Title: A magic bullet for numerous quantum-informational tasks

Date: Sep 17, 2014 04:00 PM

URL: http://pirsa.org/14090006

Abstract: A class of d-level quantum states called "magic states", whose initial purpose was to enable universal fault-tolerant computation within error-correcting codes, has a surprisingly broad range of applications. We begin by describing their structure with respect to the Clifford hierarchy, and in terms of convex geometry before proceeding to their applications. They appear to have some relevance to the search for SIC-POVMs in certain prime dimensions. A version of the CHSH non-local game, using a d-ary alphabet and Pauli measurements, has an optimal quantum strategy using magic states. Finally, magic states exhibit nice symmetries (balanced, minimum uncertainty) with respect to Pauli measurements and consequently could find applications in areas like cryptography.

A magic bullet for numerous quantum-informational tasks

Mark Howard

Sept 2014

Includes prior work with Wim van Dam, Jiri Vala,
recent results with Ingemar Bengtsson, Kate Blanchfield, Earl Campbell
and forthcoming work in preparation

Other Dimensions?

Multiple qubits are very well studied

Other Dimensions?

Multiple qubits are very well studied

Q: What can we gain by looking at d-level systems (qudits) instead?

A: Probably not anything too dramatic, however..

Practical: Robustness to noise in quantum computation, key distribution

Increased efficiency for ancilla-assisted fault-tolerance schemes

T. Durt, N. J. Cerf, N. Gisin, and M. Zukowski
"Security of quantum key distribution with entangled qutrits"
Phys. Rev. A 67, 012311 (2003)

Earl T. Campbell
"Enhanced fault-tolerant quantum computing in d-level systems"
arXiv:1406.3055 (2014)

Other Dimensions?

Multiple qubits are very well studied

Q: What can we gain by looking at d-level systems (qudits) instead?

A: Probably not anything too dramatic, however..

Practical: Robustness to noise in quantum computation, key distribution

Increased efficiency for ancilla-assisted fault-tolerance schemes

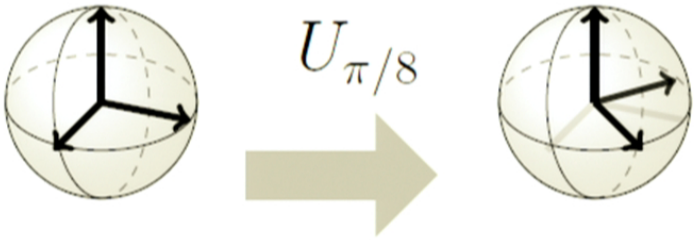
Fundamental: New phenomena: single-particle KS contextuality with qutrit, (im)possibility of state-independent contextuality via Pauli measurements for (odd) even Hilbert space dimension

(Im)possibility of certain geometrical structures e.g., Mutually Unbiased Bases. Structure of state space is not a ball!

Today: I will discuss a useful & interesting family of states and gates

The $U_{\pi/8}$ gate and its uses

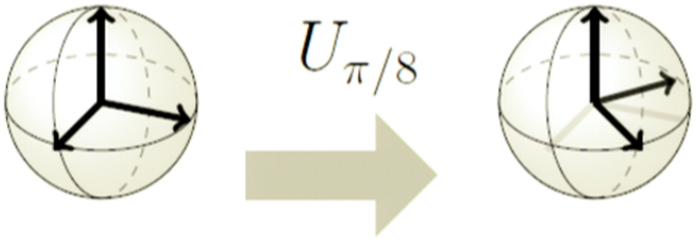
- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$



$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury and F. Vatan.
A new universal and fault-tolerant quantum basis
Information Processing Letters 75, 3 pp. 101–107, (2000).

The $U_{\pi/8}$ gate and its uses

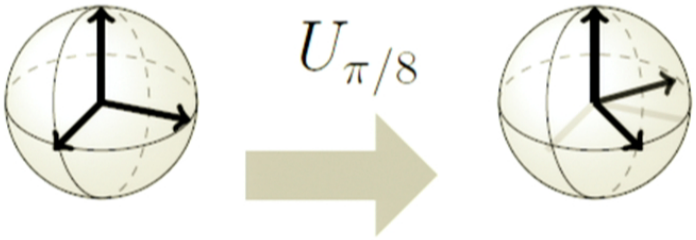


- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$
- Teleportation-based UQC

$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

D. Gottesman and I. L. Chuang,
Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations
Nature 402, 6760 pp. 390–393, (1999).

The $U_{\pi/8}$ gate and its uses

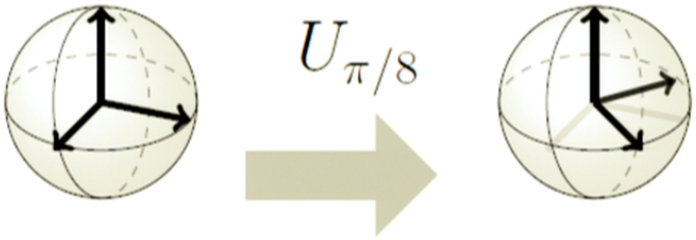


- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$
- Teleportation-based UQC
- Transversal for R-M codes

$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

B. Zeng, H. Chung, A. Cross and I. Chuang,
Local unitary versus local Clifford equivalence of stabilizer and graph states,
Phys. Rev. A 75, 032325 (2007).

The $U_{\pi/8}$ gate and its uses

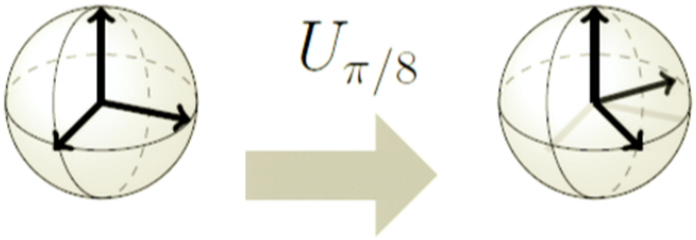


$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$
- Teleportation-based UQC
- Transversal for R-M codes
- Topological Protection (3D)
- Secure assisted UQC

A. M. Childs,
Secure assisted quantum computation
Quantum Info. Comput.5, pp. 456, (2005).

The $U_{\pi/8}$ gate and its uses



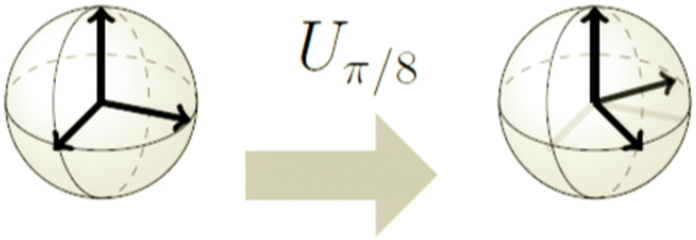
$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$
- Teleportation-based UQC
- Transversal for R-M codes
- Topological Protection (3D)
- Secure assisted UQC

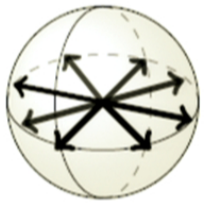
- Measurement-based UQC with graph states

M. Silva, V. Danos, E. Kashefi and H. Ollivier,
A direct approach to fault-tolerance in measurement-based quantum computation via teleportation
New Journal of Physics 9, 6 pp. 192, (2007).

