Title: Learning efficient decoders for quasi-chaotic quantum scramblers

Speakers: Lorenzo Leone

Series: Perimeter Institute Quantum Discussions

Date: November 30, 2022 - 12:30 PM

URL: https://pirsa.org/22110117

Abstract: Scrambling of quantum information is an important feature at the root of randomization and benchmarking protocols, the onset of quantum chaos, and black-hole physics.

Unscrambling this information is possible given perfect knowledge of the scrambler [ArXiv: 1710.03363].

We show that one can retrieve the scrambled information without any previous knowledge of the scrambler, by a learning algorithm that allows the building of an efficient decoder. Surprisingly, complex quantum scramblers admit Clifford decoders: the salient properties of a scrambling unitary can be efficiently described even if exponentially complex, as long as it is not fully chaotic. This is possible because all the redundant complexity can be described as an entropy, and for non-chaotic black holes can be efficiently pushed away, just like in a refrigerator. This entropy is not due to thermal fluctuations but to the non-stabilizer behavior of the scrambler.

Learning efficient decoders for quasi-chaotic quantum scramblers

Lorenzo Leone

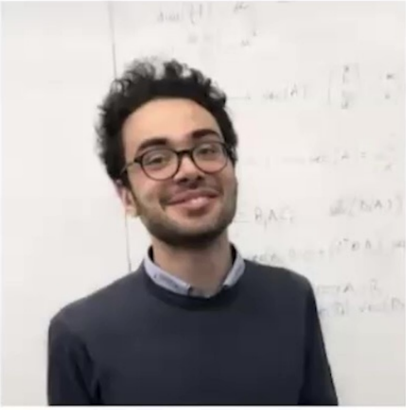
University of Massachusetts Boston
Theoretical Division (T-4), Los Alamos National Laboratory
Center for Nonlinear Studies, Los Alamos National Laboratory

Based on…

- To learn a mocking black-hole, L. Leone, S.F.E. Oliviero et. al. ArXiv: 2206.06385
- Black hole complexity, unscrambling and quantum chaos, S.F.E. Oliviero, L.Leone et. al., in preparation
- Learning efficient decoders for quasi chaotic scramblers, S.F.E. Oliviero, L.Leone et. al., in preparation

Collaborators

A. Hamma,
Univ. of Naples,
INFN



S.F.E. Oliviero,
Umass Boston

S. Lloyd,
MIT,
Turing Inc.

Introduction

- Scrambling = hide local information into non-local degrees of freedom!
- Can one recover scrambled information? Is that reversible?
- Quantum mechanics is unitary -> run the evolution backwards!
- How does quantum non-reversibility arise?
- Alternatively, can one find a mocking evolution running backwards?
- Overall, how hard is it?

Outline

Review

- Pauli group and Clifford group
- Scramblers -> Clifford good scramblers
- Decoupling theorem + Yoshida-Kitaev protocol

Main result

- Unscrambling without knowing U
- Clifford decoders for quasi-chaotic scramblers
- Proof sketch

Clifford group

- The Pauli group $\mathbb{P}$ is defined as the group generated by $\mathbb{P} = \langle \{\sigma_i^x, \sigma_i^z\}_{i=1}^{n} \rangle$

Number of qubits

2n generators

- Cardinality of the Pauli group $|\mathbb{P}| = 2^{2n} \equiv d^2$

- Local Pauli group on subsystem A $|A| + |B| = n$

$$\mathbb{P}_A := \{P_A \otimes \mathbb{I}_B\}, \quad |\mathbb{P}_A| = 2^{2|A|} = d_A^2$$

- The Clifford group Cl is the normalizer of $\mathbb{P}$ $\forall C \in \mathbb{C}, \forall P \in \mathbb{P} \quad C^\dagger P C \in \mathbb{P}$

- $\mathbb{C}_n$ is generated by: $\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $\quad H = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

* D. Gottesman, the Heisenberg representation of QC, arXiv: 9807006

non-Clifford resources

- Adding a non-Clifford gate to the set $\{\mathrm{CNOT}, H, S\}$, makes it universal for QC.
- For example, the T-gate: $$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Superposition of Pauli operators!

