Rel of Sim + Ball dimension

Notation: $B^d = d\text{-ball} \subseteq \mathbb{R}^d$, $\partial B^d = S^{d-1} = (d-1)\text{-sphere}$

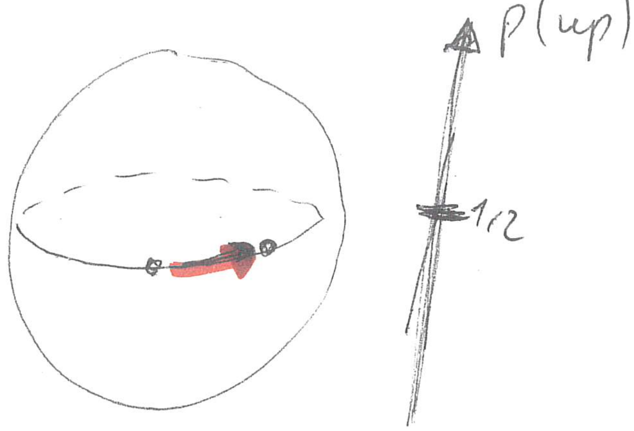
$\mathcal{G}_A, \mathcal{G}_B$: Alice's and Bob's groups of transformations

subgroups of $SO(d-1)$. May assume: topologically closed
→ Lie subgroups.

REL: $[\mathcal{G}_A, \mathcal{G}_B] = 0$

A3) $\mathcal{G}_A \simeq \mathcal{G}_B$ as Lie groups

A1) & A2):



The group $\mathcal{G}_{AB}$, generated by $\mathcal{G}_A$ and $\mathcal{G}_B$, is transitive on the "equator"

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{d-1} \\ 0 \end{pmatrix} \right\} \simeq \partial B^{d-1} = S^{d-2}$$

$\underline{d=3}$: Standard complex qubit

$$U_A^{(\theta)}(\alpha|0\rangle + \beta|1\rangle) := \alpha e^{i\theta}|0\rangle + \beta|1\rangle$$

$$U_B^{(\theta)}(\alpha|0\rangle+\beta|1\rangle) := \alpha|0\rangle+\beta e^{+i\theta}|1\rangle$$

$$\mathcal{G}_A = \{\varsigma \mapsto U_A^{(\theta)}\varsigma U_A^{(\theta)\dagger} \mid 0\leq\theta<2\pi\} \simeq SO(2)$$

$$\mathcal{G}_B = \{\varsigma \mapsto U_B^{(\theta)}\varsigma U_B^{(\theta)\dagger} \mid 0\leq\theta<2\pi\} \simeq SO(2)$$

$U_B^{(-\theta)} = e^{-i\theta} U_A^{(\theta)} \Rightarrow \mathcal{G}_A = \mathcal{G}_B$ (not just isomorphic)
$= \mathcal{G}_{AB}$.

$[\mathcal{G}_A, \mathcal{G}_B] = 0$, $\mathcal{G}_{AB}$ transitive on S^1, the unit circle.

- $d \geq 4$, d even, $d \neq 8$ is impossible

(will give a hint why $d=5$ is possible):

$\mathcal{G}_{AB}$ transitive on ∂B^{d-1}

$\Rightarrow$ connected component $\mathcal{G}_{AB}^{0}$ is also.

<u>Theorem</u> (elsewhere, Refs see paper):
If d is odd, and $\mathcal{G}$ connected Lie group acting transitively on ∂B^d,
then
- if $d \neq 7$ we have $\mathcal{G} = SO(d)$,
- if $d = 7$ we have $\mathcal{G} = SO(7)$ or $\mathcal{G} = G_2$.

Here $d \neq 8 \Rightarrow \mathcal{G}_{AB}^{0} = SO(d-1)$.

$g = \mathcal{G}_{AB} \Rightarrow g = g_1 g_2 g_3 g_4 g_5 \ldots g_n$, $g_i \in \mathcal{G}_A$ or $g_i \in \mathcal{G}_B$
$= g_A g_B$

$g_A \in \mathcal{G}_A$, $g_B \in \mathcal{G}_B$.

$g \in \mathcal{G}_{AB}^{\circ} \Rightarrow g = g_A g_B, \quad g_A \in \mathcal{G}_A^{\circ}, g_B \in \mathcal{G}_B^{\circ}.$

<u>Claim</u>: $\mathcal{G}_A^{\circ}$ [and $\mathcal{G}_B^{\circ}$] is a nontrivial connected normal subgroup of $\mathcal{G}_{AB}^{\circ}$.

