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

Debbie Leung, Laura Mancinska,
William Matthews, Maris Ozols, Aidan Roy

University of Waterloo
Institute for Quantum Computing

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y | \text{input} = x) = \mathcal{E}(y|x)$.

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1) \cdots \mathcal{E}(y_n|x_n)$

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1)\cdots\mathcal{E}(y_n|x_n)$

$P_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ for classical protocols.

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1) \cdots \mathcal{E}(y_n|x_n)$

$P_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ for classical protocols.
Shared randomness no help (use best value of random variable).

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1) \cdots \mathcal{E}(y_n|x_n)$

$P_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ for classical protocols.
Shared randomness no help (use best value of random variable).
Classical world: optimal to use ('block length n') classical code:

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1)\cdots\mathcal{E}(y_n|x_n)$

$P_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ for classical protocols.
Shared randomness no help (use best value of random variable).
Classical world: optimal to use ('block length n') classical code:
Encoder: message $\to X^n$. Decoder: $Y^n \to$ decoded message.

[1] which have equal prior probability

Sending classical data over classical channels

Alice wants to be able send one of M messages[1] to Bob, by n uses of some classical channel $\mathcal{E}$:

- Finite set of input symbols (X); output symbols (Y).
- Transition matrix: $\Pr(\text{output} = y|\text{input} = x) = \mathcal{E}(y|x)$.
  n uses: $\Pr(\text{output} = \mathbf{y}|\text{output} = \mathbf{x}) = \mathcal{E}(y_1|x_1) \cdots \mathcal{E}(y_n|x_n)$

$P_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ for classical protocols.
Shared randomness no help (use best value of random variable).
Classical world: optimal to use ('block length n') classical code:
Encoder: message $\rightarrow X^n$. Decoder: $Y^n \rightarrow$ decoded message.

The Q in the QIP for this talk:

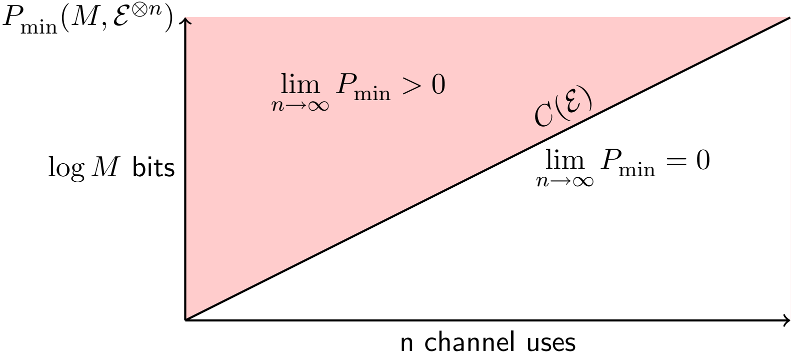
$P^{E}_{\min}(M, \mathcal{E}^{\otimes n}) :=$ minimum $\Pr(\text{error})$ with entanglement assistance: Alice and Bob have shared entangled systems.

[1] which have equal prior probability

Capacity

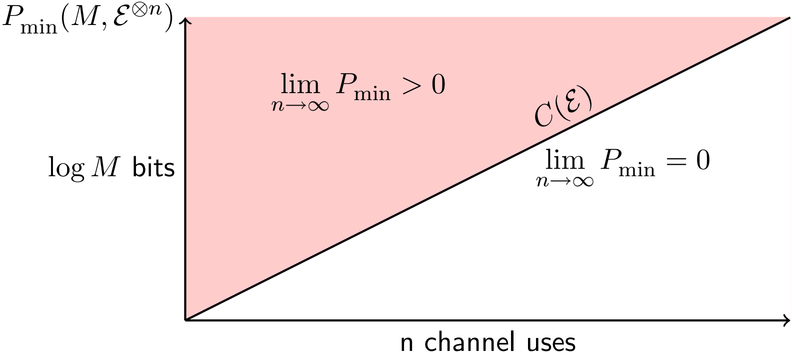
$P_{\min}(M, \mathcal{E}^{\otimes n})$: Min. Pr(error) at rate $R = \frac{1}{n} \log M$ and block length n for classical codes.

Capacity



$P_{\min}(M, \mathcal{E}^{\otimes n})$: Min. $\Pr$(error) at rate $R = \frac{1}{n}\log M$ and block length n for classical codes.

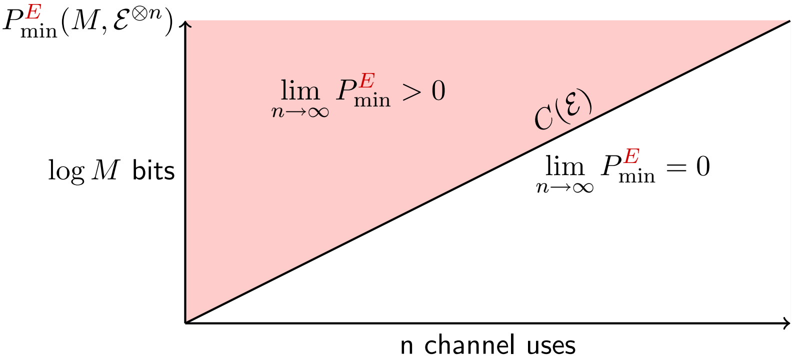
Capacity



$P_{\min}(M, \mathcal{E}^{\otimes n})$: Min. $\Pr$(error) at rate $R = \frac{1}{n} \log M$ and block length n for classical codes.

- Capacity $C(\mathcal{E}) = \max_{\text{input distribution}} I(\text{output} : \text{input})$

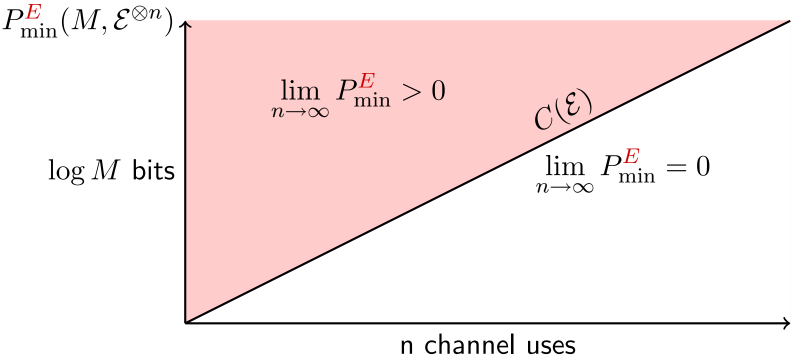
Capacity



$P^{E}_{\min}(M, \mathcal{E}^{\otimes n})$: Min. Pr(error) at rate $R = \frac{1}{n} \log M$ and block length n with entanglement assistance.

- Capacity $C(\mathcal{E}) = \max_{\text{input distribution}} I(\text{output} : \text{input})$
- Same with entanglement assistance for classical channels. Corollary of Bennett, Shor, Smolin, Thapliyal (2001)

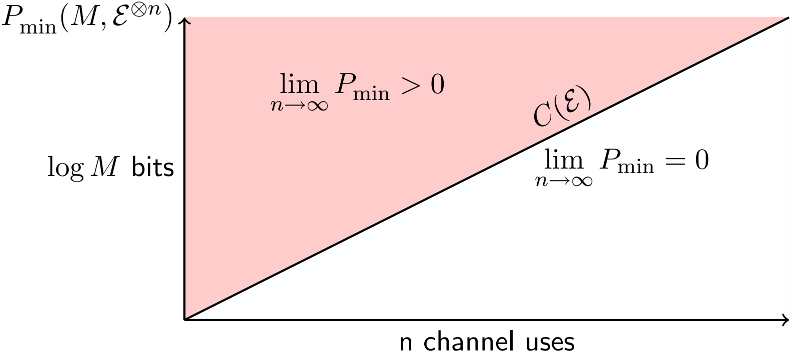
Capacity



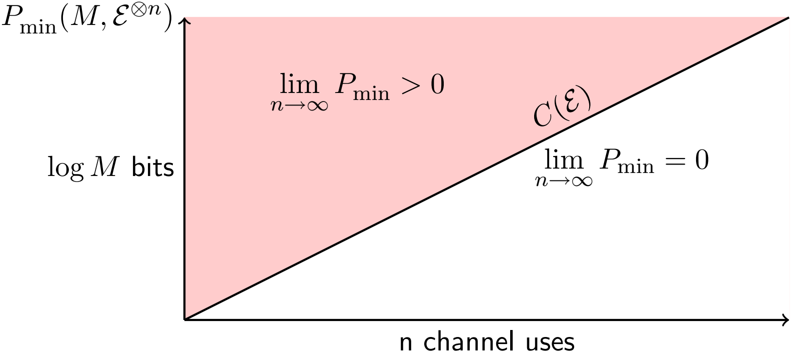
$P^{E}_{\min}(M, \mathcal{E}^{\otimes n})$: Min. $\Pr$(error) at rate $R = \frac{1}{n} \log M$ and block length n with entanglement assistance.

