Decoupling with random quantum circuits

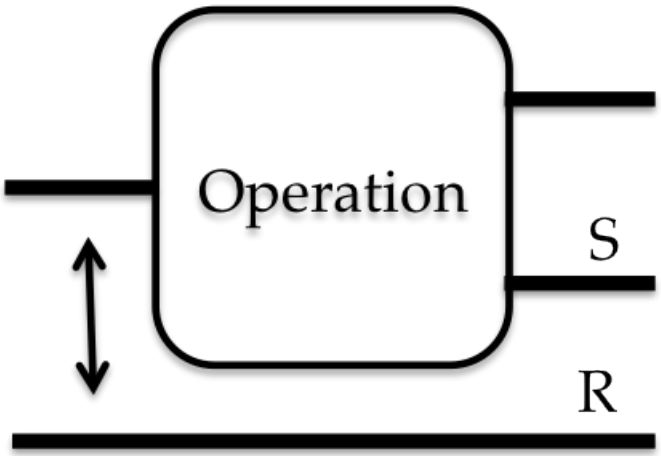
Omar Fawzi

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

joint work with Winton Brown

arXiv:1210.6644

Decoupling



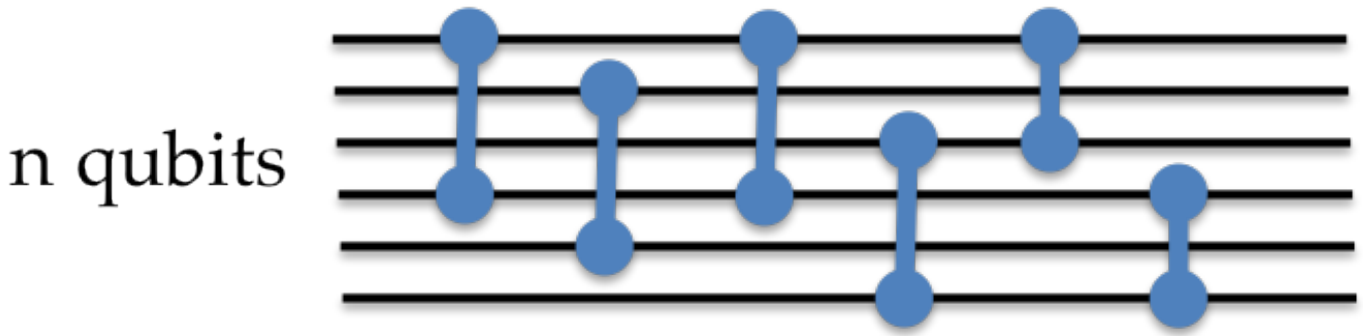
S and R are decoupled

Applications: Coding theorems, cryptography, thermodynamics,...

What operations decouple?

- Haar measure over unitary group
- (Approximate) unitary two-design
  - Random quantum circuits with $O(n^2)$ gates

Random quantum circuits



Complexity measures:

- Number of gates
- Depth (gates on disjoint pairs performed simultaneously)

Questions:

- How many gates are needed to get decoupling?
  - Between $\Omega(n)$ and $O(n^2)$
- At what depth does this happen?
  - Between $\Omega(\log n)$ and $O(n \log n)$.

