Zero-error source-channel coding with entanglement

Teresa Piovesan

CWI

Joint work with

Jop Briët*, Harry Buhrman, Monique Laurent & Giannicola Scarpa+

(*Courant Institute - NYU)

(+Universitat Autónoma de Barcelona)

QIP 2014

Barcelona, 5 February 2014

Main Question:

Does entanglement help in zero-error communication between two parties with

Main Question:

Does entanglement help in zero-error communication between two parties with

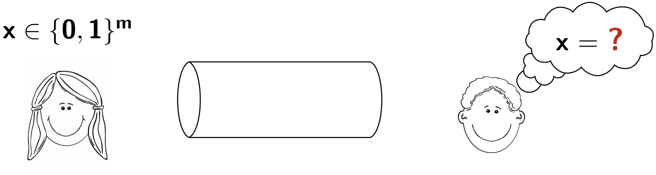
- one-way classical noisy channel

Main Question:

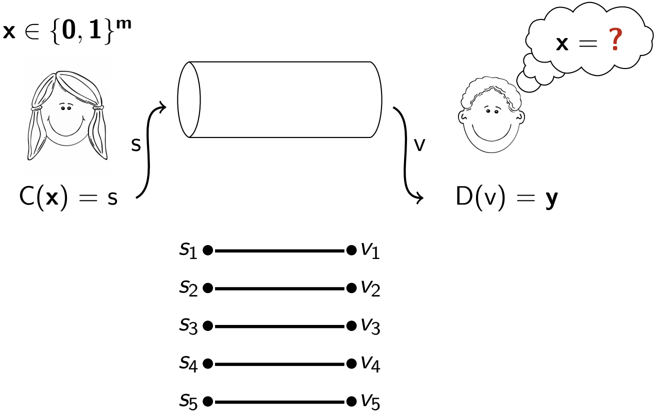
Does entanglement help in zero-error communication between two parties with

- one-way classical noisy channel
- side information from a dual source

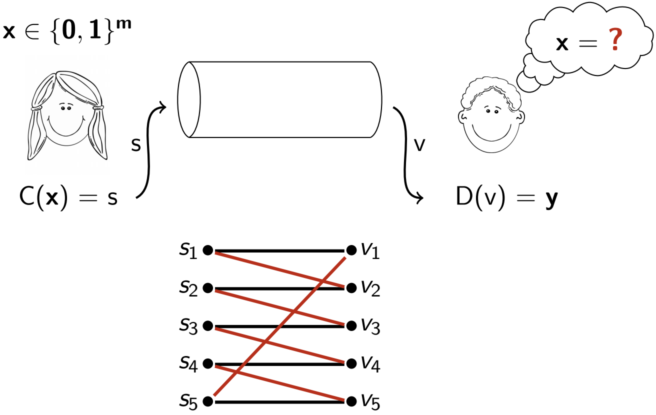
The channel coding problem



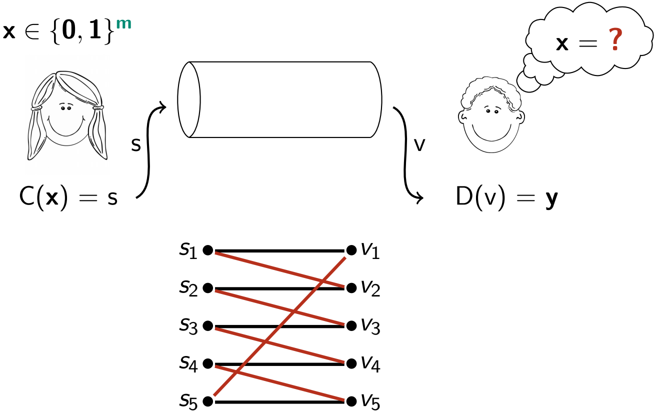
The channel coding problem



The channel coding problem



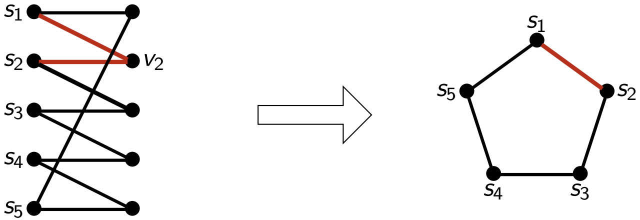
The channel coding problem



- **Goal:** $\mathbf{y} = \mathbf{x}$ with zero probability of error and maximize m

