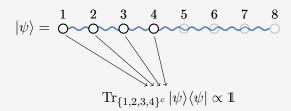
Constructing optimal quantum error correcting codes from absolutely maximally entangled states

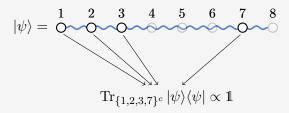
Zahra Raissi^{1,2}, Christian Gogolin¹, Arnau Riera¹, Antonio Acín^{1,3}

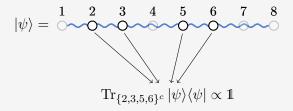
¹ICFO - The Institute of Photonic Sciences
 ²Sharif University of Technology Tehran
 ³ICREA-Institució Catalana de Recerca i Estudis Avançats

arXiv:1701.03359

AQUIS 2017 Singapore 2017-09-08





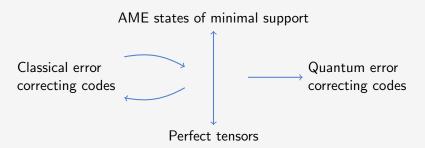


AME states

A state of n particles is AME if for all $S \subset \{1, \ldots, n\}$

$$|S| \leq |n/2| \Longrightarrow \operatorname{Tr}_{S^c} |\psi\rangle\langle\psi| \propto \mathbb{1}.$$

Content of this talk



^[1] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski, Phys. Rev. A, 92 (3 2015), 032316

^[2] W. Helwig and W. Cui, (2013), URL: https://arxiv.org/abs/1306.2536

Natural generalization of EPR and GHZ states

^[3] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Phys. Rev. A, 86 (5 2012), 052335

^[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6 (2015), 149

 $^{[5] \ \}mathsf{F.\ Huber},\ \mathsf{O.\ G\"{u}hne},\ \mathsf{and}\ \mathsf{J.\ S\acute{l}ewert},\ (2016),\ \mathsf{URL}:\ \mathtt{https://arxiv.org/abs/1608.06228}$

^[6] A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330

- Natural generalization of EPR and GHZ states
- Resource for multipartite teleportation and quantum secret sharing [3]

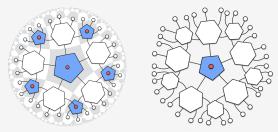
^[3] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Phys. Rev. A, 86 (5 2012), 052335

^[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6 (2015), 149

^[5] F. Huber, O. Gühne, and J. Siewert, (2016), URL: https://arxiv.org/abs/1608.06228

^[6] A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330

- Natural generalization of EPR and GHZ states
- Resource for multipartite teleportation and quantum secret sharing [3]
- Holographic models implementing the Ads/Cft correspondence [4]



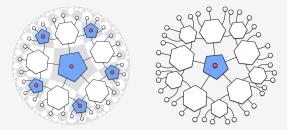
^[3] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Phys. Rev. A, 86 (5 2012), 052335

^[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6 (2015), 149

^[5] F. Huber, O. Gühne, and J. Siewert, (2016), URL: https://arxiv.org/abs/1608.06228

^[6] A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330

- Natural generalization of EPR and GHZ states
- Resource for multipartite teleportation and quantum secret sharing [3]
- Holographic models implementing the Ads/Cft correspondence [4]



Still fundamental questions open. Existence (qubits):

$$n = 2, 3, 4, 5, 6, 7, 8, 9, \dots$$
 [5, 6]

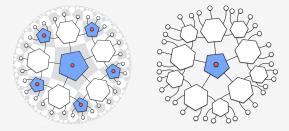
^[3] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Phys. Rev. A, 86 (5 2012), 052335

^[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6 (2015), 149

^[5] F. Huber, O. Gühne, and J. Siewert, (2016), URL: https://arxiv.org/abs/1608.06228

^[6] A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330

- Natural generalization of EPR and GHZ states
- Resource for multipartite teleportation and quantum secret sharing [3]
- Holographic models implementing the Ads/Cft correspondence [4]



Still fundamental questions open. Existence (qubits):

$$n = 2, 3, 4, 5, 6, 7, 8, 9, \dots$$
 [5, 6]

^[3] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Phys. Rev. A, 86 (5 2012), 052335

^[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6 (2015), 149

^[5] F. Huber, O. Gühne, and J. Siewert, (2016), URL: https://arxiv.org/abs/1608.06228

