# A transform of complementary aspects with applications to EURs

Prabha Mandayam
Institute of Mathematical Sciences, Chennai
Joint work with
Stephanie Wehner (CQT, Singapore)
Niranjan Balachandran(Dept. of Math., IIT Bombay)

Reference: Journal of Math Phys , **51**, 082201 (2010)

# Outline

- Entropic uncertainty relations: brief overview.

# Outline

- Entropic uncertainty relations: brief overview.
- Complementarity and uncertainty: the role of mutually unbiased bases (MUBs) in obtaining **strong** uncertainty relations.

# Outline

- Entropic uncertainty relations: brief overview.
- Complementarity and uncertainty: the role of mutually unbiased bases (MUBs) in obtaining **strong** uncertainty relations.
- A novel construction of symmetric MUBs using the generators of the Clifford algebra.

# Outline

- Entropic uncertainty relations: brief overview.
- Complementarity and uncertainty: the role of mutually unbiased bases (MUBs) in obtaining **strong** uncertainty relations.
- A novel construction of symmetric MUBs using the generators of the Clifford algebra.
- New lower bounds on the average min-entropy for *any* set of $2 < L \leq d + 1$ MUBs in $d$ dimensions.

# Outline

- Entropic uncertainty relations: brief overview.
- Complementarity and uncertainty: the role of mutually unbiased bases (MUBs) in obtaining **strong** uncertainty relations.
- A novel construction of symmetric MUBs using the generators of the Clifford algebra.
- New lower bounds on the average min-entropy for *any* set of $2 < L \leq d+1$ MUBs in $d$ dimensions.
- An optimal uncertainty relation for $4$ MUBs in $d = 4$.

# Uncertainty relations

- First formulated by Heisenberg (1927) in terms of variances, for canonically conjugate variables.

# Uncertainty relations

- First formulated by Heisenberg (1927) in terms of variances, for canonically conjugate variables.
- Generalized by Robertson (1929), for any two observables $A$ and $B$ :-
  Prepare many copies of the state $|\psi\rangle$, on each of them measure either $A$ or $B$, then,

$$\Delta A \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|$$

  $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$.

# Uncertainty relations

- First formulated by Heisenberg (1927) in terms of variances, for canonically conjugate variables.
- Generalized by Robertson (1929), for any two observables $A$ and $B$ :-
  Prepare many copies of the state $|\psi\rangle$, on each of them measure either $A$ or $B$, then,
  $$\Delta A \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|$$
  $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$.
- Other measures quantifying the spread of the distribution - **entropy**

# Uncertainty relations

- First formulated by Heisenberg (1927) in terms of variances, for canonically conjugate variables.
- Generalized by Robertson (1929), for any two observables $A$ and $B$ :-
  Prepare many copies of the state $|\psi\rangle$, on each of them measure either $A$ or $B$, then,

  $$\Delta A \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|$$

  $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$.
- Other measures quantifying the spread of the distribution - **entropy**
- An entropic uncertainty relation for canonically conjugate variables :-

  $$H(X||\psi\rangle) + H(P||\psi\rangle) \geq \log(e\pi)$$

  Formulated by Everett and Hirschmann (1957); established by Beckner and Bialynicki-Birula and Mycielski (1975).
  This implies the Hiesenberg uncertainty relation.

# Measures of entropy

- **Renyi entropies:** If $P_X(x)$ is a probability distribution over the set $\mathcal{X} = \{x_1, x_2, ..., x_d\}$, Renyi entropy of order $\alpha$ is

$$H_\alpha(P_X) := \frac{1}{1-\alpha} \log \left( \sum_{x \in \mathcal{X}} (P_X(x))^\alpha \right).$$

# Measures of entropy

- **Renyi entropies:** If $P_X(x)$ is a probability distribution over the set $\mathcal{X} = \{x_1, x_2, ..., x_d\}$, Renyi entropy of order $\alpha$ is

$$H_\alpha(P_X) := \frac{1}{1-\alpha} \log \left( \sum_{x \in \mathcal{X}} (P_X(x))^\alpha \right).$$

- **Shannon entropy:**

$$H(P_X) := \lim_{\alpha \to 1} H_\alpha(P_X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

# Measures of entropy

- **Renyi entropies:** If $P_X(x)$ is a probability distribution over the set $\mathcal{X} = \{x_1, x_2, ..., x_d\}$, Renyi entropy of order $\alpha$ is

$$H_\alpha(P_X) := \frac{1}{1-\alpha} \log \left( \sum_{x \in \mathcal{X}} (P_X(x))^\alpha \right).$$

- **Shannon entropy:**

$$H(P_X) := \lim_{\alpha \to 1} H_\alpha(P_X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

- Collision entropy: $H_2(P_X) = -\log \sum_{x \in \mathcal{X}} (P_X(x))^2$.
- Min-entropy: $H_\infty(P_X) = -\log \max_{x \in \mathcal{X}} P_X(x)$.
- Renyi entropies are monotonically *decreasing* in $\alpha$ : $H_\infty(.) \leq H_2(.) \leq H(.)$

# Entropic uncertainty relations[1]

- For a set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$ on the space $\mathbb{H}$ with a finite set of outcomes, an EUR is of the form

$$\frac{1}{L}\sum_{j=1}^{L} H_\alpha(\mathcal{M}_j|\rho) \geq c_{\{\mathcal{M}_j\}}, \;\; \forall\, \rho \in \mathcal{S}(\mathbb{H}).$$

where $c_{\{\mathcal{M}_j\}}$ is independent of the choice of state $\rho$.

[1]For a recent review, see S.Wehner and A.Winter, New Journal of Phys, **12** (2010)

# Entropic uncertainty relations[1]

- For a set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$ on the space $\mathbb{H}$ with a finite set of outcomes, an EUR is of the form

$$\frac{1}{L}\sum_{j=1}^{L} H_\alpha(\mathcal{M}_j|\rho) \geq c_{\{\mathcal{M}_j\}}, \ \ \forall\, \rho \in \mathcal{S}(\mathbb{H}).$$

  where $c_{\{\mathcal{M}_j\}}$ is independent of the choice of state $\rho$.

- Captures the extent of mutual incompatibility of the set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$.