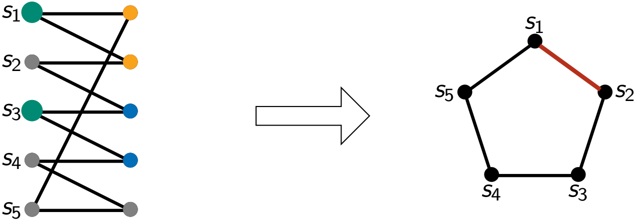
The confusability graph of a channel

- The confusability graph of a noisy channel has as vertices the channel's inputs, which are adjacent if they are confusable



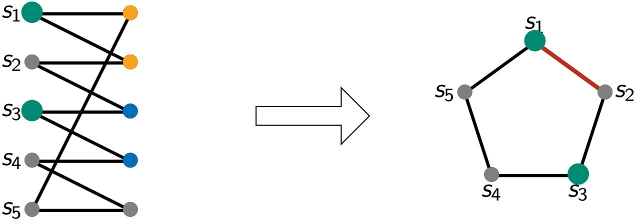
The confusability graph of a channel

- The confusability graph of a noisy channel has as vertices the channel's inputs, which are adjacent if they are confusable



The confusability graph of a channel

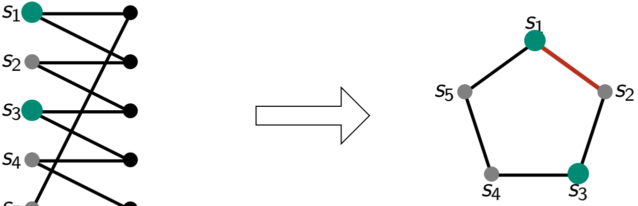
- The confusability graph of a noisy channel has as vertices the channel's inputs, which are adjacent if they are confusable



- An independent set is a set of pairwise non-adjacent vertices

The confusability graph of a channel

- The confusability graph of a noisy channel has as vertices the channel's inputs, which are adjacent if they are confusable

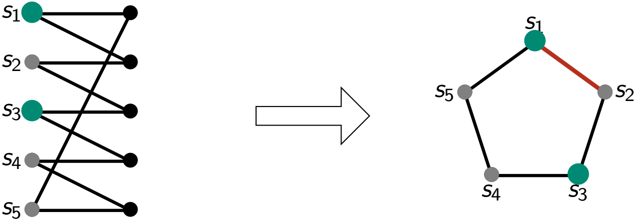


- An independent set is a set of pairwise non-adjacent vertices

- The **independence number** $\alpha(H)$ of a graph H is the size of a largest possible independent set

The confusability graph of a channel

- The confusability graph of a noisy channel has as vertices the channel's inputs, which are adjacent if they are confusable

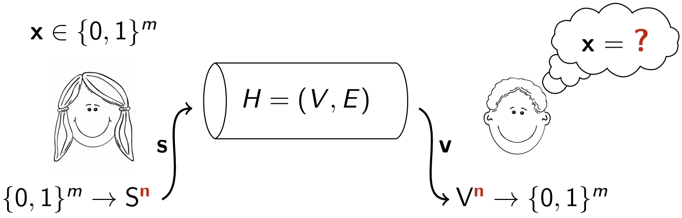


- An independent set is a set of pairwise non-adjacent vertices

- The **independence number** $\alpha(H)$ of a graph H is the size of a largest possible independent set

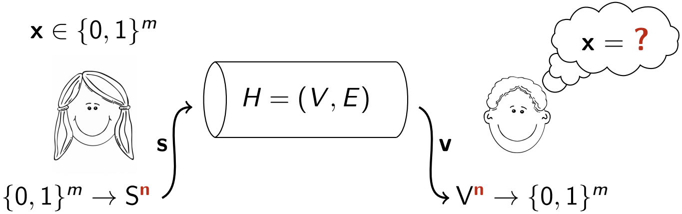
- $\alpha(H)$ is the maximum number of distinct messages Alice can send to Bob

Block coding and the Shannon capacity



- Encoding **x** into a **sequence** of channel inputs can be more efficient

Block coding and the Shannon capacity

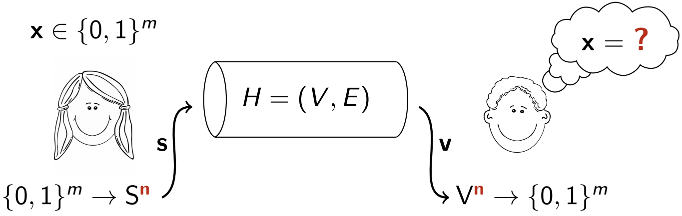


- Encoding **x** into a **sequence** of channel inputs can be more efficient
- The **Shannon capacity** of H