^[6] A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330

Message

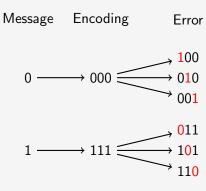
0

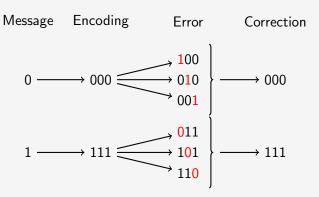
1

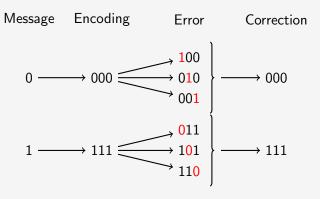
Message Encoding

$$0 \longrightarrow 000$$

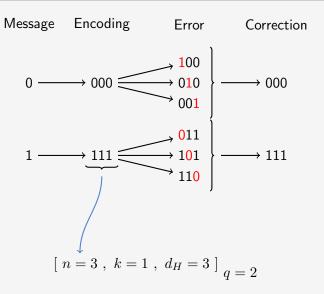
$$1 \longrightarrow 111$$

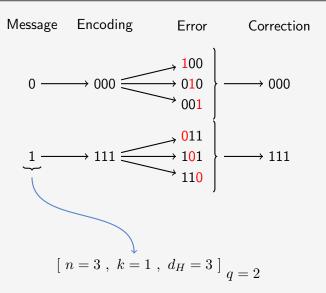


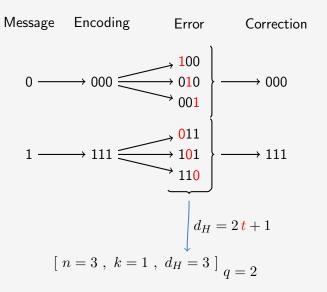


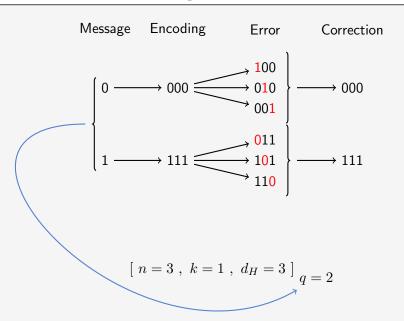


$$[n=3, k=1, d_H=3]_{q=2}$$









Maximal distance separable (MDS) codes

$$[n=3, k=1, d_H=3]_{q=2}$$

Is this optimal?

Maximal distance separable (MDS) codes

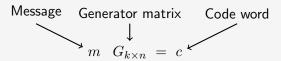
$$[n=3, k=1, d_H=3]_{q=2}$$

Is this optimal? Yes!

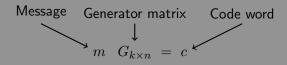
Singleton bound [7]

$$d_H \leq n - k + 1$$

Constructing linear MDS codes



Constructing linear MDS codes

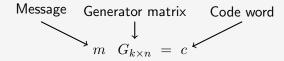


This only makes sense if you can take linear combinations of messages and code words!

Yes. Right. Solution: Finite fields

Integers modulo q for q prime are a finite field.

Constructing linear MDS codes



G Has standard form (by taking linear combinations of code words)

$$G_{k\times n}=[\mathbb{1}_k|A]$$

Message Generator matrix Code word $\frac{1}{m} G_{h \times n} = c$

G Has standard form (by taking linear combinations of code words)

$$G_{k\times n} = [\mathbb{1}_k|A]$$

Smallest Hamming dist. given by smallest dist. to all zero code word. \Longrightarrow Code is MDS iff any subset of k columns of $G_{k\times n}$ is linearly independent. \iff All square sub-matrices of A are non-singular.

■ Take an MDS code with $k = \lfloor n/2 \rfloor$

Minimal support AME states from MDS codes

- Take an MDS code with $k = \lfloor n/2 \rfloor$
- Smallest Hamming distance between any two code words $d_H = n k + 1 = \lceil n/2 \rceil + 1$

- Take an MDS code with $k = \lfloor n/2 \rfloor$
- Smallest Hamming distance between any two code words $d_H = n k + 1 = \lceil n/2 \rceil + 1$
- Consider $\vec{v}, \vec{w} \in [q]^{\lfloor n/2 \rfloor}$, then the product states

$$|\vec{v} \ G_{\lfloor n/2 \rfloor \times n} \rangle$$
 and
$$|\vec{w} \ G_{\lfloor n/2 \rfloor \times n} \rangle$$

remain orthogonal upon tracing out up to $\lceil n/2 \rceil$ subsystems.

