantum computation and, quantum search, to name a few[1–5]. The interest largely owes to a promise of outperforming their classical counterparts, or proposals of altogether novel applications not possible with purely classical resources. However, their implementations inevitably demand generation and transfer of quantum states, applications of various quantum gates and measurements, all within their coherence times.

Noise unveils itself as a major impediment in meeting with these demands[6]. In order to mitigate the effect of noise on quantum protocols, quantum error correcting codes have already been proposed in the seminal work of Shor and Steane[7,8]. In fact, various representations of the Knill-Laflamme condition[9] have been obtained, which serve as error-correcting codes for different noisy models[10–12]. These codes, in turn, require multiparty entanglement, which is a costly resource, as is reflected in the experimental challenges faced in its generation[13–15]. In fact, for orbital angular momentum of light, which is arguably at the forefront of realisation of quantum hardware for communication protocols, there is an upper limit beyond which higher dimensional multiparty entanglement cannot be generated as yet[16]. As a consequence, in spite of having a large number of very promising and elegant quantum information-theoretic protocols, their experimental implementations, those too at a scalable stage, still pose a challenge[17–19]. It has been evidenced in, for example, quantum error correction assisted quantum key distribution with higher dimensional systems[17]. These observations have been succinctly encapsulated in the phrase 'noisy-intermediate-scale-quantum computation', coined by John Preskill[20] for the current stage of quantum information processing. In fact, these observations have led to several protocols and error correction schemes that are realisable with current technologies and near-term quantum devices[21]. Examples include approximate error-correcting codes[22], error-avoiding codes[23], probabilistic error correction[24] and error-suppression techniques[25], quantum error mitigation techniques[26,27]. Almost all these schemes for combating errors aim at retrieving the quantum state at the end of a noisy channel. This demand either imposes restrictions on the choice of basis states or requires repeated interventions at appropriate times, making these techniques resource costly. Recently, recovery of noise-free observables has also been studied by employing the results of slightly different experiments[27].

This prompts us to ask a question: how do we find error-combating techniques without putting any restriction on the nature of states (i.e., without using multiparty entanglement)? That is to say, we look for resource-friendly error combating techniques for protocols that aim at solely information transfer. The answer to the above question is embedded in a new proposal of modifications of encoding and decoding procedures. For, unlike classical

Department of Physics, Indian Institute of Technology Delhi, New Delhi 110016, India. ✉email: Rajni.Bala@physics.iitd.ac.in

communication, in which bits are synonymous with the information they carry, their quantum counterparts, *viz.*, qubits carry information in sesquilinear functions of states of these qubits. This fact indicates that information can also be encoded in expectation values of different operators which are indeed sesquilinear functions of states. Since individual outcomes of different operators are random, their concatenated strings are also random. As a result, their collective property, *viz.*, average is also random. This randomness in expectation values of different operators legitimises their employment as information carriers. By extension, those combinations of expectation values that remain invariant under a noisy evolution of a state emerge as natural candidates for transferring information in an error-immune manner.

In this work, we systematically find out the quantities that remain invariant under different noisy evolutions. These invariants involve combinations of expectation values of the operators that get rescaled in a compensatory manner under a noisy evolution of a state. The invariants may be categorised into three different families—(1) in the first family, they are simply the expectation values of operators, (2) the second family consists of ratios of expectation values of two operators, and, (3) the third family consists of quantities that are combinations of expectation values of operators—not necessarily scaled by the same factor. The advantage in this approach is that with almost any state, one gets a few quantities which remain unchanged during the noisy evolution.

In this scheme, quantumness is manifested in two ways—(a) in non-commuting nature of observables whose expectation values are involved, (b) in non-orthogonality of states employed for quantum communication. These features allow for (1) transfer of more information and, (2) for security against eavesdropping in secure quantum communication protocols. As concrete applications, we propose two quantum communication protocols falling in the two categories—(1) quantum communication without security against eavesdropping, (2) secure quantum communication. These protocols act as templates for a large family of other protocols, which can be proposed for error-free information transfer through noisy channels in several other scenarios.

At this juncture, we wish to point out that this approach is not orthogonal to the conventional quantum error-correcting codes (QECC). Contrarily, we show that if the basis states are chosen to satisfy the celebrated Knill-Laflamme condition, the conventional error-correction codes result. Since the latter have been thoroughly studied, we do not elaborate on them in this work except for showing an interrelation between QECC and the approach proposed here. What this study serves to unravel is a nice interplay of consumption of resources in the techniques of error mitigation and consequent retrieval of information or state.

Many proposals and techniques exist for efficient characterisation of dephasing, depolarisation, and amplitude damping channels[28–33]. In a recent work[34], an efficient channel characterisation for higher-dimensional system is presented. Additionally, effect of these noisy channels on various communication protocols such as quantum key distribution is studied[35,36]. However, all error combating techniques such as quantum error correcting codes, decoherence free subspaces, dynamical decoupling including ours assume the knowledge of channel a priori. Recently, in[37], using the data furnished by simulation and experimental studies, we have characterised the channel and identified invariants for the same. These studies also make use of several measurements for characterisation of the channel[38–40]. A unified approach for both channel characterisation and error mitigation is of great interest for future study. In this work, we have considered those noisy channels which are usually considered in various communication protocols.