<u>Proof</u>: $h_A \in \mathcal{G}_A^{\circ}, \ g \in \mathcal{G}_{AB}^{\circ}$

$$\Rightarrow g = g_A g_B, \quad g_A \in \mathcal{G}_A^{\circ}, g_B \in \mathcal{G}_B^{\circ}$$

$$\Rightarrow g h_A g^{-1} = g_A g_B h_A g_B^{-1} g_A^{-1} = g_A h_A g_A^{-1} \cancel{g_B g_B^{-1}} \in \mathcal{G}_A^{\circ}.$$

<u>Non-trivial</u>: $\mathcal{G}_A^{\circ} = \{\mathbb{1}\} \Rightarrow \mathcal{G}_A$ discrete $\Rightarrow \mathcal{G}_A$ not transitive on continuous ∂B^{d-1} ↯

$$\mathcal{G}_A^{\circ} = \mathcal{G}_{AB}^{\circ} \Rightarrow \mathcal{G}_A^{\circ} = SO(d-1) = \mathcal{G}_B^{\circ}$$

$$\Rightarrow [\mathcal{G}_A^{\circ}, \mathcal{G}_B^{\circ}] \neq 0 \quad ↯$$

$\Rightarrow SO(d-1)$ is not a simple group

$\Rightarrow d = 5$ [redacted]

Not possible in this treatment of case, but indeed: $d=5$ is possible in general, and

$SO(4) \ni g = g_A g_B$ $\quad g_A$: left-, g_B: right-isoclinic rotation of $SO(4)$

left- and right-mult. by quaternionic phase!

Randomness Generator

Proof that $Q_{J,\alpha} = R_{J,\alpha}$

$x \in \{1,2\}$ input. $x=1$: no rotation

$x=2$: rotate by $0 \leq \alpha \leq \frac{\pi}{2J}$, α fixed.

$\vec{E} = (E_1, E_2)$, $E_x = P(+1|x) - P(-1|x)$

$$S_{J,\alpha} = \left\{ \vec{E} \;\middle|\; \tfrac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2} + \sqrt{1-E_1}\sqrt{1-E_2} \geq \cos(J\alpha)\right) \right\}.$$

Theorem: $\underbrace{Q_{J,\alpha}}_{\text{quant boxes}} = \underbrace{R_{J,\alpha}}_{\text{rotation boxes}} = S_{J,\alpha}$

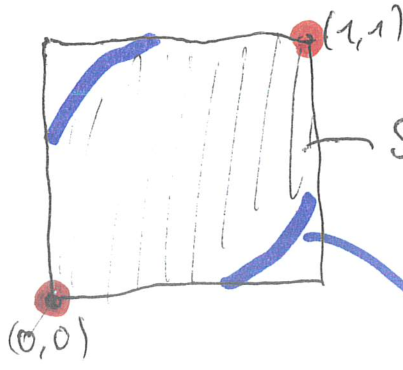
Obviously, $Q_{J,\alpha} \subseteq R_{J,\alpha}$.

Claim 1: $S_{J,\alpha} \subseteq Q_{J,\alpha}$

Claim 2: $R_{J,\alpha} \subseteq S_{J,\alpha}$

Proof of Claim 1: Reparametrize $\vec{P}^+ = (P(+1|1), P(+1|2))$

$$= \tfrac{1}{2}\vec{E} + \left(\tfrac{1}{2}, \tfrac{1}{2}\right)$$



$S_{J,\alpha}$ compact convex set

equality in def of $S_{J\alpha}$: $\sqrt{P_0^+}\sqrt{P_\alpha^+} + \sqrt{1-P_0^+}\sqrt{1-P_\alpha^+} = \cos(J\alpha)$

2

to show: (1) $\partial_{ext} S_{J,\alpha} \subseteq Q_{J,\alpha}$
(2) $Q_{J,\alpha}$ is convex
$\Big\} \Rightarrow S_{J,\alpha} \subseteq Q_{J,\alpha}$.

(2) Let $\vec{E}, \vec{F} \in Q_{J,\alpha}$, $0 < \lambda < 1$.

$$P_{\vec{E}}(+1|x) = \mathrm{tr}(E\, U_{\alpha(x)} \rho\, U_{\alpha(x)}^{\dagger})$$

$$P_{\vec{F}}(+1|x) = \mathrm{tr}(F\, V_{\alpha(x)} \sigma\, V_{\alpha(x)}^{\dagger})$$ U, V: some spin-J rep.