[1]For a recent review, see S.Wehner and A.Winter, New Journal of Phys, **12** (2010)

# Entropic uncertainty relations[1]

- For a set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$ on the space $\mathbb{H}$ with a finite set of outcomes, an EUR is of the form

$$\frac{1}{L}\sum_{j=1}^{L} H_\alpha(\mathcal{M}_j|\rho) \geq c_{\{\mathcal{M}_j\}}, \ \ \forall\, \rho \in \mathcal{S}(\mathbb{H}).$$

  where $c_{\{\mathcal{M}_j\}}$ is independent of the choice of state $\rho$.

- Captures the extent of mutual incompatibility of the set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$.
- There always exists $\rho$ such that $H_\alpha(\mathcal{M}_j|\rho) = 0$ for one of the measurements $\mathcal{M}_j$ (an eigenstate!). $\Rightarrow \left(1 - \frac{1}{L}\right)\log|\mathcal{X}| \geq c_{\{\mathcal{M}_j\}} \geq 0$.

[1] For a recent review, see S.Wehner and A.Winter, New Journal of Phys, **12** (2010)

# Entropic uncertainty relations[1]

- For a set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$ on the space $\mathbb{H}$ with a finite set of outcomes, an EUR is of the form

$$\frac{1}{L}\sum_{j=1}^{L} H_\alpha(\mathcal{M}_j|\rho) \geq c_{\{\mathcal{M}_j\}}, \;\; \forall \, \rho \in \mathcal{S}(\mathbb{H}).$$

  where $c_{\{\mathcal{M}_j\}}$ is independent of the choice of state $\rho$.

- Captures the extent of mutual incompatibility of the set of measurements $\{\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_L\}$.
- There always exists $\rho$ such that $H_\alpha(\mathcal{M}_j|\rho) = 0$ for one of the measurements $\mathcal{M}_j$ (an eigenstate!). $\Rightarrow \left(1 - \frac{1}{L}\right)\log|\mathcal{X}| \geq c_{\{\mathcal{M}_j\}} \geq 0$.
- If $c_{\{\mathcal{M}_j\}} = \left(1 - \frac{1}{L}\right)\log|\mathcal{X}|$, the set $\{\mathcal{M}_j\}$ is *maximally incompatible*, implying a **maximally strong uncertainty relation**.

[1] For a recent review, see S.Wehner and A.Winter, New Journal of Phys, **12** (2010)

# EURs for two measurement bases

- The Massen and Uffink bound (1988) :-
  For state $\rho \in \mathbb{H}$ (dim $\mathbb{H} = d$) and observables $\mathcal{A}$ and $\mathcal{B}$ with orthonormal eigenbases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$,

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A}, \mathcal{B})$$

  where[2] $c(\mathcal{A}, \mathcal{B}) := \max |\langle a|b\rangle|, \; \forall\, |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

[2] Shannon entropy: $H(P_X) := -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x)$

# EURs for two measurement bases

- The Massen and Uffink bound (1988) :-
  For state $\rho \in \mathbb{H}$ (dim $\mathbb{H} = d$) and observables $\mathcal{A}$ and $\mathcal{B}$ with orthonormal eigenbases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$,

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A},\mathcal{B})$$

  where[2] $c(\mathcal{A},\mathcal{B}) := \max |\langle a|b\rangle|, \ \forall\ |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

- Maximum value of RHS is attained when $|\langle a|b\rangle| = \frac{1}{\sqrt{d}},\ \forall |a\rangle, |b\rangle$, so that

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq \frac{1}{2}\log d$$

[2] Shannon entropy: $H(P_X) := -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x)$

# EURs for two measurement bases

- The Massen and Uffink bound (1988) :-
  For state $\rho \in \mathbb{H}$ (dim $\mathbb{H} = d$) and observables $\mathcal{A}$ and $\mathcal{B}$ with orthonormal eigenbases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$,

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A},\mathcal{B})$$

  where[2] $c(\mathcal{A},\mathcal{B}) := \max |\langle a|b\rangle|, \; \forall \, |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

- Maximum value of RHS is attained when $|\langle a|b\rangle| = \frac{1}{\sqrt{d}}, \; \forall |a\rangle, |b\rangle$, so that

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq \frac{1}{2}\log d$$

- Strongest possible uncertainty relation is obtained when the bases are *mutually unbiased*.

[2] Shannon entropy: $H(P_X) := -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x)$

# EURs for two measurements

- Massen-Uffink bound is not tight for general pairs of observables[3] – eg. components of spin along non-orthogonal directions.

[3] Shown to be tight for Stabilizer Basis States: Niekamp et al. JMP **53** (2012)

# EURs for two measurements

- Massen-Uffink bound is not tight for general pairs of observables[3] – eg. components of spin along non-orthogonal directions.
- Massen-Uffink bound for the min-entropy[4]

$$\frac{1}{2}\left(H_{\infty}(\mathcal{A}||\psi\rangle) + H_{\infty}(\mathcal{B}||\psi\rangle)\right) \geq -\log\left[\frac{1+c(\mathcal{A},\mathcal{B})}{2}\right]$$

[3]Shown to be tight for Stabilizer Basis States: Niekamp et al. JMP **53** (2012)
[4]Min-entropy: $H_{\infty}(P_X) = -\log\max_{x\in\mathcal{X}} P_X(x)$

# EURs for two measurements

- Massen-Uffink bound is not tight for general pairs of observables[3] – eg. components of spin along non-orthogonal directions.

- Massen-Uffink bound for the min-entropy[4]

$$\frac{1}{2}\left(H_\infty(\mathcal{A}||\psi\rangle) + H_\infty(\mathcal{B}||\psi\rangle)\right) \geq -\log\left[\frac{1+c(\mathcal{A},\mathcal{B})}{2}\right]$$

- Tight for some choices of $\mathcal{A}$ and $\mathcal{B}$, in particular, for $2$ mutually unbiased bases in $d=2$.