The plan of the paper is as follows: in "Notation", we setup the notation to be used throughout the paper. In "Idea advanced in this work", we elucidate the information encoding scheme proposed in this work with an example. In "The formalism", the central result of the paper, i.e., the formalism to obtain invariants for various noisy channels is presented. The information encoded in these invariants can be transferred without any error. In "Information transfer with quNits", invariants are identified for various noisy channels of a qu*N*it. As an application of the encoding scheme, in "Application: QKD employing qubits in a depolarising channel", a protocol for quantum key distribution is demonstrated. The section on "Emergence of ancilla-free quantum error correction" shows how error correction codes result from this framework if logical basis states are chosen appropriately. The section titled "Conclusion" concludes the paper with closing remarks.

Notation

In this section, we setup the notation to be used henceforth in the paper.

1. The set of linear operators acting on an N- level system forms a vector space of dimension N^2. The basis operators may be chosen to be:

$$S^{(kl)} \equiv |k\rangle\langle l| + |l\rangle\langle k|, \;\; A^{(kl)} \equiv -i(|k\rangle\langle l| - |l\rangle\langle k|), \;\; k > l; \qquad d^{(k)} \equiv |k\rangle\langle k|, \quad k, l \in \{0, 1, \ldots, N-1\} \tag{1}$$

   For future use, the diagonal operators, $D^{(kl)}$, are defined as:

$$D^{(kl)} \equiv d^{(k)} - d^{(l)}, \;\; k \neq l, \;\; k, l \in \{0, \ldots, (N-1)\}. \tag{2}$$

2. The set of generalised Pauli operators acting on a single qu*N*it consists of products of powers of operators X and Z, which are defined as:

$$X \equiv \sum_{k=0}^{N-1} |k+1\rangle\langle k|, \qquad Z \equiv \sum_{k=0}^{N-1} \omega^k |k\rangle\langle k|, \tag{3}$$

   where $\omega \equiv e^{\frac{2\pi i}{N}}$ and addition of integers is considered modulo N. Both the operators X and Z are unitary operators satisfying $X^N, \; Z^N = \mathbb{1}$.

Idea advanced in this work

Before laying down the formalism, we first elucidate the idea advanced in this work. An N- dimensional quantum state, in general, is characterised by (N^2-1) independent parameters. These parameters are expectation values of (N^2-1) generators of the group $SU(N)$. Hence, one may also envisage a scenario in which the expectation values of these generators contain the information. That is to say, the expectation values of these generators are to be treated as random variables. For encoding of information in these expectation values, we must consider a probability distribution of expectation values.

As an example, consider a two-dimensional pure state, $\rho = \frac{1}{2}(\mathbb{1} + \vec{\sigma}\cdot\hat{p}), |\hat{p}| = 1$. This state is characterised by the three dimensional vector $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. Here θ, ϕ are respectively the polar and azimuthal angles of $\hat{p}$ with $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$. The three components of this vector are expectation values of the generators of $SU(2)$, *viz.*, $\sigma_x, \sigma_y, \sigma_z$. In principle, the three dimensional vector may point along any direction on the Bloch sphere, thanks to the continuous ranges of the parameters θ and ϕ providing randomness in the expectation values of $\sigma_x, \sigma_y, \sigma_z$.

Though expectation values can take infinitely many values, however, in reality, infinite precision is just a mathematical artifice. One is bound to deal with finite precisions of detectors, which limits the information content. This motivates us to employ qu*N*its, as they belong to a larger Hilbert space. A qu*N*it is characterised by (N^2-1) independent parameters, which can be determined by measuring expectation values of the generators of the group $SU(N)$. So, higher dimensional states inevitably carry more information encoded in the expectation values of (N^2-1) generators.

Advantage of this encoding scheme. At this juncture, it is worthwhile to consider whether the proposed information encoding scheme affords any additional advantage as compared to the conventional schemes. Interestingly, the advantage best manifests itself when one considers noisy evolutions of states. In a noisy evolution, a quantum state is inevitably changed. However, as will be shown in the subsequent sections, there exist some combinations of expectation values that remain unchanged. Hence, this encoding scheme provides us with a niche for transfer of information in an error-immune manner via those invariants. Additionally, this encoding scheme does not put any constraint on the purity of states. This reduces the burden of preparation of states as mixed states can also be employed. As is hopefully clear from the discussion, this encoding-decoding scheme does not aim at retrieving the state. It serves to determine the values of invariant quantities, that too without consuming any additional resource like multiparty entanglement and sophisticated experimental techniques (like repeated interventions at precise time intervals[41]).

The formalism

In this section, we lay down the formalism to obtain invariants for noisy communication channels. Noisy channels are well studied through completely-positive-trace-preserving (CPTP) maps[42].

Let ρ be the state of the system used for communication. After passing through a noisy channel, whose action is denoted by a quantum operation $\mathscr{E}$, the state of the system changes to ρ',

$$\rho \to \rho' \equiv \mathscr{E}\ (\rho) = \sum_k E_k \rho E_k^\dagger. \tag{4}$$

The Kraus operators E_k satisfy the condition, $\sum_k E_k^\dagger E_k = \mathbb{1}$. The range of k specifies the number of Kraus operators required to represent a quantum channel of interest.

Identification of invariants. Under a noisy evolution of a state, the final state is, in general, mixed and involves parameters that determine the initial state as well as the noisy channel [see Eq. (4)]. Of particular significance for us is that we can construct those quantities (mostly in the form of ratios of expectation values of observables) that are solely functions of parameters of the initial state and are independent of those of noisy evolution operators. Since, by construction, these quantities involve parameters of initial state only, they remain invariant under a noisy evolution. As such they can be legitimately employed for information transfer in an error–immune manner.