Result

Theorem

Random circuits with $O(n \log^2 n)$ gates decouple *

After compression: depth $O(\log^3 n)$

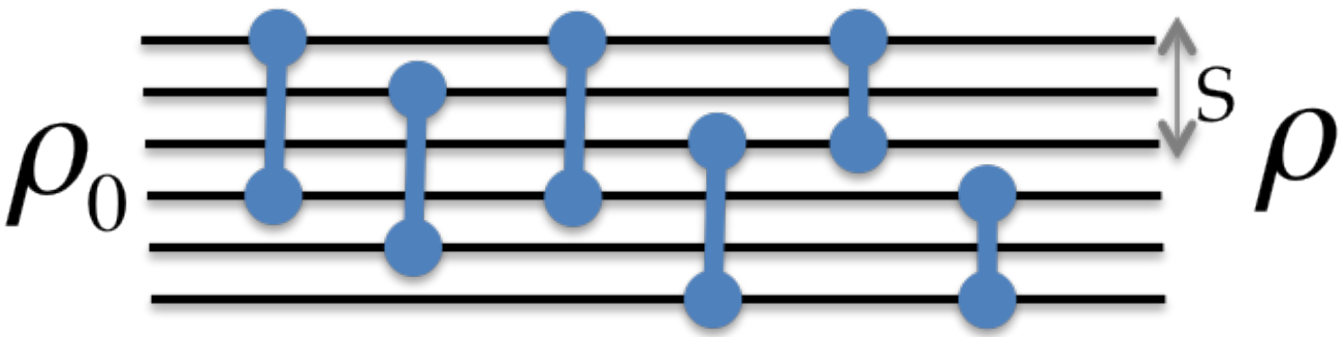
Corollary

Typical circuits of depth $O(\log^3 n)$

- *achieve capacity of erasure channel*
- *define good codes*

* : Not as general as the decoupling theorem of [Dupuis, Berta, Wullschleger, Renner, 2010]

More formal statement



Theorem

$$\mathop{\mathbf{E}}_{\textit{circuit}} \left\{ \max_{|S| \leqslant fn} \left\| \rho_S - \frac{\mathrm{id}}{2^{|S|}} \right\|_1 \right\} \leqslant \frac{1}{\mathrm{poly}(n)} + 2^{-(1-f\log 3 - h(f))n - H_2(\rho_0)}$$

Proof setup

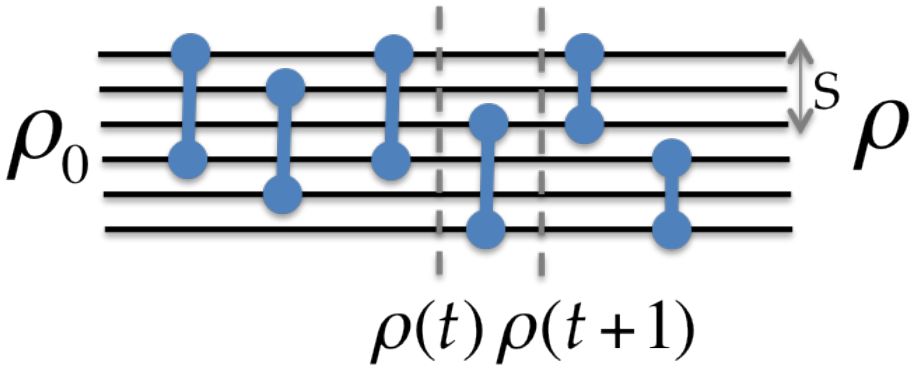
- From ℓ_1 to ℓ_2: $\left\| \rho_S - \frac{\mathrm{id}}{2^{|S|}} \right\|_1 \leqslant 2^{|S|} \operatorname{tr}[\rho_S^2] - 1$
- Expand in Pauli basis: $\rho = \frac{1}{2^n} \sum_{\nu \in \{0,1,2,3\}^n} \operatorname{tr}[\sigma_\nu \rho] \sigma_\nu$

$$\sigma_0 = \mathrm{id},\ \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

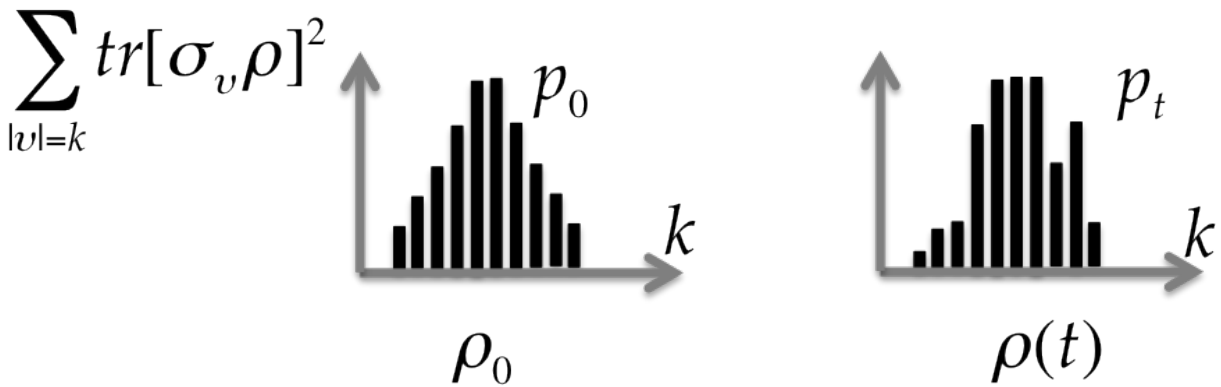
- Purity ρ: $\operatorname{tr}[\rho^2] = \frac{1}{2^n} \sum_{\nu \in \{0,1,2,3\}^n} \operatorname{tr}[\sigma_\nu \rho]^2$
- Purity ρ_S: $\operatorname{tr}[\rho_S^2] = \frac{1}{2^{|S|}} \sum_{\nu \in \{0,1,2,3\}^S} \operatorname{tr}[\sigma_\nu \rho]^2 \leqslant \frac{1}{2^{|S|}} \sum_{|\nu| \leqslant |S|} \operatorname{tr}[\sigma_\nu \rho]^2$

