# *n*-fold unbiased bases: an extension of the MUB condition

Máté Farkas

University of Gdańsk

11 July 2017

*arXiv: 1706.04446*

Jakub Borkała

Edgar Aguilar

Richard Küng

# Mutually unbiased bases (MUBs)

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^d$ and $\{|z_i\rangle\}_{i=1}^d$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^d$ and $\{|z_i\rangle\}_{i=1}^d$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

- Applications:

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^d$ and $\{|z_i\rangle\}_{i=1}^d$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

- Applications:
  - Quantum state determination [Wooters, Fields, 1989]

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^{d}$ and $\{|z_i\rangle\}_{i=1}^{d}$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

- Applications:
  - Quantum state determination [Wooters, Fields, 1989]
  - Information locking [Ballester, Wehner, 2007]

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^{d}$ and $\{|z_i\rangle\}_{i=1}^{d}$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

- Applications:
  - Quantum state determination [Wooters, Fields, 1989]
  - Information locking [Ballester, Wehner, 2007]
  - Entropic uncertainty relations [Maassen, Uffink, 1988]

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^{d}$ and $\{|z_i\rangle\}_{i=1}^{d}$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i, j \in [d]$$

- Applications:
  - Quantum state determination [Wooters, Fields, 1989]
  - Information locking [Ballester, Wehner, 2007]
  - Entropic uncertainty relations [Maassen, Uffink, 1988]
  - Quantum random access codes

# Mutually unbiased bases (MUBs)

- Two bases: $\{|y_i\rangle\}_{i=1}^d$ and $\{|z_i\rangle\}_{i=1}^d$ in $\mathbb{C}^d$ are MUB iff

$$|\langle y_i|z_j\rangle|^2 = \frac{1}{d} \quad \forall i,j \in [d]$$

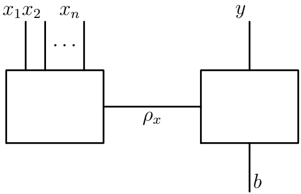
- Applications:
  - Quantum state determination [Wooters, Fields, 1989]
  - Information locking [Ballester, Wehner, 2007]
  - Entropic uncertainty relations [Maassen, Uffink, 1988]
  - Quantum random access codes
    - in $2^d \to 1$ QRAC, the optimal measurements are MUBs

$$\{|y_i\rangle\langle y_i|\}_{i=1}^d \quad \text{and} \quad \{|z_i\rangle\langle z_i|\}_{i=1}^d$$

# Quantum Random Access Codes (QRACs)

# Quantum Random Access Codes (QRACs)

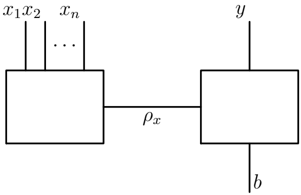
- $n^d \to 1$ QRAC:




  - $x_i \in [d]$, $y \in [n]$, $b \in [d]$ and $\rho_x$ is a $d$-dimensional quantum state
  - The players win if $b = x_y$

# Quantum Random Access Codes (QRACs)

- $n^d \to 1$ QRAC:




  - $x_i \in [d]$, $y \in [n]$, $b \in [d]$ and $\rho_x$ is a $d$-dimensional quantum state
  - The players win if $b = x_y$

- Figure of merit: average success probability:

$$\bar{p} = \frac{1}{nd^n} \sum_{x,y} \mathbb{P}(B = x_y \mid X = x \cap Y = y)$$

# Applications

# Applications

- Foundational issues

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]
  - Quantumness witness

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]
  - Quantumness witness
- Practical use

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]
  - Quantumness witness
- Practical use
  - Quantum finite automata [Ambainis et al., 1999]

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]
  - Quantumness witness
- Practical use
  - Quantum finite automata [Ambainis et al., 1999]
  - Network coding [Hayashi et al., 2006]

