

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

Laura Mancinska, Debbie Leung, William Matthews, Maris Ozols, Aidan Roy  
 Institute of Quantum Computing, University of Waterloo,  
 200 University Ave. West, Waterloo, ON N2L 3G1, Canada

September 8, 2010

## Abstract

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  $E_8$ .

## 1 Introduction

A *classical channel*  $\mathcal{N}$  which is discrete and memoryless is fully described by its conditional probability distribution  $\mathcal{N}(y|x)$  of producing output  $y$  for a given input  $x$ . The channel obtained by allowing one use of a channel  $\mathcal{N}_1$  and one use of  $\mathcal{N}_2$  is written as  $\mathcal{N}_1 \otimes \mathcal{N}_2$ , reflecting the fact that its conditional probability matrix is the tensor (or Kronecker) product of those of the two constituent channels. Similarly,  $\mathcal{N}^{\otimes n}$  denotes  $n$  uses of  $\mathcal{N}$  and we say that any code used to communicate over this channel has *block length*  $n$ .

**Definition 1.** Let  $c_0(\mathcal{N})$  denote the number of different messages which can be sent with a single use of  $\mathcal{N}$  with zero probability of a decoding error. The **zero-error capacity** of  $\mathcal{N}$  is

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

Two input symbols  $x_1, x_2$  of a channel  $\mathcal{N}$  are said to be *confusable* if they can produce the same output symbol with non-zero probability, i.e.,  $\mathcal{N}(y|x_1) > 0$  and  $\mathcal{N}(y|x_2) > 0$  for some output symbol  $y$ . The *confusability graph* of a channel  $\mathcal{N}$  is a graph  $G(\mathcal{N})$ , whose vertices correspond to different input symbols of  $\mathcal{N}$  and two vertices are joined by an edge if the corresponding symbols are confusable. The confusability graph of  $\mathcal{N}_1 \otimes \mathcal{N}_2$  is easily described in terms of those of  $\mathcal{N}_1$  and  $\mathcal{N}_2$  as follows:  $G(\mathcal{N}_1 \otimes \mathcal{N}_2) = G(\mathcal{N}_1) \boxtimes G(\mathcal{N}_2)$ , where “ $\boxtimes$ ” denotes the *strong graph product*.

**Definition 2** (Strong graph product). In general, the **strong product** of graphs  $G_1, \dots, G_n$  is a graph  $G_1 \boxtimes \dots \boxtimes G_n$ , whose vertices are the  $n$ -tuples  $V(G_1) \times \dots \times V(G_n)$  and distinct vertices  $(a_1, \dots, a_n)$  and  $(b_1, \dots, b_n)$  are joined by an edge if they are entry-wise confusable, i.e., for each  $j \in \{1, \dots, n\}$  either  $a_j b_j \in E(G_j)$  or  $a_j = b_j$ . Likewise, we define the **strong power** of graph  $G$  by  $G^{\boxtimes 1} := G$  and  $G^{\boxtimes n} := G \boxtimes G^{\boxtimes n-1}$ .

An *independent set* of a graph is a subset of its vertices with no edges between them. The *independence number*  $\alpha(G)$  of a graph  $G$  is the maximum size of an independent set of  $G$ . As Shannon observed [1],  $c_0$  and  $C_0$  depend only on the confusability graph of the channel:  $c_0(\mathcal{N}) = \alpha(G(\mathcal{N}))$  and  $C_0(\mathcal{N}) = \log \Theta(G(\mathcal{N}))$  where

$$\Theta(G) := \lim_{n \rightarrow \infty} \sqrt[n]{\alpha(G^{\boxtimes n})}$$

is known as the *Shannon capacity* of the graph  $G$ . Clearly,  $\Theta(G) \geq \alpha(G)$ , since  $G^{\boxtimes n}$  has an independent set of size  $\alpha(G)^n$ . However, in general  $\Theta(G)$  can be larger than  $\alpha(G)$ . The simplest example is the 5-cycle  $C_5$  for which  $\alpha(C_5) = 2$  but  $\Theta(C_5) = \sqrt{5}$ .

Computing the independence number of a graph is NP-hard, but conceptually simple. However, no algorithm is known to determine  $\Theta(G)$  in general, although there is a celebrated upper bound due to Lovász [6]. He defined an efficiently computable quantity  $\vartheta(G)$  called the *Lovász number* of  $G$  which satisfies  $\vartheta(G) \geq \alpha(G)$  and  $\vartheta(G_1 \boxtimes G_2) = \vartheta(G_1)\vartheta(G_2)$ . Because of these properties we also have  $\vartheta(G) \geq \Theta(G)$ .