- Capacity $C(\mathcal{E}) = \max_{\text{input distribution}} I(\text{output : input})$
- Same with entanglement assistance for classical channels. Corollary of Bennett, Shor, Smolin, Thapliyal (2001)
- Not the whole story. . .

Zero-error capacity

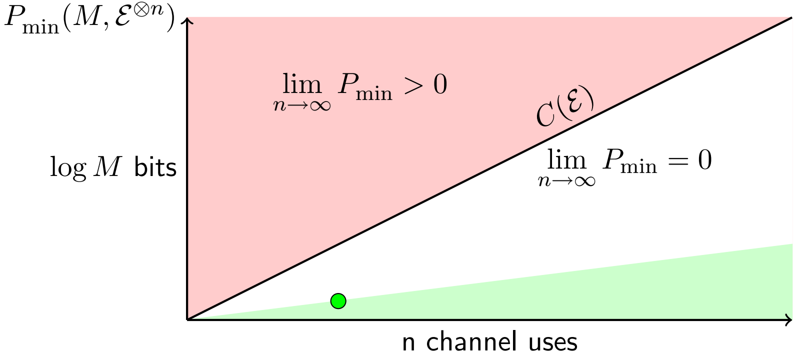


Zero-error capacity



$$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$$

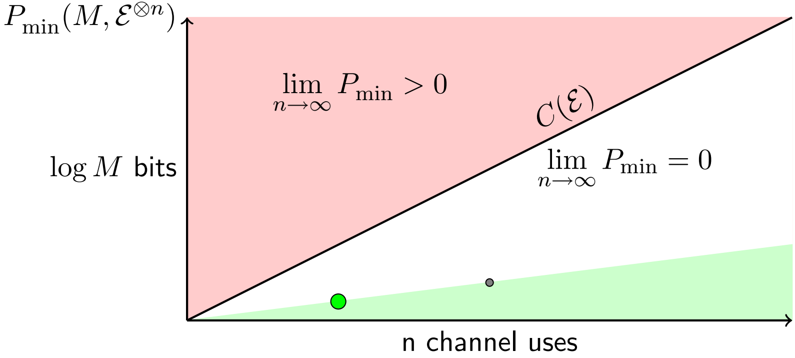
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.

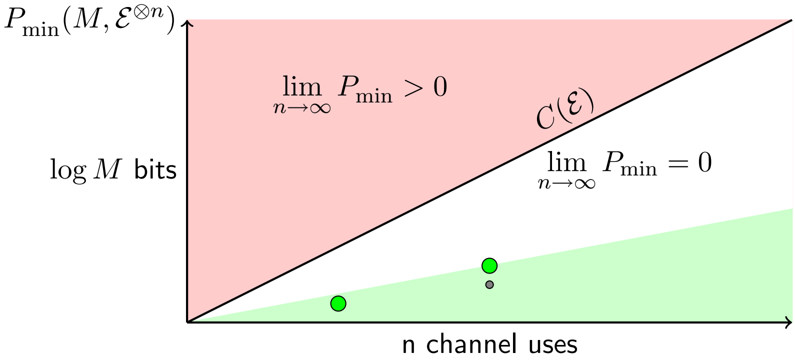
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0(\mathcal{E}^{\otimes n+m}) \geq \log M_0(\mathcal{E}^{\otimes n}) + \log M_0(\mathcal{E}^{\otimes m})$

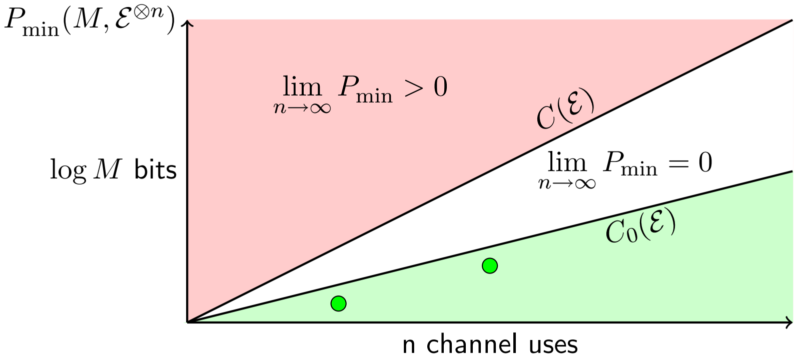
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}$.

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0(\mathcal{E}^{\otimes n+m}) \geq \log M_0(\mathcal{E}^{\otimes n}) + \log M_0(\mathcal{E}^{\otimes m})$

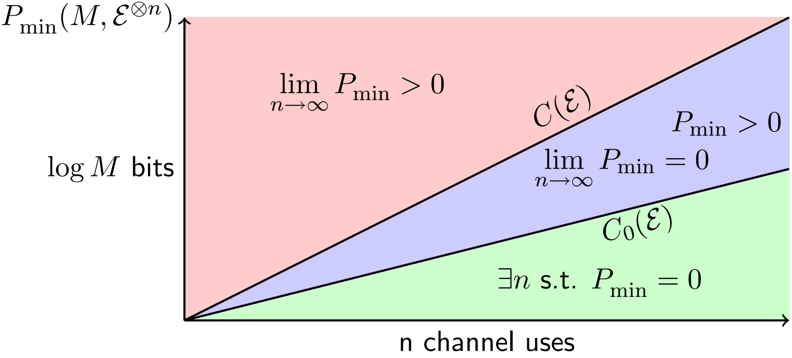
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0(\mathcal{E}^{\otimes n+m}) \geq \log M_0(\mathcal{E}^{\otimes n}) + \log M_0(\mathcal{E}^{\otimes m})$
- Zero-error capacity: $C_0(\mathcal{E}) := \sup_n \frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$

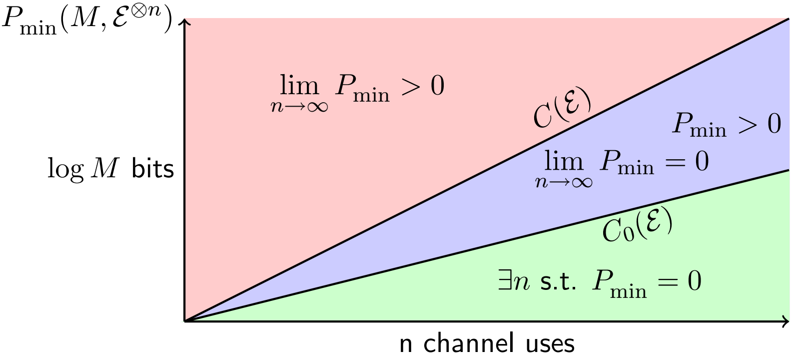
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0(\mathcal{E}^{\otimes n+m}) \geq \log M_0(\mathcal{E}^{\otimes n}) + \log M_0(\mathcal{E}^{\otimes m})$
- Zero-error capacity: $C_0(\mathcal{E}) := \sup_n \frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$

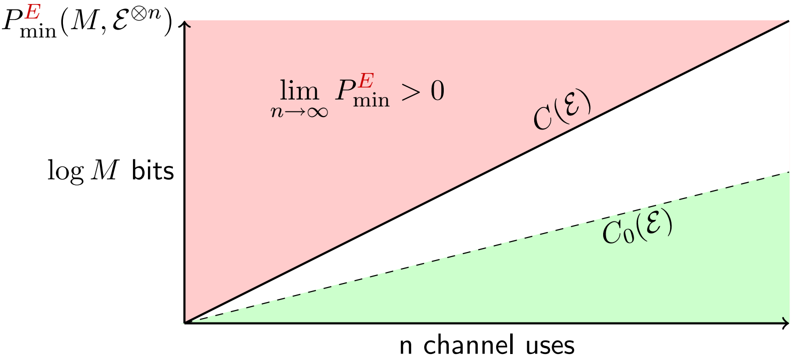
Zero-error capacity



$M_0(\mathcal{E}^{\otimes n}) := \max\{M : P_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}.$