For this, we consider those operators whose expectation values are re-scaled under a noisy evolution. Let $\{O_\alpha\}$ be the set of such operators satisfying,

$$\langle O_\alpha\rangle_{\rho'} = \lambda_\alpha \langle O_\alpha\rangle_\rho, \tag{5}$$

where the non-vanishing scaling factors λ_α are functions of noise parameters. Together with Eq. (4), we get the following equation,

$$\sum_k \mathrm{Tr}\left(\mathrm{E}_\mathrm{k}^\dagger \mathrm{O}_\alpha \mathrm{E}_\mathrm{k}\rho\right) = \lambda_\alpha \mathrm{Tr}(\mathrm{O}_\alpha\rho). \tag{6}$$

Since Eq. (6) holds for an arbitrary state ρ, the operator O_α must satisfy the following condition,

$$\sum_k E_k^\dagger O_\alpha E_k = \lambda_\alpha O_\alpha. \tag{7}$$

Suppose that there are n such operators $\{O_1, \ldots, O_n\}$, satisfying Eq. (5). Consider the following function of expectation values,

$$I(\{r_\alpha\}) \equiv \prod_{\alpha=1}^{n} \left(\langle O_\alpha \rangle_{\rho'} \right)^{r_\alpha} = \prod_{\alpha=1}^{n} \lambda_\alpha^{r_\alpha} \left(\langle O_\alpha \rangle_{\rho} \right)^{r_\alpha}, \tag{8}$$

where r_α can take real values. The quantity, $I(\{r_\alpha\})$, would remain invariant under the noisy evolution of a state, iff,

$$\prod_{\alpha=1}^{n} \lambda_\alpha^{r_\alpha} = 1. \tag{9}$$

In that case, the information encoded in the quantity, $I(\{r_\alpha\})$, remains invariant. We now categorise these invariants into three different families depending upon how the operators are re-scaled under a noisy evolution of a state.

The first family of invariants. The first family of invariants corresponds to the situation when, $r_\alpha = 1$, for a given value of α and all other r_α's vanish in Eq. (8). For this case, the condition (7) reduces to:

$$\sum_k E_k^\dagger O_\alpha E_k = O_\alpha. \tag{10}$$

This condition implies that $\langle O_\alpha \rangle$ remains unchanged under a noisy evolution of a state, and hence, can be used for encoding information. Note that the Eq. (10) is satisfied whenever $[O_\alpha, E_k] = 0,\ \forall\, k$. The range of α determines the number of independent operators whose expectation values remain invariant. For the case in which all the Kraus operators are generated by a single unitary operator U, i.e., $E_k = U^k$, the statistics of eigenprojections of U remains unchanged under the evolution. Hence, they act as invariants.

This particular set of invariant quantities arises in the study of Lindblad master equations and is used to recognize steady-state structures in a noisy state[43].

The second family of invariants. Having discussed the invariants from the first family, it is worthwhile to ask whether there exists any other independent invariants, not exhausted in the first family. It is because there may be instances in which no invariant can be obtained from the first family. Therefore, we consider a more general case and define the second family of invariants. This family involves ratios of expectation values of those operators, that scale identically under a noisy evolution.

To elaborate, the second family corresponds to the condition when only two $\lambda'_\alpha s$, say, λ_1 and λ_2 survive and are equal to each other. Then, the expectation values of the two operators follow the relation, $\langle O_1 \rangle_{\rho'} = \lambda \langle O_1 \rangle_\rho, \langle O_2 \rangle_{\rho'} = \lambda \langle O_2 \rangle_\rho$. For these operators, Eq. (8) provides invariant when $r_1 = 1$ and $r_2 = -1$ and all the other r_α's vanish. This implies that the information encoded in the quantity,

$$I \equiv \frac{\langle O_1 \rangle}{\langle O_2 \rangle}, \tag{11}$$

remains free from errors and can be transferred reliably.

The third family of invariants. Most of the invariants are exhausted by the first two families. However, there may exist a set of operators which satisfies the condition (9), but does not belong to either of the aforementioned families. They constitute the third family of invariants. This family consists of those functions for which the condition (9) is satisfied either for $n > 2$ or for $n = 2$ when $r_1 \neq -r_2 = 1$.

Results

In this section, employing the formalism, we obtain invariants for various noisy channels of a qu*N*it. This is followed by proposal of a quantum key distribution protocol employing these invariants. Finally, we also show how this formalism embeds quantum error correcting codes, contingent on suitable restrictions on choices of logical basis states.

Information transfer with qu*N*its

Recently, quantum communication protocols employing qu*N*its have attracted a lot of interest, thanks to the experimental advances in generation, manipulation and detection of photonic qu*N*its (see, for example[44], and references therein). The effect of various noisy channels such as generalised Pauli channels, depolarising channel, dephasing channel and amplitude damping channel on these protocols have been studied[45–48]. Appreciating the significance of these channels, we identify invariants for the same employing the formalism laid down in the previous section. To start with, we consider the generalised Pauli channel.