**Definition 3.** Let  $c_0^E(\mathcal{N})$  denote the number of different messages which can be sent with a single use of  $\mathcal{N}$  with zero probability of a decoding error, when both parties share an arbitrary finite-dimensional entangled state on which each can perform arbitrary local measurements. The **entanglement-assisted zero-error capacity** of  $\mathcal{N}$  is

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

As in the unassisted case, the quantities  $c_0^E$  and  $C_0^E$  also depend *only* on the confusability graph of the channel [4]. For this reason, in the rest of this paper will refer to (assisted and unassisted) zero-error capacities of *graphs*.

In [4] it was shown that graphs  $G$  exist with  $c_0^E(G) > c_0(G)$ . Shortly afterwards it was shown [7, 8] that the Lovász bound also applies to the entanglement-assisted quantities, so  $c_0^E(G) \leq \vartheta(G)$  and hence  $C_0^E(G) \leq \log \vartheta(G)$ .

Whether graphs with  $C_0^E(G) > C_0(G)$  exist, that is, whether entanglement can ever offer an advantage in terms of the *rates* achievable in the *large block length limit* was left as an open question. Clearly, the Lovász bound cannot be used to prove such a separation. Fortunately, there is another bound due to Haemers which is sometimes better than the Lovász bound [9].

**Theorem 1** (Haemers [9]). For  $u, v \in V(G)$  let  $M_{uv}$  be a matrix with entries in any field  $K$ . We say that  $M$  **fits**  $G$  if  $M_{uu} \neq 0$  and  $M_{uv} = 0$  whenever there is no edge between  $u$  and  $v$ . Then  $\Theta(G) \leq R(G) := \min\{\text{rank}(M) : M \text{ fits } G\}$ . In particular,  $C_0(G) \leq \log R(G)$ .

*Proof.* Let  $S$  be a maximal independent set in  $G$ . If  $M$  fits  $G$ , then  $M_{uv} = 0$  for all  $u \neq v \in S$  while the diagonal entries are non-zero. Hence,  $M$  has full rank on a subspace of dimension  $|S|$  and thus  $\text{rank}(M) \geq |S| = \alpha(G)$ . As this is true for any  $M$  that fits  $G$ , we get  $R(G) \geq \alpha(G)$ .

Next, note that if  $M_1$  fits  $G_1$  and  $M_2$  fits  $G_2$  then  $M_1 \otimes M_2$  fits  $G_1 \boxtimes G_2$ , and  $\text{rank}(A \otimes B) = \text{rank}(A)\text{rank}(B)$ . Hence,  $R(G_1 \boxtimes G_2) \leq R(G_1)R(G_2)$ , which implies the desired result.  $\square$

In the next section we apply Haemers bound to a particular graph to show that its unassisted zero-error capacity is small, and also provide an explicit entanglement-assisted protocol that achieves a higher rate. This shows that entanglement assistance can indeed increase the asymptotic zero-error rate, thus giving an affirmative answer to the previously open question.

The entanglement-assisted protocol is based on the fact that the graph in question can be constructed from the **root system** [16]  $E_7$ , so in Section 3 we investigate constructions based on other irreducible root systems. Most notably we show that a construction based on  $E_8$  provides another example with an even bigger gap in the capacities. In Section 4 we discuss open problems.

## 2 The zero-error capacities of the symplectic graph $sp(6, \mathbb{F}_2)$

We first define *symplectic space* over a finite field and the corresponding *symplectic graph* [14].

**Definition 4** (Symplectic form). A **non-degenerate symplectic space**  $(V, S)$  is a vector space  $V$  (over a field  $K$ ) equipped with a **non-degenerate symplectic form**, i.e., a bilinear map  $S : V \times V \rightarrow K$  which is

- skew-symmetric:  $S(u, v) = -S(v, u)$  for all  $u, v \in V$ , and
- non-degenerate: if  $S(u, v) = 0$  for all  $v \in V$ , then  $u = 0$ .

If  $K = \mathbb{F}_2$ , we also require that  $S(u, u) = 0$  for all  $u \in V$  (for other fields this is implied by the anti-symmetry property). On a  $2m$ -dimensional space, the **canonical symplectic form** is

$$\sigma(u, v) := u^T \begin{pmatrix} 0 & \mathbb{1}_m \\ -\mathbb{1}_m & 0 \end{pmatrix} v.$$

where  $\mathbb{1}_m$  is the  $m \times m$  identity matrix. Any non-degenerate symplectic space with finite dimensional vector space  $V$  is isomorphic to the canonical symplectic space  $(V, \sigma)$ .

