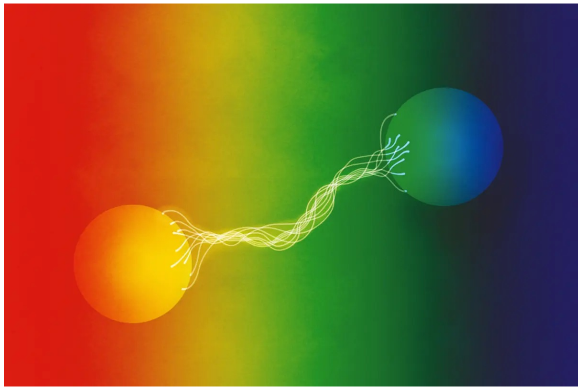
Quantum Pseudoentanglement

Bill Fefferman (University of Chicago)
Joint with Adam Bouland, Soumik Ghosh, Umesh Vazirani, Jack Zhou

Based on arXiv:2211.00747

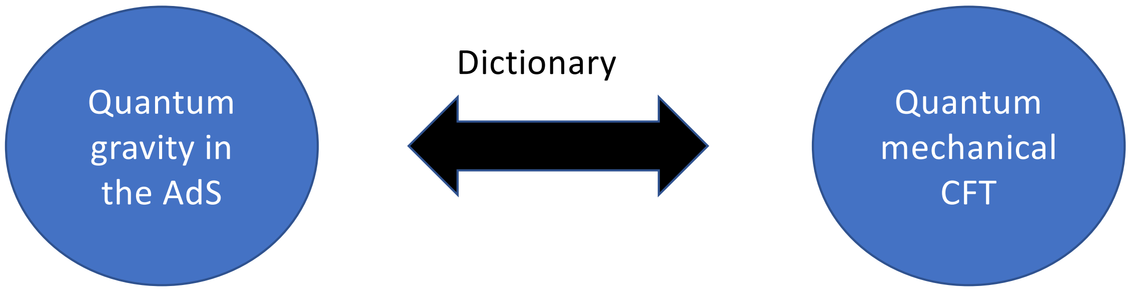
Quantum entanglement is subtle!

- Quantum entanglement is fundamental for quantum computation
- But there is still a lot we don’t understand
- **This work:** quantum entanglement “is not feelable”
  - Will construct an ensemble of quantum states with *low entanglement* which cannot be efficiently distinguished from maximally entangled states even if given many copies



(illustration of entanglement from nobelprize.org)

Motivation 1: *Entanglement, Geometry and Complexity*



AdS/CFT [Maldacena '97] is a conjectured duality between quantum gravity (the "bulk") and a quantum mechanical system (the "boundary")

- **Major theme:** Entanglement in the CFT = geometry in AdS (e.g., RT formula, ER=EPR...)
- **Our result**: Entanglement cannot be "felt" or efficiently observed
- If corresponding geometry is "feelable", then the AdS/CFT dictionary must be hard to compute (in spirit of [BFV'19][GH'20])

Motivation 2: *random quantum states*

- Random quantum states, drawn from the Haar measure, are an important resource
- But they are of limited practicality from a computational point of view
  - Basic counting arguments tell us we need $\exp(n)$ size circuits to approximately prepare most states from $|0^n\rangle$
- To get over this, a central concept in quantum information has been "*pseudorandom*" ensembles of efficiently preparable quantum states which *mimic properties* of truly random quantum states

Information theoretic pseudorandomness

- A **quantum 2-design** is an ensemble of quantum states with the property that *no algorithm* can distinguish 2 copies from truly random states
- This notion is now a very central topic in quantum information theory with many important applications e.g., to
  - randomized benchmarking
  - quantum advantage experiments
  - quantum gravity…

Computational pseudorandomness

- In computer science, we generally talk about the different notion of *computational* pseudorandomness
- i.e., these are efficiently preparable quantum states that can't be distinguished from truly Haar random states by any **efficient** quantum algorithm A given $\boldsymbol{poly}(\boldsymbol{n})$ copies
- This generally requires complexity assumptions
- Classically, this notion enables a wide variety of applications not known to be possible in the information theoretic setting
  - Public key cryptography
  - Homomorphic encryption
  - Derandomization

What is the relation between pseudorandomness and entanglement?

- A typical Haar random quantum state is *maximally* entangled.
- Quantum t-designs are also close to *maximally* entangled (for any $t \geq 2$)
- **Our result:** Computational pseudorandom states *do not need to be* extremely entangled!