- Zero-error rate $\frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0(\mathcal{E}^{\otimes n+m}) \geq \log M_0(\mathcal{E}^{\otimes n}) + \log M_0(\mathcal{E}^{\otimes m})$
- Zero-error capacity: $C_0(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \log M_0(\mathcal{E}^{\otimes n})$

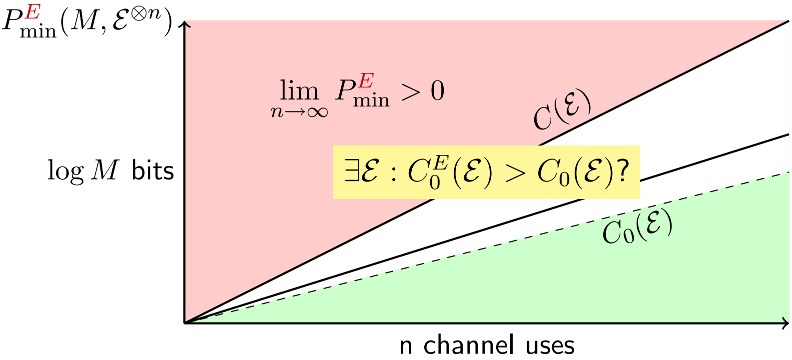
Entanglement-assisted zero-error capacity



$M_0^{E}(\mathcal{E}^{\otimes n}) := \max\{M : P^{E}_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}$.

- Zero-error rate $\frac{1}{n}\log M_0^{E}(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0^{E}(\mathcal{E}^{\otimes n+m}) \geq \log M_0^{E}(\mathcal{E}^{\otimes n}) + \log M_0^{E}(\mathcal{E}^{\otimes m})$
- E-A. zero-error capacity: $C_0^{E}(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n}\log M_0^{E}(\mathcal{E}^{\otimes n})$

Entanglement-assisted zero-error capacity



$M_0^E(\mathcal{E}^{\otimes n}) := \max\{M : P^E_{\min}(M, \mathcal{E}^{\otimes n}) = 0\}$.

- Zero-error rate $\frac{1}{n}\log M_0^E(\mathcal{E}^{\otimes n})$ with block length n.
- $\log M_0^E(\mathcal{E}^{\otimes n+m}) \geq \log M_0^E(\mathcal{E}^{\otimes n}) + \log M_0^E(\mathcal{E}^{\otimes m})$
- E-A. zero-error capacity: $C_0^E(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \log M_0^E(\mathcal{E}^{\otimes n})$

Zero-error codes: Single channel use ($n = 1$)

$$\mathcal{E} = \text{OUTPUT} \begin{array}{c} \\ \\ \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \\ \mathbf{D} \\ \mathbf{E} \end{array} \begin{array}{c} \text{INPUT} \\ \begin{array}{cccccc} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \end{array} \\ \begin{bmatrix} 1 & .2 & 0 & 0 & 0 & 0 \\ 0 & .3 & .9 & 0 & 0 & 0 \\ 0 & 0 & 0 & .4 & .3 & 1 \\ 0 & 0 & .1 & .6 & 0 & 0 \\ 0 & .5 & 0 & 0 & .7 & 0 \end{bmatrix} \end{array}$$

Zero-error codes: Single channel use ($n = 1$)

$$\mathcal{E} = \underset{\text{OUTPUT}}{\begin{matrix} \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \\ \mathbf{D} \\ \mathbf{E} \end{matrix}} \overset{\text{INPUT}}{\overset{\begin{matrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \end{matrix}}{\begin{bmatrix} 1 & .2 & 0 & 0 & 0 & 0 \\ 0 & .3 & .9 & 0 & 0 & 0 \\ 0 & 0 & 0 & .4 & .3 & 1 \\ 0 & 0 & .1 & .6 & 0 & 0 \\ 0 & .5 & 0 & 0 & .7 & 0 \end{bmatrix}}}$$

- Classical code: messages $\rightarrow$ input symbols.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

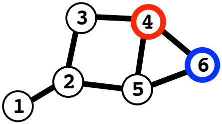
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



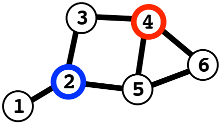
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



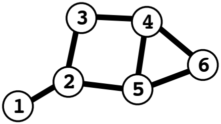
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.
- Zero-error code maps messages $\rightarrow$ non-adjacent inputs: independent set in $G(\mathcal{E})$.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



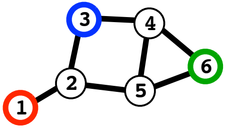
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.
- Zero-error code maps messages $\rightarrow$ non-adjacent inputs: independent set in $G(\mathcal{E})$.
- $M_0(\mathcal{E})$ = independence number $\alpha(G(\mathcal{E}))$.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



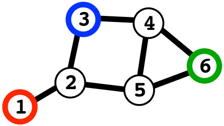
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.
- Zero-error code maps messages $\rightarrow$ non-adjacent inputs: independent set in $G(\mathcal{E})$.
- $M_0(\mathcal{E})$ = independence number $\alpha(G(\mathcal{E}))$.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



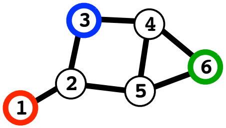
- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.
- Zero-error code maps messages $\rightarrow$ non-adjacent inputs: independent set in $G(\mathcal{E})$.
- $M_0(\mathcal{E}) =$ independence number $\alpha(G(\mathcal{E}))$.

Zero-error codes: Single channel use ($n = 1$)

$\mathcal{E} =$

OUTPUT \ INPUT	1	2	3	4	5	6
A	1	.2	0	0	0	0
B	0	.3	.9	0	0	0
C	0	0	0	.4	.3	1
D	0	0	.1	.6	0	0
E	0	.5	0	0	.7	0

$G(\mathcal{E}) =$



- Classical code: messages $\rightarrow$ input symbols.
- Input symbols $x \neq x'$ adjacent iff $\exists y$ s.t. $\mathcal{E}(y|x) > 0$ and $\mathcal{E}(y|x') > 0$. Defines the confusability graph $G(\mathcal{E})$ on the input symbols.
- Zero-error code maps messages $\rightarrow$ non-adjacent inputs: independent set in $G(\mathcal{E})$.
- $M_0(\mathcal{E}) =$ independence number $\alpha(G(\mathcal{E}))$.

Zero-error codes: Multiple channel uses ($n > 1$)

For composite channel $\mathcal{E}_1 \otimes \mathcal{E}_2$: Input sequences $(x_1', x_2') \neq (x_1, x_2)$ are adjacent iff x_i', x_i are adjacent or equal in $G(\mathcal{E}_i)$ for $i = 1, 2$.

Zero-error codes: Multiple channel uses ($n > 1$)

For composite channel $\mathcal{E}_1 \otimes \mathcal{E}_2$: Input sequences $(x'_1, x'_2) \neq (x_1, x_2)$ are adjacent iff x'_i, x_i are adjacent or equal in $G(\mathcal{E}_i)$ for $i = 1, 2$.
$G(\mathcal{E}_1 \otimes \mathcal{E}_2) = G(\mathcal{E}_1) \boxtimes G(\mathcal{E}_2)$ (strong graph product).

Zero-error codes: Multiple channel uses ($n > 1$)

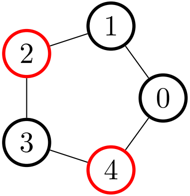
For composite channel $\mathcal{E}_1 \otimes \mathcal{E}_2$: Input sequences $(x_1', x_2') \neq (x_1, x_2)$ are adjacent iff x_i', x_i are adjacent or equal in $G(\mathcal{E}_i)$ for $i = 1, 2$.
$G(\mathcal{E}_1 \otimes \mathcal{E}_2) = G(\mathcal{E}_1) \boxtimes G(\mathcal{E}_2)$ (strong graph product).
$G(\mathcal{E}^{\otimes n}) = G(\mathcal{E})^n$: (strong graph power).