**Definition 5** (Symplectic graph). Let  $K$  be a finite field and let  $m$  be a natural number. The vertices of the **symplectic graph**  $sp(2m, K)$  are the points of the projective space  $\mathbb{P}K^{2m}$  and there is an edge between  $u, v \in \mathbb{P}K^{2m}$  if  $\sigma(u, v) = 0$ . In the case where  $K = \mathbb{F}_2$ , the points of the projective space are simply the  $2^{2m} - 1$  non-zero elements of  $\mathbb{F}_2^{2m}$ .

**Remark 1.** The symplectic graph  $sp(2m, \mathbb{F}_2)$  is isomorphic to the graph whose vertices are all the  $m$ -fold tensor products of Pauli matrices except for the identity i.e.  $\{\mathbb{1}, X, Y, Z\}^{\otimes m} \setminus \{\mathbb{1}^{\otimes m}\}$ , and which has edges between commuting matrices.

The next two subsections are devoted to prove our main result:

**Theorem 2.**  $C_0(sp(6, \mathbb{F}_2)) = \log 7$  while  $C_0^E(sp(6, \mathbb{F}_2)) = \log 9$ .

### 2.1 Capacity in the unassisted case

The fact that  $C_0(sp(6, \mathbb{F}_2)) = \log 7$  is a special case of a result in [14] but we give a full proof here.

**Theorem 3** (Peeters [14]).  $C_0(sp(2m, \mathbb{F}_2)) = \log(2m + 1)$ .

*Proof.* For the upper bound we construct a matrix over  $\mathbb{F}_2$  which fits  $sp(2m, \mathbb{F}_2)$  and which has rank  $2m + 1$  and use Haemers' bound (see Theorem 1). Let

$$U_m := \{v \in \mathbb{F}_2^{2m+1} : \langle v, v \rangle = 0\}$$

be the  $2m$ -dimensional subspace of  $\mathbb{F}_2^{2m+1}$  that consists of vectors which have an even number of entries equal to one. On  $U_m$ , the inner product  $\langle \cdot, \cdot \rangle$  is a non-degenerate symplectic form, so there is an isomorphism  $T : (\mathbb{F}_2^{2m}, \sigma) \rightarrow (U_m, \langle \cdot, \cdot \rangle)$  such that

$$\forall u, v \in \mathbb{F}_2^{2m} : \sigma(u, v) = \langle T(u), T(v) \rangle.$$

Let  $\mathbf{1}$  be the all-ones vector in  $\mathbb{F}_2^{2m+1}$  (note that  $\langle \mathbf{1}, v \rangle = 0$  for all  $v \in U_m$ ). For all  $u, v \in \mathbb{F}_2^{2m}$  let

$$\begin{aligned} M_{uv} &:= \langle \mathbf{1} + T(u), \mathbf{1} + T(v) \rangle \\ &= \langle \mathbf{1}, \mathbf{1} \rangle + \langle \mathbf{1}, T(v) \rangle + \langle T(u), \mathbf{1} \rangle + \langle T(u), T(v) \rangle \\ &= 1 + \sigma(u, v). \end{aligned}$$

Since  $\sigma(u, v) = 1$  if and only if  $u$  and  $v$  are not joined by an edge in  $sp(2m, \mathbb{F}_2)$ , matrix  $M$  fits  $sp(2m, \mathbb{F}_2)$ . Since it is the Gram matrix of a set of  $(2m + 1)$ -dimensional vectors (i.e. the entry at  $i, j$  is the inner product of the vector  $i$  and vector  $j$  for some ordering of the set of vectors), its rank is at most  $2m + 1$ . By Haemers' bound,  $C_0(sp(2m, \mathbb{F}_2)) \leq \log(2m + 1)$ .

For the matching lower bound, let  $e_i$  for  $1 \leq i \leq 2m + 1$  be the standard basis of  $\mathbb{F}_2^{2m+1}$ , and let  $f_i := e_i + \mathbf{1}$ . Then  $\langle f_i, f_j \rangle = 1 - \delta_{ij}$  so  $f_i \in U_m$  and  $\sigma(T^{-1}(f_i), T^{-1}(f_j)) = 1 - \delta_{ij}$ . Therefore  $\{T^{-1}(f_i) : i = 1, \dots, 2m + 1\}$  is an independent set of size  $2m + 1$  in  $sp(2m, \mathbb{F}_2)$ , so  $\alpha(sp(2m, \mathbb{F}_2)) \geq 2m + 1$ .

