Zero-error source-channel coding with entanglement

Jop Briët, Harry Buhrman, Monique Laurent, Teresa Piovesan, and Giannicola Scarpa*

Centrum Wiskunde & Informatica (CWI), Science Park 123, 1098 XG Amsterdam, The Netherlands

1 Introduction

We study a problem from zero-error information theory—a topic well-known for its rich connections to combinatorics [12, 14, 10, 8, 1, 11]—in a setting where a sender and receiver may use quantum entanglement, one of the most striking features of quantum mechanics. The problem that we consider is the classical *source-channel coding problem*, where Alice and Bob are each given an input from a random source and get access to a noisy channel through which Alice can send messages to Bob. Their goal is to minimize the average number of channel uses per source input while allowing Bob to learn Alice's inputs. Here we show that entanglement can allow for an unbounded decrease in the asymptotic rate of classical source-channel codes. We also consider the *source problem*, the case where Alice can send messages to Bob without noise. We prove a lower bound on the rate of source codes with entanglement in terms of a variant of the Lovász theta number [10, 13], a graph parameter given by a semidefinite program.

1.1 Classical source-channel coding

We briefly explain the three relevant problems from zero-error information theory and their well-known graph-theoretical characterizations.

A *discrete dual source* $\mathscr{M} = (\mathsf{X}, \mathsf{U}, P)$ consists of a finite set X, a (possibly infinite) set U and a probability distribution P over $\mathsf{X} \times \mathsf{U}$. In a dual-source instance, with probability $P(x,u)$, Alice gets an input $x \in \mathsf{X}$ and Bob a $u \in \mathsf{U}$. Bob needs to learn Alice's input without error by having Alice send Bob as few bits as possible. Associated to $\mathscr{M}$ is its *characteristic graph* $G = (\mathsf{X}, E)$, where $\{x,y\} \in E$ if there exists a $u \in \mathsf{U}$ such that $P(x,u) > 0$ and $P(y,u) > 0$. As observed in [14], solving the zero-error source coding problem is equivalent to

*J. B. and H. B. were supported by the European Commission under the project QCS (Grant No. 255961), and G. S. was supported by Vidi grant 639.072.803 from the Netherlands Organization for Scientific Research (NWO).

finding a proper coloring of G that uses the minimum number of colors and the *Witsenhausen rate*

$$R(G) = \lim_{m\to\infty} \frac{1}{m} \log \chi(G^{\boxtimes m}) \tag{1}$$

is the minimum asymptotic *cost rate* (i.e., the average number of bits Alice needs to send Bob per source input) of a zero-error code for $\mathscr{M}$. Here $G^{\boxtimes m}$ is the m^{th} strong graph power [12] and log is the logarithm in base 2.

A *discrete channel* $\mathscr{N} = (\mathsf{S}, \mathsf{V}, Q)$ consists of a finite input set S, a (possibly infinite) output set V and a probability distribution $Q(\cdot|s)$ over V for each $s \in \mathsf{S}$. If Alice sends $s \in \mathsf{S}$ through the channel, then Bob receives $v \in \mathsf{V}$ with probability $Q(v|s)$. Associated to a channel is its *confusability graph* $H = (\mathsf{S}, F)$, where $\{s,t\} \in F$ if there exists a $v \in \mathsf{V}$ such that both $Q(v|s) > 0$ and $Q(v|t) > 0$. As observed in [12], $\alpha(H^{\boxtimes n})$ is the maximum number of distinct possible messages that Alice can send to Bob without error by using the channel n times. The *Shannon capacity*

$$c(H) = \lim_{n\to\infty} \frac{1}{n} \log \alpha(H^{\boxtimes n}) \tag{2}$$

gives the maximum asymptotic rate of a zero-error channel code.

