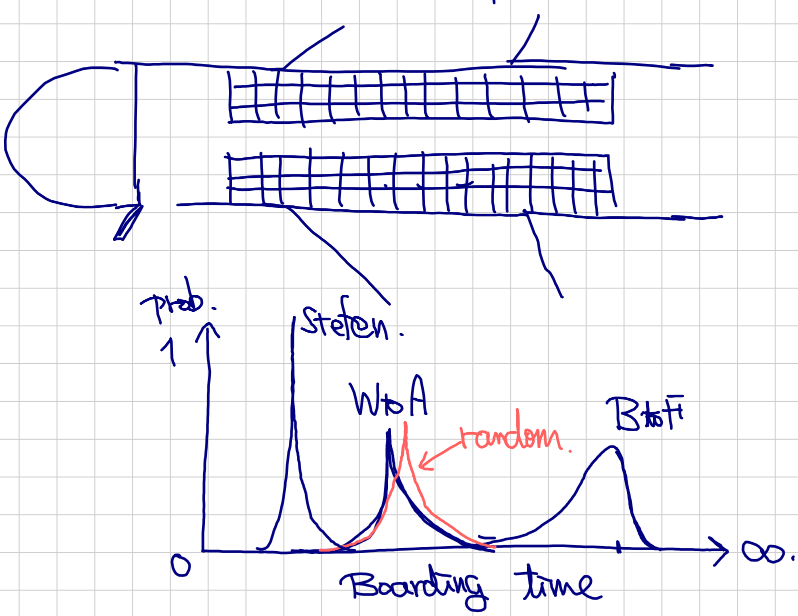
量子ランダムネス入門.

- 量子で乱数生成する話ではない
- 実は CUE とその近似の話

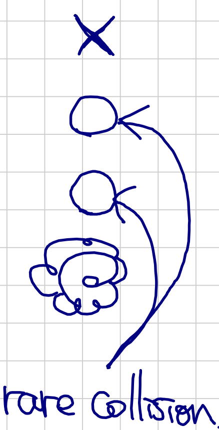
0. 初めまして、ランダムネス.
1. 量子ランダムネス : random state と random unitary.
2. 量子疑似ランダムネス : state design と unitary design.
   ↪ Algorithm.

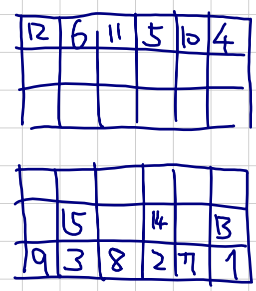
0.0. Random strategy.

How to board on airplain faster ?



1. Back to Front. ✕
2. Window to Aisle. ○
3. Random. ○
4. Stefen.





Good & bad in randomness

→ あまり構造がなく サイズが大きい難問

✔ Best ではないが、大体よい　（たまに全然だめ）.

△ サイズ : 大.

✕ 問題の構造をうまく反映した protocol にはかなわない.
　↪ 上でランダム !!.

0.1 Applications of randomness.

- 計算 : モンテカルロ法, sorting, prime check, etc...
  ゲーム !!
  sorting: ↖ n] worst : $\Theta(n^2)$
  randomized : $\Theta(n \log n)$.
  prime check: $\log^{7.5}(n) \longrightarrow \log^2(n)$
- 通信 : ランダムな符号化 (proof technique).
  暗号.

0.2. ランダムネスと擬似ランダムネス.

乱数 ⇒ これまでの値から次のbitを予測不可.

↳ e.g.) サイコロ etc.... ← ニュートン力学で計算可る

擬似乱数 ⇒ ランダムにみえるが確定的アルゴリズムで得られる.

"シーズ"を増幅 ↙

↳ e.g.) メルセンヌ・ツイスター, Xorshift etc.

⇒ これらの量子版を考える!!

Application

- 計算 : Q. supremacy. query complexity.
- 計測 : Q. device check., Q. sensing.
  [randomized benchmarking, Google method]
- 通信 : Q. random encoder., proof technique.
  data-hiding, Q. one-time pad etc....
- 物理 : Q. chaos., OTOC, scrambling etc....