Hence,  $C_0(sp(2m, \mathbb{F}_2)) = \log \alpha(sp(2m, \mathbb{F}_2)) = \log(2m + 1)$  and the upper bound on the zero-error capacity is attained by a code of block length one.  $\square$

## 2.2 Entanglement-assisted capacity

In this section we use the following result to establish the entanglement-assisted capacity of  $sp(6, \mathbb{F}_2)$ . It is Theorem 11 in [5] and its proof can be found there.

**Theorem 4.** Suppose that  $G$  is a graph with a faithful orthonormal representation in  $\mathbb{C}^d$  (or  $\mathbb{R}^d$ ). That is, each vertex is labelled with a vector in  $\mathbb{C}^d$  ( $\mathbb{R}^d$ ) such that the vectors are orthogonal iff the vertices are connected by an edge. If the vertices of  $G$  can be partitioned into exactly  $q$  cliques  $\{\mathcal{K}_1, \dots, \mathcal{K}_q\}$  each of size  $d$ , then there is a one-shot zero-error communication protocol assisted by a rank- $d$  maximally entangled state, which shows that  $C_0^E(G) \geq q$ . Also, the Lovász number  $\vartheta(G) = q$ , and since [7, 8] proved that  $C_0^E(G) \leq \vartheta(G)$ . Therefore,  $C_0^E(G) = q$ .

**Lemma 1.** The  $2^{2m} - 1$  vertices of  $sp(2m, \mathbb{F}_2)$  can be partitioned into  $2^m + 1$  cliques of size  $2^m - 1$ .

*Proof.* Such a partition of the symplectic graph is known as a *symplectic spread*, and is well-known to exist (see for example [10] or Section 10.12 of [12]). For completeness we give a simple construction [13] here. Another proof in terms of commuting sets of Pauli operators is given in [11].

Let  $q = 2^m$ , and identify the vertices of  $sp(2m, \mathbb{F}_2)$  with the non-zero vectors in  $\mathbb{F}_q^2$ . Consider the following symplectic form on  $\mathbb{F}_q^2$ :

$$\sigma_q((w, x), (y, z)) = \text{Tr}(wz + xy),$$

where  $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_2$  is the *finite field trace* defined as  $\text{Tr}(a) := a + a^2 + a^{2^2} + \dots + a^{2^{m-1}}$ . As  $\langle x, y \rangle_q := \text{Tr}(xy)$  is a non-degenerate inner product in  $\mathbb{F}_q$ , the form  $\sigma_q$  is also non-degenerate. Hence, the symplectic spaces  $(\mathbb{F}_2^m, \sigma)$  and  $(\mathbb{F}_q^2, \sigma_q)$  are isomorphic. We will describe the partition for the later space.

Denoting the multiplicative group (of order  $q - 1$ ) in  $\mathbb{F}_q$  by  $\mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$ , the cells of a partition of the elements of  $\mathbb{F}_q^2$  are:

$$\begin{aligned} \pi_a &= \{(x, ax) : x \in \mathbb{F}_q^\times\} & (a \in \mathbb{F}_q), \\ \pi_{q+1} &= \{(0, x) : x \in \mathbb{F}_q^\times\}. \end{aligned}$$

It is easy to check that these  $q + 1$  cells of size  $q - 1$  partition  $\mathbb{F}_q^2$ . Moreover, if  $(x, ax)$  and  $(y, ay)$  are in the same cell, then

$$\sigma((x, ax), (y, ay)) = \text{Tr}(xay + axy) = \text{Tr}(0) = 0.$$

Therefore each cell is a clique.  $\square$

It remains to show that

**Proposition 1.**  $C_0^E(sp(6, \mathbb{F}_2)) = \log 9$ .

*Proof.* By the previous lemma the 63 vertices of  $sp(6, \mathbb{F}_2)$  can be partitioned into 9 cliques each of size 7. Therefore, by Theorem 11 of [5],  $c_0^E(sp(6, \mathbb{F}_2)) = 9$  if it is possible to assign a vector  $\phi(v)$  in  $\mathbb{C}^7$  to each vertex  $v$  of  $sp(6, \mathbb{F}_2)$  so that  $\phi(u)$  and  $\phi(v)$  are orthogonal whenever  $uv$  is an edge. Interestingly, it is possible to do this using (real) normalized vectors from the root system [16]  $E_7$ .