[3] Shown to be tight for Stabilizer Basis States: Niekamp et al. JMP **53** (2012)
[4] Min-entropy: $H_\infty(P_X) = -\log\max_{x\in\mathcal{X}} P_X(x)$

- **Definition**:- Two orthonormal bases $\mathcal{B}^{(1)} = \{|b_1^1\rangle, |b_2^1\rangle, ..., |b_d^1\rangle\}$ and $\mathcal{B}^{(2)} = \{|b_1^2\rangle, |b_2^2\rangle, ..., |b_d^2\rangle\}$ in $\mathbb{C}^d$ are *mutually unbiased* if

$$|\langle b_k^1 | b_l^2 \rangle| = \frac{1}{\sqrt{d}}, \ \forall\, k, l = 1, ..., d$$

[6] For a recent review, see T.Durt *et al.* Int. J. Quant Info, **8**, 535-640 (2010)

# Mutually unbiased bases[6]

## Definition and examples

- **Definition**:- Two orthonormal bases $\mathcal{B}^{(1)} = \{|b_1^1\rangle, |b_2^1\rangle, ..., |b_d^1\rangle\}$ and $\mathcal{B}^{(2)} = \{|b_1^2\rangle, |b_2^2\rangle, ..., |b_d^2\rangle\}$ in $\mathbb{C}^d$ are *mutually unbiased* if

$$|\langle b_k^1 | b_l^2 \rangle| = \frac{1}{\sqrt{d}}, \ \forall \, k, l = 1, ..., d$$

- **Examples**:- Eigenvectors of $\sigma_x$ and $\sigma_z$ in $d = 2$.
  In general, the computational basis and Hadamard basis. (Eigenbases of $\mathtt{I}^{\otimes k}$ and $\mathbf{H}^{\otimes k}$ in dimension $d = 2^k$, where $\mathbf{H}$ is the Hadamard matrix.)

[6] For a recent review, see T.Durt *et al.* Int. J. Quant Info, **8**, 535-640 (2010)

- **Definition**:- Two orthonormal bases $\mathcal{B}^{(1)} = \{|b_1^1\rangle, |b_2^1\rangle, ..., |b_d^1\rangle\}$ and $\mathcal{B}^{(2)} = \{|b_1^2\rangle, |b_2^2\rangle, ..., |b_d^2\rangle\}$ in $\mathbb{C}^d$ are *mutually unbiased* if

$$|\langle b_k^1 | b_l^2 \rangle| = \frac{1}{\sqrt{d}}, \ \forall\, k, l = 1, ..., d$$

- **Examples**:- Eigenvectors of $\sigma_x$ and $\sigma_z$ in $d = 2$.
  In general, the computational basis and Hadamard basis. (Eigenbases of $\mathtt{I}^{\otimes k}$ and $\mathbf{H}^{\otimes k}$ in dimension $d = 2^k$, where $\mathbf{H}$ is the Hadamard matrix.)
- Maximal number of MUBs[5] in dimension $d$ is $N(d) \leq d + 1$.
  If $d = p^k$, $N(d) = d + 1$ – explicit construction is known using generalized Pauli operators.

[5] S.Bandyopadhyay *et al.* Algorithmica, **34**(4), 512, 2002
[6] For a recent review, see T.Durt *et al.* Int. J. Quant Info, **8**, 535-640 (2010)

- MUBs give rise to maximally strong uncertainty relations for the case of two measurements.

- MUBs give rise to maximally strong uncertainty relations for the case of two measurements.
- For measurements involving more than 2 bases, to obtain strong uncertainty relations, the bases must be mutually unbiased -
  MUBs are a *necessary* condition to achieve maximal incompatibility with multiple bases.

- MUBs give rise to maximally strong uncertainty relations for the case of two measurements.
- For measurements involving more than 2 bases, to obtain strong uncertainty relations, the bases must be mutually unbiased -
  MUBs are a *necessary* condition to achieve maximal incompatibility with multiple bases.
- When the complete set of $d+1$ MUBs exist, EURs are known[7]

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H_2(\mathcal{B}_j|\rho) \geq \log(d+1) - 1$$

Tight for states invariant under $U : \mathcal{B}_1 \rightarrow \mathcal{B}_2 \rightarrow \ldots \mathcal{B}_d \rightarrow \mathcal{B}_1$.

[7] I.D.Ivanovic, J. Phys. A: Math. Gen.**25**(7), 363, 1992;
J.Sanchez, Physic Letters A **173**, 233, 1993

- MUBs give rise to maximally strong uncertainty relations for the case of two measurements.
- For measurements involving more than 2 bases, to obtain strong uncertainty relations, the bases must be mutually unbiased -
  MUBs are a *necessary* condition to achieve maximal incompatibility with multiple bases.
- When the complete set of $d+1$ MUBs exist, EURs are known[7]

$$\frac{1}{d+1}\sum_{j=1}^{d+1} H_2(\mathcal{B}_j|\rho) \geq \log(d+1) - 1$$

  Tight for states invariant under $U : \mathcal{B}_1 \rightarrow \mathcal{B}_2 \rightarrow \ldots \mathcal{B}_d \rightarrow \mathcal{B}_1$.
- For less than $d+1$ MUBs, such relations have not been obtained.

[7] I.D.Ivanovic, J. Phys. A: Math. Gen.**25**(7), 363, 1992;
J.Sanchez, Physic Letters A **173**, 233, 1993

# Uncertainty relations for MUBs

- In square prime power dimensions ($d = p^{2l}$) there exist upto $p^l + 1$ MUBs derived from generalized Pauli matrices, which satisfy *weak* uncertainty relations[8] :-

$$\min_{\rho} \frac{1}{L} \sum_{j} H(\mathcal{B}_j|\rho) = \frac{\log d}{2}$$

[8] M.Ballester and S.Wehner, PRA, **75** 022319, 2007

# Uncertainty relations for MUBs

- In square prime power dimensions ($d = p^{2l}$) there exist upto $p^l + 1$ MUBs derived from generalized Pauli matrices, which satisfy *weak* uncertainty relations[8] :-

$$\min_{\rho} \frac{1}{L} \sum_j H(\mathcal{B}_j|\rho) = \frac{\log d}{2}$$

- This is infact the trivial lower bound obtained by combining pairwise, the Massen-Uffink bound for multiple MUBs!

[8] M.Ballester and S.Wehner, PRA, **75** 022319, 2007

# Uncertainty relations for MUBs

- In square prime power dimensions ($d = p^{2l}$) there exist upto $p^l + 1$ MUBs derived from generalized Pauli matrices, which satisfy *weak* uncertainty relations[8] :-

$$\min_{\rho} \frac{1}{L} \sum_{j} H(\mathcal{B}_j|\rho) = \frac{\log d}{2}$$

- This is infact the trivial lower bound obtained by combining pairwise, the Massen-Uffink bound for multiple MUBs!
- For 3 MUBs in prime power dimension, it has been shown[9] that the lower bound cannot exceed $\left(\frac{1}{2} + O(1)\right) \log d$ for large dimensions (assuming the Generalized Riemann Hypothesis!!).