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

gives the maximum average number of bits that can be sent per channel use

Block coding and the Shannon capacity



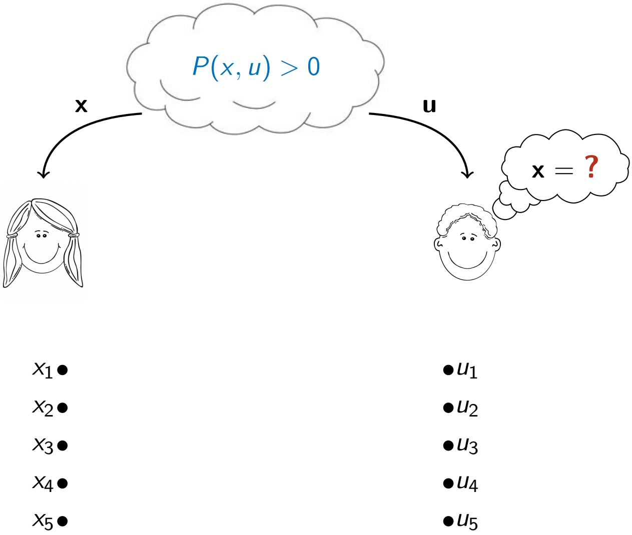
- Encoding **x** into a **sequence** of channel inputs can be more efficient
- The **Shannon capacity** of H

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

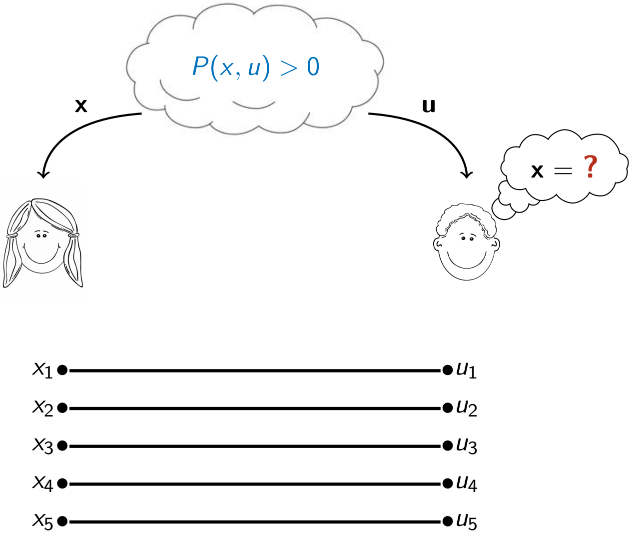
gives the maximum average number of bits that can be sent per channel use

- The Shannon capacity lead to many interesting developments in combinatorics: e.g., perfect graphs, semidefinite optimization