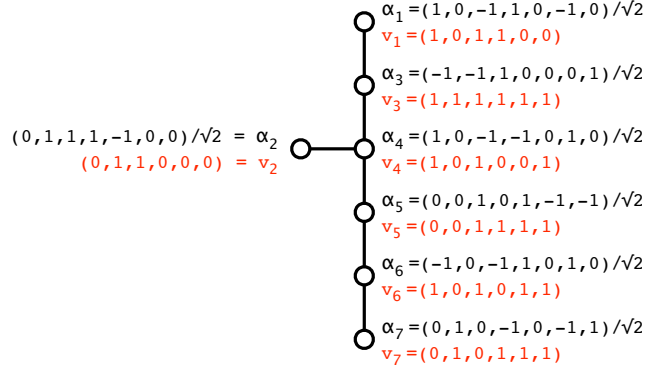


Figure 1: The Dynkin diagram of  $E_7$ , a concrete set of simple roots  $\alpha_i$ , and the associated elements of  $\mathbb{F}_2^6$ .

In Figure 1 we give a set of *simple roots*  $\alpha_1, \dots, \alpha_7$  for the root system  $E_7$ . Let  $Y_\alpha$  denote the reflection in the hyperplane perpendicular to the vector  $\alpha \in \mathbb{R}^7$ . The full root system  $R$  is equal to the orbit of  $\alpha_1$  under the action of the reflection group generated by the reflections  $Y_{\alpha_1}, \dots, Y_{\alpha_7}$  and it contains 126 vectors consisting of 63 pairs with opposite sign.

The  $E_7$  lattice consists of all integer linear combinations of the roots:

$$E_7 := \left\{ \sum_{i=1}^7 n_i \alpha_i : (n_1, \dots, n_7) \in \mathbb{Z}^7 \right\}.$$

Cherchai and Geeman [15] define a map  $\kappa : E_7 \rightarrow \mathbb{F}_2^6$  that acts on the simple roots as  $\kappa(\alpha_i) = v_i$ , where  $v_1, \dots, v_7 \in \mathbb{F}_2^6$  are given in Figure 1. On the remaining lattice it is extended by linearity:

$$\kappa : \sum_{i=1}^7 n_i \alpha_i \mapsto \sum_{i=1}^7 n_i v_i \pmod{2}.$$

One can check that the images  $v_i$  of simple roots are chosen so that for all  $\alpha, \beta \in E_7$ :

$$\alpha \cdot \beta = \sigma(\kappa(\alpha), \kappa(\beta)) \pmod{2}.$$

Moreover, if  $\alpha, \beta \in R$  then  $\alpha \cdot \beta \in \{0, \pm 1, \pm 2\}$  and  $\alpha \cdot \beta = \pm 2$  if and only if  $\alpha = \pm \beta$ . Therefore, distinct roots  $\alpha, \beta \in R$  are orthogonal if and only if  $\sigma(\kappa(\alpha), \kappa(\beta)) = 0$ . The image  $\kappa(R)$  is all 63 non-zero elements of  $\mathbb{F}_2^6$  and clearly  $\kappa(-\alpha) = \kappa(\alpha)$ . Therefore, for each non-zero  $v \in \mathbb{F}_2^6$  one can choose  $\phi(v)$  as one of the pair of vectors with opposite sign in  $R \cap \kappa^{-1}(v)$  to obtain the desired orthogonal representation of  $sp(6, \mathbb{F}_2)$ . The entire representation, grouped into 9 complete bases, is given in Appendix A. It can be used to send 9 different messages with a single use of the channel.  $\square$

### 2.3 The connection to $E_7$

A deeper coincidence underlies the orthogonal representation of  $sp(6, \mathbb{F}_2)$  by roots of  $E_7$ . The automorphism group of  $sp(2m, \mathbb{F}_2)$  is the *symplectic group*  $Sp(2m, \mathbb{F}_2)$ , which is the group of linear maps on  $\mathbb{F}_2^{2m}$  which preserve the symplectic form. This group is isomorphic to quotient  $W(E_7)/\{\pm 1\}$ , where  $W(E_7)$  is the *Weyl group* of  $E_7$ , which is generated by the reflections  $Y_{\alpha_1}, \dots, Y_{\alpha_7}$  (an explicit isomorphism is given in [15]). Transvection about a non-zero element  $x$  of a symplectic space with underlying vector space  $V$  is the map  $t_x : V \rightarrow V$  with

$$t_x(y) = y + \sigma(y, x)x$$

where  $\sigma$  is the symplectic form. It is easily checked that transvection preserves the symplectic form i.e. that  $\sigma(t_x(y), t_x(z)) = \sigma(y, z)$ . The isomorphism mentioned is induced by identifying the generating reflection  $Y_{\alpha_i}$  with the transvection  $t_{v_i}$  in  $Sp(6, \mathbb{F}_2)$  (for  $i = 1, \dots, 7$ ).