- Its action cannot be easily encoded: $$T\sigma_i^x T^\dagger = \frac{1}{\sqrt{2}}\sigma_i^x - \frac{1}{\sqrt{2}}\sigma_i^y$$
- Best known classical algorithm scales exponentially in the number of T-gates.*
- Only Clifford circuit polluted with $\log n$ T gates can be simulated classically

*S. Bravyi and D. Gosset, PRL 116 (250501)

Scramblers

- Scrambling = hide local information into non-local degrees of freedom!

- Scrambling unitary -> 4-Out-Of-Time-Order correlations $OTOC_4(U) = d^{-1}\,\mathrm{tr}(AD_U AD_U)$

$A, D \neq \mathbb{I}$ Local Pauli operators $D_U \equiv U^\dagger D U$

- A unitary is said to be scrambling iff* $OTOC_4(U_{scr}) = \mathcal{O}(d^{-1})$

- Clifford circuits are very good scramblers $\mathbb{E}_{U\in Cl}[OTOC_4(U)] = OTOC_4(U_{scr})$

- Cl fails to reproduce the value for higher order OTOCs, e.g. $OTOC_8(U) = \langle AB_U CD_U AD_U CB_U \rangle$

$$\mathbb{E}_{Cl}[OTOC_8(C)] = O(d^{-2}) \quad \text{vs} \quad \mathbb{E}_{U\in\mathbb{U}}[OTOC_8(U)] = O(d^{-4})$$

* D. Roberts and B. Yoshida, JHEP 121 (2017)

Scramblers

- Scrambling = hide local information into non-local degrees of freedom!

- Scrambling unitary -> 4-Out-Of-Time-Order correlations $OTOC_4(U) = d^{-1}\,\mathrm{tr}(AD_U AD_U)$

$A, D \neq \mathbb{I}$ Local Pauli operators $D_U \equiv U^\dagger D U$

- A unitary is said to be scrambling iff* $OTOC_4(U_{scr}) = \mathcal{O}(d^{-1})$

- Clifford circuits are very good scramblers $\mathbb{E}_{U\in Cl}[OTOC_4(U)] = OTOC_4(U_{scr})$

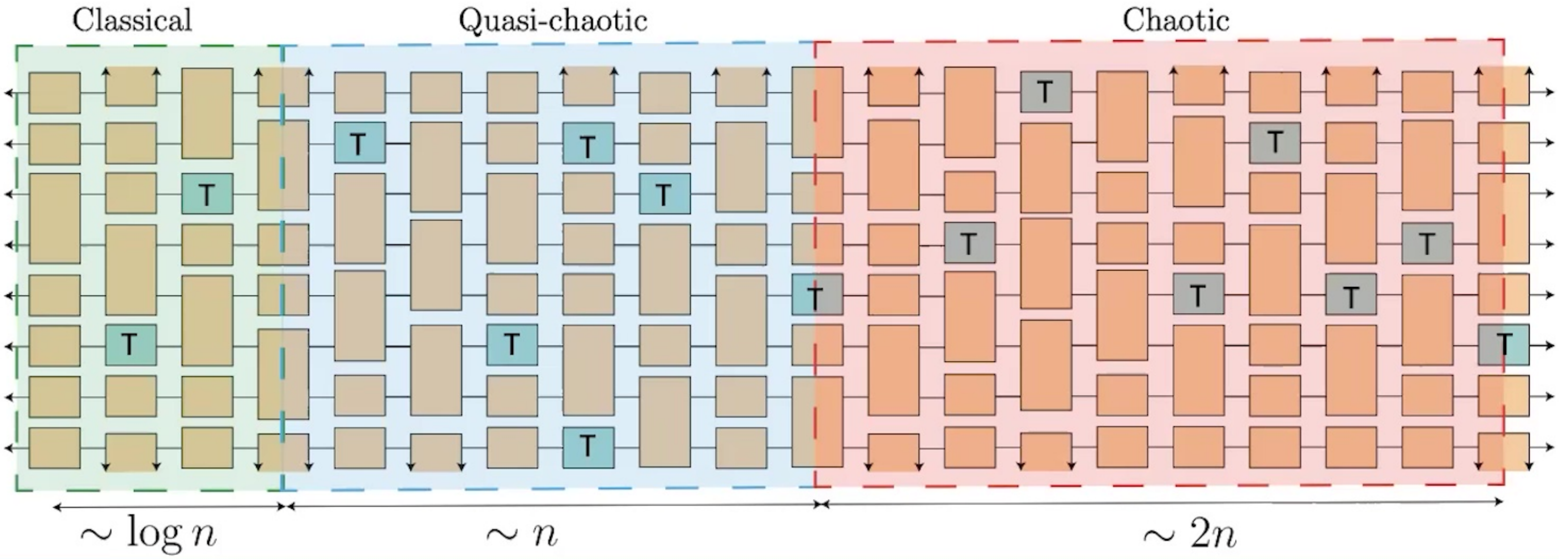
- Cl fails to reproduce the value for higher order OTOCs, e.g. $OTOC_8(U) = \langle AB_U CD_U AD_U CB_U \rangle$