- Take an MDS code with $k = \lfloor n/2 \rfloor$
- Smallest Hamming distance between any two code words $d_H = n k + 1 = \lceil n/2 \rceil + 1$
- Consider $\vec{v}, \vec{w} \in [q]^{\lfloor n/2 \rfloor}$, then the product states

$$|\vec{v} \ G_{\lfloor n/2 \rfloor \times n} \rangle$$
 and
$$|\vec{w} \ G_{\lfloor n/2 \rfloor \times n} \rangle$$

remain orthogonal upon tracing out up to $\lceil n/2 \rceil$ subsystems.

■ Hence, we can construct a minimal support AME state like this:

$$|\Psi\rangle \propto \sum_{ec{v} \in [q]^{\lfloor n/2 \rfloor}} |ec{v} \, G_{k \times n} \rangle$$

An example

Generator matrix of a $[6,3,4]_5$ MDS code:

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array} \right].$$

An example

Generator matrix of a $[6,3,4]_5$ MDS code:

$$G_{3\times 6} = \left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{array} \right].$$

Yields minimal support AME state for n = 6, q = 5:

$$|\Psi\rangle = \sum_{\vec{v} \in GF(5)^3} |\vec{v}\,G\rangle = \sum_{i,j,l=0}^4 |i,j,l,i+j+l,i+2j+3l,i+3j+4l\rangle$$

Can construct such states for all $n \leq q-1$ and q prime [arXiv:1701.03359].

Stabilizers of $|\Psi\rangle$ can be read off from the the G matrix.

MDS codes from minimal support AME states

 $\begin{array}{ccc} \mathsf{MDS}\;\mathsf{code} & & \longrightarrow & \begin{array}{c} \mathsf{Minimal}\;\mathsf{support} \\ \mathsf{AME}\;\mathsf{state} \end{array}$

MDS codes from minimal support AME states

 $\begin{array}{ccc} \mathsf{MDS} \; \mathsf{code} & & & \mathsf{Minimal} \; \mathsf{support} \\ & & \mathsf{AME} \; \mathsf{state} \end{array}$

Quantum error correcting codes

 $\left[\left[\;n\;,\;k\;,\;d\;\right]\right]_{\;q}$

Quantum error correcting codes

$$[[\; n \;,\; k \;,\; d \;]]_{\;\; q}$$

Message

Encoding

unitary

$$|\psi\rangle \in (\mathbb{C}^q)^{\otimes k} \longrightarrow |\varphi\rangle \in \mathcal{C} \subset (\mathbb{C}^q)^{\otimes n}$$

^[10] D. Gottesman, PhD thesis, Caltech, 1997, URL: https://arxiv.org/abs/quant-ph/9705052

^[11] E. Knill and R. Laflamme, Phys. Rev. A, 55 (2 1997), 900-911

^[12] N. J. Cerf and R. Cleve, Phys. Rev. A, 56 (3 1997), 1721-1732

Quantum error correcting codes

$$[[\; n \;,\; k \;,\; d \;]]_{\;\; q}$$

Message

Encoding

Error

unitary

$$|\psi\rangle \in (\mathbb{C}^q)^{\otimes k} \longrightarrow |\varphi\rangle \in \mathcal{C} \subset (\mathbb{C}^q)^{\otimes n} \longrightarrow |\tilde{\varphi}\rangle \notin \mathcal{C}$$

$$t \text{ systems affected}$$

^[10] D. Gottesman, PhD thesis, Caltech, 1997, URL: https://arxiv.org/abs/quant-ph/9705052

^[11] E. Knill and R. Laflamme, Phys. Rev. A, 55 (2 1997), 900-911

^[12] N. J. Cerf and R. Cleve, Phys. Rev. A, 56 (3 1997), 1721–1732

Quantum error correcting codes

$$[[\; n \;,\; k \;,\; d \;]]_{\;\; q}$$

Message Encoding Error Correction unitary measuring stabilizers $|\psi\rangle\in(\mathbb{C}^q)^{\otimes k}\longrightarrow|\varphi\rangle\in\mathcal{C}\subset(\mathbb{C}^q)^{\otimes n}\longrightarrow|\tilde{\varphi}\rangle\notin\mathcal{C}\longrightarrow|\varphi\rangle\in\mathcal{C}$ t systems affected

^[10] D. Gottesman, PhD thesis, Caltech, 1997, URL: https://arxiv.org/abs/quant-ph/9705052