## 3 Graphs from $E_8$ and other root systems

We define the orthogonality graph of a root system  $R$  as follows. The vectors of  $R$  occur in antipodal pairs  $\{v, -v\}$ ; the vertices  $V(R)$  of the graph are the  $|R|/2$  rays spanned by these antipodal pairs. Two vertices are adjacent if and only if their rays are orthogonal. The graph of Section 2 is precisely the orthogonality graph of  $E_7$ . This raises the question of whether a channel whose confusability graph is the orthogonality graph of another irreducible root system can also exhibit a gap between the classical and entanglement-assisted zero-error capacities. We find that the orthogonality graph of  $E_8$  provides a second example of such a gap, and furthermore, the ratio between the assisted and classical capacities is larger in this case.

The irreducible root systems consist of the infinite families  $A_n, B_n, C_n, D_n$  where  $n \in \mathbb{N}$ , and the exceptional cases  $E_6, E_7, E_8, F_4$ , and  $G_2$  (see [17]). We show that for all of the infinite families, and for  $G_2$ , there is no gap between the independence number  $\alpha$  and the Lovász number  $\vartheta$ , so  $C_0^E = C_0$  for these graphs. However, the orthogonality graph of  $E_8$  provides a second example of a gap between the classical and entanglement-assisted capacity. For  $E_8$ , we show that  $C_0 \leq \log 9$  while  $C_0^E = \log 15$ . It is interesting to note that the graph used in [4] is precisely the orthogonality graph of  $F_4$  and while we know the entanglement-assisted capacity of this graph, we still do not know its unassisted capacity or whether it is smaller than the assisted one. We do not give either capacity for the graph of  $E_6$ .

In what follows the name of the root system is also used as the name of the orthogonality graph and  $e_i$  denotes the  $i$ -th standard basis vector. We ignore correct normalisation of the root vectors for simplicity, since it clearly doesn't affect the orthogonality graph.

### Root system $E_8$

$$V(E_8) = \{e_i \pm e_j : 1 \leq i < j \leq 8\} \cup \{(x_1, \dots, x_8) : x_i = \pm 1, \prod_{i=1}^8 x_i = 1\}$$

As pointed out in [18],  $E_8$  is the graph whose vertices are the non-isotropic points in the ambient projective space of the polar space  $O^+(8, \mathbb{F}_2)$ , with vertices adjacent if they are orthogonal with respect to the associated bilinear form. The ambient projective space of  $O^+(2m, \mathbb{F}_2)$  is  $\mathbb{P}\mathbb{F}_2^{2m}$ . Since the bilinear form associated with  $O^+(2m, \mathbb{F}_2)$  is symplectic, it follows immediately that  $E_8$  is an induced subgraph of the symplectic graph  $sp(2m, \mathbb{F}_2)$  with  $m = 4$ . By Theorem 3,

$$C_0(E_8) \leq C_0(sp(8, \mathbb{F}_2)) = \log 9.$$

On the other hand, let  $q = 16$  and identify the vertices of  $sp(8, \mathbb{F}_2)$  with the non-zero vectors of  $\mathbb{F}_q^2$ . Then we may choose the quadratic form of  $O^+(8, \mathbb{F}_2)$  to be  $(x, y) \mapsto \text{Tr}(xy)$ , where

$\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_2$  is the finite field trace. The polarization of this quadratic form is the symplectic form  $\sigma((w, x), (y, z)) = \text{Tr}(wz + xy)$ . With this choice, the vertices of  $E_8$ , i.e., the non-isotropic vectors in  $sp(8, \mathbb{F}_2)$ , are those  $(x, y) \in \mathbb{F}_q^2$  such that  $\text{Tr}(xy) = 1$ . Now, consider the partition of vertices into cliques given in Lemma 1, restricted to the vertices of  $E_8$ :

$$\pi_a = \{(x, ax) : x \in \mathbb{F}_q^\times, \text{Tr}(ax^2) = 1\}, \quad (a \in \mathbb{F}_q^\times).$$