The $U_{\pi/8}$ gate and its uses



$$U_{\pi/8} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

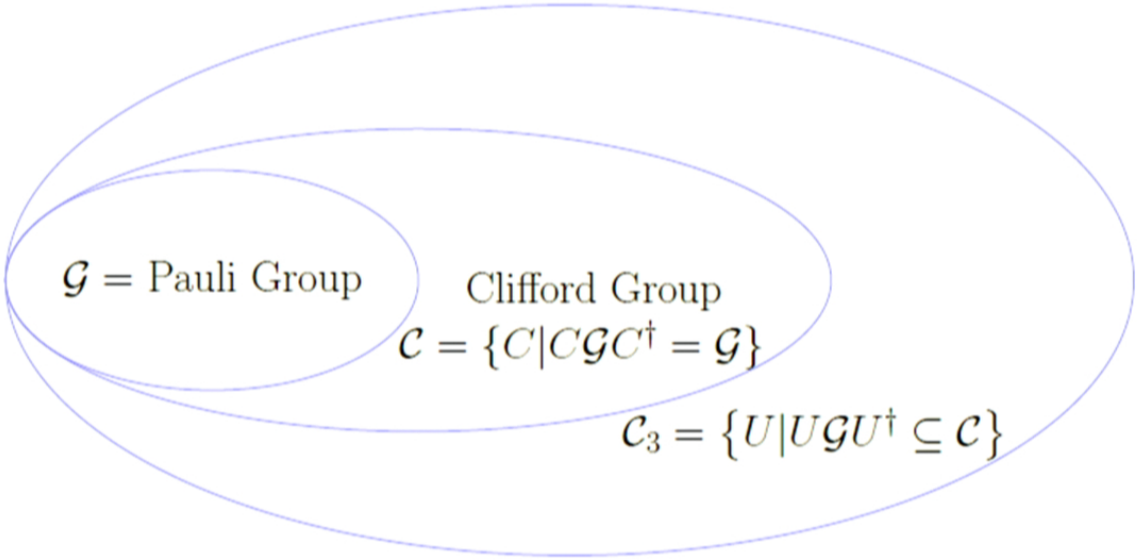


- $\mathrm{UQC} = \langle \text{Cliffords}, U_{\pi/8} \rangle$
  $\mathrm{UQC} \neq \langle \text{Cliffords} \rangle$
- Teleportation-based UQC
- Transversal for R-M codes
- Topological Protection (3D)
- Secure assisted UQC

- Measurement-based UQC with graph states
- Optimal CHSH game with $(|00\rangle + |11\rangle)/\sqrt{2}$
- Blind UQC

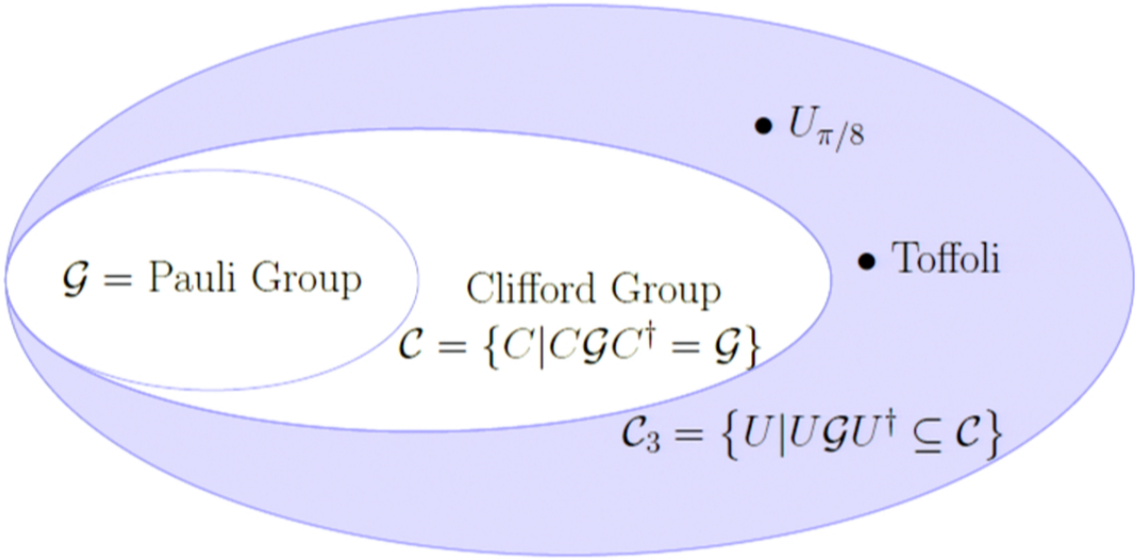
A. Broadbent, J. Fitzsimons and E. Kashefi,
Universal blind quantum computation,
Annual IEEE Symposium on Foundations of Computer Science, pp. 517 –526, (2009).

Structure of Pauli/Clifford groups



D. Gottesman and I. L. Chuang,
Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations
Nature 402, 6760 pp. 390–393, (1999).

Structure of Pauli/Clifford groups



We will focus on **single, p-level** particles

- Generalized σ_x/σ_z : $X|j\rangle = |j+1 \bmod p\rangle \quad Z|j\rangle = \omega^j|j\rangle \quad (\omega = e^{2\pi i/p})$
- Displacement operators, $D_{(x,z)} = \omega^{2^{-1}xz} X^x Z^z$, form Pauli group $\mathcal{G}$

D. Gottesman and I. L. Chuang,
Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations
Nature 402, 6760 pp. 390–393, (1999).

Magic gates M are generalized $U_{\pi/8}$ gates

Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

Magic gates M are generalized $U_{\pi/8}$ gates

Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

$$MXM^\dagger = \omega^\epsilon C_{\left(\left[\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}1\\ z\end{smallmatrix}\right]\right)}$$

A: p^3 gates $M(z, \gamma, \epsilon)$ varying over $z, \gamma, \epsilon \in \mathbb{Z}_p$.
$p^2(p-1)$ non-Clifford M varying over $z, \epsilon \in \mathbb{Z}_p$, $\gamma \in \mathbb{Z}_p^*$.

$$\text{These } M \text{ form an abelian group: } = \begin{cases} \mathbb{Z}_8 & p = 2 \\ \mathbb{Z}_9 \times \mathbb{Z}_3 & p = 3 \\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p & p > 3 \end{cases}$$

Magic gates M are generalized $U_{\pi/8}$ gates

Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

$$MXM^\dagger = \omega^\epsilon C_{\left(\left[\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}1\\ z\end{smallmatrix}\right]\right)}$$

A: p^3 gates $M(z, \gamma, \epsilon)$ varying over $z, \gamma, \epsilon \in \mathbb{Z}_p$.
$p^2(p-1)$ non-Clifford M varying over $z, \epsilon \in \mathbb{Z}_p$, $\gamma \in \mathbb{Z}_p^*$.

$$\text{These } M \text{ form an abelian group: } = \begin{cases} \mathbb{Z}_8 & p = 2 \\ \mathbb{Z}_9 \times \mathbb{Z}_3 & p = 3 \\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p & p > 3 \end{cases}$$

Magic gates M are generalized $U_{\pi/8}$ gates

Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

$$MXM^\dagger = \omega^\epsilon C_{\left(\left[\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}1\\ z\end{smallmatrix}\right]\right)}$$

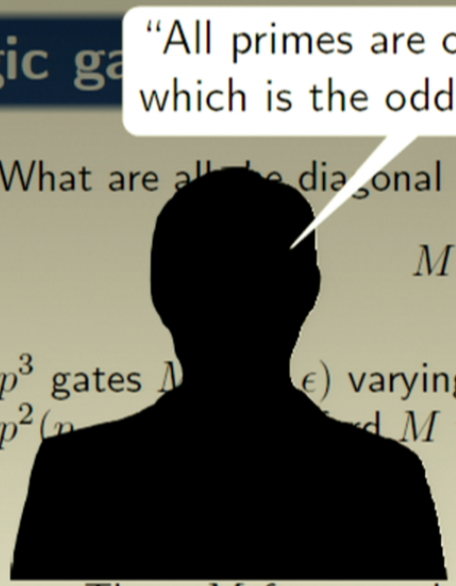
A: p^3 gates $M(z,\gamma,\epsilon)$ varying over $z,\gamma,\epsilon \in \mathbb{Z}_p$.
$p^2(p-1)$ non-Clifford M varying over $z,\epsilon \in \mathbb{Z}_p$, $\gamma \in \mathbb{Z}_p^*$.

$$\text{These } M \text{ form an abelian group: } = \begin{cases} \mathbb{Z}_8 & p=2 \\ \mathbb{Z}_9 \times \mathbb{Z}_3 & p=3 \\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p & p>3 \end{cases}$$

An more convenient way of parameterizing M is via **cubic polynomials**

$$M_{a,b,c} = \begin{cases} diag(1, i^{a+2b+4c}) & p=2 \\ diag(1, \xi^{2a+6b+3c}, \xi^{a+6b+6c}) & p=3 \quad (\xi = e^{2\pi i/9}) \\ \sum_k \omega^{ak^3+bk^2+ck} |k\rangle\langle k| & p>3 \quad (\omega = e^{2\pi i/p}) \end{cases}$$

Magic ga… $\pi/8$ gates



Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

$$MXM^\dagger = \omega^\epsilon C_{\left(\left[\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}1\\ z\end{smallmatrix}\right]\right)}$$

A: p^3 gates M (ϵ) varying over $z, \gamma, \epsilon \in \mathbb{Z}_p$.
p^2 (p … d M varying over $z, \epsilon \in \mathbb{Z}_p$, $\gamma \in \mathbb{Z}_p^*$.