In the *source-channel coding problem* the parties get inputs from a dual source $\mathscr{M}$ and get access to a channel $\mathscr{N}$. As observed in [11], if $\mathscr{M}$ has characteristic graph G and $\mathscr{N}$ has confusability graph H, then a zero-error coding scheme which encodes length m source-input-sequences into length n channel-input-sequences defines a homomorphism from $G^{\boxtimes m}$ to $\overline{H^{\boxtimes n}}$. The parameter

$$\eta(G,H) := \lim_{m\to\infty} \frac{1}{m} \min\left\{ n \in \mathbb{N} : G^{\boxtimes m} \xrightarrow{\exists \text{homomorphism}} \overline{H^{\boxtimes n}} \right\}$$

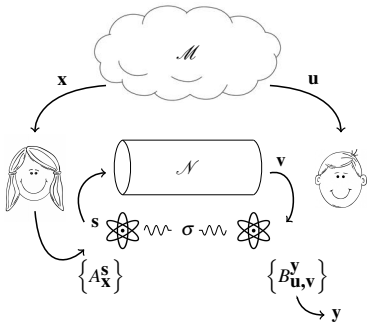
gives the minimum asymptotic cost rate (i.e., the minimum average number of channel uses per source input) of a zero-error code. Note that $R(G) = \eta(G, \overline{K_2})$ and $1/c(H) = \eta(K_2, H)$. In general $\eta(G,H) \leq R(G)/c(H)$ and in [11] it is shown that unbounded separations between $\eta(G,H)$ and $R(G)/c(H)$ can occur.

1.2 Source-channel coding with entanglement

We briefly introduce the model of entanglement-assisted coding, but a direct algebraic definition of the entanglement-assisted variant of $\eta(G,H)$ is given in Definition 1.1. A *state* is a complex positive semidefinite matrix with trace 1. The possible states of a pair of d-dimensional quantum systems $(\mathscr{A}, \mathscr{B})$ are the states in $\mathbb{C}^{d\times d} \otimes \mathbb{C}^{d\times d}$. Such a pair is *entangled* if its state is not a convex combination of states of the form $\rho_A \otimes \rho_B$ with $\rho_A \in \mathbb{C}^{d\times d}$ and $\rho_B \in \mathbb{C}^{d\times d}$. A *$t$-outcome measurement* is a collection $\mathsf{A} = \{A^i \in \mathbb{C}^{d\times d} : i \in [t]\}$ of positive semidefinite matrices A^i that satisfy $\sum_{i=1}^t A^i = I$. A measurement describes an experiment that one may perform on a d-dimensional quantum system. If $(\mathscr{A}, \mathscr{B})$ is in a state σ, and Alice performs a t-outcome measurement A on $\mathscr{A}$ and Bob performs an r-outcome measurement B on $\mathscr{B}$, then they obtain outcomes $i \in [t]$ and $j \in [r]$, respectively, with probability $\mathsf{Tr}\left((A^i \otimes B^j)\sigma\right)$.

The *entanglement-assisted* protocol for solving the source-channel coding problem is as follows:

(1) Alice and Bob get inputs $\mathbf{x} \in \mathsf{X}^m$ and $\mathbf{u} \in \mathsf{U}^m$, respectively, from the source $\mathscr{M}$;
(2) Alice performs a measurement $\{A^{\mathbf{s}}_{\mathbf{x}} \in \mathbb{C}^{d\times d} : \mathbf{s} \in \mathsf{S}^n\}$ on her system $\mathscr{A}$ (the measurement may depend on $\mathbf{x}$);
(3) Alice sends the outcome $\mathbf{s}$ over $\mathscr{N}$;
(4) Bob receives an output $\mathbf{v}$ from $\mathscr{N}$;
(5) Bob performs a measurement $\{B^{\mathbf{y}}_{\mathbf{u},\mathbf{v}} \in \mathbb{C}^{d\times d} : \mathbf{y} \in \mathsf{X}^m\}$ (which may depend on $\mathbf{u}$ and $\mathbf{v}$) on his system $\mathscr{B}$;
(6) Bob obtains a measurement outcome $\mathbf{y} \in \mathsf{X}^n$.



A zero-error entanglement-assisted coding scheme satisfies that Bob's measurement outcome $\mathbf{y}$ is Alice's input $\mathbf{x}$ with probability 1. With a similar technique as in [6], we can define the entanglement variant of $\eta(G,H)$ as follows.

