Entanglement can increase asymptotic rates of zero-error classical communication over classical channels

Debbie Leung, Laura Mancinska, William Matthews, Maris Ozols, Aidan Roy
Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L3G1, Canada

It is known that the number of different classical messages which can be communicated with a single use of a classical channel with zero probability of decoding error can sometimes be increased by using entanglement shared between sender and receiver. It has been an open question to determine whether entanglement can ever offer an advantage in terms of the zero-error communication rates achievable in the limit of many channel uses. In this paper we show, by explicit examples, that entanglement can indeed increase asymptotic zero-error capacity. Interestingly, in our examples the quantum protocols are based on the root systems of the exceptional Lie groups E_7 and E_8.

Motivation and statement of the problem

Given a classical noisy channel $\mathcal{N}$, let $c_0(\mathcal{N})$ denote the maximum number of different messages that can be transmitted without error by one use of $\mathcal{N}$. Two input symbols of $\mathcal{N}$ are **confusable** if there is an output symbol which both inputs can cause to occur. The **confusability graph** of $\mathcal{N}$ is the graph $G(\mathcal{N})$ whose vertices are the input symbols and edges connect confusable symbols. Note that $c_0(\mathcal{N})$ equals the *independence number*[1] of $G(\mathcal{N})$.

The bit rate of zero-error communication which can be achieved in the large block length limit is the **zero-error capacity** [1, 2] of $\mathcal{N}$,

$$C_0(\mathcal{N}) := \lim_{n\to\infty} \frac{1}{n} \log_2 c_0(\mathcal{N}^{\otimes n}).$$

While determining whether $c_0(\mathcal{N})$ is larger than some constant is NP-complete,[2] there is no known algorithm to compute $C_0(\mathcal{N})$ in general.

The usefulness of entanglement between sender and receiver has been studied for a variety of communication tasks with striking results. In teleportation it allows for transmission of quantum data over classical channels. In superdense coding it can increase the rate of classical communication over quantum channels. However, the rate at which classical data can be sent over a classical channel with arbitrarily small, but non-zero, error probability (the Shannon capacity [3]) cannot be increased by entanglement assistance [5].

In light of these results and recent work generalising zero-error information theory to quantum data and channels [6–9] we wanted to determine whether entanglement could increase the rate of zero-error communication of classical information over classical channels. Defining $c_0^E(\mathcal{N})$ as the maximum number of different messages that can be sent without error with one use of $\mathcal{N}$ and arbitrary entanglement assistance, the **entanglement-assisted zero-error capacity** $C_0^E(\mathcal{N})$ is defined in a similar way to $C_0(\mathcal{N})$ above.

Partial progress on this problem was made last year. It was proved that $c_0^E(\mathcal{N})$, like $c_0(\mathcal{N})$, is determined by the confusability graph $G(\mathcal{N})$. Therefore, we can talk about the values of c_0^E and C_0^E for a *graph* [11, 12]. Furthermore graphs G were constructed for which $c_0^E(G) = c_0(G)+1$, thus showing that the one-shot capacity can be increased by entanglement assistance. This result was based on proofs of the Kochen-Specker theorem and has a formal connection to the existence of certain pseudo-telepathy games.

However, our original question whether there are channels whose *asymptotic rates* of zero-error communication are improved by entanglement remained unresolved. A major obstacle was that there is no known algorithm to compute $C_0(\mathcal{N})$ and that the growth of $\frac{1}{n}\log_2 c_0(\mathcal{N}^{\otimes n})$ with n can be extremely complex [4]. A celebrated upper bound on $C_0(\mathcal{N})$ due to Lovász [15] was shown to also apply for $C_0^E(\mathcal{N})$ [10, 16]. This interesting result unfortunately shows that Lovász's bound is useless for the purposes of settling our question. In addition we do not know a simple way to compute even the one-shot entanglement assisted quantity c_0^E.

Fortunately, other approaches proved fruitful, and here we answer our initial question by finding explicit graphs for which $C_0^E > C_0$ (and so the difference between $c_0^E(\mathcal{N}^{\otimes n})$ and $c_0(\mathcal{N}^{\otimes n})$ is exponential in n, in contrast to the small constant gap shown in [11]). We summarize our results and methods here (see [20] for details).

Theorem 1 *There are channels for which entanglement-assistance increases the* asymptotic *rate of zero-error communication. In particular, there exists $\mathcal{N}$ with $C_0(\mathcal{N}) = \log 7$ and $C_0^E(\mathcal{N}) = \log 9$.*

Our methods and contributions

For a classical channel $\mathcal{N}$ with input alphabet X and output alphabet Y, an **entanglement-assisted zero-error code** of size k and block length n has this form [12]: Alice and Bob share an entangled state ρ_{AB}; To encode message q, Alice makes the q-th of k generalized measurements, each with outcome set X^n, which determines the n symbols she inputs to $\mathcal{N}$; The channel output

[1] The maximum size of a set of pairwise non-adjacent vertices.
[2] Since $c_0(\mathcal{N})$ is equal to the independence number of $G(\mathcal{N})$, this problem is equivalent to MAX CLIQUE.