Proof sketch

The Ji, Liu & Song construction [JLS'18][BS'19]

- Consider states of the form:
  - $|\psi_{f_k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} f_k(x) |x\rangle$
  - Where $f_k: \{0,1\}^n \rightarrow \{\pm 1\}$ is *any* quantum secure pseudorandom function
- **Main result [JLS'18] [BS'19]:** $\{|\psi_{f_k}\rangle\}$ is a *computational pseudorandom state* (i.e., a "PRS") assuming quantum secure cryptography is possible.
  1. Can efficiently prepare $|\psi_{f_k}\rangle$ given key k
  2. without knowledge of k, no **efficient** quantum algorithm can distinguish **polynomially many copies** of $|\psi_{f_k}\rangle$ from copies of a Haar random state
     - i.e., $| \Pr_k[A\left(|\psi_{f_k}\rangle^{\otimes poly(n)}\right) = 1] - \Pr\left[A_{|\phi\rangle \sim Haar}\left(|\phi\rangle^{\otimes poly(n)}\right) = 1\right] | < \epsilon$

How entangled is the JLS construction?

- **Lower bound** [JLS'18]: Let ρ be RDM of $|\psi_{f_k}\rangle$ wrt subsystem A on $n/2$ qubits, then $S(\rho) = \omega(\log(n))$ whp
- **Lemma**: $Tr[\rho^2] < \frac{1}{n^c}$ for all constant c, whp
- **Pf:** If not, then the swap test on subsystem A of two copies of $|\psi_{f_k}\rangle$ would be an efficient distinguisher from a Haar random state
  - This test succeeds with probability $\frac{1}{2} + \frac{Tr[\rho^2]}{2}$
- Lower bound on entanglement directly follows from Lemma
  - Since $S(\rho) \geq -\log(Tr[\rho^2])$ by Jensen's inequality
- We didn't know of a PRS with entanglement saturating this lower bound…

How to make a low entanglement PRS

- Consider the JLS construction and divide the n qubits in half, denote the subsystems A, B
  - i.e., $|\psi_f\rangle = \sum_{i\in\{0,1\}^{n/2}, j\in\{0,1\}^{n/2}} f(i,j)|i\rangle_A |j\rangle_B$
- It will be convenient to think of this state as encoded by a "pseudorandom matrix" C_f with (i,j) entry $= f(i,j)$

$$C_f = \overbrace{\begin{pmatrix} f(0^{\frac{n}{2}}, 0^{\frac{n}{2}}) & \cdots & f(0^{\frac{n}{2}}, 1^{\frac{n}{2}}) \\ \vdots & \ddots & \vdots \\ f\left(1^{\frac{n}{2}}, 0^{\frac{n}{2}}\right) & \cdots & f(1^{\frac{n}{2}}, 1^{\frac{n}{2}}) \end{pmatrix}}^{\text{Subsystem B}} \left.\vphantom{\begin{pmatrix} a \\ b \\ c \end{pmatrix}}\right\} \text{Subsystem A}$$

- It's not hard to see that the RDM on subsystem A, $\rho = \frac{1}{2^n} C_f C_f^T$

Our construction (informal)

- **Goal:** Minimize $\mathrm{S}(\rho) = S\left(\frac{1}{2^n} C_f C_f^T\right)$
- **Idea:** Pick a small subset of rows, and repeat those rows many times, e.g.,

$$\boldsymbol{C_f} = \begin{pmatrix} f(0^{\frac{n}{2}}, 0^{\frac{n}{2}}) & \cdots & f(0^{\frac{n}{2}}, 1^{\frac{n}{2}}) \\ \vdots & \ddots & \vdots \\ f\left(1^{\frac{n}{2}}, 0^{\frac{n}{2}}\right) & \cdots & f(1^{\frac{n}{2}}, 1^{\frac{n}{2}}) \end{pmatrix}$$

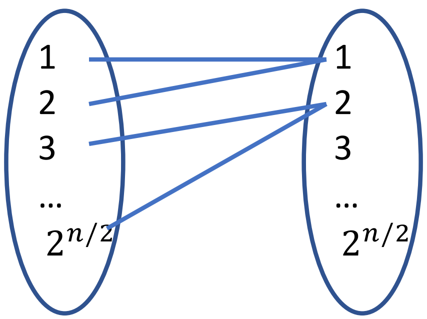
$$\boldsymbol{C'_f} = \begin{pmatrix} f\left(0^{\frac{n}{2}}, 0^{\frac{n}{2}}\right) & \ldots & f(0^{\frac{n}{2}}, 1^{\frac{n}{2}}) \\ f\left(0^{\frac{n}{2}}, 0^{\frac{n}{2}}\right) & \ldots & f(0^{\frac{n}{2}}, 1^{\frac{n}{2}}) \\ f\left(0^{\frac{n}{2}}, 0^{\frac{n}{2}}\right) & \ldots & f(0^{\frac{n}{2}}, 1^{\frac{n}{2}}) \\ \vdots & \vdots & \vdots \end{pmatrix}$$

- **Key point:** C'_f has reduced rank, so the new n qubit state $\left|\psi'_f\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{i,j} C'_f(i,j) |i,j\rangle$ has a RDM ρ' so that $S(\rho') < S(\rho)$