Zero-error codes: Multiple channel uses ($n > 1$)

For composite channel $\mathcal{E}_1 \otimes \mathcal{E}_2$: Input sequences $(x'_1, x'_2) \neq (x_1, x_2)$ are adjacent iff x'_i, x_i are adjacent or equal in $G(\mathcal{E}_i)$ for $i = 1, 2$.

$G(\mathcal{E}_1 \otimes \mathcal{E}_2) = G(\mathcal{E}_1) \boxtimes G(\mathcal{E}_2)$ (strong graph product).

$G(\mathcal{E}^{\otimes n}) = G(\mathcal{E})^n$: (strong graph power).

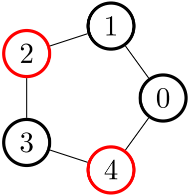


$M_0(C_5) = \alpha(C_5) = 2$

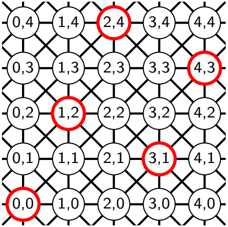
For $n = 1$, best zero-error rate is 1 bit/channel use.

Zero-error codes: Multiple channel uses ($n > 1$)

For composite channel $\mathcal{E}_1 \otimes \mathcal{E}_2$: Input sequences $(x_1', x_2') \neq (x_1, x_2)$ are adjacent iff x_i', x_i are adjacent or equal in $G(\mathcal{E}_i)$ for $i = 1, 2$.
$G(\mathcal{E}_1 \otimes \mathcal{E}_2) = G(\mathcal{E}_1) \boxtimes G(\mathcal{E}_2)$ (strong graph product).
$G(\mathcal{E}^{\otimes n}) = G(\mathcal{E})^n$: (strong graph power).



$M_0(C_5) = \alpha(C_5) = 2$
For $n = 1$, best zero-error rate is 1 bit/channel use.



With two uses:
$M_0(C_5^{\otimes 2}) = \alpha(C_5 \boxtimes C_5) = 5$
For $n = 2$, best zero-error rate is $\frac{1}{2}\log 5 = 1.16\ldots$ bits/channel use.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.
- $\exists$ graph F s.t. $M_0^E(F) > M_0(F)$.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.
- $\exists$ graph F s.t. $M_0^E(F) > M_0(F)$.
- Proof uses an entanglement assisted protocol for graphs with special structure. Will use later exhibit prove difference in capacities.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.
- $\exists$ graph F s.t. $M_0^E(F) > M_0(F)$.
- Proof uses an entanglement assisted protocol for graphs with special structure. Will use later exhibit prove difference in capacities.

An orthonormal representation, in d dimensions, of a graph G is a map: Vertices $x \to$ unit vectors $|\psi_x\rangle \in \mathbb{C}^d$, such that if x and x' are adjacent then $\langle\psi_x|\psi_{x'}\rangle = 0$.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.
- $\exists$ graph F s.t. $M_0^E(F) > M_0(F)$.
- Proof uses an entanglement assisted protocol for graphs with special structure. Will use later exhibit prove difference in capacities.

An orthonormal representation, in d dimensions, of a graph G is a map: Vertices $x \to$ unit vectors $|\psi_x\rangle \in \mathbb{C}^d$, such that if x and x' are adjacent then $\langle \psi_x | \psi_{x'} \rangle = 0$.

Theorem (ORCP Part I: CLMW)

If $G(\mathcal{E})$ has an orthonormal representation in $\mathbb{C}^d$ and partitions into m cliques of size d: $\kappa_1, \ldots, \kappa_m$. Then there is entanglement assisted protocol to send one of m messages with zero error. i.e. $M_0^E(G) \geq m$ and so $C_0^E(G) \geq \log m$.

Entanglement assisted zero-error protocols

Cubitt, Leung, Matthews, Winter 0911.5300 / 1003.3195

- $M_0^E(\mathcal{E})$ also depends only on $G(\mathcal{E})$.
- $\exists$ graph F s.t. $M_0^E(F) > M_0(F)$.
- Proof uses an entanglement assisted protocol for graphs with special structure. Will use later exhibit prove difference in capacities.

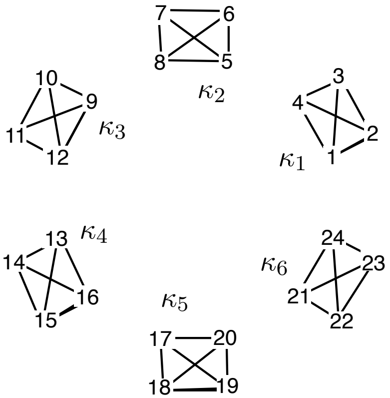
An orthonormal representation, in d dimensions, of a graph G is a map: Vertices $x \rightarrow$ unit vectors $|\psi_x\rangle \in \mathbb{C}^d$, such that if x and x' are adjacent then $\langle\psi_x|\psi_{x'}\rangle = 0$.

Theorem (ORCP Part I: CLMW)

If $G(\mathcal{E})$ has an orthonormal representation in $\mathbb{C}^d$ and partitions into m cliques of size d: $\kappa_1, \ldots, \kappa_m$. Then there is entanglement assisted protocol to send one of m messages with zero error.
i.e. $M_0^E(G) \geq m$ and so $C_0^E(G) \geq \log m$.

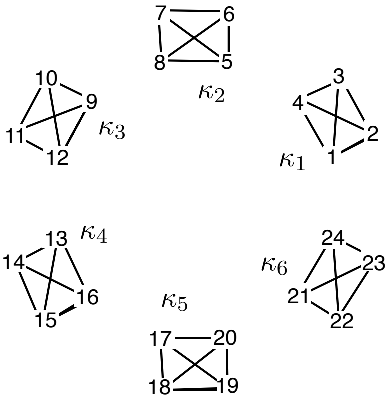
Goes like this (illustrated by $m = 6$, $d = 4$ case). . .

Entanglement assisted protocol for special graphs



+ other edges not shown...

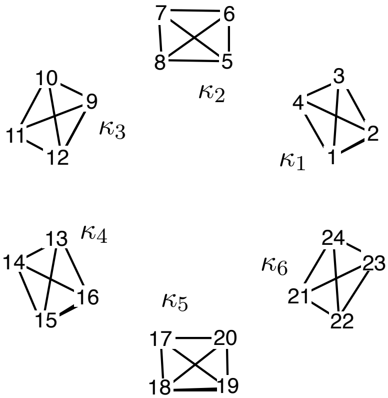
Entanglement assisted protocol for special graphs



+ other edges not shown...

- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.

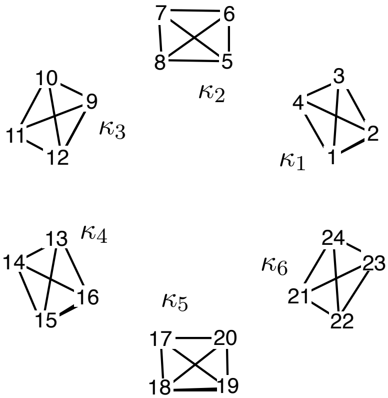
Entanglement assisted protocol for special graphs



+ other edges not shown...

- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.

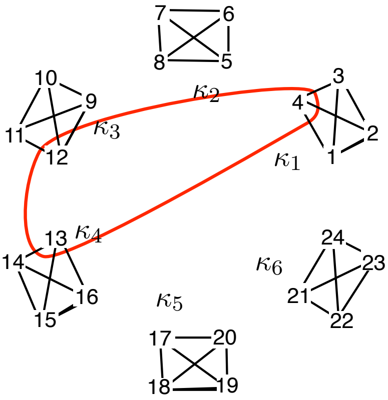
Entanglement assisted protocol for special graphs



+ other edges not shown...

- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.
- If Alice's system collapses to $|\psi_x\rangle \in B_q$, Alice makes x to channel. Conditioned on x Bob's state is $|\psi_x\rangle^*$ (c.c.).

Entanglement assisted protocol for special graphs

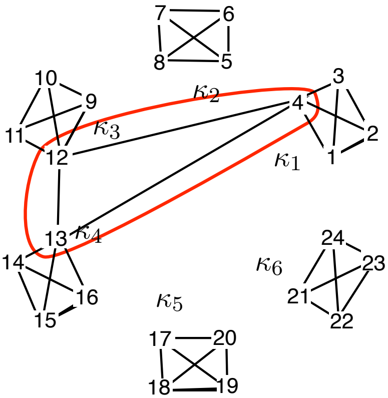


+ other edges not shown...

- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.
- If Alice's system collapses to $|\psi_x\rangle \in B_q$, Alice makes x to channel. Conditioned on x Bob's state is $|\psi_x\rangle^*$ (c.c.).

- On output y Bob only knows $x \in S_y = \{x' : \mathcal{E}(y|x') > 0\}$.

Entanglement assisted protocol for special graphs

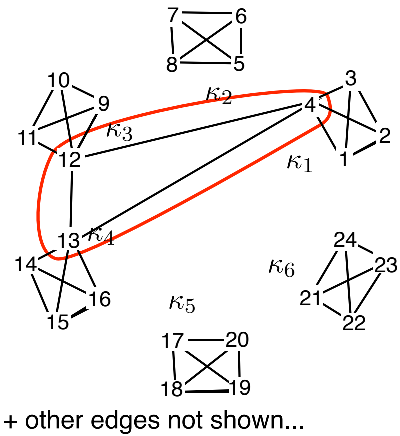


+ other edges not shown...

- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.
- If Alice's system collapses to $|\psi_x\rangle \in B_q$, Alice makes x to channel. Conditioned on x Bob's state is $|\psi_x\rangle^*$ (c.c.).

- On output y Bob only knows $x \in S_y = \{x' : \mathcal{E}(y|x') > 0\}$.

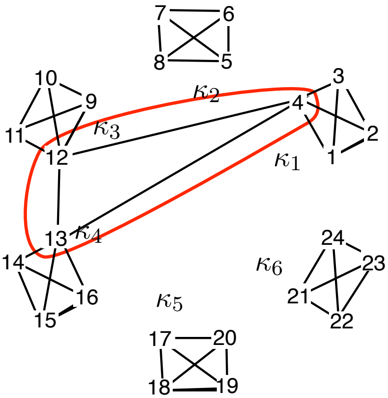
Entanglement assisted protocol for special graphs



- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.
- If Alice's system collapses to $|\psi_x\rangle \in B_q$, Alice makes x to channel. Conditioned on x Bob's state is $|\psi_x\rangle^*$ (c.c.).

- On output y Bob only knows $x \in S_y = \{x' : \mathcal{E}(y|x') > 0\}$. S_y is a clique so the states $|\psi_{x'}\rangle^*, x' \in S_y$ corresponding to possible x are orthogonal so Bob can determine x, and hence q, with certainty.

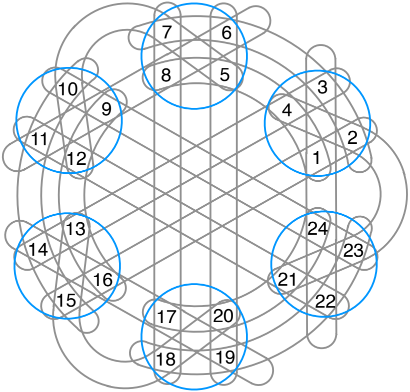
Entanglement assisted protocol for special graphs



- Alice and Bob share $\sum_{i=1}^{d} |i\rangle_A \otimes |i\rangle_B$.
- To send message $q \in \{1, \ldots, m\}$, Alice measures complete orthonormal basis $B_q := \{|\psi_{x'}\rangle : x' \in \kappa_q\}$.
- If Alice's system collapses to $|\psi_x\rangle \in B_q$, Alice makes x to channel. Conditioned on x Bob's state is $|\psi_x\rangle^*$ (c.c.).

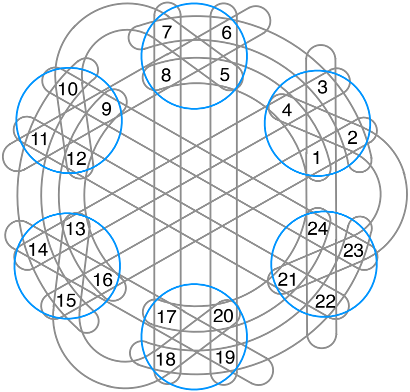
- On output y Bob only knows $x \in S_y = \{x' : \mathcal{E}(y|x') > 0\}$. S_y is a clique so the states $|\psi_{x'}\rangle^*, x' \in S_y$ corresponding to possible x are orthogonal so Bob can determine x, and hence q, with certainty. $M_0^E(G) \geq m$.

The graph F: Single use separation



Graph F: Vertices adjacent $\iff$ share a loop.

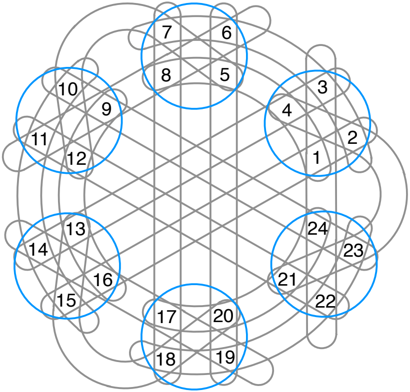
The graph F: Single use separation



Graph F: Vertices adjacent $\iff$ share a loop. F has orthonormal rep. in $\mathbb{C}^4$ and partitions into 6 cliques of size 4.

$B_1 - \|\psi_1\rangle : (1,0,0,0)$	$\|\psi_2\rangle : (0,1,0,0)$	$\|\psi_3\rangle : (0,0,1,0)$	$\|\psi_4\rangle : (0,0,0,1)$
$B_2 - \|\psi_5\rangle : (0,1,1,0)$	$\|\psi_6\rangle : (1,0,0,-1)$	$\|\psi_7\rangle : (1,0,0,1)$	$\|\psi_8\rangle : (0,1,-1,0)$
$B_3 - \|\psi_9\rangle : (1,1,1,1)$	$\|\psi_{10}\rangle : (1,-1,1,-1)$	$\|\psi_{11}\rangle : (1,-1,-1,1)$	$\|\psi_{12}\rangle : (1,1,-1,-1)$
$B_4 - \|\psi_{13}\rangle : (1,-1,0,0)$	$\|\psi_{14}\rangle : (1,1,0,0)$	$\|\psi_{15}\rangle : (0,0,1,1)$	$\|\psi_{16}\rangle : (0,0,1,-1)$
$B_5 - \|\psi_{17}\rangle : (-1,1,1,1)$	$\|\psi_{18}\rangle : (1,1,1,-1)$	$\|\psi_{19}\rangle : (1,-1,1,1)$	$\|\psi_{20}\rangle : (1,1,-1,1)$
$B_6 - \|\psi_{21}\rangle : (1,0,1,0)$	$\|\psi_{22}\rangle : (0,1,0,1)$	$\|\psi_{23}\rangle : (1,0,-1,0)$	$\|\psi_{24}\rangle : (0,1,0,-1)$

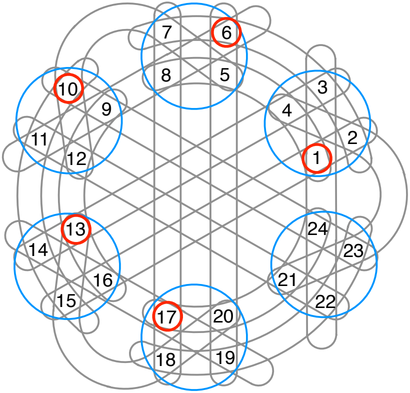
The graph F: Single use separation



Graph F: Vertices adjacent $\iff$ share a loop. F has orthonormal rep. in $\mathbb{C}^4$ and partitions into 6 cliques of size 4.
By ORCP: $M_0^E(F) \geq 6$