[8] M.Ballester and S.Wehner, PRA, **75** 022319, 2007

[9] A.Ambainis, arXiV:0909.3720

# Uncertainty relations for MUBs

- In square prime power dimensions ($d = p^{2l}$) there exist upto $p^l + 1$ MUBs derived from generalized Pauli matrices, which satisfy *weak* uncertainty relations[8] :-

$$\min_{\rho} \frac{1}{L} \sum_j H(\mathcal{B}_j|\rho) = \frac{\log d}{2}$$

- This is infact the trivial lower bound obtained by combining pairwise, the Massen-Uffink bound for multiple MUBs!
- For 3 MUBs in prime power dimension, it has been shown[9] that the lower bound cannot exceed $\left(\frac{1}{2} + O(1)\right) \log d$ for large dimensions (assuming the Generalized Riemann Hypothesis!!).
- Thus, for more than two measurements with multiple outcomes, whether there exist maximally strong uncertainty relations remains an interesting open question.

[8] M.Ballester and S.Wehner, PRA, **75** 022319, 2007
[9] A.Ambainis, arXiV:0909.3720

# Some practical motivations!

- Apart from their significance in understanding the foundations of quantum mechanics, EURs play a central role in cryptography.

# Some practical motivations!

- Apart from their significance in understanding the foundations of quantum mechanics, EURs play a central role in cryptography.

- Applications of Shannon entropic uncertainty relations: security proof of QKD[10], phenomenon of information locking[11].

[10] M. Koashi, e-print arXiv:quant-ph/0505108.
[11] D. DiVincenzo *et al.*, Phys. Rev. Lett. 92, 067902 (2004).

# Some practical motivations!

- Apart from their significance in understanding the foundations of quantum mechanics, EURs play a central role in cryptography.
- Applications of Shannon entropic uncertainty relations: security proof of QKD[10], phenomenon of information locking[11].
- Application of min-entropic uncertainty relations: noisy-storage model[12]. The security of two-party protocols in this model is directly related to a lower bound on the average min-entropy.

[10] M. Koashi, e-print arXiv:quant-ph/0505108.
[11] D. DiVincenzo *et al.*, Phys. Rev. Lett. 92, 067902 (2004).
[12] P.Mandayam and S.Wehner, PRA, **83** (2012)

# Some practical motivations!

- Apart from their significance in understanding the foundations of quantum mechanics, EURs play a central role in cryptography.
- Applications of Shannon entropic uncertainty relations: security proof of QKD[10], phenomenon of information locking[11].
- Application of min-entropic uncertainty relations: noisy-storage model[12]. The security of two-party protocols in this model is directly related to a lower bound on the average min-entropy.
- There exists a direct correspondence between the lower bounds on the average min-entropy and the extrema of discrete Wigner functions.

[10] M. Koashi, e-print arXiv:quant-ph/0505108.
[11] D. DiVincenzo *et al.*, Phys. Rev. Lett. 92, 067902 (2004).
[12] P.Mandayam and S.Wehner, PRA, **83** (2012)

# Some practical motivations!

- Apart from their significance in understanding the foundations of quantum mechanics, EURs play a central role in cryptography.
- Applications of Shannon entropic uncertainty relations: security proof of QKD[10], phenomenon of information locking[11].
- Application of min-entropic uncertainty relations: noisy-storage model[12]. The security of two-party protocols in this model is directly related to a lower bound on the average min-entropy.
- There exists a direct correspondence between the lower bounds on the average min-entropy and the extrema of discrete Wigner functions.
- Separability criteria based on EURs are known[13].

[10] M. Koashi, e-print arXiv:quant-ph/0505108.
[11] D. DiVincenzo *et al.*, Phys. Rev. Lett. 92, 067902 (2004).
[12] P.Mandayam and S.Wehner, PRA, **83** (2012)
[13] O.Guehne, M.Lewenstein, PRA, **70**(2004)

# *Symmetric* MUBs from Clifford generators[14]

- Given the $2n$ generators of the Clifford algebra $\{\Gamma_0, \Gamma_1, ..., \Gamma_{2n-1}\}$ in dimension $d = 2^n$,

[14] P.Mandayam, N.Balachandran and S.Wehner, J Math Phys. **51**, 082201 (2010)

# *Symmetric* MUBs from Clifford generators[14]

- Given the $2n$ generators of the Clifford algebra $\{\Gamma_0, \Gamma_1, ..., \Gamma_{2n-1}\}$ in dimension $d = 2^n$,
  - $\{\Gamma_0, \Gamma_1, ...., \Gamma_{2n-1}\}$ can be viewed as $2n$ orthogonal vectors forming a basis for $\mathbb{R}^{2n}$.
    
    $\Rightarrow$ There exists a unitary $U$ that cyclically permutes the $\Gamma$-operators.
  - This symmetry can be extended to $SO(2n+1)$, including $\Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}$
  - The set of operators $\mathcal{S} = \{\mathtt{I}, \Gamma_j, i\Gamma_i\Gamma_j, \Gamma_i\Gamma_j\Gamma_k, ..., \Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}\}$ forms an orthogonal basis for $d \times d$ Hermitian matrices, where $d = 2^n$.

[14] P.Mandayam, N.Balachandran and S.Wehner, J Math Phys. **51**, 082201 (2010)

# *Symmetric* MUBs from Clifford generators[14]

- Given the $2n$ generators of the Clifford algebra $\{\Gamma_0, \Gamma_1, ..., \Gamma_{2n-1}\}$ in dimension $d = 2^n$,
  - $\{\Gamma_0, \Gamma_1, ...., \Gamma_{2n-1}\}$ can be viewed as $2n$ orthogonal vectors forming a basis for $\mathbb{R}^{2n}$.

    $\Rightarrow$ There exists a unitary $U$ that cyclically permutes the $\Gamma$-operators.
  - This symmetry can be extended to $SO(2n+1)$, including $\Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}$
  - The set of operators $\mathcal{S} = \{\mathtt{I}, \Gamma_j, i\Gamma_i\Gamma_j, \Gamma_i\Gamma_j\Gamma_k, ..., \Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}\}$ forms an orthogonal basis for $d \times d$ Hermitian matrices, where $d = 2^n$.