$$\mathbb{E}_{Cl}[OTOC_8(C)] = O(d^{-2}) \quad \text{vs} \quad \mathbb{E}_{U\in\mathbb{U}}[OTOC_8(U)] = O(d^{-4})$$

∗ D. Roberts and B. Yoshida, JHEP 121 (2017)

T-doped Clifford scramblers

- Clifford circuits + t non-Clifford resources are scramblers for every t (typically)



‘Classical’	quasi-chaotic $t \sim n$	chaotic $t \sim 2n$
$\mathbb{E}_{t\sim\log n}[OTOC_8(U_t)] = \mathcal{O}\left(\frac{1}{d^2\,\mathrm{poly(n)}}\right)$	$\mathbb{E}_{t\sim n}[OTOC_8(U)] = \mathcal{O}\left(\frac{1}{d^3}\right)$	$\mathbb{E}_{t\sim 2n}[OTOC_8(U)] = \mathcal{O}\left(\frac{1}{d^4}\right)$

*L. Leone, S. Oliviero, A. Hamma, Quantum 5, 453 (2021)

Decoupling theorem

EPR pair

$$|\Lambda\Lambda'\rangle = \frac{1}{\sqrt{d_\Lambda}} \sum_i |i\rangle_\Lambda \otimes |i\rangle_{\Lambda'}$$

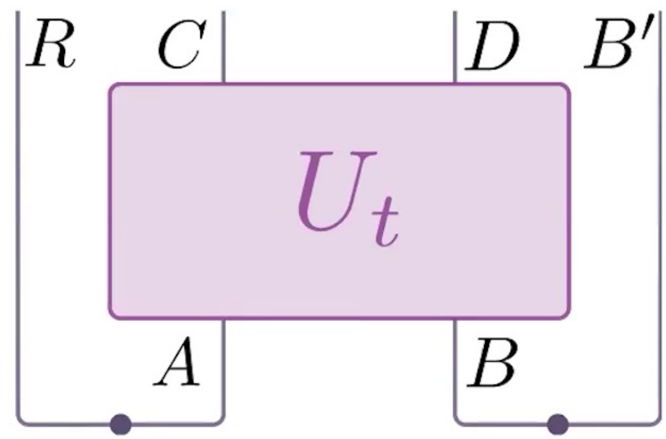
- Alice R and Bob B' share a EPR pair with the input of a scrambler

$$U_t |RA\rangle |BB'\rangle$$

- Question: how much information is in Bob's possession?

- Mutual information: $I(R|DB') := S(\rho_R) + S(\rho_{DB'}) - S(\rho_{RDB'})$

- Decoupling theorem: $|D| \geq |A| + \log \epsilon^{-1/2}$



- $I(R|C) \leq \epsilon$
- $I(R|C) + I(R|DB') = |A|$
- $I(R|DB') \geq |A| - \epsilon$

* P. Hayden, J. Preskill, JHEP 09 (2007) 120

Decoupling theorem: take-home message

If Bob looks at B' together with ANY subsystem D, with $|D| = |A| + \log \epsilon^{-1/2}$, Bob knows all about Alice R, i.e. $I(R|DB') = |A| - \epsilon$

In principle Bob can decode the information from Alice by looking only and $B' \cup D$

Yoshida-Kitaev recovery protocol (I)

- $I(R|DB') \simeq |A| \implies$ There must exist a unitary V that unscramble the information!