1. Q. randomness. とは?

1-1. Random state.

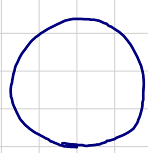
古典 : N random bit $\underbrace{0110\cdots\cdots}_{N}0 \in \{0,1\}^N$. ← uniform

量子 : N "random qubit" $|0110\cdots 0\rangle \in (\mathbb{C}^2)^{\otimes N}$. ← Not uniform (no ent. etc...)

↖ ダメ.

What is uniform?

e.g.) S^1



uniform distribution = 回転不変

⇓

ユニタリ不変

Q. state = complex unit vector.

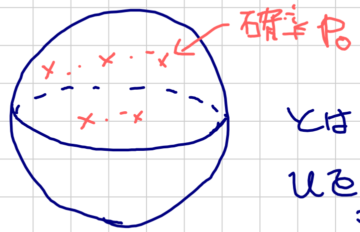
A Haar random state of N qubits.

$\overset{\text{def.}}{\Longleftrightarrow}$ A distribution $\{|\psi_\mu\rangle\}_\mu$ s.t. $\forall U \in \mathcal{U}(2^N)$, $\{U|\psi_\mu\rangle\}_\mu = \{|\psi_\mu\rangle\}_\mu$

↑ probability

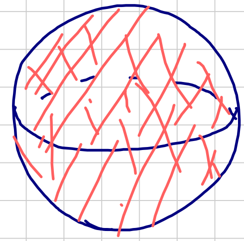
---

e.g.) 1 qubit ..... Bloch 球.



とはかけない。

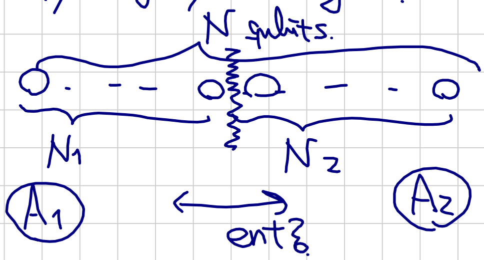
μをかけると
変わってしまう。



連続的.

1-2. Properties.

- Extremely highly entangled.



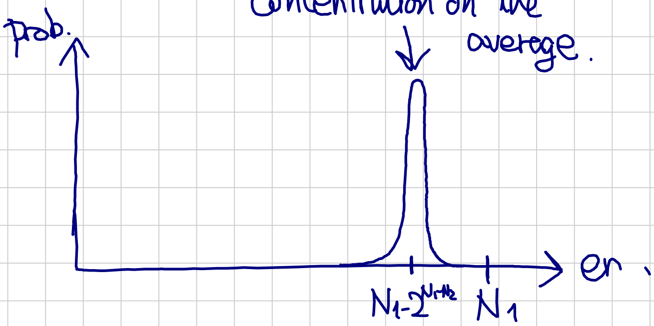
$$\{|\psi_\mu\rangle\}_\mu \xmapsto{Tr_{A_2}} \{\rho_\mu\}_\mu$$

> 1. ほとんど maximal.
> 2. でも、max ではない。

$$N_1 \geq \int S(\rho_\mu)\, d\mu \geq N_1 - 2^{N_1 - N_2}$$

$\int S(\rho_\mu)\, d\mu$ // $\mathbb{E}[S(\rho_\mu)]$

[Page 93
HLW 16]



$\Rightarrow$ Thermalization との関連.
[PSW06]

- Concentration phenomena.

Levy's lemma [Led01]

f : function on $\mathbb{C}^d$ ..

(Lipschitz continuous)

$$\text{Prob.}\left[\, |f - \mathbb{E}[f]| \geq \delta \,\right] \leq \exp\left[- C_f \frac{d}{\delta^2} \right].$$

(C_f: small const. dep. on f.)

N qubitsだと
$d = 2^N$ ..... wow!!