Suppose $G(\mathcal{N})$ partitions into k cliques of size d. Label the vertices (input symbols) by pairs (c, i) where $c \in [k]$ identifies the clique and $i \in [d]$ the vertex within the clique. Further suppose that $G(\mathcal{N})$ has an orthogonal representation mapping (c, i) to $|\psi(c, i)\rangle$ i.e. $\langle\psi(c, i)|\psi(c', i')\rangle = 0$ if (c, i) and (c', i') are confusable. To send one of k messages with zero-error:

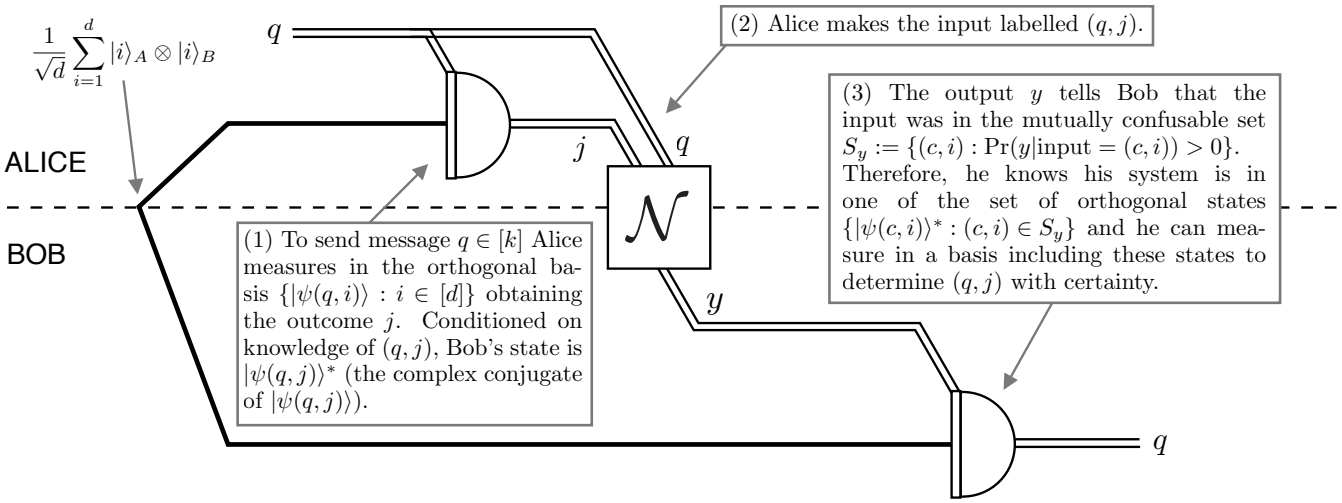

FIG. 1: If the confusability graph of $\mathcal{N}$ can partitioned into k cliques of size d then $C_0(\mathcal{N}) \leq k$ by the Lovász bound. If it also has a d-dimensional orthogonal representation then this rate can be *achieved* by the entanglement-assisted zero-error code (of block length one) described in this figure.

$\mathbf{y} \in Y^n$, determines the generalized measurement (with k outcomes) which Bob makes on his subsystem. When Alice makes measurement q, Bob should obtain outcome q with certainty.

To prove the existence of an asymptotic separation, we aimed to identify a graph G for which it was possible to *simultaneously* prove an upper bound u on $C_0(G)$, and to prove the existence of an entanglement assisted zero-error code showing that $C_0^E(G) > u$.

A particularly promising family are the symplectic graphs $\mathrm{sp}(m)$, whose vertices are the $2^{2m}-1$ non-identity Pauli matrices on m qubits and edges connect commuting ones. Peeters [17] has used Haemers bound [18] to show that $C_0(\mathrm{sp}(m)) = \log(2m+1)$ while the logarithm of the Lovász number of $\mathrm{sp}(m)$ is $\log(2^m+1)$. Hence, the Lovász bound does not rule out a separation when $m \geq 3$.

It remains to find good entanglement-assisted zero-error codes for these graphs. It is known [12] that if the vertices of G can be partitioned into k cliques each of size d, and it is possible to find an *orthogonal d-dimensional representation*[3] then $C_0^E(G) = \log k$. The entanglement-assisted protocol achieving this is described in Figure 1. Moreover, the capacity is achieved in a single use of the channel, consuming $\log d$ ebits, and it saturates Lovász's bound.