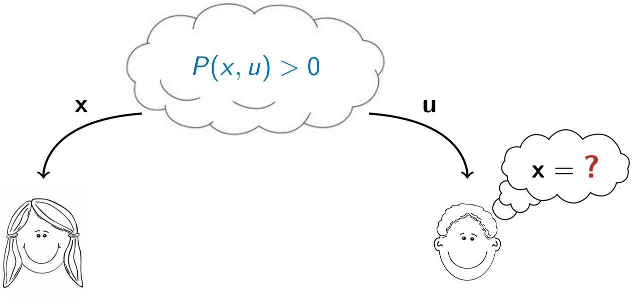
The source coding problem

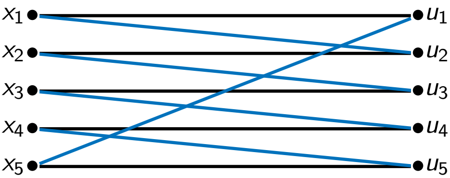


The source coding problem

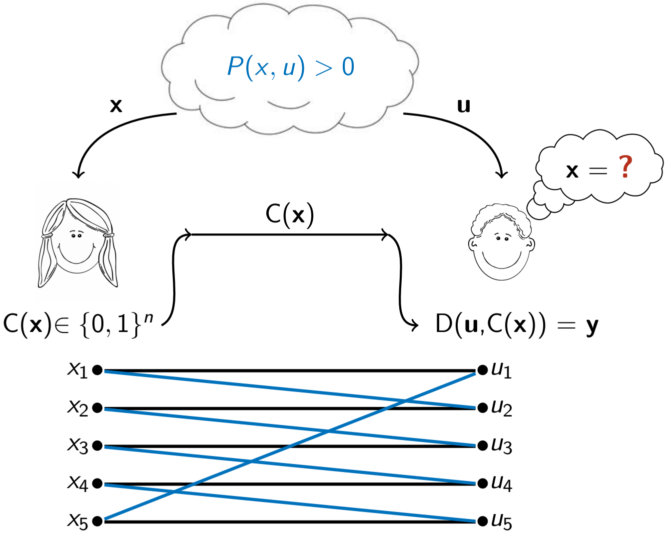


The source coding problem

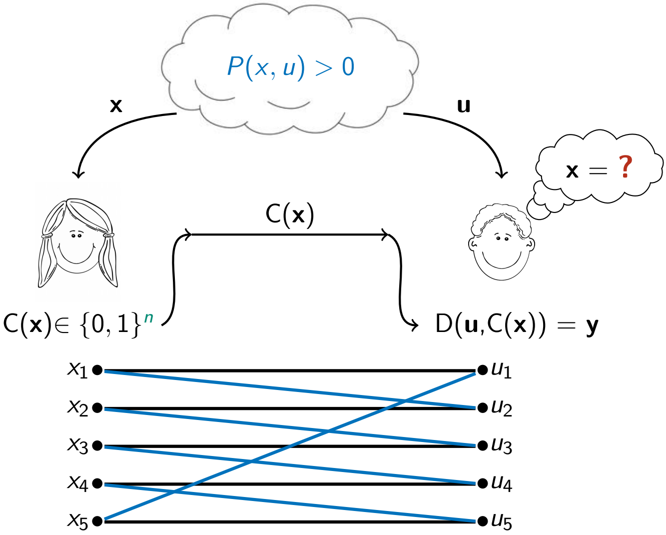




The source coding problem



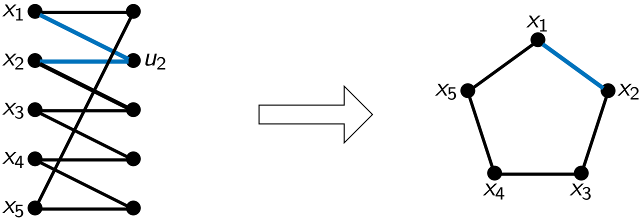
The source coding problem



- **Goal:** $\mathbf{y} = \mathbf{x}$ with zero probability of error and minimize n

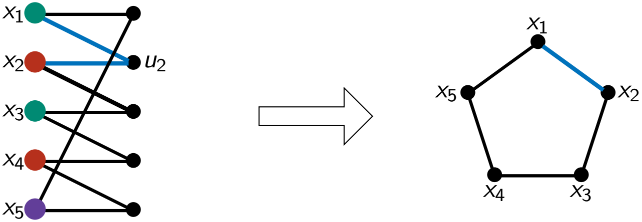
The characteristic graph of a dual source

- The characteristic graph of a dual source has as vertices Alice's inputs, which are adjacent if they are confusable to Bob



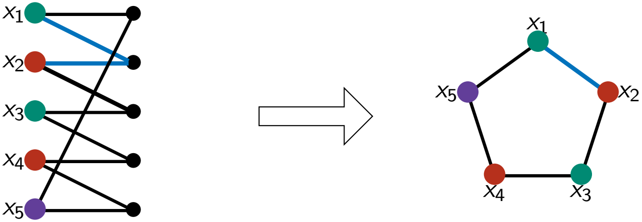
The characteristic graph of a dual source

- The characteristic graph of a dual source has as vertices Alice's inputs, which are adjacent if they are confusable to Bob



The characteristic graph of a dual source

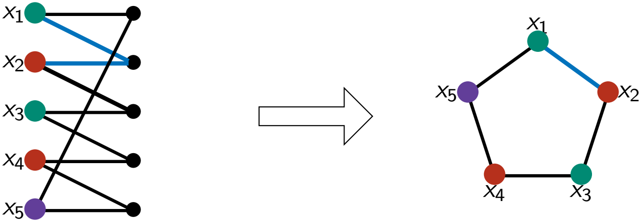
- The characteristic graph of a dual source has as vertices Alice's inputs, which are adjacent if they are confusable to Bob



- A proper coloring assigns different colors to adjacent vertices

The characteristic graph of a dual source

- The characteristic graph of a dual source has as vertices Alice's inputs, which are adjacent if they are confusable to Bob