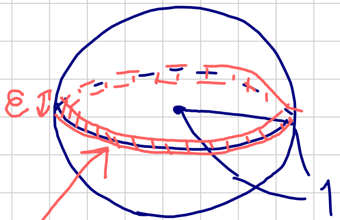
$\Rightarrow$ なので、random state は"大体"みんな同じ。

直感: State on N qubits $\simeq S^{2\times 2^N - 1 =: D}$

単位超球の表面.

volume $\frac{\pi^{D/2}}{\Gamma(\frac{D}{2}+1)} \xrightarrow{D\to\infty} 0.$

ガンマ関数 $\sim (\frac{D}{2}+1)!$ ($D/2 \in \mathbb{Z}$の場合)



D:大だと、"赤道"がほぼ全て。(でも、どの赤道でもよい…)

Surface area $\xrightarrow{D\to\infty} 0$.

⇒ fの赤道の値だけを考えれば十分

concentration.

1-3 Random unitary.

Stateはどうせ Unitaryで作る!! ⇒ unitaryを考えよう.

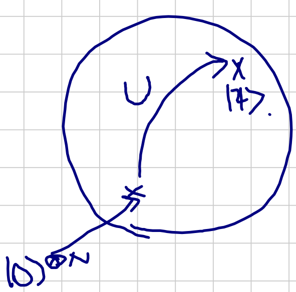
A Haar random unitary (CUE)

$\overset{\text{def}}{\Longleftrightarrow}$ 〃 〃 $\{U_\mu\}_\mu$ s.t. $\forall V \in \mathcal{U}(2^N)$, $\{VU_\mu\}_\mu = \{U_\mu V\}_\mu = \{U_\mu\}_\mu$

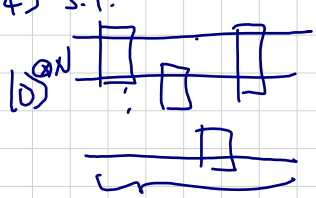
※ Random unitary > random states.

- random unitaryがあれば random states を作れる.
- random state を $|0\rangle^{\otimes N}$から作れる unitary が Haar random とは限らない.

⇒ 実装は inefficient !!



$\exists|\psi\rangle$ s.t.



$\geq 2^N$ gates.

[Nielsen & Chuang].

↳ Haar random = "uniform" なので、作れない state はないはず.

本当は measure zero じゃないとか近似とかの話がいる

∴ Haar needs $\geq 2^N$ gates.

近似を考えよう ⇒ **design**

2. Q. pseudo-randomness.

2-1. State t-design & unitary t-design.

Idea: functions on $(\mathbb{C}^2)^{\otimes N}$ or $\mathcal{U}(2^N)$ are important.
↳ polynomials.

e.g.)
- entropy
- meas. outcome
- exp. value.

note: functions on a group = Harmonic analysis.
(group ← irrep)
⇓
Design theory.

In the following, only unitary is concerned.

Def) Monomial of degree (t,t) $(t \in \mathbb{N})$ of $\mathcal{U} = (\mathcal{U}_{\alpha\beta})_{\alpha,\beta}$.
$\Leftrightarrow$ monomial of degree t in $\{\mathcal{U}_{\alpha\beta}\}_{\alpha,\beta}$
& 〃 〃 〃 t in $\{\mathcal{U}^*_{\alpha\beta}\}_{\alpha,\beta}$. ← complex conjugate

e.g.) $\mathcal{U}_{13}\mathcal{U}_{42}\mathcal{U}^*_{54}\mathcal{U}^*_{23}$ .... (2,2)-monomial.
↖ Q.I. では $U \rho U^\dagger$ なので、(t,t) で十分.

Def) Unitary t-design is $\{\mathcal{U}_i\}_{i=1}^K$ [Low 10]

$\overset{\text{def}}{\Leftrightarrow}$ $\forall f$: monomial, $\frac{1}{K}\sum_{i=1}^{K} f(\mathcal{U}_i) = \mathbb{E}_{\text{Haar}}[f(\mathcal{U}_i)]$ (monomial)
↖
- Haar random の "t次" までを再現.
- "$\forall f$" はちょっとイヤ.