Generalised Pauli channel. The effect of the generalised Pauli channel (GPC) on a state can be modelled with the help of operators[49] $X \equiv \sum_{k=0}^{N-1} |k+1\rangle\langle k|$ and $Z \equiv \sum_{k=0}^{N-1} \omega^k |k\rangle\langle k|$. An arbitrary state ρ, after passing through this channel changes to the state ρ',

$$\rho \to \rho' \equiv \sum_{r,s=0}^{N-1} p_{rs} (X^r Z^s)\ \rho\ (X^r Z^s)^\dagger, \qquad \sum_{r,s=0}^{N-1} p_{rs} = 1, \tag{12}$$

where $0 \leq p_{rs} \leq 1$ is the probability with which the unitary operator $X^r Z^s$ corrupts the state. It is straightforward to verify that the GPC does not lead to any invariant. Since the set of Kraus operator $\{X^r Z^s\}$ forms an irreducible representation of Weyl algebra, following Schur's lemma, there cannot be any invariant subspace except the trivial identity. Hence, there cannot exist any invariant from the first family. There does not exist any invariant from the second or the third family, given the fact that all the probabilities p_{rs} are distinct. The proof for the same is given in section (S1) of the supplementary material. Hence GPC admits no invariant except the trivial identity.

However, there exist many special cases of GPC whose effect have been studied on various communication protocols[45,50,51]. We now consider these special cases of GPC.

Generalised flip error. In a generalised flip error, all the relevant Kraus operators are generated by the operator X. Let ρ be the state used to send information through such a channel. After passing through this channel, it changes to the state ρ':

$$\rho \to \rho' \equiv \sum_{r=0}^{N-1} p_r X^r \rho \, (X^r)^\dagger, \quad 0 \leq p_r \leq 1, \quad \sum_{r=0}^{N-1} p_r = 1. \tag{13}$$

Employing cyclicity property of the trace one may immediately see that the expectation values of operators, $I_1^{(m)} \equiv \langle X^m \rangle$, are invariant, and thus the encoded information remains error–free. In addition, employing the relation, $ZX = \omega XZ$, we obtain the following set of invariants belonging to the second family,

$$I_2^{(ml)} \equiv \frac{\langle Z^m \rangle}{\langle Z^m X^l \rangle}, \tag{14}$$

information encoded in which remains immune to errors. Enumeration of these quantities is given in section (S2) of the supplementary material respectively.

Since the operators X, Z and $Y = XZ$ are unitarily equivalent to each other, invariants for generalised phase [replacing X in the Eq. (13) by Z] and for generalised combined flip and phase error [replacing X in the Eq. (13) by $Y = XZ$] can be identified in the same manner. The invariants for these two channels are given in the Table 1.

Depolarising channel. The effect of a depolarizing channel on a state is to incoherently mix the state with white noise with a nonzero probability. The effect of this channel on various quantum communication protocols, for example, (1) on quantum teleportation[45], (2) for a qutrit[46], (3) on the key rate and hence, on security of quantum key distribution protocol[50], and, (4) on quantum secret sharing protocol[51] have been studied.

Let p be the probability with which white noise is incoherently mixed with a state. Let ρ be the state of a qu$N$it used to transmit information through a depolarizing channel. After passing through the channel, the state of the system changes to[52]:

$$\rho \to \rho' \equiv (1-p)\rho + p\frac{\mathbb{1}}{N}, \quad 0 \leq p \leq 1. \tag{15}$$

The invariants, in which information can be encoded for error-free transmission are,

$$I_1^{(kl)} \equiv \frac{\langle S^{(kl)} \rangle}{\langle D^{(kl)} \rangle}, \qquad I_2^{(kl)} \equiv \frac{\langle A^{(kl)} \rangle}{\langle D^{(kl)} \rangle}, \qquad k > l; \qquad I_3^{(m)} \equiv \frac{\langle d^{(m)} \rangle - \frac{1}{N}}{\langle d^{(0)} \rangle - \frac{1}{N}}, \qquad 1 \leq m \leq (N-2). \tag{16}$$

Noisy channel	First family of invariants	Number of Invariants	Second and third families of invariants	Number of invariants	Total number of invariants
Generalised flip error	$\langle X^m \rangle$	$N-1$	$\frac{\langle Z^m \rangle}{\langle Z^m X^l \rangle}$	$(N-1)^2$	$N(N-1)$
Generalised phase-error	$\langle Z^m \rangle$	$N-1$	$\frac{\langle X^m \rangle}{\langle X^m Z^l \rangle}$	$(N-1)^2$	$N(N-1)$
Generalised combined flip and phase errors	$\langle Y^m \rangle$	$N-1$	$\frac{\langle Z^m \rangle}{\langle Z^m Y^l \rangle}$	$(N-1)^2$	$N(N-1)$
Dephasing channel	$\langle D^{(k,k+1)} \rangle$	$N-1$	$\frac{\langle S^{(kl)} \rangle}{\langle A^{(kl)} \rangle}$	$\binom{N}{2}$	$\frac{(N-1)(N+2)}{2}$
Depolarizing channel	–	–	$\frac{\langle S^{(kl)} \rangle}{\langle D^{(kl)} \rangle}$, $\frac{\langle A^{(kl)} \rangle}{\langle D^{(kl)} \rangle}$, $\frac{\langle d^{(m)} \rangle - \frac{1}{N}}{\langle d^{(0)} \rangle - \frac{1}{N}}$	$\binom{N}{2}, \binom{N}{2}, N-2$	N^2-2
ADC	–	–	$\frac{\langle S^{(kl)} \rangle}{\langle A^{(kl)} \rangle}$, $\frac{\langle S^{(N-1,0)} \rangle \langle A^{(N-1,0)} \rangle}{\langle \pi_{N-1} \rangle}$	$\binom{N}{2}, 1$	$\binom{N}{2}+1$

Table 1. The sets of invariants for various noisy channels of a qu$N$it.