These M form an abelian group: $= \begin{cases} \mathbb{Z}_8 & p = 2 \\ \mathbb{Z}_9 \times \mathbb{Z}_3 & p = 3 \\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p & p > 3 \end{cases}$

An more convenient way of parameterizing M is via **cubic polynomials**

$$M_{a,b,c} = \begin{cases} diag(1, i^{a+2b+4c}) & p = 2 \\ diag(1, \xi^{2a+6b+3c}, \xi^{a+6b+6c}) & p = 3 \quad (\xi = e^{2\pi i/9}) \\ \sum_k \omega^{ak^3+bk^2+ck} |k\rangle\langle k| & p > 3 \quad (\omega = e^{2\pi i/p}) \end{cases}$$

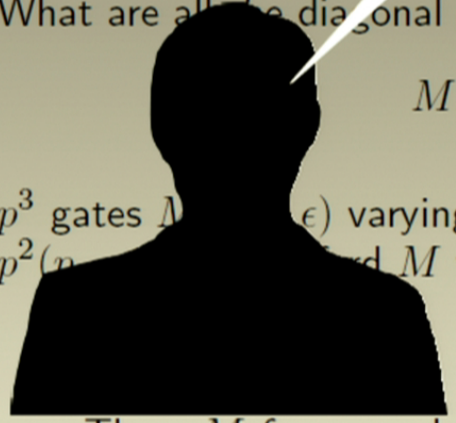
Magic ga… $\pi/8$ gates

"All primes are odd except two, which is the oddest prime of all!"

Q: What are all the diagonal gates $M \in SU(p)$ from third level of hierarchy?

$$MXM^\dagger = \omega^\epsilon C_{\left(\left[\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}1\\ z\end{smallmatrix}\right]\right)}$$

A: p^3 gates M (ϵ) varying over $z, \gamma, \epsilon \in \mathbb{Z}_p$.
p^2 (p … and M var…



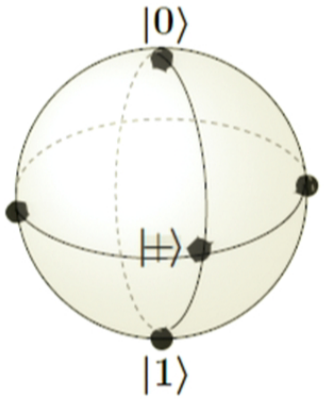
Perhaps, in Quantum Information, three is the **second oddest** prime!

These M form an abelian group: $= \begin{cases} \mathbb{Z}_8 & p = 2 \\ \mathbb{Z}_9 \times \mathbb{Z}_3 & p = 3 \\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p & p > 3 \end{cases}$

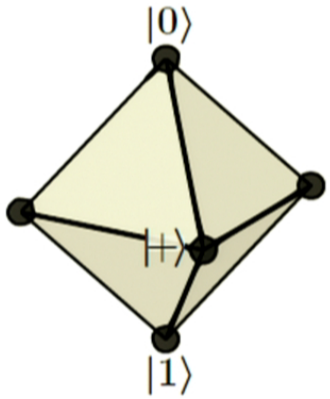
An more convenient way of parameterizing M is via **cubic polynomials**

$$M_{a,b,c} = \begin{cases} diag(1, i^{a+2b+4c}) & p = 2 \\ diag(1, \xi^{2a+6b+3c}, \xi^{a+6b+6c}) & p = 3 \quad (\xi = e^{2\pi i/9}) \\ \sum_k \omega^{ak^3+bk^2+ck} |k\rangle\langle k| & p > 3 \quad (\omega = e^{2\pi i/p}) \end{cases}$$

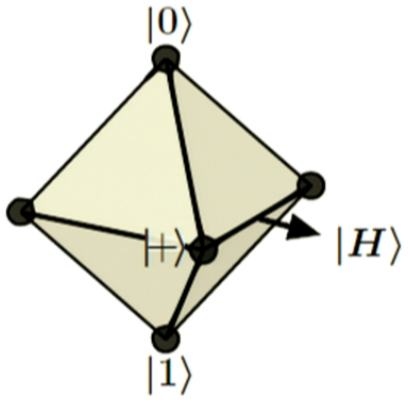
Geometry: Magic States and Gates



Geometry: Magic States and Gates



Geometry: Magic States and Gates



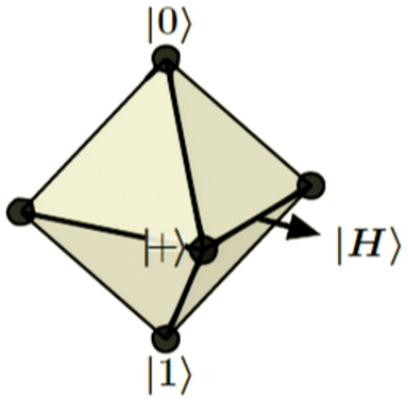
$$|H\rangle = U_{\pi/8}|+\rangle$$

$$|H\rangle\langle H| = \frac{1}{2}\left(\mathbb{I} + \frac{\sigma_x + \sigma_y}{\sqrt{2}}\right)$$

$$|f_{a,b,c}\rangle = M_{a,b,c}|+\rangle$$

$$|f_{a,b,c}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + i^{a+2b+4c}|1\rangle) & p = 2 \\ \frac{1}{\sqrt{3}}(|0\rangle + \xi^{2a+6b+3c}|1\rangle + \xi^{a+6b+6c}|2\rangle) & p = 3 \\ \frac{1}{\sqrt{p}}\sum_k \omega^{ak^3+bk^2+ck}|k\rangle & p > 3 \end{cases}$$

Geometry: Magic States and Gates



$$|H\rangle = U_{\pi/8}|+\rangle$$

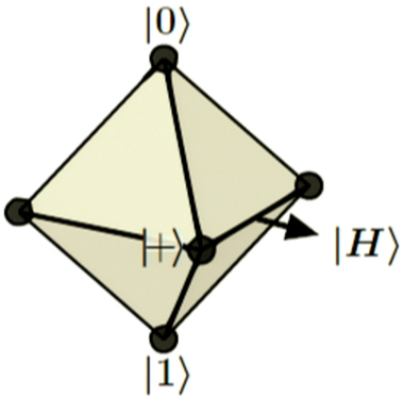
$$|H\rangle\langle H| = \frac{1}{2}\left(\mathbb{I} + \frac{\sigma_x + \sigma_y}{\sqrt{2}}\right)$$

$$|f_{a,b,c}\rangle = M_{a,b,c}|+\rangle$$

$$|f_{a,b,c}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + i^{a+2b+4c}|1\rangle) & p = 2 \\ \frac{1}{\sqrt{3}}(|0\rangle + \xi^{2a+6b+3c}|1\rangle + \xi^{a+6b+6c}|2\rangle) & p = 3 \\ \frac{1}{\sqrt{p}}\sum_k \omega^{ak^3+bk^2+ck}|k\rangle & p > 3 \end{cases}$$