- Task: distill a EPR pair between R and R': $|RR'\rangle$

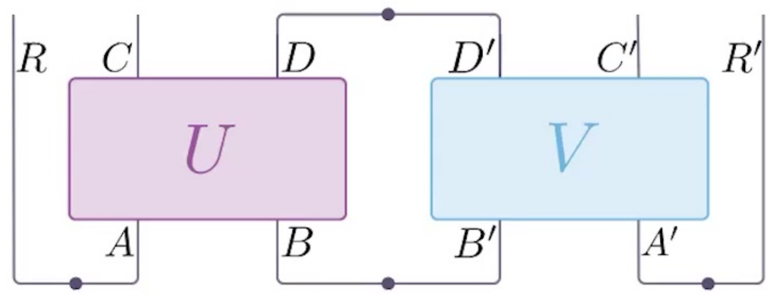
Protocol:

- Append EPR $|R'A'\rangle$
- Apply the decoder V on $B'A'$
- Project onto $|DD'\rangle$

$$|\psi_V\rangle = \frac{1}{\pi_V}|DD'\rangle\langle DD'|V_{B'A'}U_{AB}|RA\rangle|BB'\rangle|R'A'\rangle$$

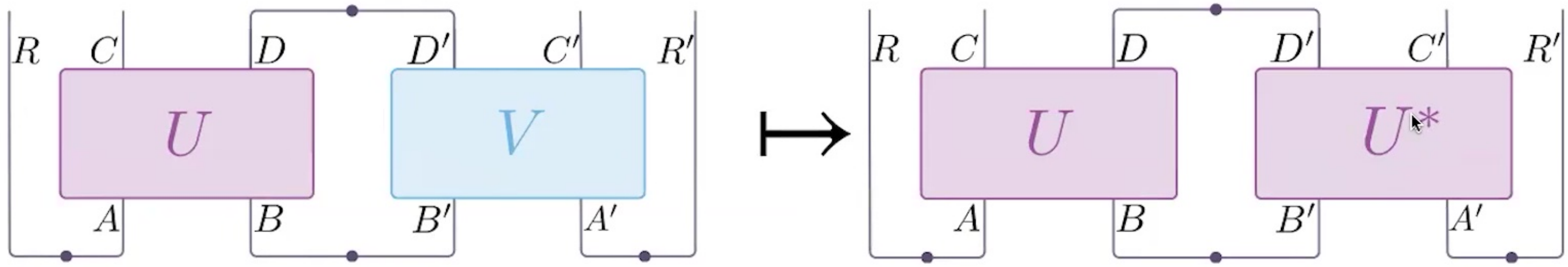
- Fidelity between $|\psi_V\rangle$ and $|RR'\rangle$

$$\mathcal{F}(V) = |\langle RR'|\psi_V\rangle|^2$$



* B. Yoshida, A. Kitaev , ArXiv: 1710.03363

Yoshida-Kitaev recovery protocol (II)



- $V \equiv U^* \implies \mathcal{F}(U^*) = 1 - \epsilon$ $\qquad \epsilon = \dfrac{d_A^2}{d_D^2}$

- It requires a complete knowledge of the scrambler U!

- Question: does unscrambling require complete knowledge of the scrambler and can be achieved by U^* only?

* B. Yoshida, A. Kitaev , ArXiv: 1710.03363

Unscrambling without knowledge of U?