$\Leftrightarrow$ $\frac{1}{K}\sum_{i=1}^{K} \mathcal{U}_i^{\otimes t} \otimes \mathcal{U}_i^{*\otimes t} = \mathbb{E}_{\text{Haar}}[\mathcal{U}_i^{\otimes t} \otimes \mathcal{U}_i^{*\otimes t}]$ (TPE)
(matrix element)
↖ 物理的意味?

$\Leftrightarrow$ $\mathcal{G}^{(t)}_{\{\mathcal{U}_i\}}(\rho) := \mathbb{E}_{\{\mathcal{U}_i\}}[U_i^{\otimes t} \rho\, U_i^{\dagger\otimes t}]$ ← CPTP map $(\rho \in \mathcal{L}(\mathcal{H}^{\otimes t}))$.
$\mathcal{G}^{(t)}_{\{\mathcal{U}_i\}} = \mathcal{G}^{(t)}_{\text{Haar}}$ (Diamond)
↖ t-copy あっても見分けがつかないよ. (相関をみている).
↖ ぶーつーりー.

$\Leftrightarrow \quad P_t(\{U_i\}) := \frac{1}{K^2}\sum_{i,j=1}^{K} \left| \mathrm{Tr}[U_i U_j^\dagger] \right|^{2t}$: frame potential of order t.

$\quad \| $

$P_t(\mathrm{Haar}) = t!$ $(d \geq t \,\&\, d > 2)$ [GAE07]

↑

- For any $\{U_i\}$, $F_t(\{U_i\}) \geq F_t(\mathrm{Haar})$ potential!!
- 内積を最小に!! ⇔ uniform.
- OTOC の"平均" [RY17]

↳ State t-design は $\{U_i|0\rangle^{\otimes N}\}_i$ で作る.

$\qquad\qquad\qquad\qquad\qquad \| $

$\qquad\qquad\qquad\qquad\quad |\psi_i\rangle$

$$\frac{1}{K}\sum_{i=1}^{K} |\psi_i\rangle\langle\psi_i|^{\otimes t} = \mathbb{E}_{\mathrm{Haar}}\left[|\psi\rangle\langle\psi|^{\otimes t}\right]$$

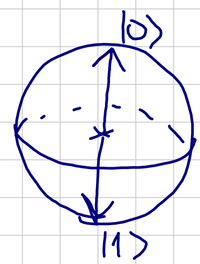
$$= \frac{P_{sym}}{d_{sym}} \leftarrow \text{symmetric subspace.}$$

↑ Schur's lemma

2-2. Examples.

- State t-design (1 qubit).

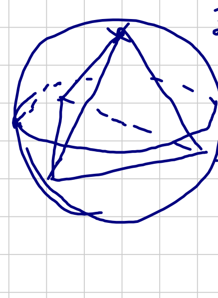
$\underline{t=1}$ $\quad \mathbb{E}_H[|\psi\rangle\langle\psi|^{\otimes 1}] = I/2.$



$\{|0\rangle, |1\rangle\}$

$\{|+\rangle, |-\rangle\}$ etc.

$\underline{t=2}$ $\quad \mathbb{E}_H[|\psi\rangle\langle\psi|^{\otimes 2}] = \frac{\Pi_{triplet}}{3}$

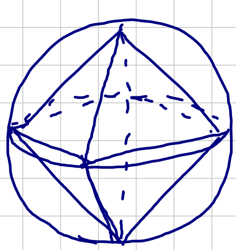


正四面体

- $(0, 0, 1)$
- $(\sin\theta, 0, \cos\theta)$
- $(\sin\theta\cos\frac{2\pi}{3}, \sin\frac{2\pi}{3}, \cos\theta)$
- $(\sin\theta\cos\frac{4\pi}{3}, \sin\frac{4\pi}{3}, \cos\theta)$

where $\cos\theta = \frac{1}{3}$

$\underline{t=3}$



正八面体.