# Applications

- Foundational issues
  - Quantum supremacy [Ambainis et al., 2009]
  - Quantumness witness
- Practical use
  - Quantum finite automata [Ambainis et al., 1999]
  - Network coding [Hayashi et al., 2006]
  - Locally decodable codes [Kerenidis, 2004]

# General QRAC strategies ($n^d \to 1$)

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \operatorname{tr}\left( |\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right)$$

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \mathrm{tr}\left( |\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right)$$

- For any choice of measurements the optimal encoding:

$$\left( \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right) |\psi_x\rangle = \lambda_x^{\max} |\psi_x\rangle \implies \bar{p} = \frac{1}{nd^n} \sum_x \lambda_x^{\max}$$

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \mathrm{tr}\left( |\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right)$$

- For any choice of measurements the optimal encoding:

$$\left( \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right) |\psi_x\rangle = \lambda_x^{\max} |\psi_x\rangle \implies \bar{p} = \frac{1}{nd^n} \sum_x \lambda_x^{\max}$$

- Matrix of $\sum_y |y_{x_y}\rangle\langle y_{x_y}|$: Gramian matrix of $\{|y_{x_y}\rangle\}_{y=1}^{n}$

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \text{tr}\left(|\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}|\right)$$

- For any choice of measurements the optimal encoding:

$$\left(\sum_y |y_{x_y}\rangle\langle y_{x_y}|\right)|\psi_x\rangle = \lambda_x^{\max}|\psi_x\rangle \implies \bar{p} = \frac{1}{nd^n}\sum_x \lambda_x^{\max}$$

- Matrix of $\sum_y |y_{x_y}\rangle\langle y_{x_y}|$: Gramian matrix of $\{|y_{x_y}\rangle\}_{y=1}^n$
- For any x: $\lambda^n - n\lambda^{n-1} + c_2\lambda^{n-2} + \cdots + c_n = 0$

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \operatorname{tr} \left( |\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right)$$

- For any choice of measurements the optimal encoding:

$$\left( \sum_y |y_{x_y}\rangle\langle y_{x_y}| \right) |\psi_x\rangle = \lambda_x^{\max} |\psi_x\rangle \implies \bar{p} = \frac{1}{nd^n} \sum_x \lambda_x^{\max}$$

- Matrix of $\sum_y |y_{x_y}\rangle\langle y_{x_y}|$: Gramian matrix of $\{|y_{x_y}\rangle\}_{y=1}^n$
- For any x: $\lambda^n - n\lambda^{n-1} + c_2\lambda^{n-2} + \cdots + c_n = 0$
- $\lambda_x^{\max}$ is a concave function of every $(c_k)_x$

# General QRAC strategies ($n^d \to 1$)

- Pure states and projective measurements are enough for optimality

$$\bar{p} = \frac{1}{nd^n} \sum_x \mathrm{tr}\left(|\psi_x\rangle\langle\psi_x| \sum_y |y_{x_y}\rangle\langle y_{x_y}|\right)$$

- For any choice of measurements the optimal encoding:

$$\left(\sum_y |y_{x_y}\rangle\langle y_{x_y}|\right)|\psi_x\rangle = \lambda_x^{\max}|\psi_x\rangle \implies \bar{p} = \frac{1}{nd^n} \sum_x \lambda_x^{\max}$$

- Matrix of $\sum_y |y_{x_y}\rangle\langle y_{x_y}|$: Gramian matrix of $\{|y_{x_y}\rangle\}_{y=1}^n$
- For any x: $\lambda^n - n\lambda^{n-1} + c_2\lambda^{n-2} + \cdots + c_n = 0$
- $\lambda_x^{\max}$ is a concave function of every $(c_k)_x$
- $\implies \bar{p}$ is a Schur-concave function of every $\mathbf{c}_k$