$G := E \oplus F$, $\tau := \lambda\rho \oplus (1-\lambda)\sigma$, $W_{\alpha(x)} := U_{\alpha(x)} \oplus V_{\alpha(x)}$

$\Rightarrow p(+1|x) := \mathrm{tr}(G\, W_{\alpha(x)} \tau\, W_{\alpha(x)}^{\dagger})$ gives correlations $\lambda\vec{E} + (1-\lambda)\vec{F} \in Q_{J,\alpha}$.

(1) **Corner points:**

$\vec{p}^{+} = (1,1) \Leftrightarrow p(+1|x) = 1$ regardless of x

$= \mathrm{tr}(\mathbb{1}\, U_{\alpha(x)} \rho\, U_{\alpha(x)}^{\dagger})$, ρ, U arbitrary

$\Rightarrow \vec{E} \in Q_{J,\alpha}$. Similarly for $\vec{p}^{+} = (0,0)$, $\vec{E} = (-1,-1)$.

Curves:

$$C_1(\theta) := \left(\cos^2(J\theta), \cos^2(J(\theta+\alpha))\right), \quad \theta \in \left[0, \frac{\pi}{2J} - \alpha\right]$$

$$C_2(\theta) := \left(\cos^2(J\theta), \cos^2(J(\theta-\alpha))\right), \quad \theta \in \left[\alpha, \frac{\pi}{2J}\right]$$

On c_1: $\sqrt{P_0^+(\theta)}\sqrt{P_\alpha^+(\theta)} + \sqrt{1-P_0^+(\theta)}\sqrt{1-P_\alpha^+(\theta)}$

$$= \cos(J\theta)\cos(J(\theta+\alpha)) + \sin(J\theta)\sin(J(\theta+\alpha))$$

$$= \cos(J\alpha)$$ similarly on c_2.

$\mathcal{H} := \mathrm{span}\{|-J\rangle, \dots, |J\rangle\}$ $\quad U_\theta |j\rangle = e^{ij\theta}|j\rangle$

$|\phi\rangle := \frac{1}{\sqrt{2}}(|-J\rangle + |J\rangle)$,

$M_+ := U_\theta^\dagger |\phi\rangle\langle\phi| U_\theta$, $\quad M_- := \mathbb{1} - M_+$

$$\Rightarrow P(+|\theta) = P_0^+ = \langle\phi|M_+|\phi\rangle = |\langle\phi|U_\theta|\phi\rangle|^2$$

$$= \frac{1}{4}\left|(\langle -J| + \langle J|)(e^{-iJ\theta}|-J\rangle + e^{iJ\theta}|J\rangle)\right|^2$$

$$= \frac{1}{4}|e^{-iJ\theta} + e^{iJ\theta}|^2 = \cos^2(J\theta)$$

Similarly $P_\alpha^+ = \cos^2(J(\theta+\alpha))$.

This reproduces all $\vec{E} \in c_1$ in QT. Similarly for c_2.

<u>Proof of Claim 2</u>

[redacted] $\vec{E} \in \mathcal{R}_{J,\alpha}$. Set $T(\theta) := P(+|\theta) - P(-|\theta) = 1 - 2P(+|\theta)$.

$\Rightarrow T$ is a trig. poly of degree $n = 2J$ and $-1 \leq T(\theta) \leq 1$ $\forall\theta$

DeVore and Lorentz, Constructive Approximation, Ch. 4, Thm. 1.1:

$\Rightarrow T'(x)^2 + n^2 T(x)^2 \leq n^2$. $\Rightarrow T'(x) \leq 2J\sqrt{1-T(x)^2}$.

$E_1 = T(0),\quad E_2 = T(\alpha)$

$y = T(\beta)$

$$\Rightarrow \alpha = \int_0^\alpha d\beta \geq \int_0^\alpha \frac{T'(\beta)\, d\beta}{2J\sqrt{1-T(\beta)^2}} = \frac{1}{2J}\int_{E_1}^{E_2} \frac{dy}{\sqrt{1-y^2}}$$

$$= \frac{1}{2J}\left(\arcsin E_2 - \arcsin E_1\right)$$

$$\Rightarrow \frac{1}{2}\left|\arcsin E_2 - \arcsin E_1\right| \leq J\alpha$$

Take "cos" of both sides

$$\Rightarrow \frac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2} + \sqrt{1-E_1}\sqrt{1-E_2}\right) \geq \cos(J\alpha)$$

$$\Rightarrow \vec{E} \in S_{J\alpha}. \qquad \square$$

$$\Rightarrow Q_{J,\alpha} = R_{J,\alpha}.$$

Non-zero private randomness

Claim: If SDI assumption "spin $\leq J$" is with high prob. satisfied approximately, [redacted] and the observed correlations $\vec{E}$ are far from classical, then a non-zero amount of randomness is certified against Eve.