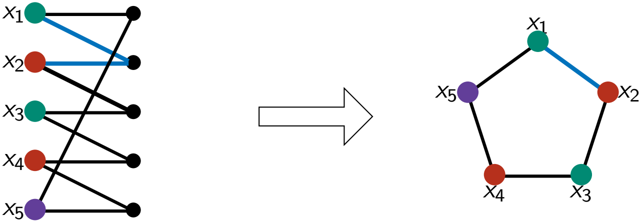


- A proper coloring assigns different colors to adjacent vertices

- The **chromatic number** $\chi(G)$ of a graph G is the minimum number of colors needed for a proper coloring

The characteristic graph of a dual source

- The characteristic graph of a dual source has as vertices Alice's inputs, which are adjacent if they are confusable to Bob

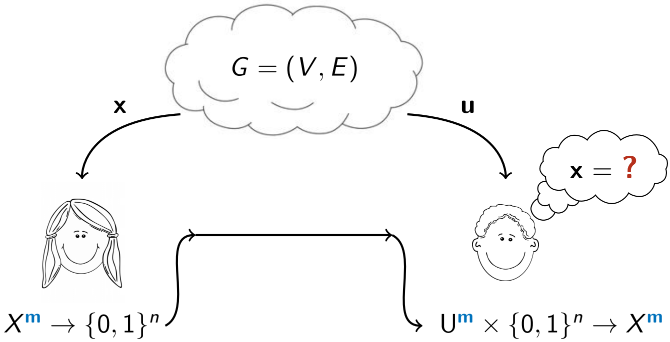


- A proper coloring assigns different colors to adjacent vertices

- The **chromatic number** $\chi(G)$ of a graph G is the minimum number of colors needed for a proper coloring

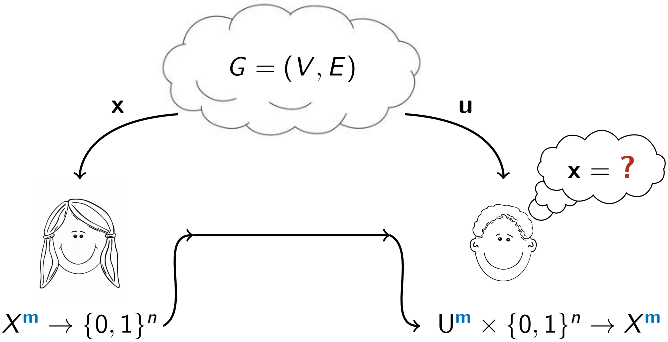
- $\chi(G)$ is the minimum size of the message set that Alice must use

Block coding and the Witsenhausen rate



- Jointly coloring input **sequences** can be more efficient

Block coding and the Witsenhausen rate

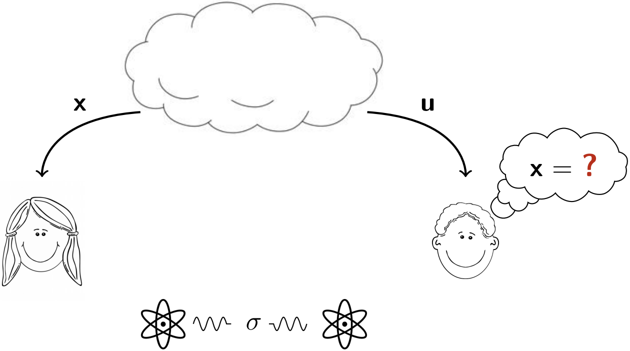


- Jointly coloring input **sequences** can be more efficient
- The **Witsenhausen rate** of G

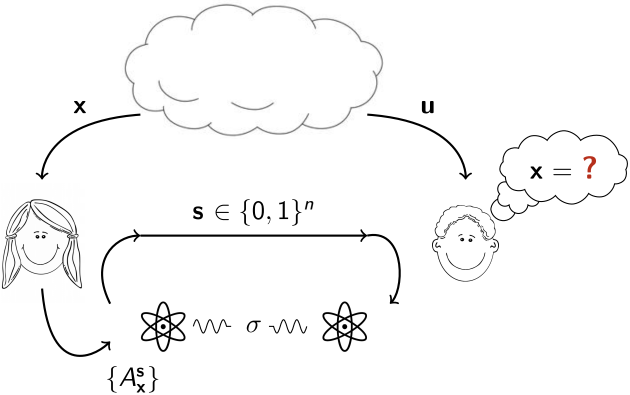
$$R(G) = \lim_{m \to \infty} \frac{1}{m} \log \chi(G^{\boxtimes m})$$