Definition 1.1. *For graphs G,H and $m \in \mathbb{N}$, define $\eta^\star_m(G,H)$ as the minimum positive integer n such that there exist $d \in \mathbb{N}$ and $d \times d$ positive semidefinite matrices $\{\rho^{\mathbf{s}}_{\mathbf{x}} : \mathbf{x} \in V(G^{\boxtimes m}), \mathbf{s} \in V(H^{\boxtimes n})\}$ and ρ such that $\mathsf{Tr}(\rho) = 1$,*

$$\begin{aligned} \sum_{\mathbf{s}\in V(H^{\boxtimes n})} \rho^{\mathbf{s}}_{\mathbf{x}} &= \rho \quad \forall \mathbf{x} \in V(G^{\boxtimes m}), \\ \rho^{\mathbf{s}}_{\mathbf{x}}\rho^{\mathbf{t}}_{\mathbf{y}} &= 0 \quad \forall \{\mathbf{x},\mathbf{y}\} \in E(G^{\boxtimes m}), \{\mathbf{s},\mathbf{t}\} \in V(H^{\boxtimes n}) \cup E(H^{\boxtimes n}). \end{aligned}$$

Define $\eta^\star(G,H) = \lim_{m\to\infty} \eta^\star_m(G,H)/m$.

We regain the parameter $\eta(G,H)$ if we restrict the above matrices ρ and $\rho^{\mathbf{s}}_{\mathbf{x}}$ to be $\{0,1\}$-valued scalars. As in the classical setting, we obtain the entangled variants of the Witsenhausen rate $R^\star(G) = \eta^\star(G,\overline{K_2})$ and Shannon capacity $1/c^\star(H) = \eta^\star(K_2,H)$. Alternatively these parameters can be defined analogously to (1) and (2) based on entangled variants of the chromatic and independence numbers $\chi^\star(G)$ and $\alpha^\star(H)$, whose definitions are similar to Definition 1.1. The parameters $\alpha^\star(H)$ and $c^\star(H)$ were first defined in [6], where it was first shown that a separation $\alpha < \alpha^\star$ is possible. It was later shown in [9, 5] that even the zero-error *capacity* can be increased with entanglement (i.e., $c < c^\star$). To the best of our knowledge, neither source nor source-channel coding has been considered in the context of shared entanglement before.

2 Our results

2.1 The entangled chromatic number and Szegedy's number

Our first result gives a lower bound for the entangled chromatic number, which can be efficiently computed with semidefinite programming.

Theorem 2.1. *For every graph G, $\vartheta^+(G) \leq \chi^\star(\overline{G})$ and $\log \vartheta(G) \leq R^\star(\overline{G})$.*

Here $\vartheta(G)$ is the celebrated theta number of Lovász [10] defined by

$$\vartheta(G) = \min\{\lambda : \exists Z \in \mathbb{R}^{V\times V}_{\succeq 0}, Z_{u,u} = \lambda - 1 \text{ for } u \in V, Z_{u,v} = -1 \text{ for } \{u,v\} \notin E\},$$

where $\mathbb{R}^{V\times V}_{\succeq 0}$ is the space of positive semidefinite matrices, and $\vartheta^+(G) \geq \vartheta(G)$ is the variant of Szegedy [13] obtained by adding the constraint $Z_{u,v} \geq -1$ for $\{u,v\} \in E$. Combining with results of [3, 7], we get the chain of inequalities

$$c(G) \leq c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G}) \leq R(\overline{G}).$$

As in the classical setting, the problem of giving stronger bounds on the entangled Witsenhausen rate and Shannon capacity is wide open.

2.2 Classical versus entangled source-channel coding rates

Our second result says that entanglement allows for an unbounded advantage in the asymptotic cost rate of a zero-error source-channel coding scheme. For this we use (as in [5]) the "*quarter orthogonality graph*" H_k (for odd k), with vertices all vectors in $\{-1,1\}^k$ with an even number of "-1" entries and with edges the pairs with inner product -1. We also use the result of [15] showing the existence of a Hadamard matrix (i.e., a matrix $A \in \{-1,1\}^{N\times N}$ that satisfies $AA^\mathsf{T} = NI$) of size $N = 4q^2$ if q is an odd prime power with $q \equiv 1 \bmod 4$.

