monogamy of entanglement

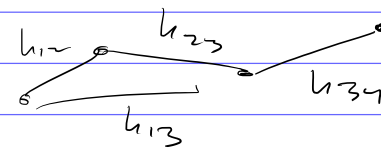
$\exists ?\ \rho_{ABC}$ s.t $\rho_{AB} = \Phi_{AB}$ $\quad \rho_{AC} = \Phi_{AC}$ $\quad$ No

$\omega = \frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}$ $\quad \rho_{AB} = \omega_{AB}$ $\quad \rho_{AC} = \omega_{AC}$ $\quad$ fine

monogamy: entanglement cannot be shared without limit

Application mean-field theory

$H = \sum_{i\sim j} h_{ij}$



fully connected limit $\quad H_{MF} = \frac{D}{n} \sum_{i<j} h_{ij}$

ground state (= eigvector for λ_{min}) $\quad |\psi_{gs}\rangle$

claim $\approx \rho^{\otimes n}$

specifically $\quad \psi_{gs}^{S} \approx \mathbb{E}_{\rho\sim\mu}\, \rho^{\otimes S}$ $\quad$ if $|S| \ll n$

WLOG $\quad P_\pi |\psi_{gs}\rangle = |\psi_{gs}\rangle$

symmetric states have marginals $\approx$ mixture of tensor powers

de Finetti thm

given $\quad \omega \in D_{d^n}$ $\quad$ s.t $\quad P_\pi \omega P_\pi^\dagger = \omega \quad \forall \pi$

$\exists \mu$ on D_d st. $\quad$ (weaker than $\operatorname{supp} \omega \in \mathrm{Sym}^n \mathbb{C}^d$)

$\| \omega_{1\ldots k} - \int d\mu(\rho)\, \rho^{\otimes k} \|_1 \le \frac{d^2 k}{n}$

$k=2$ for mean-field-theory example

classical analogue: $\quad p(z_1, z_2, \ldots) = p(z_{\pi(1)}, z_{\pi(2)}, \ldots)$ $\quad$ "exchangeable"

$p(z_1 \ldots, z_k) = \int d\mu(q)\, q^{\otimes k}$ $\quad$ μ depends on p

Pf

purify $\rho_{A_1 \ldots A_n}$ to $|\psi\rangle_{A_1\ldots A_n B_1 \ldots B_n} \in \mathrm{Sym}^n(A \otimes B)$ $\quad A \cong B \cong \mathbb{C}^d$

canonical purification $\quad (\sqrt{\rho} \otimes I) \sqrt{d^n}\, |\Phi\rangle_{AB}^{\otimes n}$ $\quad$ works

reduces to pure-state dF thm

$|\psi\rangle \in \mathrm{Sym}^{n+k} \mathbb{C}^d \implies F(\mathrm{tr}_n \psi, \int d\mu(\phi)\, \phi^{\otimes k}) \ge 1 - \frac{dk}{n}$

$|\Psi\rangle \in \text{span}\{|\phi\rangle^{\otimes n+k}\}$

$= \sum_i c_i |\phi_i\rangle^{\otimes n+k}$

but $\langle\phi_i|\phi_j\rangle \neq 0$ but $\langle\phi_i|\phi_j\rangle^n \approx 0$

(Reminiscent of coherent states for harmonic oscillator $\int \frac{|\alpha\rangle\langle\alpha|}{2\pi} = I$ corresponds to $SU(1,1)$. we'll use "spin coherent states" with $SU(1,1) \to U(d)$)

idea $M_{\hat\phi} = \hat\phi^{\otimes n}\, d[n]$ $\qquad d[n] := \binom{d+n-1}{n}$

$\text{tr}_n \Psi = \int d\phi \; \text{tr}_n\left[\left(d[n]\phi^{\otimes n} \otimes I^{\otimes k}\right)\Psi\right]$

$= \underbrace{\int d\phi \quad p(\phi)}_{\text{call this } d\mu(\phi)} \Psi_\phi$ $\qquad$ claim $\Psi_\phi \approx \phi^{\otimes n}$

$F\left(\text{tr}_n \Psi, \int d\phi\, p(\phi)\, \phi^{\otimes k}\right)^2$

$\geq \int d\phi\; p(\phi)\; F(\Psi_\phi, \phi^{\otimes k})^2$

$= \int d\phi\, \text{tr}\left[\left(\text{tr}_n(\phi^{\otimes n} \otimes I)\Psi\right) \cdot \phi^{\otimes k}\right] \quad d[n]$

$= \int d\phi \quad \text{tr}\, \phi^{\otimes n+k}\, \Psi\; d[n]$

$= \frac{d[n]}{d[n+k]} = \frac{d(d+1)\cdots(d+n-1)}{(d+k)\cdots(d+k+n-1)} \geq 1 - \frac{dk}{n}$

Examples

(1) $\frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ all marginals separable