[3] An assignment of a non-zero vector in $\mathbb{C}^d$ to each vertex of G such that adjacent vertices have orthogonal vectors.

The maximum clique size of $\mathrm{sp}(m)$ is 2^m-1 and the vertices can be shown to partition into 2^m+1 such cliques. Thus, $C_0^E(\mathrm{sp}(m)) = 2^m+1$ *if an* (2^m-1)*-dimensional orthogonal representation can indeed be found.*

We found an orthogonal representation for $\mathrm{sp}(3)$ (see Appendix) thus establishing Theorem 1. It turns out that these seven-dimensional vectors form the root system E_7. Underlying this beautiful construction is an isomorphism between the automorphism group of $\mathrm{sp}(3)$ and the quotient of the Weyl group of E_7 by reflections about the origin. A similar result can be obtained for a subgraph of $\mathrm{sp}(4)$ for which E_8 provides an orthogonal representation, and $C_0^E = \log 15$ (whereas $C_0 \leq \log 9$).

Our result has an interesting interpretation in terms of Kochen-Specker (KS) proofs of non-contextuality. Such a proof specifies a set of complete, projective measurements, with some projectors in common, such that there is no way to consistently assign a truth value to each projector. An assignment is consistent if (a) precisely one projector in each measurement is "true" and (b) no two "true" projectors are orthogonal.

Ruuge [14] shows that the root systems E_7 and E_8 can be used to construct KS proofs using computer search to nullify the possibility of a consistent assignment. This is a corollary of our results, but our proof is analytic due to the novel application of the Haemers bound. In fact, the use of the Haemers bound provides a whole sequence of KS proofs which are increasingly strong in the following quantitative sense: For the set of 9^n measurements which are obtained by tensoring together n of Alice's 9 measurements, only 7^n can be assigned values in accordance with

property (a) before property (b) must be violated.

Three main avenues for further research are apparent to us. First, is it possible to give a general algorithm to compute C_0^E? An interesting sub-problem is to determine whether C_0^E/C_0 can be arbitrarily large. Second, we have already shown that there are some connections to multi-prover games and to non-contextuality, but we feel that a deeper understanding of these connections is possible and desirable. For example, the application of our result to KS proofs mentioned above suggests some stronger notion of non-contextuality in quantum mechanics. Finally, our work on entanglement-assisted zero-error codes can be placed in the wider context of using entanglement to reduce decoding error in finite block length coding of classical information for classical channels (demonstrating this effect is even experimentally feasible [19]), and characterising this phenomenon presents an even wider set of questions.

[1] C. E. Shannon, IRE Trans. Inform. Theory, vol. IT-2(3):8-19 (1956).

[2] J. Körner, A. Orlitsky, IEEE Trans. Inf. Theory **44**(6):2207-2229 (1998).

[3] C. E. Shannon, Bell Syst. Tech. J. **27**:379–423, 623–656 (1948).

[4] Alon, N.; Lubetzky, E.; , Information Theory, IEEE Transactions on , vol.52, no.5, pp. 2172- 2176, May 2006 doi: 10.1109/TIT.2006.872856

[5] C. H. Bennett, P. Shor, J. Smolin, A. V. Thapliyal, IEEE Trans. Info. Theory 48, 2637-2655, (2002) arXiv:quant-ph/0106052.

[6] R. A. C. Medeiros, R. Alleaume, G. Cohen, F. M. de Assis, arXiv:quant-ph/0611042 (2006).

[7] R. Duan, arXiv:0906.2527 (2009).

[8] T. S. Cubitt, J. Chen, A. W. Harrow, arXiv:0906.2547 (2009).

[9] T. S. Cubitt, G. B. Smith, arXiv:0912.2737 (2009).

[10] R. Duan, S. Severini, A. Winter, arXiv:1002.2514.

[11] T. S. Cubitt, D. Leung, W. Matthews, A. Winter, Phys. Rev. Lett. 104, 230503 (2010) arXiv:0911.5300.

[12] T. S. Cubitt, D. Leung, W. Matthews, A. Winter, arXiv:1003.3195 (2010)

[13] S. Kochen and E. P. Specker, Journal of Mathematics and Mechanics 17, 59-87 (1967).

[14] Artur Ruuge, J. Phys. A 40 (2007), no. 11, 2849-2859. arXiv:0906.2696.

[15] L. Lovász, IEEE Trans. Inf. Theory **25**(1):1-7 (1979).

[16] S. Beigi, arXiv:1002.2488 (2010).

[17] R. Peeters, Combinatorica **16**(3):417-431 (1996).

[18] W. Haemers, IEEE Trans. Inf. Theory **25**(2):231-232 (1979). W. Haemers, Coll. Math. Soc. János Bolyai **25**:267-272 (1978).