gives the minimum average number of bits needed per source input

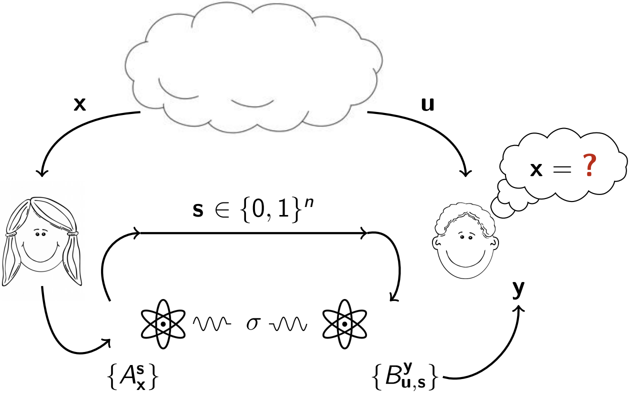
The source coding problem with entanglement



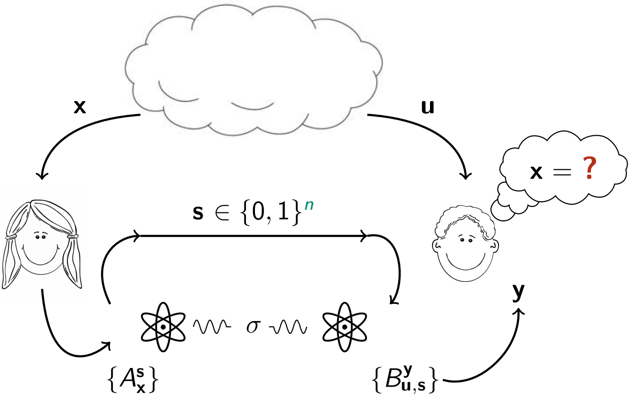
The source coding problem with entanglement



The source coding problem with entanglement

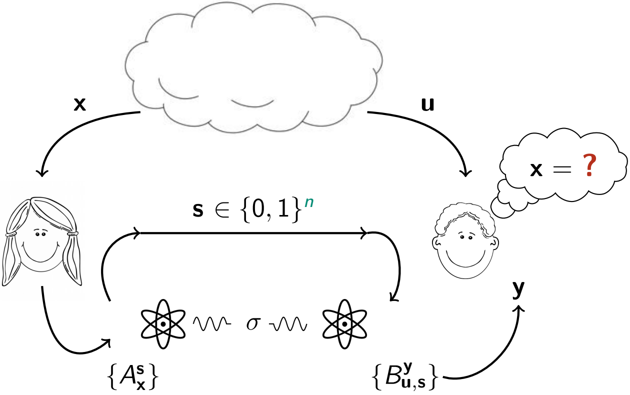


The source coding problem with entanglement



- As for the classical case, the goal is to have $\mathbf{y} = \mathbf{x}$ with zero probability of error and minimize n

The source coding problem with entanglement



- As for the classical case, the goal is to have $\mathbf{y} = \mathbf{x}$ with zero probability of error and minimize n
- The entangled Witsenhausen rate $R^\star$ depends on the characteristic graph G and can be defined by simple constraints on $\sigma, \{A^{\mathbf{s}}_{\mathbf{x}}\}$

Entangled Shannon capacity

The entangled Shannon capacity $c^\star$ of a graph H is defined as

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

- [Cubitt et al. '10] introduced $\alpha^\star, c^\star$ and showed that entanglement can increase that number of possible messages that can be sent with one use of the channel (i.e. $\alpha < \alpha^\star$)
- [Leung et al. '12] and [Briët et al. '12] showed that entanglement can increase the capacity of a channel (i.e. $c < c^\star$ by a constant factor)

Lovász ϑ number

$$\vartheta(G) = \min \quad \lambda \in \mathbb{R}$$
$$\text{such that} \quad \exists \text{ PSD matrix } Z \in \mathbb{R}^{V \times V}$$
$$Z(u,u) = \lambda - 1 \text{ for all } u \in V$$
$$Z(u,v) = -1 \text{ for all } \{u,v\} \notin E$$

- Introduced by Lovász ['79] to compute $c(C_5)$
- ϑ can be computed efficiently (up to any approximation)
- $c(G) \leq \log \vartheta(G) \leq R(\overline{G})$ ([Lovász '79] and [Nayak et al. '06])
- [Beigi '10] and [Duan et al. '13] proved $c^\star(H) \leq \log \vartheta(H)$