Dephasing channel. In a dephasing channel, coherence of a state decreases without any change in its population. Let ρ be the state of a quNit system used to transfer information. After passing through a dephasing channel, it changes to[53]:

$$\rho \rightarrow \rho' \equiv \sum_{j=0}^{N} p_j \, E_j \rho E_j^{\dagger}, \qquad 0 \leq p_j \leq 1, \quad \sum_{j=0}^{N} p_j = 1, \tag{17}$$

where the relevant Kraus operators are $E_j = \mathbb{1} - 2|j\rangle\langle j| \, (0 \leq j \leq N-1)$ and $E_N = \mathbb{1}$. Under this evolution, the entries of the density matrix change in the following manner,

$$\rho'_{ii} = \rho_{ii}, \ \ \forall i, \qquad \rho'_{ij} = (1 - 2p_i - 2p_j) \, \rho_{ij}, \qquad \forall i \neq j. \tag{18}$$

Employing the relations given in (18), the invariants in which information can be encoded for error-free transmission are:

$$I_1^{(k)} \equiv \langle D^{(k+1,k)} \rangle, \qquad I_2^{(kl)} \equiv \frac{\langle S^{(kl)} \rangle}{\langle A^{(kl)} \rangle}, \qquad k > l. \tag{19}$$

Amplitude damping channel (ADC). In this section, we obtain a set of invariants for a qu*N*it passing through an amplitude damping channel. The effect of an amplitude-damping channel on several communication protocols such as quantum teleportation, secret sharing protocol, entanglement swapping protocol and quantum key distribution protocols has been studied[45,50,51,54–56].

An arbitrary state ρ, after passing through an amplitude damping channel, changes to the state ρ':

$$\rho \rightarrow \rho' = \mathscr{E} \ (\rho) \equiv E_0 \rho E_0^{\dagger} + \sum_{m<n=0}^{N-1} E_{mn} \rho E_{mn}^{\dagger}. \tag{20}$$

The relevant Kraus operators are given as[57]:

$$E_0 \equiv |0\rangle\langle 0| + \sum_{n=1}^{N-1} \sqrt{1 - \xi_n} |n\rangle\langle n|, \qquad E_{mn} \equiv \sqrt{\gamma_{nm}} |m\rangle\langle n|, \tag{21}$$

where γ_{nm} describes the rate with which population from the nth level is transferred to the mth level. The conditions of complete positivity and trace preserving nature of the channel translates to the following inequalities: $0 \leq \gamma_{nm} \leq 1, \ \ \xi_n \equiv \sum_{0 \leq m < n} \gamma_{nm} \leq 1, \ \forall \, m, n \ \text{ s.t. } 0 \leq m < n \leq N-1$.

The set of invariants for this channel is given by the second and the third family as follows:

$$I_1^{(kl)} = \frac{\langle S^{(kl)} \rangle}{\langle A^{(kl)} \rangle}, \quad k > l; \qquad I_2 = \frac{\langle S^{(N-1,0)} \rangle \langle A^{(N-1,0)} \rangle}{\langle \pi_{N-1} \rangle}, \quad \text{where } \pi_{\mathrm{N}-1} \equiv |\mathrm{N}-1\rangle\langle \mathrm{N}-1|. \tag{22}$$

We, now, summarise the results obtained for various noisy channels of a qu*N*it succinctly in Table 1. The salient features of the table are given below:

1. The invariants belonging to the first family are limited in number in comparison to the second family. This owes to the fact that there are a larger number of expectation values that change in a scaled manner in comparison to the ones that do not change at all.
2. The third family provides an invariant for an amplitude–damping channel. It is because amplitude damping channel is the sole channel (among the ones studied in this paper) in which entries of the density matrix change with different powers of noise parameters.
3. The increase in the number of invariants with N (i.e., the dimension of the qu*N*it) further strengthens the observation that larger information can be transferred with higher-dimensional states.

Table 1 also gives insight into the relative impact of noisy channels. In the noisy channels such as the generalised flip error, phase error, and combination of flip and phase error, the loss of information is $O(N)$. Whereas, in the channels such as dephasing and ADC, the loss of information is $O(\frac{N^2}{2})$. For the sake of better elucidation, we recall that information is encoded in the expectation values of operators or functions thereof. In a noiseless case, there are (N^2-1) independent expectation values that characterize a state and hence carry information. However, for transferring error-free information, it is encoded in the invariants whose number is less than (N^2-1). This decrement in the number of invariants is accounted as loss of information.

Appreciating the employment of qubits in communication protocols, the invariants for qubits passing through different noisy channels have been explicitly given in section (S3) of the supplementary material. This concludes our discussion of invariants in various noisy channels. Following a similar procedure, the invariants for any channel can be straightforwardly obtained.

Application: QKD employing qubits in a depolarising channel

Having laid down the framework, in this section, we demonstrate a protocol for quantum key distribution employing qubits passing through depolarising channel. The invariants explicitly found in section (S3) of the supplementary material are employed for transferring information. The generalisation of the protocol to quNits and to various noisy channels is straightforward. The only difference would be in the set of invariants that are employed, as depicted in Table 1.