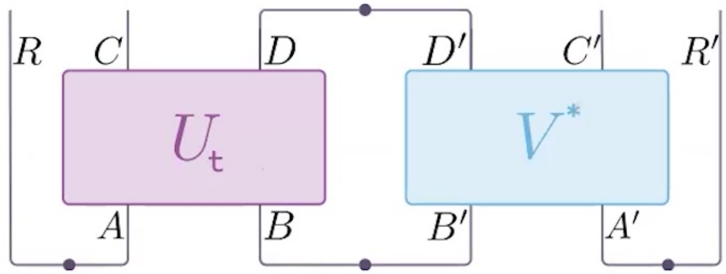
Question:

Can Bob…

1. Finite query access to U_t
2. Reading only a subsystem of the output qubit D

Unscramble the information?

Quasi-chaotic scramblers admit Clifford decoders (I)



Main claim:

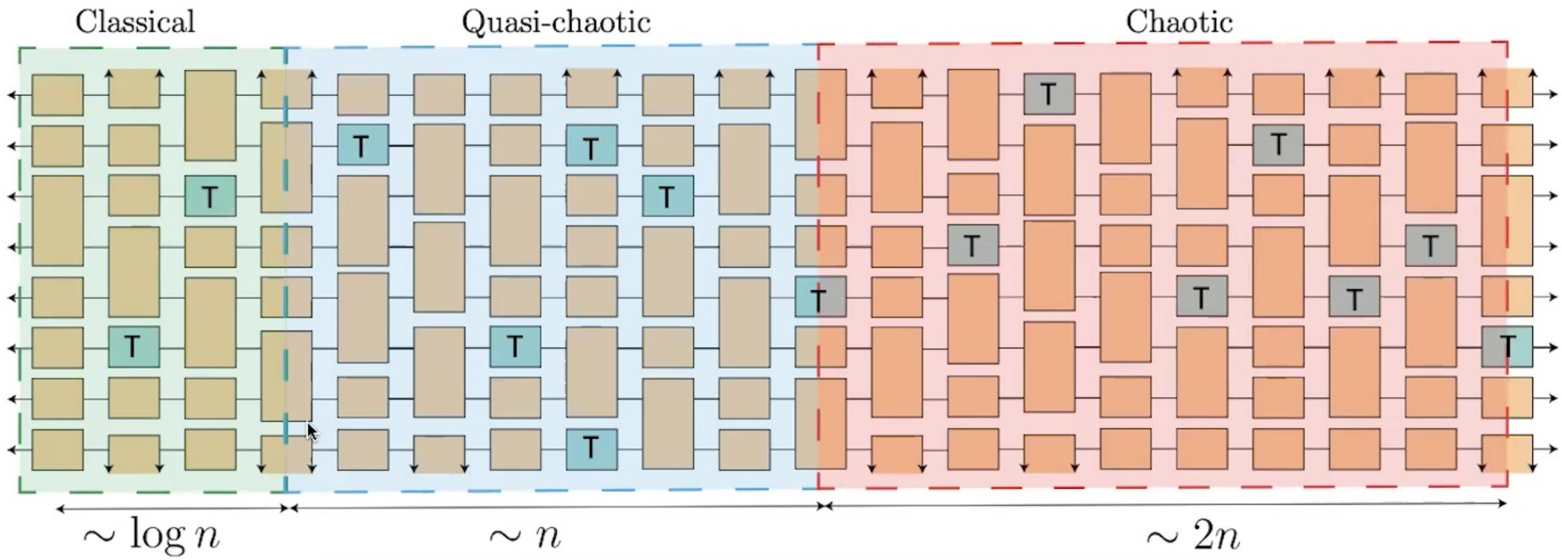
- $t < n, \quad |D| < \frac{n}{2}$
- There exists a algorithm scaling as $\mathcal{O}(\text{poly}(n)\exp(t))$ that learn a CLIFFORD OPERATOR V that unscramble the information with fidelity:

$$\mathcal{F}(V) \simeq 1 - \epsilon$$

- The probability of finding such Clifford obeys to

$$\mathcal{P}(V) \geq 1 - \exp(-\alpha n)$$

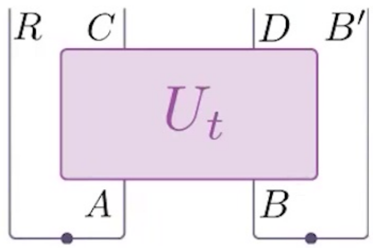
Quasi-chaotic scramblers admit Clifford decoders (II)