Our construction (formal)

- How to select subset of repeated rows?
  - Rows of C_f' selected via a 2^{ℓ}-to-1 function g: $\left[2^{\frac{n}{2}}\right] \to \left[2^{\frac{n}{2}}\right]$ (i.e., $\forall y, |g^{-1}(y)| = 2^{\ell}$ or 0)
  - That is, we define C_f' to be the matrix: $\left(C'_f\right)_{i,j} = \left(C_f\right)_{g(i),j}$ for all i, j
  - E.g., $\ell = 1$

g:



- Notice that $Rank(\rho') = Rank\left(C'_f C'^T_f\right) = Rank\left(C'_f\right) \leq 2^{\frac{n}{2}-\ell}$
- And so the entanglement entropy of new state $S(\rho') \leq \frac{n}{2} - \ell$
  - By Jensen's inequality: $S(\rho') \leq \log\left(\mathrm{rank}(\rho')\right)$

Can we *distinguish* this reduction in rank?

- Recall, C'_f is constructed by taking pseudorandom matrix C_f and selecting repeated rows via a 2^ℓ-to-1 function g
  - **Construction:** $\mathrm{g}(\mathrm{x}) = h\left(h'(x)\ mod\ 2^{\frac{n}{2}-\ell}\right)$ where $h, h': \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}$ are pseudorandom permutations
- We prove that a distinguisher that can tell apart C'_f from a uniformly random matrix can either distinguish C_f from a *truly* random matrix OR g from a *truly* random function
  - Neither can be done, as long as $\ell \leq \frac{n}{2} - \log^2 n$
  - Proof follows from quantum collision bound [Aaronson and Shi’2004][Zhandry’12]

What have we done?

- We've shown that C'_f is a pseudorandom matrix
  - But it has rank $\leq 2^{\frac{n}{2}-\ell} = \log^2 n$ if $\ell = \frac{n}{2} - \log^2 n$
- Correspondingly, the state $\left|\psi'_f\right\rangle = \sum_{i,j} \left(C'_f\right)_{i,j} |i\rangle|j\rangle$ is a PRS
- And the entanglement entropy $S(\rho') \leq \frac{n}{2} - \ell = O(\log^2 n)$
- Very different from nearly maximal entanglement in quantum t-designs!

Extension: PRS with "tunable" entanglement

- We can construct a PRS so that $S(\rho) = \Theta(k)$ for any $\log^2(\mathrm{n}) \leq k \leq n$ whp
- **Main technical hurdle:** we need to lower bound how much entanglement we start with!
  - i.e., we construct a particular PRF $f\colon \{0,1\}^n \to \{\pm 1\}$ so that the corresponding state $|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x f(x)|x\rangle$ has entanglement $S(\rho) = \Theta(n)$
- Then we can use our previous idea with a 2^ℓ-to-1 function, for suitable choice of ℓ, to give matching upper and lower bounds on entanglement

"Pseudoentanglement"

- Two ensembles of n-qubit quantum states $\{|\psi_k\rangle\}$ and $\{|\Phi_k\rangle\}$ indexed by a secret key $k \in \{0,1\}^{poly(n)}$ are $(\boldsymbol{f(n)}, \boldsymbol{g(n)})$ **−pseudoentangled** if:
  1. Given k, both $|\psi_k\rangle$ and $|\Phi_k\rangle$ are efficiently preparable by a quantum algorithm
  2. If we aren't given k the ensembles are *computationally indistinguishable*
  3. The entanglement entropy between the first $n/2$ and second $n/2$ qubits of $\{|\psi_k\rangle\}$ is $\Theta\big(f(n)\big)$ whp, whereas the entanglement entropy of $\{|\Phi_k\rangle\}$ is $\Theta(g(n))$
- **Prior work** [Gheorghiu & Hoban'20]: Assuming LWE is secure against quantum attack, there are $\big(\boldsymbol{n}, \boldsymbol{n - O(1)}\big)$**-pseudoentangled** state ensembles
  - Interestingly these ensembles *are distinguishable* from Haar
- **Our result:** Assuming any quantum secure cryptography is possible, we can construct states that are $(\boldsymbol{n}, \boldsymbol{log^2(n)})$ **-pseudoentangled**.
  - Our ensembles are also *computationally indistinguishable* from Haar random states

Open questions

- Is it possible to create pseudoentanglement using holographic states in which AdS/CFT is well-defined?
- Is it possible to construct pseudorandom quantum states to have **area law** entanglement?
  - So far, the low-entangled states we've constructed do not have a well-defined spatial geometry
- Do **sufficiently deep** random 2D spatially local quantum circuits give rise to pseudorandom states?
  - i.e., suppose I give you $(C|0^n\rangle)^{\otimes p(n)}$, without telling you the description of the random circuit C
  - Can you "feel" the difference between this and Haar random states?
- Applications of pseudoentanglement?

Thanks!