- To construct MUBs, we group the elements of $\mathcal{S}$ into classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L \mid \mathcal{C}_j \subset \mathcal{S}\}$ of size $|\mathcal{C}_j| = d$ such that (i) the elements of $\mathcal{C}_j$ commute for all $j = 1, 2, ..., L$ and (ii) $\mathcal{C}_j \cap \mathcal{C}_k = \{\mathtt{I}\} \forall j \neq k$.

[14] P.Mandayam, N.Balachandran and S.Wehner, J Math Phys. **51**, 082201 (2010)

# *Symmetric* MUBs from Clifford generators[14]

- Given the $2n$ generators of the Clifford algebra $\{\Gamma_0, \Gamma_1, ..., \Gamma_{2n-1}\}$ in dimension $d = 2^n$,
  - $\{\Gamma_0, \Gamma_1, ...., \Gamma_{2n-1}\}$ can be viewed as $2n$ orthogonal vectors forming a basis for $\mathbb{R}^{2n}$.

    $\Rightarrow$ There exists a unitary $U$ that cyclically permutes the $\Gamma$-operators.
  - This symmetry can be extended to $SO(2n+1)$, including $\Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}$
  - The set of operators $\mathcal{S} = \{\mathtt{I}, \Gamma_j, i\Gamma_i\Gamma_j, \Gamma_i\Gamma_j\Gamma_k, ..., \Gamma_{2n} = i\Gamma_0\Gamma_1..\Gamma_{2n-1}\}$ forms an orthogonal basis for $d \times d$ Hermitian matrices, where $d = 2^n$.
- To construct MUBs, we group the elements of $\mathcal{S}$ into classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L \mid \mathcal{C}_j \subset \mathcal{S}\}$ of size $|\mathcal{C}_j| = d$ such that (i) the elements of $\mathcal{C}_j$ commute for all $j = 1, 2, ..., L$ and (ii) $\mathcal{C}_j \cap \mathcal{C}_k = \{\mathtt{I}\} \forall j \neq k$.
- The common eigenbases of such classes are MUBs that get cyclically permuted under the action of $U$.

[14] P.Mandayam, N.Balachandran and S.Wehner, J Math Phys. **51**, 082201 (2010)

# Constructing *symmetric* MUBs from Clifford generators

- A simple example in $d = 4$. For $k = 3$ MUBs, the classes are given by

$$
\begin{aligned}
\mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_3\Gamma_2\} \\
\mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\
\mathcal{C}_2 &= \{\Gamma_2, i\Gamma_0\Gamma_4, i\Gamma_3\Gamma_1\}
\end{aligned}
$$

# Constructing *symmetric* MUBs from Clifford generators

- A simple example in $d = 4$. For $k = 3$ MUBs, the classes are given by

$$\begin{aligned} \mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_3\Gamma_2\} \\ \mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\ \mathcal{C}_2 &= \{\Gamma_2, i\Gamma_0\Gamma_4, i\Gamma_3\Gamma_1\} \end{aligned}$$

- $U$ that transforms $\Gamma_0 \to \Gamma_1 \to \Gamma_2 \to \Gamma_0$, but leaves $\Gamma_3$ and $\Gamma_4$ invariant, cyclically permutes the corresponding bases.

# Constructing *symmetric* MUBs from Clifford generators

- A simple example in $d = 4$. For $k = 3$ MUBs, the classes are given by

$$
\begin{aligned}
\mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_3\Gamma_2\} \\
\mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\
\mathcal{C}_2 &= \{\Gamma_2, i\Gamma_0\Gamma_4, i\Gamma_3\Gamma_1\}
\end{aligned}
$$

- $U$ that transforms $\Gamma_0 \rightarrow \Gamma_1 \rightarrow \Gamma_2 \rightarrow \Gamma_0$, but leaves $\Gamma_3$ and $\Gamma_4$ invariant, cyclically permutes the corresponding bases.
- Since each class can contain only $1$ Clifford generator, maximum number of such classes possible is $2n + 1$.

# Constructing *symmetric* MUBs from Clifford generators

- A simple example in $d = 4$. For $k = 3$ MUBs, the classes are given by

$$\begin{aligned}
\mathcal{C}_0 &= \{\Gamma_0, i\Gamma_1\Gamma_4, i\Gamma_3\Gamma_2\} \\
\mathcal{C}_1 &= \{\Gamma_1, i\Gamma_2\Gamma_4, i\Gamma_3\Gamma_0\} \\
\mathcal{C}_2 &= \{\Gamma_2, i\Gamma_0\Gamma_4, i\Gamma_3\Gamma_1\}
\end{aligned}$$

- $U$ that transforms $\Gamma_0 \rightarrow \Gamma_1 \rightarrow \Gamma_2 \rightarrow \Gamma_0$, but leaves $\Gamma_3$ and $\Gamma_4$ invariant, cyclically permutes the corresponding bases.
- Since each class can contain only $1$ Clifford generator, maximum number of such classes possible is $2n + 1$.
- Imposing the additional constraint that $U : \mathcal{C}_i \rightarrow \mathcal{C}_{i+1}$, we show by an explicit construction that there exist $2 < k \leq 2n + 1$ such classes in dimension $d = 2^n$ whenever
  - $k$ is prime, and
  - $k$ divides $n$ or $k = 2n + 1$.

# New lower bounds on the average min-entropy

- Let $\{\mathcal{B}^{(b)},\ b = 0, ..., L-1\}$ be a set of MUBs in a $d-$dimensional space $\mathbb{H}$. Then, we show,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_{\infty}(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right], \ \ \forall \rho \in \mathbb{H}.$$

# New lower bounds on the average min-entropy

- Let $\{\mathcal{B}^{(b)},\ b = 0, ..., L-1\}$ be a set of MUBs in a $d-$dimensional space $\mathbb{H}$. Then, we show,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_{\infty}(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{L}\left(1+\frac{L-1}{\sqrt{d}}\right)\right],\ \ \forall\rho\in\mathbb{H}.$$

- Corresponds to the Massen-Uffink bound for 2 observables in $d = 2$.

# New lower bounds on the average min-entropy

- Let $\{\mathcal{B}^{(b)},\ b = 0, ..., L-1\}$ be a set of MUBs in a $d-$dimensional space $\mathbb{H}$. Then, we show,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_{\infty}(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right], \ \ \forall \rho \in \mathbb{H}.$$

- Corresponds to the Massen-Uffink bound for 2 observables in $d = 2$. For any less-than-maximal set of MUBs ($2 < L < d$), our bound is stronger than previously obtained bounds.