- $|f_{a,b,c}\rangle$ are eigenvectors of Clifford gates
- $|f_{a,b,c}\rangle$ seem to be the most non-stabilizer states in the equatorial plane
- $M_{a,b,c}$ seem to be the most non-Clifford unitaries (Jamiołkowski)

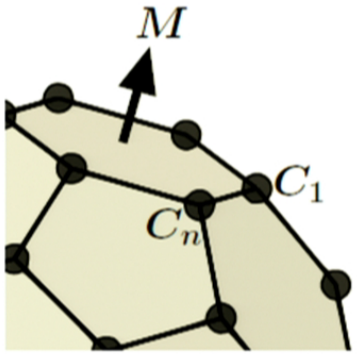
Geometry: Magic States and Gates



$$|H\rangle = U_{\pi/8}|+\rangle$$

$$|H\rangle\langle H| = \frac{1}{2}\left(\mathbb{I} + \frac{\sigma_x + \sigma_y}{\sqrt{2}}\right)$$

$$|f_{a,b,c}\rangle = M_{a,b,c}|+\rangle$$



$$|f_{a,b,c}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + i^{a+2b+4c}|1\rangle) & p = 2 \\ \frac{1}{\sqrt{3}}(|0\rangle + \xi^{2a+6b+3c}|1\rangle + \xi^{a+6b+6c}|2\rangle) & p = 3 \\ \frac{1}{\sqrt{p}}\sum_k \omega^{ak^3+bk^2+ck}|k\rangle & p > 3 \end{cases}$$

- $|f_{a,b,c}\rangle$ are eigenvectors of Clifford gates
- $|f_{a,b,c}\rangle$ seem to be the most non-stabilizer states in the equatorial plane
- $M_{a,b,c}$ seem to be the most non-Clifford unitaries (Jamiołkowski)

(WH-covariant) SIC-POVMs

In dimension N : $\{|\psi_j\rangle,\ j=1,\ldots,N^2\}$
$=\{D_{(x,z)}|\psi_{\text{fid}}\rangle,\ x,z\in\mathbb{Z}_N\}$

where $D_{(x,z)}=\omega^{2^{-1}}X^xZ^z$, satisfying

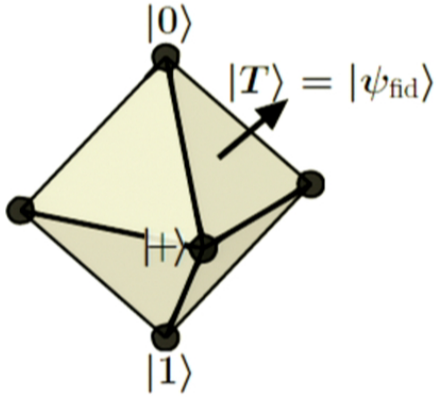
$$\sum_{j=1}^{N^2}|\psi_j\rangle\langle\psi_j|=N\mathbb{I}_N \quad \text{and} \quad |\langle\psi_j|\psi_{k\neq j}\rangle|^2=\frac{1}{N+1}$$

(WH-covariant) SIC-POVMs

In dimension N : $\{|\psi_j\rangle,\ j=1,\ldots,N^2\}$
$=\{D_{(x,z)}|\psi_{\text{fid}}\rangle,\ x,z\in\mathbb{Z}_N\}$

where $D_{(x,z)}=\omega^{2^{-1}}X^xZ^z$, satisfying

$$\sum_{j=1}^{N^2}|\psi_j\rangle\langle\psi_j|=N\mathbb{I}_N \quad \text{and} \quad |\langle\psi_j|\psi_{k\neq j}\rangle|^2=\frac{1}{N+1}$$



(WH-covariant) SIC-POVMs

In dimension N : $\{|\psi_j\rangle,\ j=1,\dots,N^2\}$
$=\{D_{(x,z)}|\psi_{\text{fid}}\rangle,\ x,z\in\mathbb{Z}_N\}$

where $D_{(x,z)}=\omega^{2^{-1}}X^xZ^z$, satisfying

$$\sum_{j=1}^{N^2}|\psi_j\rangle\langle\psi_j|=N\mathbb{I}_N \quad\text{and}\quad |\langle\psi_j|\psi_{k\neq j}\rangle|^2=\frac{1}{N+1}$$

$p=7$

$$\begin{pmatrix}
\frac{-1+\sqrt{2}}{4\sqrt{7}}+\frac{1}{28}\left(5-2\sqrt{2}\right. \\
\frac{1}{28}\left(6-\sqrt{2}\right)\cos^2\left(\frac{\pi}{7}\right)+ \\
\left(\frac{-1+\sqrt{2}}{4\sqrt{7}}-\frac{1}{28}\right)\cos^2\left(\frac{\pi}{7}\right)+\left(\frac{1-}{8}\right. \\
\left(\frac{1-\sqrt{2}}{4\sqrt{7}}+\frac{1}{28}\left(-5+\sqrt{2}\right)\right)\cos^2 \\
\left(\frac{1-\sqrt{2}}{4\sqrt{7}}+\frac{1}{28}\left(-5+\sqrt{2}\right)\right)\cos^2 \\
\left(\frac{-1+\sqrt{2}}{4\sqrt{7}}-\frac{1}{28}\right)\cos^2\left(\frac{\pi}{7}\right)+\left(\frac{1-}{8}\right. \\
\frac{1}{28}\left(6-\sqrt{2}\right)\cos^2\left(\frac{\pi}{7}\right)+\left(\frac{-1+\sqrt{2}}{8\sqrt{7}}-\frac{1}{56}\right.
\end{pmatrix}$$

Zauner conjecture:

For all Hilbert space dimension N, $|\psi_{\text{fid}}\rangle$ can be found in the largest eigenspace of an order 3 Clifford unitary $C_{\left(\left[\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right]\middle|\left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right)}$ s.t. $C^3=\mathbb{I}$

	$N=3k$	$N=3k+1$	$N=3k+2$
1	$k+1$	$k+1$	$k+1$
$e^{2\pi i/3}$	k	k	$k+1$
$e^{4\pi i/3}$	$k-1$	k	k

(WH-covariant) SIC-POVMs & Magic states

Connecting SICs & MUBs

D. M. Appleby,
"SIC-POVMs and MUBs: Geometrical relationships in prime dimensions"
Foundations of probability and physics 5, 223232." AIP Conf. Proc. Vol. 1101. (2009)

- For $p > 3$, magic states coincide with second most famous MUB construction – **the Alltop MUB construction**
- For fixed $a \in \mathbb{Z}_p$, $|\langle f_{a,b,c}|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1-\delta_{b,b'})/\sqrt{p}$
- Complete set $p+1$ MUBs $= \{|j\rangle, j \in \mathbb{Z}_p\} \cup \{|f_{a,b,c}\rangle, b, c \in \mathbb{Z}_p\}$
  ($a = 0$: Standard/Ivanovic/Stabilizer, $a \neq 0$: Alltop)

$\Rightarrow$ Standard & Alltop MUBs are unitarily equivalent under $M_{a,*,*}$

(WH-covariant) SIC-POVMs & Magic states

Connecting SICs & MUBs

D. M. Appleby,
"SIC-POVMs and MUBs: Geometrical relationships in prime dimensions"
Foundations of probability and physics 5, 223232." AIP Conf. Proc. Vol. 1101. (2009)

- For $p > 3$, magic states coincide with second most famous MUB construction – **the Alltop MUB construction**
- For fixed $a \in \mathbb{Z}_p$, $|\langle f_{a,b,c}|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1-\delta_{b,b'})/\sqrt{p}$
- Complete set $p+1$ MUBs $= \{|j\rangle, j \in \mathbb{Z}_p\} \cup \{|f_{a,b,c}\rangle, b, c \in \mathbb{Z}_p\}$
  ($a = 0$: Standard/Ivanovic/Stabilizer, $a \neq 0$: Alltop)