$$\text{Objective: } \mathop{\mathbf{E}}_{\text{circuit}} \left\{ \sum_{1 \leqslant |\nu| \leqslant fn} \operatorname{tr}[\sigma_\nu \rho]^2 \right\} \leqslant \epsilon$$

Evolution of the distribution of weights

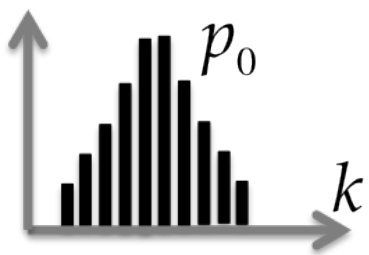


- $\mathrm{tr}[\rho(t+1)^2] = \mathrm{tr}[\rho(t)^2] = \mathrm{tr}[\rho_0]^2$
- Distribution $p_t(k) = \dfrac{\sum_{|\nu|=k} \mathbf{E}\{\mathrm{tr}[\sigma_\nu \rho(t)]^2\}}{\mathrm{tr}[\rho^2]}$

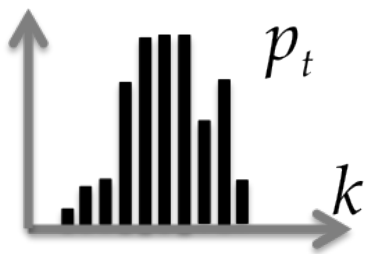


Evolution as a Markov chain

$$\sum_{|\upsilon|=k} tr[\sigma_\upsilon \rho]^2$$



ρ_0



$\rho(t)$

Distribution $p_t(k) = \dfrac{\sum_{|\nu|=k} \mathbf{E}\{\mathrm{tr}[\sigma_\nu \rho(t)]^2\}}{\mathrm{tr}[\rho^2]}$

$p_0 - p_1 - \cdots - p_t$ distributions of Markov chain on $\{1, \ldots, n\}$

Transition probabilities:

$$P(x,y) = \begin{cases} 1 - \frac{2x(3n-2x-1)}{5n(n-1)} & \text{if } y = x \\ \frac{2x(x-1)}{5n(n-1)} & \text{if } y = x-1 \\ \frac{6x(n-x)}{5n(n-1)} & \text{if } y = x+1 \\ 0 & \text{otherwise.} \end{cases}$$

Studying the Markov chain

$X_0, \ldots, X_t, \ldots$ Markov chain transition P

Objective: Analyse $\mathbf{P}\{X_t \leqslant fn\}$ as a function of X_0

Theorem

If $X_0 = \ell$ *and* $t > cn \log^2 n$,

$$\mathbf{P}\{X_t \leqslant fn\} \lesssim \mathbf{P}\{\textit{Stat. dist.} \leqslant fn\} + \frac{1}{3^\ell \binom{n}{\ell}} \frac{1}{\mathrm{poly}(n)}$$

- Mixing time bound only works for $t > cn^2$
- The dependence in ℓ is optimal
  - It is possible that $t > cn \log n$ is sufficient

References

Talk based on

- Brown, Fawzi, *Scrambling speed of random quantum circuits*, 2012 `arXiv:1210.6644`

Some other references

- Abeyesinghe, Devetak, Hayden, Winter, *The mother of all protocols: reconstructing quantum information's family tree*, 2006
- Dupuis, Berta, Wullschleger, Renner, *The decoupling theorem*, 2010
- Harrow, Low, *Random Quantum Circuits are Approximate 2-designs*, 2008
- Oliveira, Dahlsten, Plenio, *Efficient Generation of Generic Entanglement*, 2006
- Szehr, Dupuis, Tomamichel, Renner, *Decoupling with unitary almost two-designs*, 2012