# New lower bounds on the average min-entropy

- Let $\{\mathcal{B}^{(b)},\ b = 0, ..., L-1\}$ be a set of MUBs in a $d-$dimensional space $\mathbb{H}$. Then, we show,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_{\infty}(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{L}\left(1+\frac{L-1}{\sqrt{d}}\right)\right],\ \ \forall\rho\in\mathbb{H}.$$

- Corresponds to the Massen-Uffink bound for 2 observables in $d = 2$. For any less-than-maximal set of MUBs ($2 < L < d$), our bound is stronger than previously obtained bounds.
- For the complete set of $L = d+1$ MUBs, we obtain a slightly stronger bound,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_{\infty}(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{d}\left(1+\frac{d-1}{\sqrt{L}}\right)\right],\ \ \forall\rho\in\mathbb{H}.$$

# New lower bounds on the average min-entropy

- Let $\{\mathcal{B}^{(b)},\ b = 0, ..., L-1\}$ be a set of MUBs in a $d-$dimensional space $\mathbb{H}$. Then, we show,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_\infty(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{L}\left(1 + \frac{L-1}{\sqrt{d}}\right)\right], \ \forall\rho \in \mathbb{H}.$$

- Corresponds to the Massen-Uffink bound for 2 observables in $d = 2$. For any less-than-maximal set of MUBs ($2 < L < d$), our bound is stronger than previously obtained bounds.
- For the complete set of $L = d + 1$ MUBs, we obtain a slightly stronger bound,

$$\frac{1}{L}\sum_{b=0}^{L-1} H_\infty(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{d}\left(1 + \frac{d-1}{\sqrt{L}}\right)\right], \ \forall\rho \in \mathbb{H}.$$

- An optimal and tight uncertainty relation in some cases, but not always.

# An optimal EUR for 4 MUBs in $d = 4$

- $4$ MUBs in $d = 4$ via our construction:-

$$\begin{aligned}
\mathcal{C}_1 &= \{\Gamma_1, \Gamma_2\Gamma_0, i\Gamma_3\Gamma_4\} \\
\mathcal{C}_2 &= \{\Gamma_2, \Gamma_3\Gamma_0, i\Gamma_4\Gamma_1\} \\
\mathcal{C}_3 &= \{\Gamma_3, \Gamma_4\Gamma_0, i\Gamma_1\Gamma_2\} \\
\mathcal{C}_4 &= \{\Gamma_4, \Gamma_1\Gamma_0, i\Gamma_2\Gamma_3\}
\end{aligned}$$

# An optimal EUR for 4 MUBs in $d = 4$

- $4$ MUBs in $d = 4$ via our construction:-

$$
\begin{aligned}
\mathcal{C}_1 &= \{\Gamma_1, \Gamma_2\Gamma_0, i\Gamma_3\Gamma_4\} \\
\mathcal{C}_2 &= \{\Gamma_2, \Gamma_3\Gamma_0, i\Gamma_4\Gamma_1\} \\
\mathcal{C}_3 &= \{\Gamma_3, \Gamma_4\Gamma_0, i\Gamma_1\Gamma_2\} \\
\mathcal{C}_4 &= \{\Gamma_4, \Gamma_1\Gamma_0, i\Gamma_2\Gamma_3\}
\end{aligned}
$$

- There exists a unitary $U : \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to \Gamma_4 \to \Gamma_1$, leaving $\Gamma_0$ invariant. $U$ cyclically permutes the corresponding bases.

# An optimal EUR for 4 MUBs in $d = 4$

- $4$ MUBs in $d = 4$ via our construction:-

$$\begin{aligned} \mathcal{C}_1 &= \{\Gamma_1, \Gamma_2\Gamma_0, i\Gamma_3\Gamma_4\} \\ \mathcal{C}_2 &= \{\Gamma_2, \Gamma_3\Gamma_0, i\Gamma_4\Gamma_1\} \\ \mathcal{C}_3 &= \{\Gamma_3, \Gamma_4\Gamma_0, i\Gamma_1\Gamma_2\} \\ \mathcal{C}_4 &= \{\Gamma_4, \Gamma_1\Gamma_0, i\Gamma_2\Gamma_3\} \end{aligned}$$

- There exists a unitary $U : \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to \Gamma_4 \to \Gamma_1$, leaving $\Gamma_0$ invariant. $U$ cyclically permutes the corresponding bases.
- The EUR $\frac{1}{4}\sum_{b=1}^{4} H_\infty(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{4}\left(1 + \frac{3}{2}\right)\right]$ is tight.
  The minimum value is attained for a state that is an invariant of $U$.

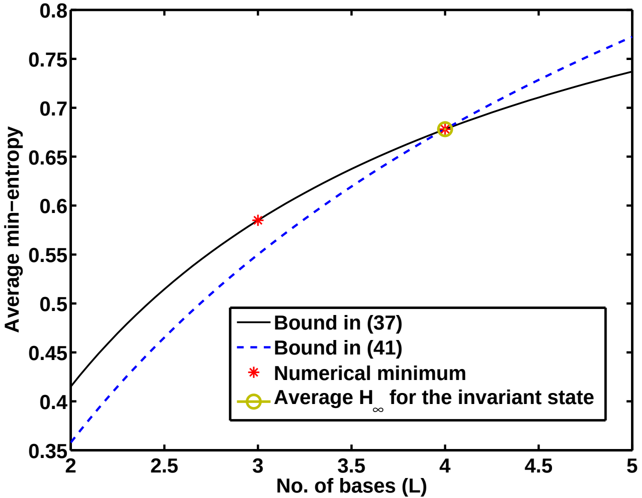
# An optimal EUR for 4 MUBs in $d = 4$

- $4$ MUBs in $d = 4$ via our construction:-

$$\begin{aligned}
\mathcal{C}_1 &= \{\Gamma_1, \Gamma_2\Gamma_0, i\Gamma_3\Gamma_4\} \\
\mathcal{C}_2 &= \{\Gamma_2, \Gamma_3\Gamma_0, i\Gamma_4\Gamma_1\} \\
\mathcal{C}_3 &= \{\Gamma_3, \Gamma_4\Gamma_0, i\Gamma_1\Gamma_2\} \\
\mathcal{C}_4 &= \{\Gamma_4, \Gamma_1\Gamma_0, i\Gamma_2\Gamma_3\}
\end{aligned}$$