$B_1 - \|\psi_1\rangle : (1,0,0,0)$	$\|\psi_2\rangle : (0,1,0,0)$	$\|\psi_3\rangle : (0,0,1,0)$	$\|\psi_4\rangle : (0,0,0,1)$
$B_2 - \|\psi_5\rangle : (0,1,1,0)$	$\|\psi_6\rangle : (1,0,0,-1)$	$\|\psi_7\rangle : (1,0,0,1)$	$\|\psi_8\rangle : (0,1,-1,0)$
$B_3 - \|\psi_9\rangle : (1,1,1,1)$	$\|\psi_{10}\rangle : (1,-1,1,-1)$	$\|\psi_{11}\rangle : (1,-1,-1,1)$	$\|\psi_{12}\rangle : (1,1,-1,-1)$
$B_4 - \|\psi_{13}\rangle : (1,-1,0,0)$	$\|\psi_{14}\rangle : (1,1,0,0)$	$\|\psi_{15}\rangle : (0,0,1,1)$	$\|\psi_{16}\rangle : (0,0,1,-1)$
$B_5 - \|\psi_{17}\rangle : (-1,1,1,1)$	$\|\psi_{18}\rangle : (1,1,1,-1)$	$\|\psi_{19}\rangle : (1,-1,1,1)$	$\|\psi_{20}\rangle : (1,1,-1,1)$
$B_6 - \|\psi_{21}\rangle : (1,0,1,0)$	$\|\psi_{22}\rangle : (0,1,0,1)$	$\|\psi_{23}\rangle : (1,0,-1,0)$	$\|\psi_{24}\rangle : (0,1,0,-1)$

The graph F: Single use separation



Graph F: Vertices adjacent $\iff$ share a loop. F has orthonormal rep. in $\mathbb{C}^4$ and partitions into 6 cliques of size 4.
By ORCP: $M_0^E(F) \geq 6$
Independence number = 5: $M_0(F) = 5$.

$B_1 - \|\psi_1\rangle : (1,0,0,0)$	$\|\psi_2\rangle : (0,1,0,0)$	$\|\psi_3\rangle : (0,0,1,0)$	$\|\psi_4\rangle : (0,0,0,1)$
$B_2 - \|\psi_5\rangle : (0,1,1,0)$	$\|\psi_6\rangle : (1,0,0,-1)$	$\|\psi_7\rangle : (1,0,0,1)$	$\|\psi_8\rangle : (0,1,-1,0)$
$B_3 - \|\psi_9\rangle : (1,1,1,1)$	$\|\psi_{10}\rangle : (1,-1,1,-1)$	$\|\psi_{11}\rangle : (1,-1,-1,1)$	$\|\psi_{12}\rangle : (1,1,-1,-1)$
$B_4 - \|\psi_{13}\rangle : (1,-1,0,0)$	$\|\psi_{14}\rangle : (1,1,0,0)$	$\|\psi_{15}\rangle : (0,0,1,1)$	$\|\psi_{16}\rangle : (0,0,1,-1)$
$B_5 - \|\psi_{17}\rangle : (-1,1,1,1)$	$\|\psi_{18}\rangle : (1,1,1,-1)$	$\|\psi_{19}\rangle : (1,-1,1,1)$	$\|\psi_{20}\rangle : (1,1,-1,1)$
$B_6 - \|\psi_{21}\rangle : (1,0,1,0)$	$\|\psi_{22}\rangle : (0,1,0,1)$	$\|\psi_{23}\rangle : (1,0,-1,0)$	$\|\psi_{24}\rangle : (0,1,0,-1)$

C_0^E vs. C_0

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?
- E.A. and classical zero-error capacities depend only on $G(\mathcal{E})$: write $C_0(G)$, $C_0^E(G)$ to denote their values for channels with graph G.

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?
- E.A. and classical zero-error capacities depend only on $G(\mathcal{E})$: write $C_0(G)$, $C_0^E(G)$ to denote their values for channels with graph G.
- Are there graphs G with $C_0^E(G) > C_0(G)$?

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?
- E.A. and classical zero-error capacities depend only on $G(\mathcal{E})$: write $C_0(G)$, $C_0^E(G)$ to denote their values for channels with graph G.
- Are there graphs G with $C_0^E(G) > C_0(G)$?
- No algorithm computing C_0 is known! Same for C_0^E.

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?
- E.A. and classical zero-error capacities depend only on $G(\mathcal{E})$: write $C_0(G)$, $C_0^E(G)$ to denote their values for channels with graph G.
- Are there graphs G with $C_0^E(G) > C_0(G)$?
- No algorithm computing C_0 is known! Same for C_0^E.
- ≈ 20 years to prove that $C_0(C_5) = \frac{1}{2}\log 5$! Still unknown for larger odd cycles.

The problem

- Examples with $M_0^E > M_0$ for some finite n don't settle our original question:
  Maybe classical protocols can always "catch up" with assisted protocols as $n \to \infty$?
- E.A. and classical zero-error capacities depend only on $G(\mathcal{E})$: write $C_0(G)$, $C_0^E(G)$ to denote their values for channels with graph G.
- Are there graphs G with $C_0^E(G) > C_0(G)$?
- No algorithm computing C_0 is known! Same for C_0^E.
- ≈ 20 years to prove that $C_0(C_5) = \frac{1}{2}\log 5$! Still unknown for larger odd cycles.
- Proof of separation will involve: Lower bounds on C_0^E and upper bounds on C_0.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log\vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log\vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).
- (Beigi 1002.2488; Duan, Severini, Winter 1002.2514) $C_0^E(G) \leq \log\vartheta(G)$, also!

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log \vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).
- (Beigi 1002.2488; Duan, Severini, Winter 1002.2514) $C_0^E(G) \leq \log \vartheta(G)$, also!
- Can't use Lovász to prove separation.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log \vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).
- (Beigi 1002.2488; Duan, Severini, Winter 1002.2514) $C_0^E(G) \leq \log \vartheta(G)$, also!
- Can't use Lovász to prove separation.

Theorem (ORCP Part I)

If G has orthonormal representation in $\mathbb{C}^d$ and partitions into m d-cliques then $C_0^E(G) \geq \log m$.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log \vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).
- (Beigi 1002.2488; Duan, Severini, Winter 1002.2514) $C_0^E(G) \leq \log \vartheta(G)$, also!
- Can't use Lovász to prove separation.

Theorem (ORCP Full: CLMW 1003.3195)

If G has orthonormal representation in $\mathbb{C}^d$ and partitions into m d-cliques then $C_0^E(G) = \log m$.

Upper bounds on C_0: Lovász bound

- Lovász 1979: $C_0(C_5) = \frac{1}{2}\log 5$.
- $\vartheta(G)$ solution to SDP determined by G. Easy to compute.
- $C_0(G) \leq \log \vartheta(G)$. ($\vartheta(C_5) = \sqrt{5}$).
- (Beigi 1002.2488; Duan, Severini, Winter 1002.2514) $C_0^E(G) \leq \log \vartheta(G)$, also!
- Can't use Lovász to prove separation.

Theorem (ORCP Full: CLMW 1003.3195)

If G has orthonormal representation in $\mathbb{C}^d$ and partitions into m d-cliques then $C_0^E(G) = \log m$.

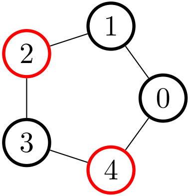
$C_0^E(F) = \log 6$. Nice, but only know $\log 5 \leq C_0(F) \leq \log 6$

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

Upper bounds on C_0: Haemers bound

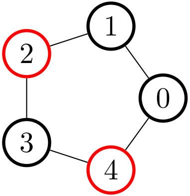
Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:



$$\begin{pmatrix} 1 & * & 0 & 0 & * \\ * & 1 & * & 0 & 0 \\ 0 & * & 1 & * & 0 \\ 0 & 0 & * & 1 & * \\ * & 0 & 0 & * & 1 \end{pmatrix}$$

Upper bounds on C_0: Haemers bound

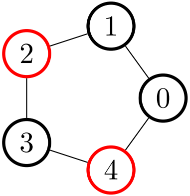
Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:



$$\begin{pmatrix} 1 & * & 0 & 0 & * \\ * & 1 & * & 0 & 0 \\ 0 & * & 1 & * & 0 \\ 0 & 0 & * & 1 & * \\ * & 0 & 0 & * & 1 \end{pmatrix}$$

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

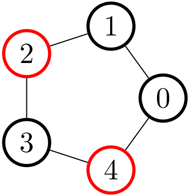


$$\begin{pmatrix} 1 & * & 0 & 0 & * \\ * & 1 & * & 0 & 0 \\ 0 & * & 1 & * & 0 \\ 0 & 0 & * & 1 & * \\ * & 0 & 0 & * & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

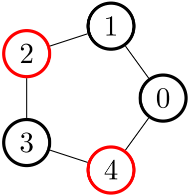


$$\begin{pmatrix} 1 & * & 0 & 0 & * \\ * & 1 & * & 0 & 0 \\ 0 & * & 1 & * & 0 \\ 0 & 0 & * & 1 & * \\ * & 0 & 0 & * & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$
- $A^{\otimes n}$ fits G^n so $\alpha(G^n) \leq (\text{rank } A^{\otimes n}) = (\text{rank } A)^n$.