	'Classical'	quasi-chaotic $t \sim n$	chaotic $t \sim 2n$
Clifford-decoding	✓	✓	✗
Algorithm-cost	$\mathcal{O}(\mathrm{poly}(n))$	$\mathcal{O}(\exp(n))$	✗

T-doped Cliffords preserve a subgroup of Paulis

- Question: How to retrieve the information with a Clifford decoder?
- Bob can measure expectation values of Pauli operators in the subsystem D



$P_D \mapsto U_t^\dagger P_D U_t$ non-Pauli string in general…

Subgroup of $\mathbb{P}_D$, $|\mathbb{P}_D| = d_D^2$

- For any subsystem D $G_D(U_t) := \{P_D \in \mathbb{P}_D \,|\, U_t^\dagger P_D U_t \in \mathbb{P}\}$
- For a Clifford operator $G_D(U_0 \in Cl) \equiv \mathbb{P}_D$

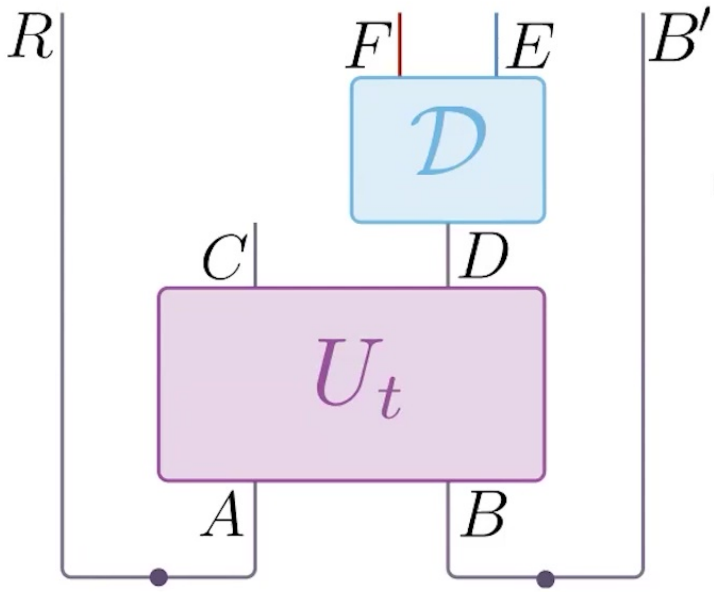
$$\boxed{|G_D(U_t)| \geq \frac{d_D^2}{2^t}}$$

- Idea: move the non-Cliffordness (non-preserved Pauli) and decode from the Clifford system

Diagonalizer operation: move non-Cliffordness away

- Simplified settings: there exist a Clifford operator

$$\boxed{\begin{array}{l} \mathscr{D} \;: D \mapsto E \cup F \\ \mathscr{D}^\dagger G_D(U_t)\mathscr{D} = \mathbb{P}_E \end{array}}$$



- If Bob measures Pauli in E, it looks like a Clifford

$$U_t^\dagger \mathscr{D}^\dagger P_E \mathscr{D} U_t \in \mathbb{P}$$

- Bob can decode looking at the joint system $E \cup B'$ if

$$|E| \geq |A| + \log \epsilon^{-1}$$

- But needs to forget about F…

- Chaotic circuits -> no way to move non-Cliffordness away!

What did we learn?

Move non-Cliffordness away with suitable Clifford operation

+

Forget non-Cliffordness

+

Decoupling theorem

=

Up to t~n, quantum scrambling is efficiently (clifford) reversible!

Conclusions and outlooks

- Quantum irreversibility arises for Cliffords doped with (at least) 2n T-gates
- Evolution (up to) quasi-chaotic quantum scramblers is Clifford-reversible
- Existence of 3 regions of complexity in t-doped Clifford circuits
- Why is that possible:

Move the non-Cliffordness away	Work in a magic-free subspace

Thanks