(2) $\rho = \binom{n}{n/2}^{-1} \sum_{|x| = n/2} |x\rangle\langle x|$

$\rho_{1\cdots k}$ has H wt ~ hypergeometric dist
var $\leq \frac{k}{4}$ prediction from iid

(3) $\frac{1}{\sqrt{n!}} \sum_{\pi \in S_n} \text{sgn}(\pi)\, |\pi_1 \ldots \pi_n\rangle \in (\mathbb{C}^n)^{\otimes n}$

Application to QKD

- protocol treats bits symmetrically
- reduces Eve's attacks to IID
- problem: error $\sim k/n$

need better ideas for error $\exp(-\Omega(n))$

de Finetti reduction

$[\rho, P_\pi] = 0 \ \forall \pi \Rightarrow \rho \leq n^{O(d^2)} \int d\mu(\sigma)\ \sigma^{\otimes n}$

$\Rightarrow$ error ϵ for IID $\Rightarrow$ error $\leq n^{O(d^2)} \epsilon$ for symmetric

Pf purify $\rightarrow |\psi\rangle \in \mathrm{Sym}^n(\mathbb{C}^d \otimes \mathbb{C}^d)$ $\quad \psi \leq \underbrace{\binom{n+d^2-1}{n}}_{\leq n^{O(d^2)}} \int_{|\phi\rangle \in \mathbb{C}^{d^2}} d\phi\ \phi^{\otimes n}$

Application to optimization

$$\mathrm{Sep} = \mathrm{Sep}(d_A, d_B) = \mathrm{conv}\{\alpha \otimes \beta : \alpha \in D_{d_A}, \beta \in D_{d_B}\}$$

will set $d_A = d_B = d$

$$h_{\mathrm{sep}}(M) = \max_{\sigma \in \mathrm{Sep}} \mathrm{tr}[M\sigma] = \max_{\alpha, \beta} \mathrm{tr}\, M(\alpha \otimes \beta)$$

Similar in difficulty to $h_{\mathrm{sepSym}}(M) = \max_{\alpha} \mathrm{tr}\, M(\alpha \otimes \alpha)$

$= \max$ of deg-4 poly over unit sphere

NP-complete. Also $\max_{\|p\|_1 \leq 1} \langle p, Ap \rangle = 1 - \dfrac{1}{\text{biggest clique of } A}$ when A is adj matrix of a graph

ρ_{AB} k-extendable if $\exists\ \tilde{\rho}_{AB_1 \ldots B_k}$ s.t. $\rho_{AB} = \tilde{\rho}_{AB_i}$ $\forall i \in [k]$

dF thm $\Rightarrow \tilde{\rho}_{AB_i} \approx \sum_x p_x\, \alpha_x^A \otimes \beta_x^{B_i}$ error $\lesssim \dfrac{d^2}{k}$

run time $\sim d^{O(k)}$

This is not efficient, but on your pset you used info theory methods to analyze

$k \sim \dfrac{\log d}{\epsilon^2}$ for $h_{\mathrm{sep}}(M)$ when M is 1-LOCC

SOS (sum of squares) SDP hierarchy

$\mathrm{SepSym} = \mathrm{conv}\{\alpha \otimes \alpha\} \subseteq \mathrm{DPS}_k :=$

$\{\rho_{A_1A_2} : \exists\, \tilde{\rho}_{A_1 \cdots A_k}$ s.t. $\tilde{\rho}_{A_1A_2} = \rho_{A_1A_2}$, $P_\pi \tilde{\rho} = \tilde{\rho} = \tilde{\rho} P_\pi$, $\tilde{\rho}^{T_S} \geq 0$ $\forall\, S \subseteq \{A_1, \ldots, A_k\}\}$

$\sigma \in \mathrm{SepSym}$

Interpret σ_{ijkl} as $\mathbb{E}[\alpha_i \alpha_j \alpha_k^* \alpha_l^*]$

for $|\alpha\rangle \in \mathbb{C}^d$ a random variable

$\tilde{\rho}_{i_1 \ldots i_k, j_1 \ldots j_k} \overset{\text{hopefully}}{=} \mathbb{E}[\alpha_{i_1} \cdots \alpha_{i_k} \alpha^*_{j_1} \cdots \alpha^*_{j_k}]$

can say $= \tilde{\mathbb{E}}[x_{i_1} \cdots x_{i_k} x^*_{j_1} \cdots x^*_{j_k}]$

$\max \{\mathrm{tr}\, M\sigma : \sigma \in \mathrm{DPS}_k\}$

$= \min \{\lambda : \mathrm{tr}\, M |x\rangle\langle x| \otimes |x\rangle\langle x| = \lambda + p(x, x^*)(\|x\|_2^2 - 1) + \sum_i |q_i(x)|^2\}$

$\deg \leq 2k-2$ $\qquad$ $\deg \leq k$