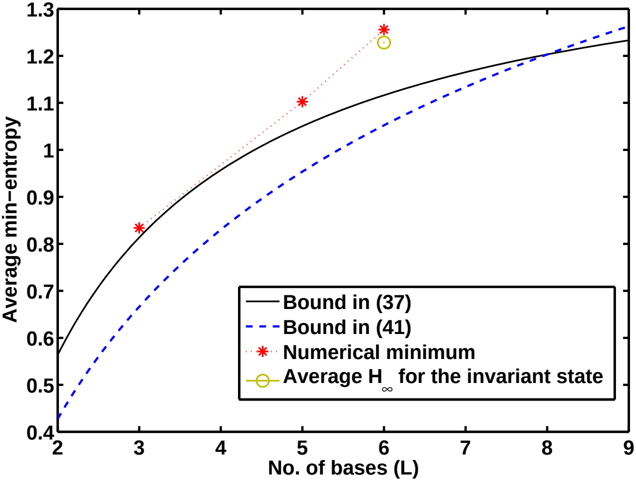
- There exists a unitary $U : \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to \Gamma_4 \to \Gamma_1$, leaving $\Gamma_0$ invariant. $U$ cyclically permutes the corresponding bases.
- The EUR $\frac{1}{4}\sum_{b=1}^{4} H_\infty(\mathcal{B}^{(b)}|\rho) \geq -\log\left[\frac{1}{4}\left(1 + \frac{3}{2}\right)\right]$ is tight. The minimum value is attained for a state that is an invariant of $U$.
- However, for 3 MUBs in $d = 4$, numerical estimates show our bound is not tight.

# EUR bounds for MUBs in $d = 4$




Average min-entropy for different sets of MUBs in dimension $d = 4$.

# EUR bounds for MUBs in $d = 8$




Average min-entropy for different sets of MUBs in dimension $d = 8$.

# Summary of results

- We outline a new construction of symmetric MUBs using the generators of the Clifford algebra, that are cyclically permuted under the action of a unitary transformation $U$.

# Summary of results

- We outline a new construction of symmetric MUBs using the generators of the Clifford algebra, that are cyclically permuted under the action of a unitary transformation $U$.
- We show explicit constructions of $2 \leq L \leq 2n+1$ such MUBs in dimension $d = 2^n$, whenever (a) $L$ is prime and (b) $L|n$ or $L = 2n+1$.

# Summary of results

- We outline a new construction of symmetric MUBs using the generators of the Clifford algebra, that are cyclically permuted under the action of a unitary transformation $U$.
- We show explicit constructions of $2 \leq L \leq 2n+1$ such MUBs in dimension $d = 2^n$, whenever (a) $L$ is prime and (b) $L|n$ or $L = 2n+1$.
- We demonstrate new lower bounds for the average min-entropy for any set of MUBs, stronger than existing lower bounds.

# Summary of results

- We outline a new construction of symmetric MUBs using the generators of the Clifford algebra, that are cyclically permuted under the action of a unitary transformation $U$.
- We show explicit constructions of $2 \leq L \leq 2n+1$ such MUBs in dimension $d = 2^n$, whenever (a) $L$ is prime and (b) $L|n$ or $L = 2n+1$.
- We demonstrate new lower bounds for the average min-entropy for any set of MUBs, stronger than existing lower bounds.
- Using our construction, we can explicitly write down a set of $4$ MUBs in $d = 4$ and show that they satisfy an optimal, tight uncertainty relation. Minimizing state is invariant under the unitary transform.

# Open questions

- Can we extend our construction to other dimensions/number of bases?

# Open questions

- Can we extend our construction to other dimensions/number of bases?
- Is it possible to obtain a condition as to when the uncertainty relation is tight?

# Open questions

- Can we extend our construction to other dimensions/number of bases?
- Is it possible to obtain a condition as to when the uncertainty relation is tight?
- Can we obtain similar lower bounds for the average collision entropy and Shannon entropy?

# Open questions

- Can we extend our construction to other dimensions/number of bases?
- Is it possible to obtain a condition as to when the uncertainty relation is tight?
- Can we obtain similar lower bounds for the average collision entropy and Shannon entropy?
- Can the maximally strong EUR for the $d = 4$ case be used to improve existing cryptographic protocols in a practical way?

Thank You!

# Evaluating the lower bound - I

- Recall, Average min-entropy is

$$\frac{1}{L}\sum_{b=0}^{L-1}\mathcal{H}_{\infty}(\mathcal{B}^{(b)}|\rho) \quad = \quad -\frac{1}{L}\sum_{b}\log \max_{y\in\{0,\ldots,d-1\}}\langle y^{(b)}|\rho|y^{(b)}\rangle$$

# Evaluating the lower bound - I

- Recall, Average min-entropy is

$$\begin{aligned} \frac{1}{L}\sum_{b=0}^{L-1}\mathcal{H}_\infty(\mathcal{B}^{(b)}|\rho) &= -\frac{1}{L}\sum_{b}\log \max_{y\in\{0,\ldots,d-1\}}\langle y^{(b)}|\rho|y^{(b)}\rangle \\ &\geq -\log\frac{1}{L}\sum_{b=0}^{L-1}\max_{y}\langle y^{(b)}|\rho|y^{(b)}\rangle \end{aligned}$$

(Using Jensen's inequality)

# Evaluating the lower bound - I

- Recall, Average min-entropy is

$$\frac{1}{L}\sum_{b=0}^{L-1}\mathcal{H}_\infty(\mathcal{B}^{(b)}|\rho) = -\frac{1}{L}\sum_{b}\log \max_{y\in\{0,\ldots,d-1\}}\langle y^{(b)}|\rho|y^{(b)}\rangle$$
$$\geq -\log\frac{1}{L}\sum_{b=0}^{L-1}\max_{y}\langle y^{(b)}|\rho|y^{(b)}\rangle$$

(Using Jensen's inequality)

- Define $P_{\vec{y}} := \frac{1}{L}\sum_{y^{(k)}}|y^{(k)}\rangle\langle y^{(k)}|$ for $\vec{y} = (y^{(0)}, y^{(1)}, ..., y^{(L-1)})$ denotes a string of basis elements, i.e. $y^{(k)} \in \{0, 1, ..., d-1\}$. Then,

$$\frac{1}{L}\sum_{k=0}^{L-1}\mathcal{H}_\infty(\mathcal{B}^{(k)}||\psi\rangle\langle\psi|) \geq -\log\max_{|\psi\rangle}\mathrm{Tr}(P_{\vec{y}}|\psi\rangle\langle\psi|)$$

# Evaluating the lower bound - II

- Reduces the problem to finding the largest eigenvalue for any operator $P_{\vec{y}}$. Any $\zeta$ such that $P_{\vec{y}} \leq \zeta\mathbb{I}$ for all $\vec{y}$, gives us a lower bound for the avergae min-entropy.