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

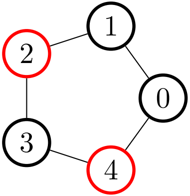


$$\begin{pmatrix} 1 & * & 0 & 0 & * \\ * & 1 & * & 0 & 0 \\ 0 & * & 1 & * & 0 \\ 0 & 0 & * & 1 & * \\ * & 0 & 0 & * & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$
- $A^{\otimes n}$ fits G^n so $\alpha(G^n) \leq (\text{rank } A^{\otimes n}) = (\text{rank } A)^n$.
- If A fits G: $C_0(G) \leq \log \text{rank } A$

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

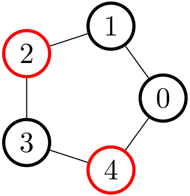


$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$
- $A^{\otimes n}$ fits G^n so $\alpha(G^n) \leq (\text{rank } A^{\otimes n}) = (\text{rank } A)^n$.
- If A fits G: $C_0(G) \leq \log \text{rank } A$

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:

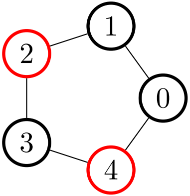


$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$
- $A^{\otimes n}$ fits G^n so $\alpha(G^n) \leq (\text{rank } A^{\otimes n}) = (\text{rank } A)^n$.
- If A fits G: $C_0(G) \leq \log \text{rank } A$
- Generally hard to minimize rank over fitting matrices, and often worse bound than Lovász.

Upper bounds on C_0: Haemers bound

Matrix A (with rows and cols indexed by vertices) fits G if: $A_{xx} = 1$, $A_{xx'} = 0$ when x and x' not adjacent. E.g. for the pentagon:



$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- If A fits G: $\alpha(G) \leq \text{rank } A$
- $A^{\otimes n}$ fits G^n so $\alpha(G^n) \leq (\text{rank } A^{\otimes n}) = (\text{rank } A)^n$.
- If A fits G: $C_0(G) \leq \log \text{rank } A$
- Generally hard to minimize rank over fitting matrices, and often worse bound than Lovász.
- Idea: Look for graphs where Haemers bound $<$ Lovász bound

Pauli graphs Γ_j

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$

Edges: $u \neq v$ are adjacent iff $uv = vu$

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties. . .

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).
  In fact $M_0(\Gamma_j) = 2j+1$: $C_0(\Gamma_j)$ achieved by $n = 1$ code.

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).
  In fact $M_0(\Gamma_j) = 2j+1$: $C_0(\Gamma_j)$ achieved by $n = 1$ code.
- $\vartheta(\Gamma_j) = 2^j + 1$. (Beigi; DSW) $C_0^E(\Gamma_j) \leq \log(2^j + 1)$.

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).
  In fact $M_0(\Gamma_j) = 2j+1$: $C_0(\Gamma_j)$ achieved by $n=1$ code.
- $\vartheta(\Gamma_j) = 2^j + 1$. (Beigi; DSW) $C_0^E(\Gamma_j) \leq \log(2^j+1)$.
  Doesn't *rule out* entanglement advantage for $j \geq 3$.

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).
  In fact $M_0(\Gamma_j) = 2j+1$: $C_0(\Gamma_j)$ achieved by $n = 1$ code.
- $\vartheta(\Gamma_j) = 2^j + 1$. (Beigi; DSW) $C_0^E(\Gamma_j) \leq \log(2^j + 1)$.
  Doesn't *rule out* entanglement advantage for $j \geq 3$.
- The $4^j - 1$ vertices of Γ_j can be partitioned into $2^j + 1$ cliques each of size $2^j - 1$.

Pauli graphs Γ_j

Definition

Vertices: $\{I, \sigma_X, \sigma_Y, \sigma_Z\}^{\otimes j} \setminus \{I^{\otimes j}\}$
Edges: $u \neq v$ are adjacent iff $uv = vu$

Promising properties...

- $C_0(\Gamma_j) = \log(2j+1)$ by application of Haemers bound over $GF(2)$ (Peeters 1996).
  In fact $M_0(\Gamma_j) = 2j+1$: $C_0(\Gamma_j)$ achieved by $n = 1$ code.
- $\vartheta(\Gamma_j) = 2^j + 1$. (Beigi; DSW) $C_0^E(\Gamma_j) \leq \log(2^j + 1)$.
  Doesn't *rule out* entanglement advantage for $j \geq 3$.
- The $4^j - 1$ vertices of Γ_j can be partitioned into $2^j + 1$ cliques each of size $2^j - 1$.

If orthonormal rep. of Γ_j exists with dimension $2^j - 1$ then $C_0^E(\Gamma_j) = \log(2^j + 1)$ by Theorem ORCP. Can we find one for $j \geq 3$?

Root systems

We found one in an interesting place. . .

Root systems

We found one in an interesting place...

Simple root systems: Finite set of vectors with certain special properties. 4 infinite families: A_n, B_n, C_n, D_n.

5 exceptional cases: G_2, F_4, E_6, E_7, E_8.

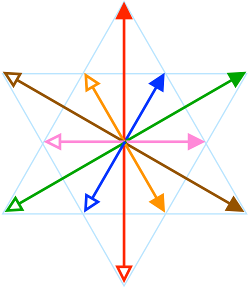
Root systems

We found one in an interesting place...

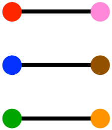
Simple root systems: Finite set of vectors with certain special properties. 4 infinite families: A_n, B_n, C_n, D_n.

5 exceptional cases: G_2, F_4, E_6, E_7, E_8.

G_2



$\Delta(G_2)$



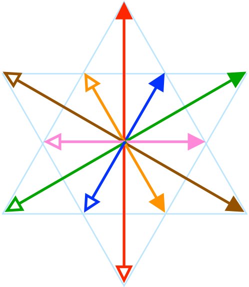
Root systems

We found one in an interesting place. . .

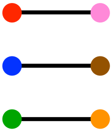
Simple root systems: Finite set of vectors with certain special properties. 4 infinite families: A_n, B_n, C_n, D_n.

5 exceptional cases: G_2, F_4, E_6, E_7, E_8.

G_2



$\Delta(G_2)$



Orthogonality graph of d dimensional root system has d dimensional orthonormal representation.

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension $7 \dots$

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension 7. . . .
So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension $7 \ldots$. So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

while, by Peeters result

$$C_0(\Gamma_3) = \log 7.$$

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension $7\ldots.$ So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

while, by Peeters result

$$C_0(\Gamma_3) = \log 7.$$

For the orthogonality graphs of other root systems, we have found:

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension 7. . . . So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

while, by Peeters result

$$C_0(\Gamma_3) = \log 7.$$

For the orthogonality graphs of other root systems, we have found:

- A_n, B_n, C_n, D_n, G_2: $C_0^E = C_0$

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3 + 1 = 9$ cliques of size $2^3 - 1 = 7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension $7 \ldots$. So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

while, by Peeters result

$$C_0(\Gamma_3) = \log 7.$$

For the orthogonality graphs of other root systems, we have found:

- A_n, B_n, C_n, D_n, G_2: $C_0^E = C_0$
- E_8: $C_0^E(\Delta(E_8)) = \log 15$ whereas $C_0(\Delta(E_8)) \leq 9$.