ϑ bound on the entangled Witsenhausen rate

Theorem

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

- Thus

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

Separation between the classical and entangled Witsenhausen rate

Theorem

There exists an infinite family of graphs H_k such that

$$\frac{R^\star(H_k)}{R(H_k)} \quad \leq \quad O\Big(\frac{\log k}{k}\Big).$$

Separation between the classical and entangled Witsenhausen rate

Theorem

There exists an infinite family of graphs H_k such that

$$\frac{R^\star(H_k)}{R(H_k)} \quad \leq \quad O\Big(\frac{\log k}{k}\Big).$$

- The *orthogonality graph* (a.k.a. Hadamard graph) has vertex set $\{\pm 1\}^k$ and two vertices are adjacent if and only if they are orthogonal

Separation between the classical and entangled Witsenhausen rate

Theorem

There exists an infinite family of graphs H_k such that

$$\frac{R^\star(H_k)}{R(H_k)} \quad \leq \quad O\Big(\frac{\log k}{k}\Big).$$

- The *orthogonality graph* (a.k.a. Hadamard graph) has vertex set $\{\pm 1\}^k$ and two vertices are adjacent if and only if they are orthogonal
- The quarter orthogonality graph H_k is a subgraph of the orthogonality graph induced by the vertices $x \in \{\pm 1\}^k$ with $x_1 = +1$ and an even number of -1's

Separation between the classical and entangled Witsenhausen rate

Theorem

Let $k = 4p^\ell - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{R^\star(H_k)}{R(H_k)} \leq O\Big(\frac{\log k}{k}\Big).$$

Separation between the classical and entangled Witsenhausen rate

Theorem

Let $k = 4p^{\ell} - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{R^{\star}(H_k)}{R(H_k)} \leq O\left(\frac{\log k}{k}\right).$$

- The lower bound on $R(H_k)$ is derived from a technique that upper bounds $c(H_k)$. It is obtained using an instance of the linear algebra method due to [Alon '98] with a construction of certain low-degree polynomials over finite field due to [Barrington et al. '94]

Separation between the classical and entangled Witsenhausen rate

Theorem

Let $k = 4p^{\ell} - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{R^{\star}(H_k)}{R(H_k)} \leq O\Big(\frac{\log k}{k}\Big).$$

- The lower bound on $R(H_k)$ is derived from a technique that upper bounds $c(H_k)$. It is obtained using an instance of the linear algebra method due to [Alon '98] with a construction of certain low-degree polynomials over finite field due to [Barrington et al. '94]
- The upper bound on $R^{\star}(H_k)$ relies on the construction of a orthogonal representation of the graph H_k (similar idea as used by [Cameron et al. '07])

Separation between the classical and entangled Shannon capacity

Theorem

Let $k = 4p^\ell - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{c^\star(H_k)}{c(H_k)} > 1.$$

Separation between the classical and entangled Shannon capacity

Theorem

Let $k = 4p^\ell - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{c^\star(H_k)}{c(H_k)} > 1.$$

- The upper bound on $c(H_k)$ is obtained using an instance of the linear algebra method due to [Alon '98] *(as before)*

Separation between the classical and entangled Shannon capacity

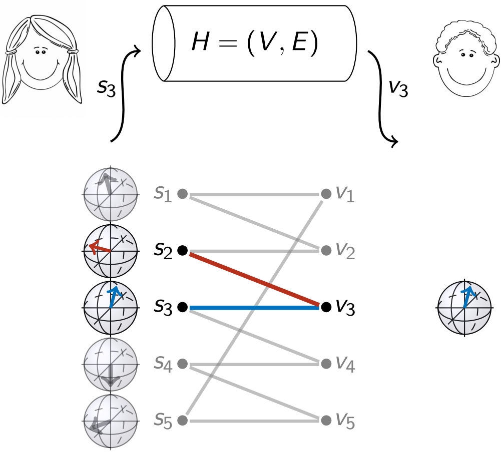
Theorem

Let $k = 4p^\ell - 1$ where p is an odd prime and $\ell \in \mathbb{N}$, then

$$\frac{c^\star(H_k)}{c(H_k)} > 1.$$

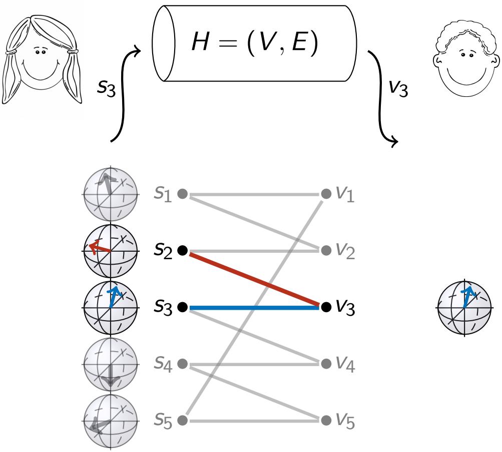
- The upper bound on $c(H_k)$ is obtained using an instance of the linear algebra method due to [Alon '98] *(as before)*
- The lower bound on $c^\star(H_k)$ uses a new method based on the teleportation scheme of [Bennet et al. '93]