$\Rightarrow$ Standard & Alltop MUBs are unitarily equivalent under $M_{a,*,*}$

(WH-covariant) SIC-POVMs & Magic states

Connecting SICs & MUBs

D. M. Appleby,
"SIC-POVMs and MUBs: Geometrical relationships in prime dimensions"
Foundations of probability and physics 5, 223232." AIP Conf. Proc. Vol. 1101. (2009)

- For $p > 3$, magic states coincide with second most famous MUB construction – **the Alltop MUB construction**
- For fixed $a \in \mathbb{Z}_p$, $|\langle f_{a,b,c}|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1-\delta_{b,b'})/\sqrt{p}$
- Complete set $p+1$ MUBs $= \{|j\rangle, j \in \mathbb{Z}_p\} \cup \{|f_{a,b,c}\rangle, b, c \in \mathbb{Z}_p\}$
  ($a = 0$: Standard/Ivanovic/Stabilizer, $a \neq 0$: Alltop)

$\Rightarrow$ Standard & Alltop MUBs are unitarily equivalent under $M_{a,*,*}$

Orbits:

- Standard MUB is an orbit of Clifford group
- For fixed $a \neq 0$, Alltop MUB is an orbit of WH group
- The complete set of $(p+1)p^2(p-1)$ magic states in dim p forms:

(i) A single orbit under Cliffords when $p = 2 \bmod 3$

(ii) Three distinct orbits under Cliffords when $p = 1 \bmod 3$

(WH-covariant) SIC-POVMs & Magic states

Connecting SICs & MUBs

D. M. Appleby,
"SIC-POVMs and MUBs: Geometrical relationships in prime dimensions"
Foundations of probability and physics 5, 223232." AIP Conf. Proc. Vol. 1101. (2009)

- For $p > 3$, magic states coincide with second most famous MUB construction – **the Alltop MUB construction**
- For fixed $a \in \mathbb{Z}_p$, $|\langle f_{a,b,c}|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1-\delta_{b,b'})/\sqrt{p}$
- Complete set $p+1$ MUBs $= \{|j\rangle, j \in \mathbb{Z}_p\} \cup \{|f_{a,b,c}\rangle, b, c \in \mathbb{Z}_p\}$
  ($a = 0$: Standard/Ivanovic/Stabilizer, $a \neq 0$: Alltop)

$\Rightarrow$ Standard & Alltop MUBs are unitarily equivalent under $M_{a,*,*}$

Orbits:
- Standard MUB is an orbit of Clifford group
- For fixed $a \neq 0$, Alltop MUB is an orbit of WH group
- The complete set of $(p+1)p^2(p-1)$ magic states in dim p forms:

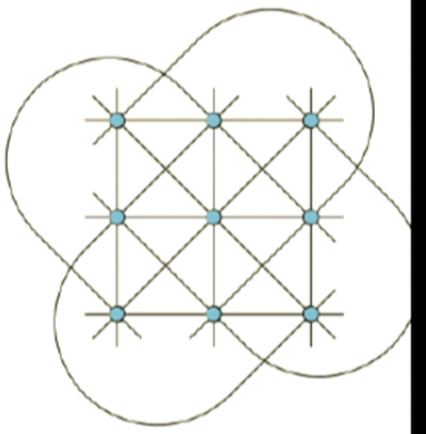
(i) A single orbit under Cliffords when $p = 2 \bmod 3$
(ii) Three distinct orbits under Cliffords when $p = 1 \bmod 3$

Upshot: Surprising inequivalence between magic states (cubic residues)
$a \in \mathbb{Z}_{13}^* = \{1,5,8,12\} \cup \{2,3,10,11\} \cup \{4,6,7,9\}$

(WH-covariant) SIC-POVMs & Magic states

$\mathbf{p = 3}$: 9 points and 12 lines (Hesse configuration)

- Each point belongs to 4 lines
- Each line goes through 3 points
- This a $(9_4, 12_3)$ configuration



Encodes relationships relevant to MUBs/SICs

- 12 Zauner subspaces whose complements form 12 MUB vectors
- 9 points of intersection between subspaces corresponding to 9 SIC vectors

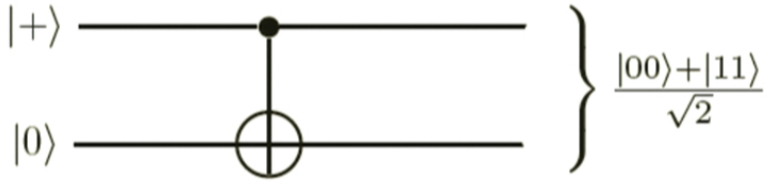
$\mathbf{p = 3k + 1}$: $(p^2 - 1)p^2$ magic states and $p^3(p+1)/2$ Zauner subspaces

- Every Zauner subspace contains $2(p-1)$ magic states
- Every magic state belongs to p Zauner subspaces
- This a $\left((p^2-1)p^2_{\mathbf{p}}, p^3(p+1)/2_{\mathbf{2(p-1)}}\right)$ configuration

Upshot: Understand a little more about the Zauner subspace

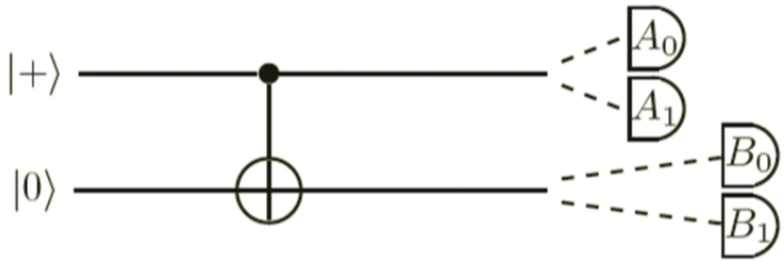
CHSH Bell Inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$



CHSH Bell Inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

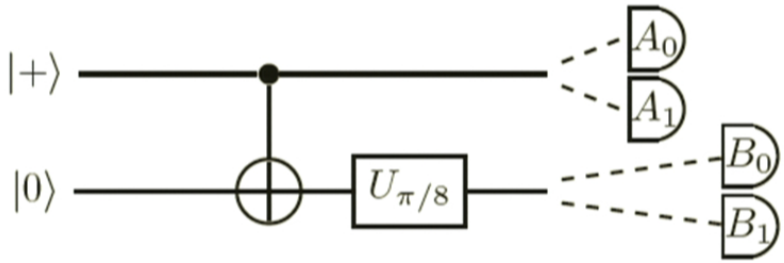


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = (X - Y)/\sqrt{2}$$
$$B_1 = (X + Y)/\sqrt{2}$$

- $2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

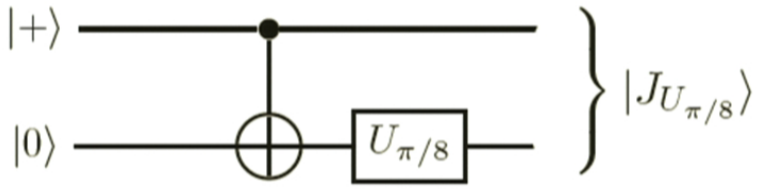


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

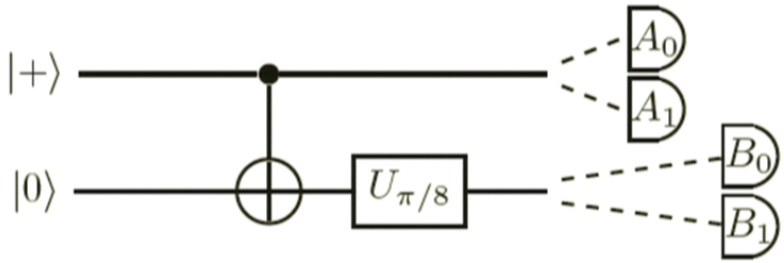


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$



$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} = 2\sqrt{2} \not\leq 2$

Maximizing quantity $\langle \mathcal{B} \rangle$ is related to maximizing

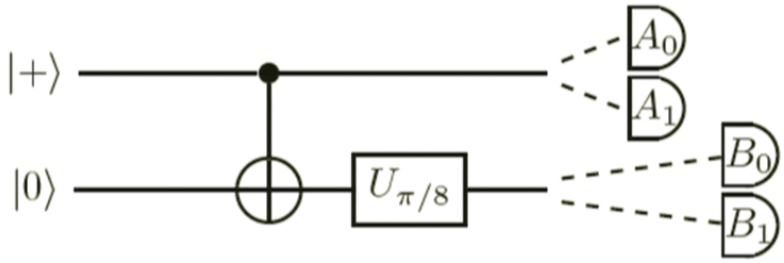
$$\sum_{\substack{a+b=xy \bmod 2 \\ (a,b,x,y \in \mathbb{Z}_2)}} p(a,b|x,y)$$

where $p(a,b|\overbrace{x,y}^{\text{settings}})$ is a conditional prob.