# Optimal $n^d \to 1$ QRAC strategy

# Optimal $n^d \to 1$ QRAC strategy

- Maximal average success probability: uniform $(c_k)_x$

# Optimal $n^d \to 1$ QRAC strategy

- Maximal average success probability: uniform $(c_k)_x$

$$\sum_{\substack{\sigma \in S_n \\ \sigma:\ n\text{-cycle}}} \prod_{y=1}^{n} \left\langle y_{x_y} \middle| \sigma(y)_{x_{\sigma(y)}} \right\rangle = \frac{(n-1)!}{d^{n-1}} \quad \forall x_1, \ldots, x_n \in [d]$$

$n$UB condition

# Optimal $n^d \to 1$ QRAC strategy

- Maximal average success probability: uniform $(c_k)_x$

$$\sum_{\substack{\sigma \in S_n \\ \sigma:\ n\text{-cycle}}} \prod_{y=1}^{n} \langle y_{x_y} | \sigma(y)_{x_{\sigma(y)}} \rangle = \frac{(n-1)!}{d^{n-1}} \quad \forall x_1, \ldots, x_n \in [d]$$

*n*UB condition

- Example: $n = 3$, 3UB-condition:

$$\langle y_{x_y} | z_{x_z} \rangle \langle z_{x_z} | a_{x_a} \rangle \langle a_{x_a} | y_{x_y} \rangle + \langle y_{x_y} | a_{x_a} \rangle \langle a_{x_a} | z_{x_z} \rangle \langle z_{x_z} | y_{x_y} \rangle = \frac{2}{d^2} \quad \forall x_y, x_z, x_a \in [d]$$

# Existence of nUBs

# Existence of nUBs

- $n\mathrm{UB} \implies (n-1)\mathrm{UB}$

# Existence of nUBs

- $n\text{UB} \implies (n-1)\text{UB}$
  - This means that any $n$UBs must consist of MUBs

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB
- $d=3,4,5$: no 3UBs exist $\implies$ no $n$UBs for $n \geq 3$

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB
- $d=3,4,5$: no 3UBs exist $\implies$ no $n$UBs for $n \geq 3$
- $d \geq 6$: unclear if $n$UBs exist for $n \geq 3$

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB
- $d=3,4,5$: no 3UBs exist $\implies$ no $n$UBs for $n \geq 3$
- $d \geq 6$: unclear if $n$UBs exist for $n \geq 3$
- Probabilistic arguments:

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB
- $d=3,4,5$: no 3UBs exist $\implies$ no $n$UBs for $n \geq 3$
- $d \geq 6$: unclear if $n$UBs exist for $n \geq 3$
- Probabilistic arguments:
  - For $n$ random states, $\mathbb{E}\left[\sum_{\substack{\sigma \in S_n \\ \sigma:\ n\text{-cycle}}} \prod_{y=1}^{n} \langle y|\sigma(y)\rangle\right] = \frac{(n-1)!}{d^{n-1}}$

# Existence of nUBs

- $n$UB $\implies$ $(n-1)$UB
  - This means that any $n$UBs must consist of MUBs
- $d+1$ $d$UBs in dimension $d$ $\implies$ $(d+1)$UB
- $d=2$: any 3 MUBs form a 3UB
- $d=3,4,5$: no 3UBs exist $\implies$ no $n$UBs for $n \geq 3$
- $d \geq 6$: unclear if $n$UBs exist for $n \geq 3$
- Probabilistic arguments:
  - For $n$ random states, $\mathbb{E}\left[\sum_{\substack{\sigma \in S_n \\ \sigma:\ n\text{-cycle}}} \prod_{y=1}^{n} \langle y|\sigma(y)\rangle\right] = \frac{(n-1)!}{d^{n-1}}$
  - Lévy's lemma: concentration of measure on $S^{2d-1}$ $\implies$ functions admit their expectation value with high probability, when the dimension is high

# Applications of nUBs

# Applications of nUBs

- If they exist

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations
    - Information locking

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations
    - Information locking
- If they don't exist

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations
    - Information locking
- If they don't exist
  - Close-to-tight upper bound on QRAC strategies (close to the success probability of MUB strategies)