In a depolarising channel for qubits, a state ρ evolves as[42],

$$\rho \to (1-p)\rho + p\frac{\mathbb{1}}{2}. \tag{23}$$

There are two invariants for this channel, given by,

$$I_1 = \frac{\langle\sigma_x\rangle}{\langle\sigma_z\rangle}, \qquad I_2 = \frac{\langle\sigma_y\rangle}{\langle\sigma_z\rangle}. \tag{24}$$

The security of the protocol is assured by employing decoy states. The decoy states are four in number and may be chosen to be, $\frac{1}{2}(\mathbb{1} \pm \vec{\sigma}\cdot\hat{p})$, $\frac{1}{2}(\mathbb{1} \pm \vec{\sigma}\cdot\hat{p}')$, where $\hat{p}$ and $\hat{p}'$ are fixed. With this proviso, the steps for the protocol are listed as follows:

1. Alice prepares N copies of each of k different states, $\rho_1, \ldots, \rho_k$, to transfer information to Bob. The value of k depends upon the length of the information to be transmitted. The value of N is so chosen that there is sufficient statistics to determine expectation values. She sends these states to Bob in a random sequence. Intermittently, she inserts a decoy state in that sequence and sends it to Bob.
2. On receiving a state, Bob measures randomly one of the observables σ_x, σ_y, and σ_z. This constitutes a round. This process is repeated for many rounds.
3. After a sufficient number of rounds, Alice reveals the rounds in which she had sent the decoy states. Bob reveals the observables and the corresponding outcomes for these rounds. Alice uses this information to check for the presence of an eavesdropper, if any.
4. If Alice is convinced about the absence of an eavesdropper, she reveals to Bob the positions of those rounds in which she has sent the same states. Note that Alice does not reveal any information beyond that.
5. Bob determines $\langle\sigma_x\rangle$, $\langle\sigma_y\rangle$, and $\langle\sigma_z\rangle$ for each of the states ρ_k and thus determines the values of the invariants, $I_1^{(r)}$ and $I_2^{(r)}$, $1 \le r \le k$, given in Eq. (24), for all the k states to retrieve the message sent by Alice. These invariants carry the uncorrupted information to him.
6. By employing signs of I_1 and I_2, a key consisting of binary symbols can be generated in the following manner: $I_1, I_2 > 0 \to 00$, $I_1 > 0, I_2 < 0 \to 01$, $I_1 < 0, I_2 > 0 \to 10$, $I_1 < 0, I_2 < 0 \to 11$.

In this way, Bob securely receives the error–free message sent by Alice even after passing through a depolarizing noisy channel. Security of this protocol against intercept-resend attack and entangle-and-measure attack has been discussed in section (S4) of the supplementary material.

In this manner, by encoding information in the invariants, error–free information can be transmitted through various noisy channels in a secure manner. Though we have shown this encoding scheme for a QKD protocol, this template can be applied to all the information transfer protocols, e.g., quantum secure direct communication, quantum secret sharing, quantum mutual identification. In fact, the same procedure with appropriate modifications can also be opted for semi-quantum communication protocols. As another application of this encoding scheme, we have shown remote transfer of information employing qubits through a depolarising channel in section (S5) of the supplementary material. In the next section, we show the emergence of standard quantum error correcting codes by putting more constraints on the choice of logical states.

Emergence of ancilla-free quantum error correction

It might appear that the method outlined in this paper is dissimilar and unrelated to the standard quantum error-correcting codes (QECC). On the contrary, the method is more general. In fact, by imposing additional constraints on the choice of states, standard QECC can be retrieved. In the following, we show that this is indeed the case.

As an example, consider a six-dimensional system in which dominant errors are due to the action of X and X^2, occurring with respective probabilities of p_1 and p_2. Recall that operators X and X^2 are $X = \sum_{k=0}^{5} |k+1\rangle\langle k|$, $X^2 = \sum_{k=0}^{5} |k+2\rangle\langle k|$, with addition of integers is modulo 6.

In QECC, encoding is done in a way that each error projects the initial state onto orthogonal subspaces. This condition allows to prepare the initial state in the subspace spanned by basis states $|0\rangle$ and $|3\rangle$. That is to say, the state $|\psi_0\rangle$ carrying the information is given by,

$$|\psi_0\rangle = \alpha|0\rangle + \beta|3\rangle. \tag{25}$$

After passing through the noisy channel, the final state will have the form,

$$\rho \equiv \sum_{i=0}^{2} p_i X^i |\psi_0\rangle\langle\psi_0| (X^i)^\dagger = \sum_{i=0}^{2} p_i |\psi_i\rangle\langle\psi_i|; \qquad X^0 \equiv \mathbb{1}, \tag{26}$$

where the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are defined as,

$$|\psi_1\rangle = \alpha|1\rangle + \beta|4\rangle, \quad |\psi_2\rangle = \alpha|2\rangle + \beta|5\rangle. \tag{27}$$

Since each of the errors X and X^2 have projected the state onto the respective orthogonal subspaces spanned by $\{|1\rangle, |4\rangle\}$ and $\{|2\rangle, |5\rangle\}$, they can be discriminated unambiguously. To do so, the measurement of the following stabiliser can be performed,

$$S = c_0\big(|0\rangle\langle 0| + |3\rangle\langle 3|\big) + c_1\big(|1\rangle\langle 1| + |4\rangle\langle 4|\big) + c_2\big(|2\rangle\langle 2| + |5\rangle\langle 5|\big), \quad c_0 \neq c_1 \neq c_2. \tag{28}$$

The outcome of the measurement determines the error, whose action can be undone by applying the corresponding inverse unitary transformation. That is to say, if the outcome of measurement result is c_0, the state is uncorrupted whereas for the outcome $c_1(c_2)$, the error $X(X^2)$ has corrupted the state, whose effect can be mitigated by performing the inverse transformation $X^\dagger((X^2)^\dagger)$. Thus, by applying the appropriate unitary transformation based on the received outcomes, errors can be corrected. Note that unlike the formalism laid down in this paper, in conventional QECC codes, the basis states are fixed, which makes their implementations relatively more demanding.