[19] Y. Lu, W. Matthews, R. Kaltenbaek, K. J. Resch, http://arxiv.org/abs/1010.2566 (2010).

[20] D. Leung, L. Mancinska, W. Matthews, M. Ozols, and A. Roy, arXiv:1009.1195 (2010).

Appendix A: The orthogonal representation of sp(3)

The orthogonal representation for sp(3) grouped into Alice's 9 measurement bases. The normalization of the vectors are omitted, and "−" stands for −1.

$$\begin{pmatrix} ZII & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ IZI & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ IIZ & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ ZZI & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ ZIZ & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ IZZ & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ ZZZ & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} XII & 1 & 0 & 0 & 1 & 1 & 0 & - \\ IXI & 0 & - & 0 & 1 & 0 & 1 & 1 \\ IIX & 0 & 0 & 1 & 0 & 1 & - & 1 \\ XXI & - & 1 & 0 & 0 & 1 & 1 & 0 \\ XIX & 1 & 0 & 1 & - & 0 & 1 & 0 \\ IXX & 0 & 1 & 1 & 1 & - & 0 & 0 \\ XXX & 1 & 1 & - & 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} YII & 1 & 0 & 0 & - & - & 0 & 1 \\ IXZ & 0 & 1 & 0 & 1 & 0 & - & 1 \\ IZX & 0 & 0 & - & 0 & 1 & 1 & 1 \\ YXZ & - & 1 & 0 & 0 & - & 1 & 0 \\ YZX & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ IYY & 0 & 1 & 1 & - & 1 & 0 & 0 \\ YYY & 1 & 1 & - & 0 & 0 & 0 & - \end{pmatrix}$$

$$\begin{pmatrix} XZI & 1 & 0 & 0 & 1 & - & 0 & 1 \\ ZXZ & 0 & 1 & 0 & 1 & 0 & 1 & - \\ IZY & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ YYZ & 1 & 1 & 0 & 0 & 1 & - & 0 \\ XIY & - & 0 & 1 & 1 & 0 & - & 0 \\ IYX & 0 & 1 & 1 & - & - & 0 & 0 \\ YXX & 1 & - & 1 & 0 & 0 & 0 & - \end{pmatrix} \quad \begin{pmatrix} XIZ & 1 & 0 & 0 & - & 1 & 0 & 1 \\ IYI & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ ZIY & 0 & 0 & 1 & 0 & - & - & 1 \\ XYZ & 1 & - & 0 & 0 & - & 1 & 0 \\ YIX & - & 0 & 1 & - & 0 & 1 & 0 \\ ZYY & 0 & - & 1 & 1 & 1 & 0 & 0 \\ YYX & 1 & 1 & 1 & 0 & 0 & 0 & - \end{pmatrix}$$

$$\begin{pmatrix} YZI & - & 0 & 0 & 1 & - & 0 & 1 \\ ZXI & 0 & 1 & 0 & - & 0 & 1 & 1 \\ IIY & 0 & 0 & 1 & 0 & - & 1 & - \\ XYI & 1 & 1 & 0 & 0 & - & - & 0 \\ YZY & 1 & 0 & - & 1 & 0 & 1 & 0 \\ ZXY & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ XYY & 1 & - & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} YIZ & 1 & 0 & 0 & 1 & - & 0 & - \\ IYZ & 0 & 1 & 0 & - & 0 & 1 & - \\ ZZY & 0 & 0 & - & 0 & - & 1 & 1 \\ YYI & 1 & - & 0 & 0 & 1 & 1 & 0 \\ XZX & - & 0 & 1 & 1 & 0 & 1 & 0 \\ ZXX & 0 & 1 & - & 1 & 1 & 0 & 0 \\ XXY & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} XZZ & - & 0 & 0 & 1 & 1 & 0 & 1 \\ ZYZ & 0 & - & 0 & 1 & 0 & 1 & - \\ ZZX & 0 & 0 & 1 & 0 & - & 1 & 1 \\ YXI & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ YIY & 1 & 0 & 1 & 1 & 0 & - & 0 \\ IXY & 0 & 1 & - & 1 & - & 0 & 0 \\ XYX & - & 1 & 1 & 0 & 0 & 0 & - \end{pmatrix} \quad \begin{pmatrix} YZZ & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ ZYI & 0 & 1 & 0 & 1 & 0 & - & - \\ ZIX & 0 & 0 & 1 & 0 & 1 & 1 & - \\ XXZ & 1 & 1 & 0 & 0 & - & 1 & 0 \\ XZY & 1 & 0 & 1 & - & 0 & - & 0 \\ IYI & 0 & - & 1 & 1 & - & 0 & 0 \\ YXY & - & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$