Entanglement can increase zero-error capacity

Recall that Γ_3 partitions into $2^3+1=9$ cliques of size $2^3-1=7$. Remarkably,

$$\Gamma_3 = \Delta(E_7)!$$

Therefore, it has an orthonormal representation of dimension 7.... So, by Theorem ORCP

$$C_0^E(\Gamma_3) = \log 9.$$

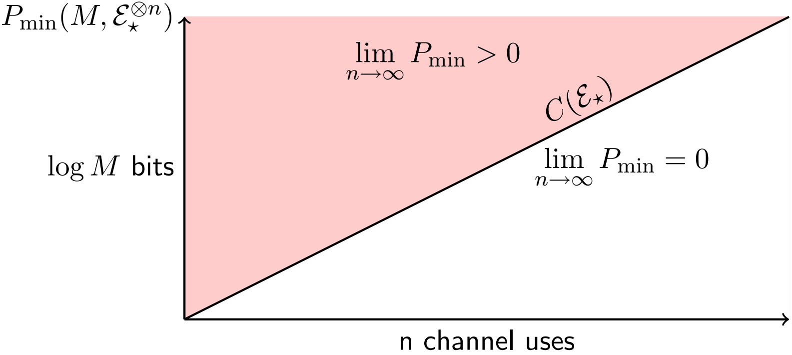
while, by Peeters result

$$C_0(\Gamma_3) = \log 7.$$

For the orthogonality graphs of other root systems, we have found:

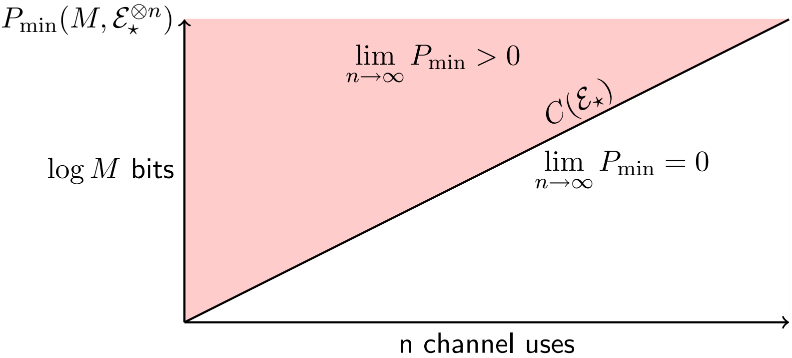
- A_n, B_n, C_n, D_n, G_2: $C_0^E = C_0$
- E_8: $C_0^E(\Delta(E_8)) = \log 15$ whereas $C_0(\Delta(E_8)) \leq 9$.
- F_4, E_6: Don't know if there is a separation.

The channel $\mathcal{E}_\star$.



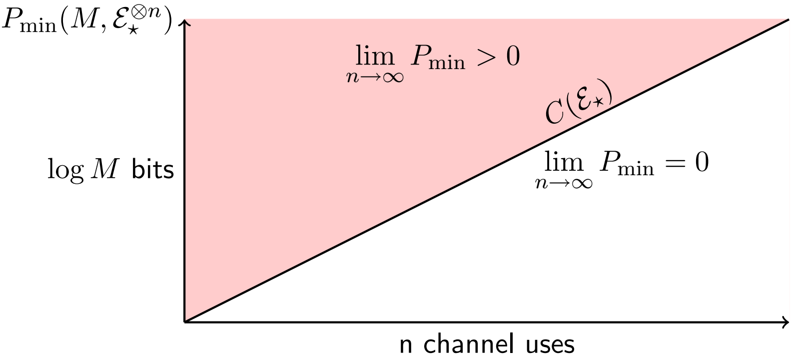
Channel $\mathcal{E}_\star$: Input symbols: Vertices of Γ_3.

The channel $\mathcal{E}_\star$.



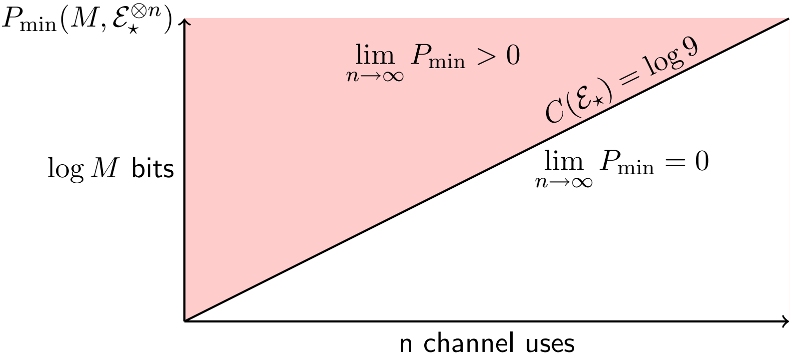
Channel $\mathcal{E}_\star$: Input symbols: Vertices of Γ_3. The output is a 7-clique in Γ_3. There are 135 of these and each input symbol is contained in 15 of them.

The channel $\mathcal{E}_\star$.



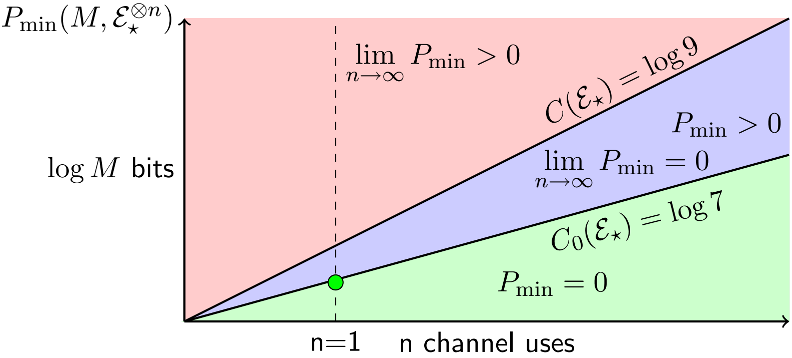
Channel $\mathcal{E}_\star$: Input symbols: Vertices of Γ_3. The output is a 7-clique in Γ_3. There are 135 of these and each input symbol is contained in 15 of them. Output is selected uniformly at random from these 15. $G(\mathcal{E}_\star) = \Gamma_3$.

The channel $\mathcal{E}_\star$.



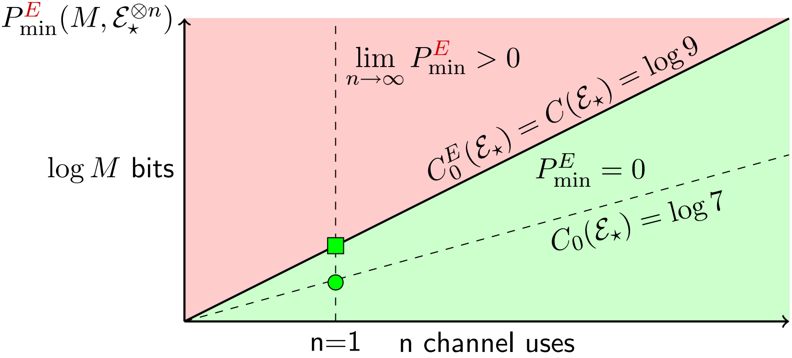
Capacity $C(\mathcal{E}_\star) = \log 9$.

The channel $\mathcal{E}_\star$.



Capacity $C(\mathcal{E}_\star) = \log 9$.
$G(\mathcal{E}_\star) = \Gamma_3$. Zero-error capacity $C_0(\mathcal{E}_\star) = \log 7$.

The channel $\mathcal{E}_\star$.



Capacity $C(\mathcal{E}_\star) = \log 9$.
$G(\mathcal{E}_\star) = \Gamma_3$. Zero-error capacity $C_0(\mathcal{E}_\star) = \log 7$.
Entanglement-assisted zero-error capacity $C_0^E(\mathcal{E}_\star) = \log 9$!

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.

Striking qualitative changes to asymptotic error dependence at rates $< C$.

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.
Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E?

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.

Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E? C_0^E?

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.
Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E? C_0^E?
- Graphs with separation between $C_0^E(G)$ and $\log \vartheta(G)$?

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.
Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E? C_0^E?
- Graphs with separation between $C_0^E(G)$ and $\log \vartheta(G)$?
- Beyond zero-error: Effect of entanglement on error probability vs. n at rates below capacity?

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.
Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E? C_0^E?
- Graphs with separation between $C_0^E(G)$ and $\log \vartheta(G)$?
- Beyond zero-error: Effect of entanglement on error probability vs. n at rates below capacity?
- Relationship to non-contextuality.

Conclusion and open questions

Entanglement assistance can increase the $n \to \infty$ rate of zero-error communication over some classical channels.
Striking qualitative changes to asymptotic error dependence at rates $< C$.

- Computing M_0^E? C_0^E?
- Graphs with separation between $C_0^E(G)$ and $\log \vartheta(G)$?
- Beyond zero-error: Effect of entanglement on error probability vs. n at rates below capacity?
- Relationship to non-contextuality.

Thanks!