# Evaluating the lower bound - II

- Reduces the problem to finding the largest eigenvalue for any operator $P_{\vec{y}}$. Any $\zeta$ such that $P_{\vec{y}} \leq \zeta \mathbb{I}$ for all $\vec{y}$, gives us a lower bound for the avergae min-entropy.
- For a set of $L$ orthogonal projectors $A_0, A_1, \ldots, A_{L-1}$, the following bound holds[15]:

$$\| \sum_{j=0}^{L-1} A_j \| \leq 1 + (L-1) \max_{0 \leq j < k \leq L-1} \| A_j A_k \|$$

where $\| (.) \|$ denotes the operator norm, or simply the maximum eigenvalue for Hermitian operators.

[15] F. Kittaneh, J. Funct. Anal. **143**, 337 (1997).

# Evaluating the lower bound - II

- Reduces the problem to finding the largest eigenvalue for any operator $P_{\vec{y}}$. Any $\zeta$ such that $P_{\vec{y}} \leq \zeta \mathbb{I}$ for all $\vec{y}$, gives us a lower bound for the avergae min-entropy.
- For a set of $L$ orthogonal projectors $A_0, A_1, \ldots, A_{L-1}$, the following bound holds[15]:

$$\| \sum_{j=0}^{L-1} A_j \| \leq 1 + (L-1) \max_{0 \leq j < k \leq L-1} \| A_j A_k \|$$

where $\| (.) \|$ denotes the operator norm, or simply the maximum eigenvalue for Hermitian operators.

- Applying this result to sums of basis vectors $|y^{(b)}\rangle$, and using $\langle b^{(j)} | b^{(k)} \rangle = e^{i\phi} \frac{1}{\sqrt{d}}$, for any $j \neq k$, gives the desired bound.

[15] F. Kittaneh, J. Funct. Anal. **143**, 337 (1997).

# MUBs from generalized Pauli matrices[17]

- Let $\{|0\rangle, |1\rangle, ..., |p-1\rangle\}$ denote the computational basis in $\mathbb{C}^p$. The generalized Paulis are defined by

$$X_p|k\rangle = |(k+1) \bmod p\rangle \;\; ; \;\; Z_p|k\rangle = \omega^k |k\rangle,$$

where $\omega = e^{2\pi i/p}$.

[17] S.Bandyopadhyay, P.Boykin, V.Roychowdhury and F.Vatan, Algorithmica, **34**(4), 512, 2002

# MUBs from generalized Pauli matrices[17]

- Let $\{|0\rangle, |1\rangle, ..., |p-1\rangle\}$ denote the computational basis in $\mathbb{C}^p$. The generalized Paulis are defined by

$$X_p|k\rangle = |(k+1) \bmod p\rangle \;\; ; \;\; Z_p|k\rangle = \omega^k|k\rangle,$$

  where $\omega = e^{2\pi i/p}$.

- If $d = p^k$ (a prime power), the Hilbert space $\mathbb{H}$ can be written as a tensor product of $k$ copies of $\mathbb{C}^p$.
  Group all $d^2$ possible strings of tensor products of $X_p$ and $Z_p$ into sets $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_{d+1}$ such that, (i) $|\mathcal{C}_i| = d$, (ii) $\mathcal{C}_i \cap \mathcal{C}_j = \{\mathtt{I}\}$ for $i \neq j$ and (iii) all elements of $\mathcal{C}_i$ commute.
  Let $\mathcal{B}^{(i)}$ be the common eigenbasis of the elements of $\mathcal{C}_i$. The bases $\{\mathcal{B}^{(1)}, \mathcal{B}^{(2)}, ..., \mathcal{B}^{(d+1)}\}$ are mutually unbiased.

[17] S.Bandyopadhyay, P.Boykin, V.Roychowdhury and F.Vatan, Algorithmica, **34**(4), 512, 2002

# MUBs from generalized Pauli matrices[17]

- Let $\{|0\rangle, |1\rangle, ..., |p-1\rangle\}$ denote the computational basis in $\mathbb{C}^p$. The generalized Paulis are defined by

$$X_p|k\rangle = |(k+1) \bmod p\rangle \;\; ; \;\; Z_p|k\rangle = \omega^k|k\rangle,$$

  where $\omega = e^{2\pi i/p}$.

- If $d = p^k$ (a prime power), the Hilbert space $\mathbb{H}$ can be written as a tensor product of $k$ copies of $\mathbb{C}^p$.
  Group all $d^2$ possible strings of tensor products of $X_p$ and $Z_p$ into sets $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_{d+1}$ such that, (i) $|\mathcal{C}_i| = d$, (ii) $\mathcal{C}_i \cap \mathcal{C}_j = \{\mathtt{I}\}$ for $i \neq j$ and (iii) all elements of $\mathcal{C}_i$ commute.
  Let $\mathcal{B}^{(i)}$ be the common eigenbasis of the elements of $\mathcal{C}_i$. The bases $\{\mathcal{B}^{(1)}, \mathcal{B}^{(2)}, ..., \mathcal{B}^{(d+1)}\}$ are mutually unbiased.

- **Symmetry property**[16]:- There exists an ordering $\mathcal{B}^{(1)}, ..., \mathcal{B}^{(d+1)}$, and a unitary $U$ such that $U\mathcal{B}^{(j)}U^\dagger = \mathcal{B}^{(j+1)}$, where $U\mathcal{B}^{(d)}U^\dagger = \mathcal{B}^{(1)}$.

[16] W.K.Wootters and D.M.Sussman, 2007, arXiv:0704.1277

[17] S.Bandyopadhyay, P.Boykin, V.Roychowdhury and F.Vatan, Algorithmica, **34**(4), 512, 2002