^[11] E. Knill and R. Laflamme, Phys. Rev. A, 55 (2 1997), 900-911

^[12] N. J. Cerf and R. Cleve, Phys. Rev. A, 56 (3 1997), 1721–1732

Quantum error correcting codes

$$[[\ n\ ,\ k\ ,\ d\]]\ _{q}$$

Message

Encoding

Error

Correction

unitary

measuring stabilizers

$$|\psi\rangle\in(\mathbb{C}^q)^{\otimes k}\longrightarrow|\varphi\rangle\in\mathcal{C}\subset(\mathbb{C}^q)^{\otimes n}\longrightarrow|\tilde{\varphi}\rangle\notin\mathcal{C}\longrightarrow|\varphi\rangle\in\mathcal{C}$$
 t systems affected

Quantum singleton bound [10–12]

$$2t + 1 = d \le \frac{n - k}{2} + 1$$

^[10] D. Gottesman, PhD thesis, Caltech, 1997, URL: https://arxiv.org/abs/quant-ph/9705052

^[11] E. Knill and R. Laflamme, Phys. Rev. A, 55 (2 1997), 900-911

^[12] N. J. Cerf and R. Cleve, Phys. Rev. A, 56 (3 1997), 1721-1732

Conjecture

For every prime $q \geq n-1$ and n even there exists a $[[n,1,n/2]]_q$ QECC, whose code space $\mathcal C$ is spanned by AME states.

Conjecture

For every prime $q \geq n-1$ and n even there exists a $[[n,1,n/2]]_q$ QECC, whose code space $\mathcal C$ is spanned by AME states.

Conjecture

For every prime $q \ge n-1$ and n even there exists a $[[n,1,n/2]]_q$ QECC, whose code space $\mathcal C$ is spanned by AME states.

Conjecture

For every prime $q \geq n-1$ and n even there exists a $[[n,1,n/2]]_q$ QECC, whose code space $\mathcal C$ is spanned by AME states.

- We can explicitly construct the codes up to n = 8.
- The conjecture is true if there exist certain operators M whose weight cannot be decreased by multiplying it with stabilizers of $|\Psi\rangle$...

Conjecture

For every prime $q \ge n-1$ and n even there exists a $[[n,1,n/2]]_q$ QECC, whose code space $\mathcal C$ is spanned by AME states.

- We can explicitly construct the codes up to n = 8.
- The conjecture is true if there exist certain operators M whose weight cannot be decreased by multiplying it with stabilizers of $|\Psi\rangle$. . . and we can almost show that such M exist for all even n.

The code

Given a minimal support AME state $|\Psi\rangle$:

The code

$$\mathcal{C} \coloneqq \operatorname{span}(\{|\Psi_m\rangle\}) \quad \text{with} \quad |\Psi_m\rangle \coloneqq M^m |\Psi\rangle$$

The code

Given a minimal support AME state $|\Psi\rangle$:

The code
$$\mathcal{C}\coloneqq \mathrm{span}(\{|\Psi_m
angle\}) \quad ext{ with } \quad |\Psi_m
angle\coloneqq M^m|\Psi
angle$$

lacktriangle To correct errors E,F from some set of errors, we must have that

$$m \neq m' \implies \langle \psi_m | E^{\dagger} F | \psi_{m'} \rangle = 0.$$

The code

Given a minimal support AME state $|\Psi\rangle$:

The code
$$\mathcal{C}\coloneqq \mathrm{span}(\{|\Psi_m
angle\}) \quad ext{ with } \quad |\Psi_m
angle\coloneqq M^m|\Psi
angle$$

lacktriangle To correct errors E,F from some set of errors, we must have that

$$m \neq m' \implies \langle \psi_m | E^{\dagger} F | \psi_{m'} \rangle = 0.$$

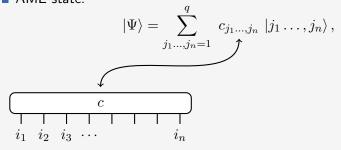
■ Claim: If M is an incompressible Pauli string operator, then $\mathcal C$ is a $[[n,1,n/2]]_q$ QECC.

■ Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$

- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$

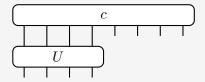
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:



"perfect tensor"

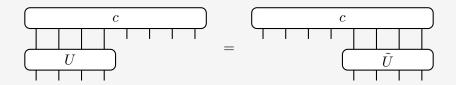
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



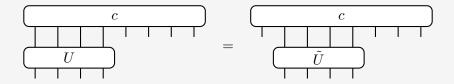
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



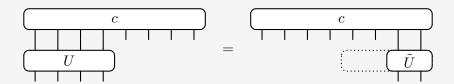
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



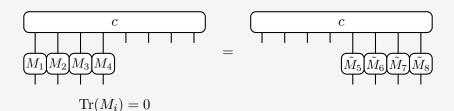
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



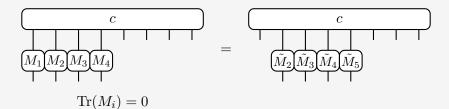
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



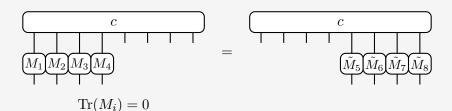
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



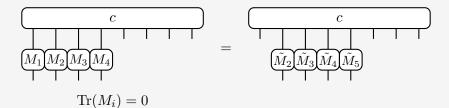
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



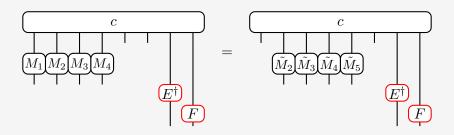
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



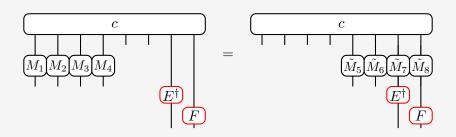
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$



- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

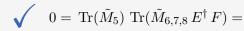
$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$

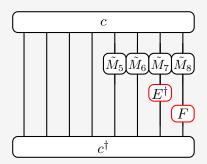
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$

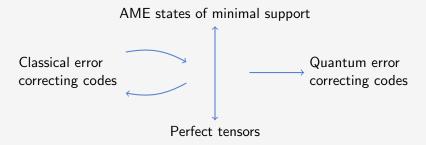
- Remember EPR state: $(U \otimes 1)|\psi^+\rangle = (1 \otimes U^{\dagger})|\psi^+\rangle$
- AME state:

$$|\Psi\rangle = \sum_{j_1,\dots,j_n=1}^q c_{j_1,\dots,j_n} |j_1,\dots,j_n\rangle,$$

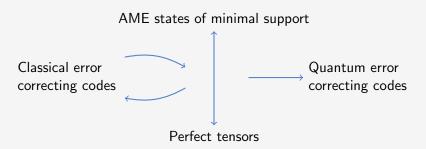




Summary



Thank you for your attention!



D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and

A. J. Scott, Phys. Rev. A, 69 (5 2004), 052330.

R. Singleton, IEEE Trans. Inf. Theor., 10.2 (2006),

References

[6]

	K. Życzkowski, Phys. Rev. A, 92 (3 2015), 032316.		116–118.
[2]	W. Helwig and W. Cui, (2013), URL: https://arxiv.org/abs/1306.2536.	[8]	R. M. Roth and G. Seroussi, IEEE Trans. Inf. Theor., 31.6 (1985), 826–830.
[3]	W. Helwig, W. Cui, J. I. Latorre, A. Riera, and HK. Lo, Phys. Rev. A, 86 (5 2012), 052335.	[9]	T. Maruta, Discrete Mathematics, 81.1 (1990), 33 –36.
[4]	F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics, 2015.6	[10]	D. Gottesman, PhD thesis, Caltech, 1997, URL: https://arxiv.org/abs/quant-ph/9705052.
[5]	(2015), 149. F. Huber, O. Gühne, and J. Siewert, (2016), URL:	[11]	E. Knill and R. Laflamme, Phys. Rev. A, 55 (2 1997), 900-911.
[5]	https://arxiv.org/abs/1608.06228.	[12]	N. J. Cerf and R. Cleve, Phys. Rev. A, 56 (3 1997),

Funded by: the European Research Council (ERC AdG OSYRIS and CoG QITBOX), Axa Chair in Quantum Information Science, The John Templeton Foundation, Spanish MINECO (FOQUS FIS2013-46768 and Severo Ochoa Grant No. SEV-2015-0522). Fundació Privada Cellex, and Generalitat de Catalunya (Grant No. SGR 874 and 875). C. G. acknowledges support by MPQ-ICFO, ICFOnest+ (FP7-PEOPLE-2013-COFUND), and co-funding by the European Union's Marie Skłodowska-Curie Individual Fellowships (IF-EF) programme under GA: 700140. A. R. is supported by the Beatriu de Pinós fellowship (BP-DGR 2013).