$\underbrace{}_{\text{outcomes}}$

CHSH Bell Inequality

$$\langle \mathcal{B} \rangle \leq 2 \qquad \mathcal{B} = \sum_{x,y \in \mathbb{Z}_2} (-1)^{xy} A_x B_y \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

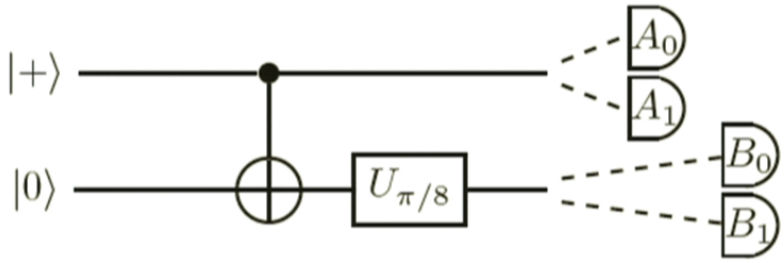


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} = 2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle \mathcal{B} \rangle \leq 2 \qquad \mathcal{B} = \sum_{x,y \in \mathbb{Z}_2} (-1)^{xy} A_x B_y \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

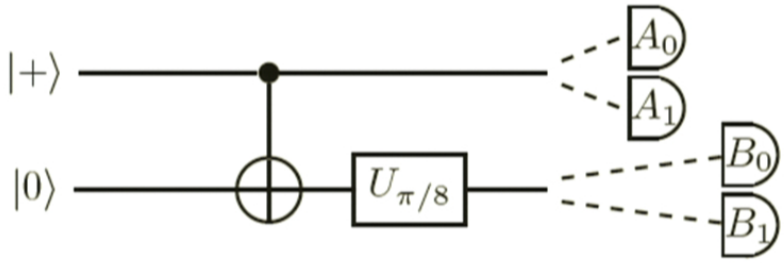


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} = 2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle \mathcal{B} \rangle \leq 2 \qquad \mathcal{B} = \sum_{x,y \in \mathbb{Z}_2} (e^{\frac{2\pi i}{2}})^{xy} A_x B_y \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$

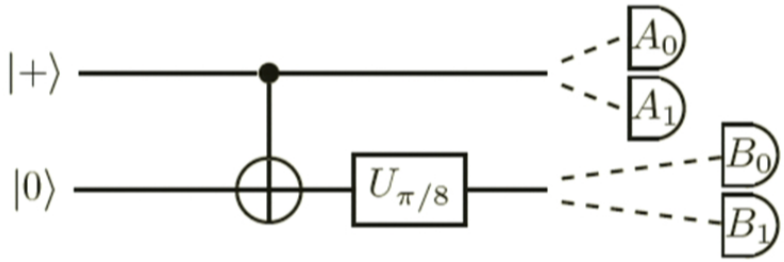


$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} = 2\sqrt{2} \not\leq 2$

CHSH Bell Inequality

$$\langle \mathcal{B} \rangle \leq 2 \qquad \mathcal{B} = \sum_{x,y \in \mathbb{Z}_2} \omega^{xy} A_x B_y \qquad (\lambda(A_x), \lambda(B_y) = \pm 1)$$



$$A_0 = X$$
$$A_1 = Y$$
$$B_0 = X$$
$$B_1 = Y$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} = 2\sqrt{2} \not\leq 2$

CHSH Bell Inequality for $p = 3$

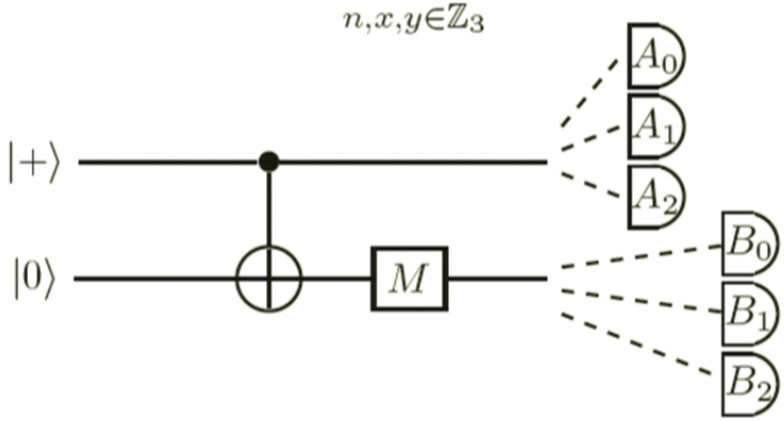
$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$

CHSH Bell Inequality for $p = 3$

$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$

CHSH Bell Inequality for $p = 3$

$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$



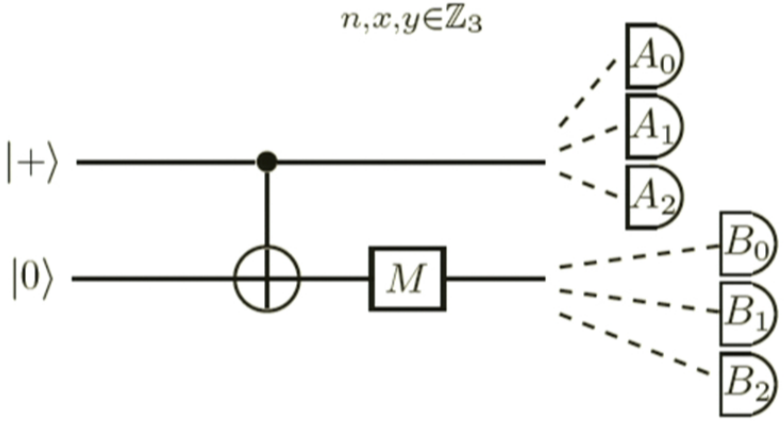
$$A_x = \omega^{x(x+1)} X Z^x$$

$$B_y = \omega^{y(y+2)} X Z^{2y}$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \approx 6.4 \not\leq 6$

CHSH Bell Inequality for $p = 3$

$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$



$$A_x = \omega^{x(x+1)} X Z^x$$

$$B_y = \omega^{y(y+2)} X Z^{2y}$$

- $\langle \mathcal{B} \rangle_{\max}^{\text{QM}} \approx 6.4 \not\leq 6$

Maximizing quantity $\langle \mathcal{B} \rangle_{\max}$ is related to maximizing

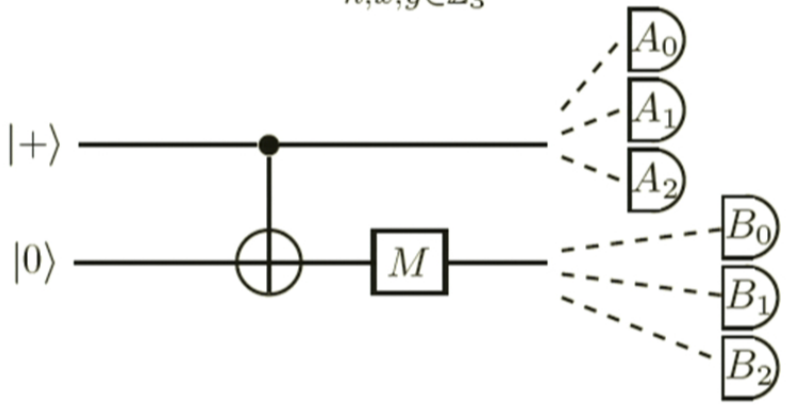
$$\sum_{\substack{a+b+xy=0 \bmod 3 \\ (a,b,x,y \in \mathbb{Z}_3)}} p(a,b|x,y)$$

where $p(a,b|\overbrace{x,y}^{\text{settings}})$ is a conditional prob.