Lower bound on entangled Shannon capacity



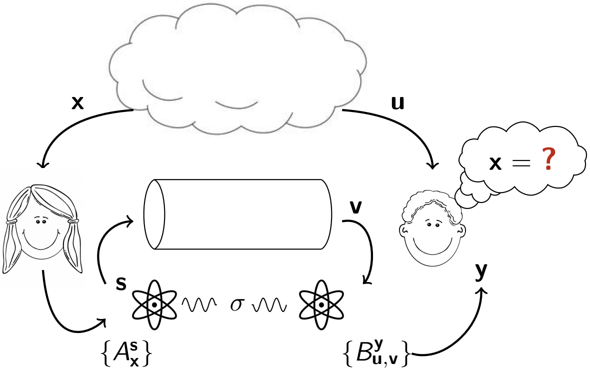
- Main idea: Teleport a state of an orthonormal representation to Bob

Lower bound on entangled Shannon capacity



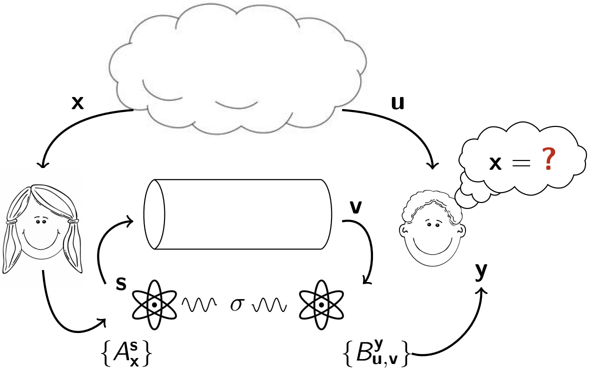
- Main idea: Teleport a state of an orthonormal representation to Bob
- Send $|V|^t$ messages in $t+1$ steps if $\log \alpha(H) \geq 2t \log \mathrm{orthdim}(H)$

Further results



- We study the zero-error source-channel coding problem with entanglement, a generalization of the zero-error channel coding and of the source coding with entanglement

Further results



- We study the zero-error source-channel coding problem with entanglement, a generalization of the zero-error channel coding and of the source coding with entanglement
- We present an infinite family of source and channels combinations for which entanglement allows an exponential saving in communication in zero-error source-channel coding

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$
- We prove that entanglement helps in the zero-error source, channel and source-channel coding problem

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$
- We prove that entanglement helps in the zero-error source, channel and source-channel coding problem

Open Questions:

- Can we find a class of channels for which entanglement allows an exponential increase in communication (i.e. $c^\star \gg c$)?

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$
- We prove that entanglement helps in the zero-error source, channel and source-channel coding problem

Open Questions:

- Can we find a class of channels for which entanglement allows an exponential increase in communication (i.e. $c^\star \gg c$)?
- What is the computational complexity of $R^\star, \chi^\star, c^\star, \alpha^\star$?

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$
- We prove that entanglement helps in the zero-error source, channel and source-channel coding problem

Open Questions:

- Can we find a class of channels for which entanglement allows an exponential increase in communication (i.e. $c^\star \gg c$)?
- What is the computational complexity of $R^\star, \chi^\star, c^\star, \alpha^\star$?
- Does strict inequality hold in $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$?

Conclusions and open questions

- We introduced the zero-error source-channel coding problem with entanglement
- We prove an efficiently computable lower bound on $R^\star$ which implies $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$
- We prove that entanglement helps in the zero-error source, channel and source-channel coding problem

Open Questions:

- Can we find a class of channels for which entanglement allows an exponential increase in communication (i.e. $c^\star \gg c$)?
- What is the computational complexity of $R^\star, \chi^\star, c^\star, \alpha^\star$?
- Does strict inequality hold in $c^\star(G) \leq \log \vartheta(G) \leq R^\star(\overline{G})$?

arXiv:1308.4283

Thank you!