Conclusion

In summary, we have laid down a formalism to extract invariants for a number of noisy channels, which can be employed for transfer of information in an uncorrupted manner. This scheme alleviates the need for an entangled state, whose preparation is a difficult task. It also works for mixed states, which further reduces the burden of preparation of pure states. As applications of this encoding scheme, we have demonstrated protocols for quantum key distribution and remote transfer of information.

This work opens up a number of possibilities. For example, transfer of information using this formalism for multi-party systems constitutes an interesting study. Multi-party states can then also be employed to transfer error-free information to multiple users under noisy communication channels. Additionally, the formalism proposed in this work can also be used to transfer error-free information in several other scenarios. For example, the information may be encoded in the invariants in such a manner that it can be retrieved only if all the parties collaborate. Besides, several communication protocols such as quantum secure direct communication, quantum secret sharing can be proposed. In conclusion, semi-quantum communication protocols can also be demonstrated for error-free information transfer through noisy channels.

Data availability

The data analysed during this study are available from the corresponding author on reasonable request.

Received: 24 June 2022; Accepted: 17 February 2023
Published online: 20 February 2023

References

1. Bennett, C. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (ICCSSP)* 175 (1984).
2. Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. Deutsch, D. & Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. Ser. A Math. Phys. Sci.* **439**, 553–558 (1992).
5. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219 (1996).
6. Chubb, C. *Noise in Quantum Information Processing*. Ph.D. Thesis, School of Physics,The University of Sydney (2019).
7. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493–R2496 (1995).
8. Steane, A. M. Simple quantum error-correcting codes. *Phys. Rev. A* **54**, 4741 (1996).
9. Knill, E. & Laflamme, R. Theory of quantum error-correcting codes. *Phys. Rev. A* **55**, 900 (1997).
10. Layden, D., Zhou, S., Cappellaro, P. & Jiang, L. Ancilla-free quantum error correction codes for quantum metrology. *Phys. Rev. Lett.* **122**, 040502 (2019).
11. Bény, C., Kempf, A. & Kribs, D. W. Generalization of quantum error correction via the Heisenberg picture. *Phys. Rev. Lett.* **98**, 100502 (2007).
12. Bény, C., Kempf, A. & Kribs, D. W. Quantum error correction of observables. *Phys. Rev. A* **76**, 042303 (2007).
13. Huang, Y.-F. *et al.* Experimental generation of an eight-photon Greenberger–Horne–Zeilinger state. *Nat. Commun.* **2**, 1–6 (2011).
14. Lu, C.-Y. *et al.* Experimental entanglement of six photons in graph states. *Nat. Phys.* **3**, 91–95 (2007).
15. Proietti, M. *et al.* Experimental quantum conference key agreement. *Sci. Adv.* **7**, eabe0395 (2021).
16. Erhard, M., Malik, M., Krenn, M. & Zeilinger, A. Experimental Greenberger–Horne–zeilinger entanglement beyond qubits. *Nat. Photonics* **12**, 759–764 (2018).
17. Jing, Y., Alsina, D. & Razavi, M. Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool. *Phys. Rev. Appl.* **14**, 064037 (2020).
18. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photonics* **9**, 641–652 (2015).
19. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 1–12 (2016).
20. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
21. Lo, H.-K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. arXiv:quant-ph/0610203 (2006).
22. Crépeau, C., Gottesman, D. & Smith, A. Approximate quantum error-correcting codes and secret sharing schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 285–301 (Springer, 2005).
23. Zanardi, P. & Rasetti, M. Error avoiding quantum codes. *Mod. Phys. Lett. B* **11**, 1085–1093 (1997).
24. Koashi, M. & Ueda, M. Reversing measurement and probabilistic quantum error correction. *Phys. Rev. Lett.* **82**, 2598–2601 (1999).
25. Koczor, B. Exponential error suppression for near-term quantum devices. *Phys. Rev. X* **11**, 031057 (2021).