$\underbrace{}_{\text{outcomes}}$

CHSH Bell Inequality for $p = 3$

$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$



$$A_x = \omega^{x(x+1)} X Z^x$$

$$B_y = \omega^{y(y+2)} X Z^{2y}$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \approx 6.4 \not\leq 6$

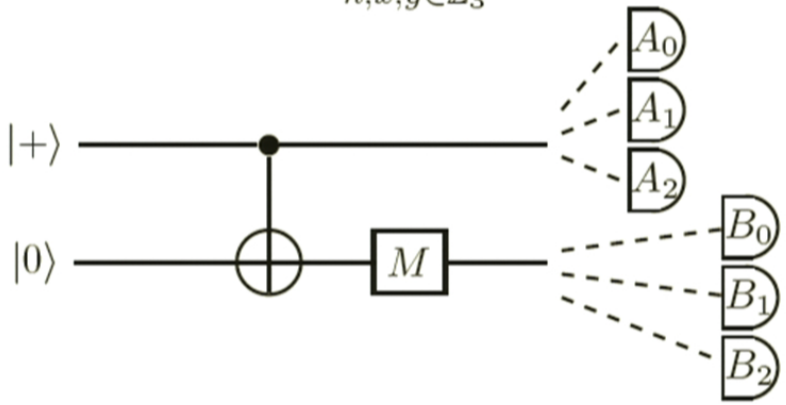
Result: Magic gates are optimal for all prime p (they maximize $\mathcal{B}$)

$\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \leq 4p$ and probably saturates this as $p \to \infty$

Information causality says $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \leq p\left(1 + \frac{p-1}{\sqrt{p}}\right)$ with no restrictions

CHSH Bell Inequality for $p = 3$

$$\langle \mathcal{B} \rangle \leq 6 \qquad \mathcal{B} = \sum_{n,x,y \in \mathbb{Z}_3} \omega^{nxy} A_x^n B_y^n \qquad (\lambda(A_x), \lambda(B_y) = \{\omega^0, \omega^1, \omega^2\})$$



$$A_x = \omega^{x(x+1)} X Z^x$$

$$B_y = \omega^{y(y+2)} X Z^{2y}$$

- $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \approx 6.4 \not\leq 6$

Result: Magic gates are optimal for all prime p (they maximize $\mathcal{B}$)

$\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \leq 4p$ and probably saturates this as $p \to \infty$

Information causality says $\langle \mathcal{B} \rangle_{\max}^{\mathsf{QM}} \leq p\left(1 + \frac{p-1}{\sqrt{p}}\right)$ with no restrictions

Magic in CHSH games

The proof is actually enlightening!
First, one definition:

Def: The V-th vector in the B-th Weyl-Heisenberg basis is given by (eigenvectors of $\{X, XZ, \ldots, XZ^{p-1}\}$ respectively)

$$|\psi_B^V\rangle\langle\psi_B^V| = \frac{1}{p}\sum_j \omega^{-jV} D^j_{(1,B)},$$

$$\text{so that } |\psi_B^V\rangle = \frac{1}{\sqrt{p}}\sum_{k\in\mathbb{F}_q} \omega^{(\frac{1}{2}Bk^2 - Vk)}|k\rangle \qquad (\frac{1}{a} = a^{-1} \bmod p)$$

Magic in CHSH games

The proof is actually enlightening!
First, one definition:

Def: The V-th vector in the B-th Weyl-Heisenberg basis is given by (eigenvectors of $\{X, XZ, \ldots, XZ^{p-1}\}$ respectively)

$$|\psi_B^V\rangle\langle\psi_B^V| = \frac{1}{p}\sum_j \omega^{-jV} D^j_{(1,B)},$$

$$\text{so that } |\psi_B^V\rangle = \frac{1}{\sqrt{p}}\sum_{k\in\mathbb{F}_q} \omega^{(\frac{1}{2}Bk^2 - Vk)}|k\rangle \qquad (\frac{1}{a} = a^{-1} \bmod p)$$

and one result from number theory (Weil bound)

Weil: A polynomial f of degree n over a prime field $\mathbb{Z}_p$ satisfies

$$|\sum_x \omega^{f(x)}| \leq (n-1)\sqrt{p}$$

provided p does not divide n.

Magic in CHSH games

- $\mathcal{B} \mapsto \mathcal{S} \otimes |0\rangle\langle 0|$ under CNOT, so that $\langle \mathcal{B} \rangle_{\max} = \lambda_{\max}(\mathcal{B}) = \lambda_{\max}(\mathcal{S})$
- $\mathcal{S} = \sum_B |\psi_B^{-B(B+\frac{1}{2})}\rangle\langle\psi_B^{-B(B+\frac{1}{2})}|$ i.e. one vector from each basis
- The magic states $\{|f_{-1/12,-1/8,c}\rangle, c \in \mathbb{Z}_p\}$ form an eigenbasis for $\mathcal{S}$

$$\begin{aligned}
\lambda_{\max}(\mathcal{S}) &= \sum_B |\langle\psi_B^{-B(B+\frac{1}{2})}|f_{-1/12,-1/8,c}\rangle|^2 \\
&= p|\langle +|f_{-1/12,-1/8,c}\rangle|^2 \qquad \text{(because "balanced"...)} \\
&= |\sum_x \omega^{\sim x^3}|^2 \\
&\leq [(3-1)\sqrt{p}]^2 = 4p
\end{aligned}$$

- Sato-Tate conjecture describes distrib $\dfrac{|\sum_x \omega^{\sim x^3}|}{2\sqrt{p}}$ as $p \to \infty$

Balancedness of Magic States

Recent work has motivated the search for "balanced" states
i.e., states that look the same in every basis

Ilya Amburg, Roshan Sharma, Daniel Sussman, William K. Wootters
"States that "look the same" with respect to every basis in a mutually unbiased set"
arXiv:1407.4074 [quant-ph]

Such states

- are analagous to harmonic oscillator eigenstates (directionless)
- are automatically minimum uncertainty states (important for QKD)

Balancedness of Magic States

Recent work has motivated the search for "balanced" states
i.e., states that look the same in every basis

Ilya Amburg, Roshan Sharma, Daniel Sussman, William K. Wootters
"States that "look the same" with respect to every basis in a mutually unbiased set"
arXiv:1407.4074 [quant-ph]

Such states

- are analagous to harmonic oscillator eigenstates (directionless)
- are automatically minimum uncertainty states (important for QKD)

Notation: The MUB decomposition of an arbitrary operator K in dim. 3 is

$$K \leftrightarrow \left(\begin{array}{c|c|c|c} \langle 0|K|0\rangle & \langle \psi_0^0|K|\psi_0^0\rangle & \langle \psi_1^0|K|\psi_1^0\rangle & \langle \psi_2^0|K|\psi_2^0\rangle \\ \langle 1|K|1\rangle & \langle \psi_0^1|K|\psi_0^1\rangle & \langle \psi_1^1|K|\psi_1^1\rangle & \langle \psi_2^1|K|\psi_2^1\rangle \\ \langle 2|K|2\rangle & \langle \psi_0^2|K|\psi_0^2\rangle & \langle \psi_1^2|K|\psi_1^2\rangle & \langle \psi_2^2|K|\psi_2^2\rangle \end{array}\right)$$

$$= \left(\begin{array}{c|c|c|c} c_{0,\infty} & c_{0,0} & c_{0,1} & c_{0,2} \\ c_{1,\infty} & c_{1,0} & c_{1,1} & c_{1,2} \\ c_{2,\infty} & c_{2,0} & c_{2,1} & c_{2,2} \end{array}\right) \quad \text{columns} \sim \text{prob. distributions}$$