Recall that  $\text{Tr}(ax^2) = \text{Tr}(a^2x^4) = \dots = \text{Tr}(a^8x)$ . For each  $a \in \mathbb{F}_q^\times$ , there are exactly 8 choices of  $x \in \mathbb{F}_q^\times$  such that  $\text{Tr}(a^8x) = 1$ . Therefore,  $\{\pi_a : a \in \mathbb{F}_q^\times\}$  is a partition of the vertices of  $E_8$  into 15 cliques of size 8. By Theorem 11 of [5],

$$C_0^E(E_8) = \log 15.$$

### Root system $A_n$ ( $n \geq 1$ )

$$V(A_n) = \{e_i - e_j : 1 \leq i < j \leq n + 1\}.$$

This graph is isomorphic to the Kneser graph  $KG_{n+1,2}$ . By a result of Lovász (Theorem 13 of [6]),

$$\alpha(A_n) = \vartheta(A_n) = \Theta(A_n) = n.$$

### Root system $D_n$ ( $n \geq 4$ )

$$V(D_n) = \{e_i \pm e_j : 1 \leq i < j \leq n\}.$$

Note that the vertices  $\{e_i - e_j : 1 \leq i < j \leq n\}$  induce a subgraph isomorphic to  $A_{n-1} \cong KG_{n,2}$ . Also note that  $e_i + e_j$  and  $e_i - e_j$  are adjacent and have the same neighbourhood (apart from themselves). It follows that  $D_n$  is isomorphic to  $KG_{n,2} \boxtimes K_2$ , the strong graph product of a Kneser graph and a complete graph on 2 vertices. By Theorem 7 of [6],

$$\Theta(D_n) = \Theta(KG_{n,2})\Theta(K_2) = n - 1.$$

Since  $\{e_1 - e_j : 2 \leq j \leq n\}$  is an independent set of size  $n - 1$ , it follows that

$$\alpha(D_n) = \vartheta(D_n) = \Theta(D_n) = n - 1.$$

### Root system $B_n$ ( $n \geq 2$ )

$$V(B_n) = \{e_i \pm e_j : 1 \leq i < j \leq n\} \cup \{e_i : 1 \leq i \leq n\}.$$

To find the Lovász number we consider even and odd  $n$  separately. When  $n$  is odd, partition the vertices into sets  $\pi_1, \dots, \pi_n$ , where

$$\pi_k = \{e_i \pm e_j : i < j, i + j \equiv 2k \pmod{n}\} \cup \{e_k\}.$$

Each  $\pi_k$  is a clique of size  $n$ . When  $n$  is even, partition the vertices into sets  $\pi_1, \dots, \pi_n$ , where

$$\begin{aligned} \pi_k &= \{e_i \pm e_j : i < j, i + j \equiv 2k \pmod{n-1}\} \cup \{e_k \pm e_n\} \quad (k \leq n-1); \\ \pi_n &= \{e_1, \dots, e_n\}. \end{aligned}$$

Again each  $\pi_k$  is a clique of size  $n$ . In either case, we have partitioned the graph into  $n$  cliques of size  $n$ . By Theorem 11 of [5],  $\Theta(B_n) = n$ .

Since  $\{e_1 - e_j : 2 \leq j \leq n\} \cup \{e_1\}$  is an independent set of size  $n$ , we have

$$\alpha(B_n) = \vartheta(B_n) = \Theta(B_n) = n.$$

## Root system $C_n$ ( $n \geq 2$ )

$$V(C_n) = \{e_i \pm e_j : 1 \leq i < j \leq n\} \cup \{2e_i : 1 \leq i \leq n\}.$$

$C_n$  has the same orthogonality graph as  $B_n$ .

## Root system $G_2$

$$V(G_2) = \{(1, -1, 0), (1, 0, -1), (0, 1, -1), (1, 1, -2), (1, -2, 1), (-2, 1, 1)\}.$$

By inspection  $G_2$  has an independent set of size 3 and can be partitioned into 3 cliques of size 2. By Theorem 11 of [5],

$$\alpha(G_2) = \vartheta(G_2) = \Theta(G_2) = 3.$$

## 4 Conclusion

We have shown that it is possible for entanglement to increase the asymptotic rate of zero-error classical communication over some classical channels. This is quite different from the situation for families of codes which only achieve arbitrarily small error rates asymptotically. The best rate that can be achieved by classical codes in this context is the Shannon capacity and entanglement *cannot* increase this rate. The entanglement-assisted capacity has a simple formula which reduces to the formula for the Shannon capacity when the channel is classical [3].