Theorem 2.2. *For every odd integer $k \geq 5$, we have*

$$\eta^\star(H_k, H_k) \leq \frac{\log(k+1)}{(k-1)\left(1 - \frac{4\log(k+1)}{k-3}\right)}. \tag{3}$$

Moreover, if p is an odd prime and $\ell \in \mathbb{N}$ such that there exists a Hadamard matrix of size $4p^\ell$ (which holds e.g. for $p = 5$ and ℓ even) and $k = 4p^\ell - 1$, then

$$\eta(H_k, H_k) > \frac{0.154k - 1}{k - 1 - \log(k+1)}. \tag{4}$$

The proof of the bound (3) uses the inequality $\eta^\star(H_k, H_k) \leq R^\star(H_k)/c^\star(H_k)$. To show $R^\star(H_k) \leq \log(k+1)$, we prove $\chi^\star(H_k) \leq k+1$ (by constructing feasible operators from a $(k+1)$-dimensional orthonormal representation of H_k) and then conclude using the sub-multiplicativity of $\chi^\star$ under strong graph powers. To show $c^\star(H_k) \geq (k-1)\left(1 - \frac{4\log(k+1)}{k-3}\right)$, we use the celebrated *quantum teleportation* scheme of [4] to exhibit an explicit protocol that achieves such capacity on any channel with confusability graph H_k. This proof-technique appears to be new in the context of zero-error entanglement-assisted communication.

To show (4) we use properties of the fractional chromatic number and vertex transitivity of H_k by which we lower bound $\eta(H_k, H_k)$ by lower bounding $\alpha(\overline{H_k})$ and upper bounding $\alpha(H_k)$. The lower bound uses the existence of a Hadamard matrix of size $k+1$ and the upper bound combines the linear algebra method of Alon [1] with the beautiful construction of certain polynomials in [2].

References

[1] N. Alon. The Shannon capacity of a union. *Combinatorica*, 18(3):301–310, 1998.

[2] D. Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Comput. Complexity*, 4(4):367–382, 1994.

[3] S. Beigi. Entanglement-assisted zero-error capacity is upper-bounded by the Lovász ϑ function. *Phys. Rev. A*, 82(1):010303, 2010.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[5] J. Briët, H. Buhrman, and D. Gijswijt. Violating the Shannon capacity of metric graphs with entanglement. *Proc. Nat. Acad. Sci. U.S.A.*, 2012.

[6] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.*, 104(23):230503, 2010.

[7] R. Duan, S. Severini, and A. Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number. *IEEE Trans. Inf. Theory*, 59(2):1164 –1174, 2013.

[8] J. Körner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Inf. Theory*, 44(6):2207–2229, 1998.

[9] D. Leung, L. Mancinska, W. Matthews, M. Ozols, and A. Roy. Entanglement can increase asymptotic rates of zero-error classical communication over classical channels. *Comm. Math. Phys.*, 311:97–111, 2012.

[10] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inf. Theory*, 25(1):1–7, 1979.

[11] J. Nayak, E. Tuncel, and K. Rose. Zero-error source-channel coding with side information. *IEEE Trans. Inf. Theory,*, 52(10):4626–4629, 2006.

[12] C. Shannon. The zero error capacity of a noisy channel. *IRE Trans. Inf. Theory*, 2(3):8–19, 1956.

[13] M. Szegedy. A note on the ϑ number of Lovász and the generalized Delsarte bound. *FOCS 1994*, pp. 36–39, 1994.

[14] H. S. Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Trans. Inf. Theory*, 22(5):592–593, 1976.

[15] M. Xia and G. Liu. An infinite class of supplementary difference sets and Williamson matrices. *J. Combin. Theory Ser. A*, 58(2):310–317, 1991.