26. Cai, Z. Quantum error mitigation using symmetry expansion. *Quantum* **5**, 548 (2021).
27. Otten, M. & Gray, S. K. Recovering noise-free quantum observables. *Phys. Rev. A* **99**, 012338 (2019).
28. Fujiwara, A. Estimation of a generalized amplitude-damping channel. *Phys. Rev. A* **70**, 012317 (2004).
29. Collins, D. & Stephens, J. Depolarizing-channel parameter estimation using noisy initial states. *Phys. Rev. A* **92**, 032324 (2015).
30. Sasaki, M., Ban, M. & Barnett, S. M. Optimal parameter estimation of a depolarizing channel. *Phys. Rev. A* **66**, 022308 (2002).
31. Amaral, G. C. & Temporão, G. P. Characterization of depolarizing channels using two-photon interference. *Quantum Inf. Process.* **18**, 1–11 (2019).
32. Urrego, D. F. *et al.* Implementation and characterization of a controllable dephasing channel based on coupling polarization and spatial degrees of freedom of light. *Opt. Express* **26**, 11940–11949 (2018).
33. Liu, Y. Decoherence-free subspace and entanglement sudden death of multi-photon polarization states in fiber channels. arXiv: 2212.07627 (2022).
34. Mabena, C. M. & Roux, F. S. High-dimensional quantum channel estimation using classical light. *Phys. Rev. A* **96**, 053860 (2017).
35. Thapliyal, K. & Pathak, A. Applications of quantum cryptographic switch: Various tasks related to controlled quantum communication can be performed using bell states and permutation of particles. *Quantum Inf. Process.* **14**, 2599–2616 (2015).
36. Sharma, V., Thapliyal, K., Pathak, A. & Banerjee, S. A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols. *Quantum Inf. Process.* **15**, 4681–4710 (2016).
37. Bala, R., Asthana, S. & Ravishankar, V. Combating errors in propagation of orbital angular momentum modes of light in turbulent media. *Int. J. Theor. Phys.* **61**, 263 (2022).
38. Zhai, S., Zhu, Y., Zhang, Y. & Hu, Z. Effects of oceanic turbulence on orbital angular momenta of optical communications. *J. Mar. Sci. Eng.* **8**, 869 (2020).
39. Yan, X., Zhang, P.-F., Fan, C.-Y. & Zhang, J.-H. Effect of atmospheric turbulence on orbital angular momentum entangled state. *Commun. Theor. Phys.* **74**, 025102 (2022).
40. Bachmann, D., Shatokhin, V. N. & Buchleitner, A. Universal entanglement decay of photonic orbital angular momentum qubit states in atmospheric turbulence: An analytical treatment. *J. Phys. A Math. Theor.* **52**, 405303 (2019).
41. Gupta, M. K. & Dowling, J. P. Dephasing of single-photon orbital angular momentum qudit states in fiber: Limits to correction via dynamical decoupling. *Phys. Rev. Appl.* **5**, 064013 (2016).
42. Nielsen, M. A. & Chuang, I. L. Chapter 8- quantum noise and quantum operations. In *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 353–398 (Cambridge University Press, 2010).
43. Albert, V. V. & Jiang, L. Symmetries and conserved quantities in lindblad master equations. *Phys. Rev. A* **89**, 022118 (2014).
44. Shen, Y. *et al.* Optical vortices 30 years on: OAM manipulation from topological charge to multiple singularities. *Light: Sci. Appl.* **8**, 1–29 (2019).
45. Fonseca, A. High-dimensional quantum teleportation under noisy environments. *Phys. Rev. A* **100**, 062311 (2019).
46. Xu, R., Zhou, R.-G., Li, Y., Jiang, S. & Ian, H. Enhancing robustness of noisy qutrit teleportation with Markovian memory. *EPJ Quantum Technol.* **9**, 1–17 (2022).
47. Fortes, R. & Rigolin, G. Fighting noise with noise in realistic quantum teleportation. *Phys. Rev. A* **92**, 012338 (2015).
48. Fortes, R. & Rigolin, G. Probabilistic quantum teleportation in the presence of noise. *Phys. Rev. A* **93**, 062330 (2016).
49. Miller, D., Holz, T., Kampermann, H. & Bruß, D. Propagation of generalized Pauli errors in qudit Clifford circuits. *Phys. Rev. A* **98**, 052316 (2018).
50. Iqbal, H. & Krawec, W. O. Analysis of a high-dimensional extended b92 protocol. *Quantum Inf. Process.* **20**, 1–22 (2021).
51. Hu, W., Zhou, R.-G., Li, X., Fan, P. & Tan, C. A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quantum Inf. Process.* **20**, 1–28 (2021).
52. Wilde, M. M. *Chapter 4—The Noisy Quantum Theory* 2nd edn. (Cambridge University Press, 2017).
53. Marques, B. *et al.* Experimental simulation of decoherence in photonics qudits. *Sci. Rep.* **5**, 1–11 (2015).
54. Hu, W. W., Zhou, R.-G. & Luo, G. F. Conclusive multiparty quantum state sharing in amplitude-damping channel. *Quantum Inform. Process.* **21**, 1–34 (2022).
55. DG, Im. *et al.* Optimal teleportation via noisy quantum channels without additional qubit resources. *Npj Quantum Inf.* **7**, 1–7 (2021).
56. Trávníček, V., Bartkiewicz, K., Černoch, A. & Lemr, K. Experimental diagnostics of entanglement swapping by a collective entanglement test. *Phys. Rev. Appl.* **14**, 064071 (2020).
57. Chessa, S. & Giovannetti, V. Quantum capacity analysis of multi-level amplitude damping channels. *Commun. Phys.* **4**, 1–12 (2021).

Acknowledgements

Rajni thanks UGC for funding her research in the initial stage of the work. Sooryansh thanks the Council for Scientific and Industrial Research (Grant No. -09/086 (1278)/2017-EMR-I) for funding his research.

Author contributions

All the authors have contributed equally in all the respects at all the stages.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-023-30178-x.

Correspondence and requests for materials should be addressed to R.B.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.