It is interesting to note that in every example of a graph with  $c_0(G) > c_0^E(G)$  found to date, the entanglement-assisted capacity is attained by a code of block length one. This certainly is not true of the entanglement-assisted capacities of all graphs. In [2], an interesting observation of Arikan is reported: The graph consisting of a five cycle and one more isolated vertex has  $\Theta = \sqrt{5} + 1$ . Since no (positive integer) power of this quantity is an integer, the capacity is not attained by any finite length block code for this graph. Since the Lovász number of this graph is also  $\sqrt{5} + 1$  (the Lovász number is additive for disjoint unions of graphs, and was calculated for cycles in [6]), the same observation is true for the entanglement-assisted capacity, which in this case is equal to the unassisted capacity.

A very general family of open problems remains, namely, is there an algorithm, an efficient algorithm or even a simple formula for the entanglement-assisted capacity in the one-shot or asymptotic case? While it is not even known if there is an algorithm for the unassisted zero-error capacity, it is possible that the entanglement assistance actually simplifies the calculation. This is the case for determining the traditional classical and quantum capacities of quantum channels [3] and it was shown in [5] that the zero-error capacity of a channel assisted by generalized non-signaling correlations is given by a simple linear program determined by the channel. It would also be interesting to determine whether the ratio  $C_0^E/C_0$  can be arbitrarily large and, more generally, to find upper and lower bounds on it in terms of the number of vertices in the graph.

## Acknowledgements

We would like to thank Andrew Childs, Richard Cleve, David Roberson, Simone Severini and Andreas Winter for useful discussions. This work was supported by NSERC, QuantumWorks, CIFAR, CFI, and ORF. Aidan Roy acknowledges support by a UW/Fields Institute Award.

## References

- [1] C. E. Shannon, “The zero-error capacity of a noisy channel”, IRE Trans. Inform. Theory, vol. IT-2(3):8-19 (1956).



- [2] J. Körner, A. Orlitsky, “Zero-Error Information Theory”, *IEEE Trans. Inf. Theory* **44**(6):2207-2229 (1998).
- [3] C. H. Bennett, P. Shor, J. Smolin, A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem”, *IEEE Trans. Info. Theory* **48**, 2637-2655, (2002) arXiv:quant-ph/0106052.
- [4] T. S. Cubitt, D. Leung, W. Matthews, A. Winter, “Improving zero-error classical communication with entanglement”, arXiv:0911.5300 (2009).
- [5] T. S. Cubitt, D. Leung, W. Matthews, A. Winter, “Zero-error channel capacity and simulation assisted by non-local correlations”, arXiv:1003.3195 (2010).
- [6] L. Lovász, “On the Shannon Capacity of a Graph”, *IEEE Trans. Inf. Theory* **25**(1):1-7 (1979).
- [7] S. Beigi, “Entanglement-assisted zero-error capacity is upper bounded by the Lovasz theta function”, arXiv:1002.2488 (2010).
- [8] R. Duan, S. Severini, A. Winter, “Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász  $\vartheta$  function”, arXiv:1002.2514 (2010).
- [9] W. Haemers, “On Some Problems of Lovász Concerning the Shannon Capacity of a Graph”, *IEEE Trans. Inf. Theory* **25**(2):231-232 (1979). W. Haemers, “An upper bound for the Shannon capacity of a graph”, *Coll. Math. Soc. János Bolyai* **25**:267-272 (1978).
- [10] R. H. Dye, “Partitions and their stabilizers for line complexes and quadrics”, *Ann. Mat. Pura Appl. (4)* **114**:173-194 (1977).
- [11] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, F. Vatan, “A New Proof for the Existence of Mutually Unbiased Bases”, *Algorithmica* **34**(4):512-528
- [12] C. Godsil, G. Royle, *Algebraic graph theory*, Springer, New York, 2001.
- [13] S. Ball, J. Bamberg, M. Lavrauw and T. Penttila, *Symplectic Spreads, Designs, Codes and Cryptography*, Volume 32, Numbers 1-3, 9-14, ISSN 0925-1022, DOI: 10.1023/B:DESI.0000029209.24742.89.
- [14] R. Peeters, “Orthogonal Representations over Finite Fields and the Chromatic Number of Graphs”, *Combinatorica* **16**(3):417-431 (1996).
- [15] B. L. Cherchai, B. van Geeman, “From qubits to E7”, arXiv:1003.4255 (2010)
- [16] K. Erdmann and M. Wildon, *Introduction to Lie Algebras*, Springer, London (2006).
- [17] J. Humphreys, *Reflection groups and Coxeter groups*, Cambridge University Press, Cambridge, 1992.
- [18] P. Panigrahi, “The Diameters Graph of the Root System  $E_8$  is Uniquely Geometrisable”, *Geom. Dedicata*, **78**(2):121-141 (1999).