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations
    - Information locking

| | | classical | MUB | $n$UB |
|---|---|---|---|---|
| $d = 3$ | $n = 3$ | 0.6296 | 0.6971 | 0.6989 |
| $d = 4$ | $n = 3$ | 0.5625 | 0.6443 | 0.6466 |
| | $n = 4$ | 0.5313 | 0.5779 | 0.5872 |
| $d = 5$ | $n = 3$ | 0.5200 | 0.6109 | 0.6114 |
| | $n = 4$ | 0.4880 | 0.5430 | 0.5477 |

- If they don't exist
  - Close-to-tight upper bound on QRAC strategies (close to the success probability of MUB strategies)

# Applications of nUBs

- If they exist
  - Tight upper bound on QRAC strategies
  - Potential tight bounds on other tasks
    - Entropic uncertainty relations
    - Information locking

| | | classical | MUB | $n$UB |
|---|---|---|---|---|
| $d = 3$ | $n = 3$ | 0.6296 | 0.6971 | 0.6989 |
| $d = 4$ | $n = 3$ | 0.5625 | 0.6443 | 0.6466 |
| | $n = 4$ | 0.5313 | 0.5779 | 0.5872 |
| $d = 5$ | $n = 3$ | 0.5200 | 0.6109 | 0.6114 |
| | $n = 4$ | 0.4880 | 0.5430 | 0.5477 |

- If they don't exist
  - Close-to-tight upper bound on QRAC strategies (close to the success probability of MUB strategies)
  - Potential close-to-tight upper bounds on other tasks

# Foundational questions

# Foundational questions

- Quantum theory: only second order genuine interference

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only
- Nature: higher order interference?

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only
- Nature: higher order interference?
  - Experimental bounds: $\sim 10^{-2}$ times weaker than second order

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only
- Nature: higher order interference?
  - Experimental bounds: $\sim 10^{-2}$ times weaker than second order
  - Density Cubes [Dakić et al., 2014]: quantum states as tensors, e.g. $\rho_{ijk}$ for third order genuine interference

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only
- Nature: higher order interference?
  - Experimental bounds: $\sim 10^{-2}$ times weaker than second order
  - Density Cubes [Dakić et al., 2014]: quantum states as tensors, e.g. $\rho_{ijk}$ for third order genuine interference
    - Maybe in this theory, there always exist some analogue bases to 3UBs

# Foundational questions

- Quantum theory: only second order genuine interference
  - Two-slit pattern is not a sum of one-slit patterns
  - More-than-two-slit pattern is a sum of two- and one-slit patterns
  - $\rho_{ij}$ expresses correlations between two levels only
- Nature: higher order interference?
  - Experimental bounds: $\sim 10^{-2}$ times weaker than second order
  - Density Cubes [Dakić et al., 2014]: quantum states as tensors, e.g. $\rho_{ijk}$ for third order genuine interference
    - Maybe in this theory, there always exist some analogue bases to 3UBs
  - Quartic Quantum Theory [Życzkowski, 2008]

# Summary

# Summary

- New, extended MUB criterion

# Summary

- New, extended MUB criterion
- Practical implications

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies
  - Entropic uncertainty relations, state discrimination, information locking

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies
  - Entropic uncertainty relations, state discrimination, information locking
- Foundational implications

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies
  - Entropic uncertainty relations, state discrimination, information locking
- Foundational implications
  - Existence, geometry of quantum states

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies
  - Entropic uncertainty relations, state discrimination, information locking
- Foundational implications
  - Existence, geometry of quantum states
  - The question of genuine third order interference

# Summary

- New, extended MUB criterion
- Practical implications
  - QRAC strategies
  - Entropic uncertainty relations, state discrimination, information locking
- Foundational implications
  - Existence, geometry of quantum states
  - The question of genuine third order interference

Thank you for your attention!

*arXiv: 1706.04446*