Balancedness of Magic States

Recent work has motivated the search for "balanced" states
i.e., states that look the same in every basis

Ilya Amburg, Roshan Sharma, Daniel Sussman, William K. Wootters
"States that "look the same" with respect to every basis in a mutually unbiased set"
arXiv:1407.4074 [quant-ph]

Such states

- are analagous to harmonic oscillator eigenstates (directionless)
- are automatically minimum uncertainty states (important for QKD)

Notation: The MUB decomposition of an arbitrary operator K in dim. 3 is

$$K \leftrightarrow \left(\begin{array}{c|c|c|c} \langle 0|K|0\rangle & \langle \psi_0^0|K|\psi_0^0\rangle & \langle \psi_1^0|K|\psi_1^0\rangle & \langle \psi_2^0|K|\psi_2^0\rangle \\ \langle 1|K|1\rangle & \langle \psi_0^1|K|\psi_0^1\rangle & \langle \psi_1^1|K|\psi_1^1\rangle & \langle \psi_2^1|K|\psi_2^1\rangle \\ \langle 2|K|2\rangle & \langle \psi_0^2|K|\psi_0^2\rangle & \langle \psi_1^2|K|\psi_1^2\rangle & \langle \psi_2^2|K|\psi_2^2\rangle \end{array}\right)$$

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \leftrightarrow \left(\begin{array}{c|c|c|c} 0 & 0 & 0 & 0 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \end{array}\right)$$

Balancedness of Magic States

Recent work has motivated the search for "balanced" states
i.e., states that look the same in every basis

Ilya Amburg, Roshan Sharma, Daniel Sussman, William K. Wootters
"States that "look the same" with respect to every basis in a mutually unbiased set"
arXiv:1407.4074 [quant-ph]

Such states

- are analagous to harmonic oscillator eigenstates (directionless)
- are automatically minimum uncertainty states (important for QKD)

Notation: The MUB decomposition of an arbitrary operator K in dim. 3 is

$$K \leftrightarrow \left(\begin{array}{c|c|c|c} \langle 0|K|0\rangle & \langle \psi_0^0|K|\psi_0^0\rangle & \langle \psi_1^0|K|\psi_1^0\rangle & \langle \psi_2^0|K|\psi_2^0\rangle \\ \langle 1|K|1\rangle & \langle \psi_0^1|K|\psi_0^1\rangle & \langle \psi_1^1|K|\psi_1^1\rangle & \langle \psi_2^1|K|\psi_2^1\rangle \\ \langle 2|K|2\rangle & \langle \psi_0^2|K|\psi_0^2\rangle & \langle \psi_1^2|K|\psi_1^2\rangle & \langle \psi_2^2|K|\psi_2^2\rangle \end{array}\right)$$

$$|f_{1,1,0}\rangle \leftrightarrow \left(\begin{array}{c|c|c|c} 0.333 & 0.7124 & 0.7124 & 0.0859 \\ 0.333 & 0.2017 & 0.2017 & 0.7124 \\ 0.333 & 0.0859 & 0.0859 & 0.2017 \end{array}\right)$$

Balancedness of Magic States

Result: All magic states $|f_{a,b,c}\rangle$ have flat distribution in computational basis, and the same distribution in every other basis

Moreover, can prove exactly which permutation occurs in moving from basis to basis (depends on the magic state)

$$\left(\begin{array}{c|c|c|c} 1/3 & c_{0,0} & c_{0,1} & c_{0,2} \\ 1/3 & c_{1,0} & c_{1,1} & c_{1,2} \\ 1/3 & c_{2,0} & c_{2,1} & c_{2,2} \end{array}\right) \qquad c_{V_0,0} = c_{V_B,B}, \qquad \forall B \in \mathbb{Z}_p$$

$$V_B = V_0 + \frac{1}{12a}\left(B^2 - 4Bb\right)$$

Balancedness of Magic States

Result: All magic states $|f_{a,b,c}\rangle$ have flat distribution in computational basis, and the same distribution in every other basis

Moreover, can prove exactly which permutation occurs in moving from basis to basis (depends on the magic state)

$$\left(\begin{array}{c|c|c|c} 1/3 & c_{0,0} & c_{0,1} & c_{0,2} \\ 1/3 & c_{1,0} & c_{1,1} & c_{1,2} \\ 1/3 & c_{2,0} & c_{2,1} & c_{2,2} \end{array}\right) \qquad c_{V_0,0} = c_{V_B,B}, \qquad \forall B \in \mathbb{Z}_p$$

$$V_B = V_0 + \frac{1}{12a}\left(B^2 - 4Bb\right)$$

Note: The max entry of a column is $\sim$ the min-entropy. Minimizing the average min-entropy across a number of bases involves trade-offs. Are magic states optimal amongst flat-balanced states?

Balancedness of Magic States

Result: All magic states $|f_{a,b,c}\rangle$ have flat distribution in computational basis, and the same distribution in every other basis

Moreover, can prove exactly which permutation occurs in moving from basis to basis (depends on the magic state)

$$\left(\begin{array}{c|c|c|c} 1/3 & c_{0,0} & c_{0,1} & c_{0,2} \\ 1/3 & c_{1,0} & c_{1,1} & c_{1,2} \\ 1/3 & c_{2,0} & c_{2,1} & c_{2,2} \end{array}\right) \qquad c_{V_0,0} = c_{V_B,B}, \qquad \forall B \in \mathbb{Z}_p$$

$$V_B = V_0 + \frac{1}{12a}\left(B^2 - 4Bb\right)$$

Note: The max entry of a column is $\sim$ the min-entropy. Minimizing the average min-entropy across a number of bases involves trade-offs. Are magic states optimal amongst flat-balanced states?

QKD: The most informative eavesdropping basis for Eve in the BB'84 scheme is given by magic states, $\{|H\rangle, |H^{\perp}\rangle\}$.

Open Questions

- How much of this structure carries over to power-of-(odd)-prime dimension?
- Further applications in QRACs, Eavesdropping, entropic uncertainty relations etc.?
- Higher order polynomials and/or higher levels of Clifford hierarchy

Refs:

Mark Howard and Jiri Vala,
"Qudit versions of the qubit $\pi/8$ gate"
Phys. Rev. A 86, 022316 (2012)

Ingemar Bengtsson, Kate Blanchfield, Earl Campbell, Mark Howard,
"Order 3 Symmetry in the Clifford Hierarchy"
arXiv:1407.2713 (2014)

M. Howard et al.,
In preparation
(2014)

References

Se-Wan Ji, Jinhyoung Lee, James Lim, Koji Nagata, and Hai-Woong Lee
Multisetting Bell inequality for qudits,
Phys. Rev. A 78, 052103 (2008).

Yeong-Cherng Liang, Chu-Wee Lim, Dong-Ling Deng
Reexamination of a multisetting Bell inequality for qudits,
Phys. Rev. A 80, 052116 (2009).

Mohammad Bavarian, Peter W. Shor,
"Information Causality, Szemerdi-Trotter and Algebraic Variants of CHSH"
arXiv:1311.5186 (2013).

Ilya Amburg, Roshan Sharma, Daniel Sussman, William K. Wootters
"States that "look the same" with respect to every basis in a mutually unbiased set"
arXiv:1407.4074 [quant-ph]

C. H. Bennett, F. Bessette, G. Brassard,L. Salvail, and J. Smolin,
"Experimental quantum cryptography"
Journal of Cryptology, 5, 1, 3–28 (1992)