Without assuming QT!

Exact SDI assumption: $\vec{E}^\lambda \in R_{J,\alpha}$ for all λ

Related: With prob. $\geq 1-\varepsilon$, we have $\vec{E}^\lambda \in R^w_{J,\alpha} = (1-w)R_{J,\alpha} + w[-1,1]^2$

Example: Coherent (photon) state

$$|\beta\rangle = e^{-\frac{|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{\beta^n}{\sqrt{n!}} |n\rangle$$

has large overlap with $\mathcal{H}_N := \operatorname{span}\{|n\rangle \mid 1 \leq n \leq N\}$ for small photon number N

$\rightarrow$ approx. $J \leq N$, but not exactly, hence

$$\vec{E} \in Q^{\omega}_{J,\alpha} \text{ for } \omega = O(e^{-cN}).$$

Want to certify non-zero $H(B|X,\Lambda) = \sum_{\lambda} p(\lambda) H(\vec{E}^{\lambda})$

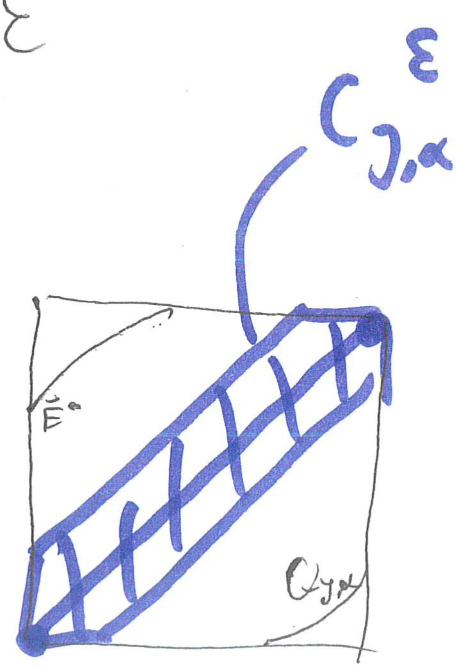
where $H(\vec{F}) = -\frac{1}{2} \sum_{b,x} \frac{1+bE_x}{2} \log \frac{1+bE_x}{2}$

Optimization problem:

$$H^* = \min_{\{p(\lambda), \vec{E}^{\lambda}\}} \sum_{\lambda} p(\lambda) H(\vec{E}^{\lambda})$$

subject to $\displaystyle\sum_{\lambda : \vec{E}^{\lambda} \in Q^{\omega}_{J,\alpha}} p(\lambda) \geq 1 - \varepsilon$

and $\displaystyle\sum_{\lambda} p(\lambda) \vec{E}^{\lambda} = \vec{E}$.



Claim: If $\vec{E} \notin C^{\varepsilon}_{J,\alpha}$ then $H^* > 0$.

$$C_{J,\alpha} = \operatorname{conv}\{\underbrace{(-1,-1), (+1,+1)}_{\text{determ. correlations}}\}$$

$$C^{\varepsilon}_{J,\alpha} = (1-\varepsilon) C_{J,\alpha} + \varepsilon [-1,1]^2$$

⑥

Proof: $H^* = 0 \Rightarrow \exists \Lambda : \sum_{\lambda \in \Lambda} p(\lambda) = 1-\delta \geq 1-\varepsilon$

and $H(\vec{E}^\lambda) = 0 \quad \forall \lambda \in \Lambda$

i.e. $\lambda \in \Lambda \Rightarrow \vec{E}^\lambda \in C_{J,\alpha}$.

$$\Rightarrow \vec{E} = \sum_\lambda p(\lambda) \vec{E}^\lambda = (1-\delta) \underbrace{\sum_{\lambda \in \Lambda} \frac{p(\lambda)}{1-\delta} \vec{E}^\lambda}_{\in C_{J,\alpha}} + \text{something}$$

$$\in C^\delta_{J,\alpha} \subseteq C^\varepsilon_{J,\alpha}. \qquad \square$$

Randomness against classical side-information about post-quantum physics.