どんどん uniform

$t \to \infty$ で大体 Haar になる.

- Unitary t-design (Diamond or F.P. が楽).

$\underline{t=1}$ $\quad \frac{1}{K}\sum_i U_i \rho U_i^\dagger = \mathrm{Tr}[\rho]\frac{I}{d}$ であればよい. e.g.) Pauli grp. etc...

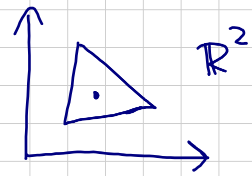
$t=2$ Clifford grp.

$t=3$. $\mathcal{U}(2^N)$ の場合. Clifford grp.
（次2が重要.）

↳ これ以上になると、"accidental" にしかみつかっていない.
（かった）
[ONK, before prep.]

- If $d \geq 5$ ($\mathcal{U}(d)$) & $t \geq 4$, ∄ t-design that is a group.
[BNRT18]

- Existence follows from Caratheodory's thm



[$\mathbb{R}^d$内の convex hull に属する点xは $d+1$点の確率混合でかける]
↳ TPE def に使えばよい.

2-3. Simple facts.

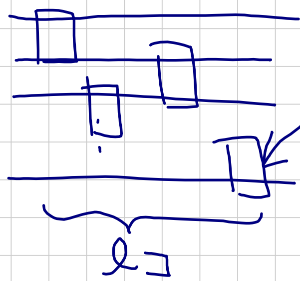
- t-design ⇒ (t−1)-design.
- $\{\mathcal{U}_i\}_{i=1}^K$: t-design on $\mathcal{U}(d)$ ⇒ $K \geq d^{2t} - o(d^{2t})$
- In most applications in Q.I.T., 2-designs are enough.
  ↳ t-des. が必要かつ有用な application?
  { • compressed sensing., query complexity.
    • Q. chaos.
- "Exact" implementations of t-designs are still hard.....
  ↳ Approximate t-des. が重要.
  $\|$Def の L.H.S. − R.H.S.$\| \leq \varepsilon$.
  ⇒ 各defで少し異なる (が、多くの場合はムシできる).

2-4 Quantum circuits for unitary t-designs on N qubits.

How many gates?

✓ Lower bound :

$\{U_i\}_{i=1}^{K}$: t-des. $\Rightarrow$ $K \geq d^{2t} = 2^{2Nt}$.



S コの中から選ぶ $\Rightarrow$ S^{l} コのユニタリを作れる.

$\therefore$ $S^{l} \geq 2^{2Nt}$

$\Leftrightarrow$ $\boxed{l \geq \frac{2}{\log S} \times Nt}$

↳ 少なくとも Nt コは必要.

t=2 の場合 ⇒ Clifford grp を使える. (exact!!)

Best known : $O(N \log N)$ gates [CLLW16].

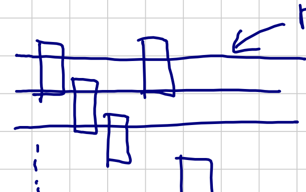
t≥3 の場合 : 基本は ε-approximate

	HL09	BHH16	NHKW17
method	Expander graph + Fourier	Local random circuit	Diagonal + Hadamard
# of gates	$O(t^3N^3)$	$O(t^{10}N^2)$	$O(tN^2)$
works if	$t = O\left(\frac{N}{\log N}\right)$	$t = O(\text{poly}(N))$	$t = o(\sqrt{N})$
Architecture	All-to-all	nearest-neighbor (1D)	All-to-all

↳ 超伝導 qubit (Google)

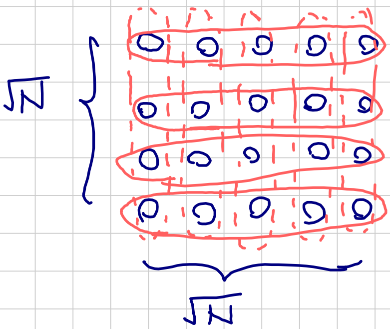
↳ NMR.

近年の発展あり.



randomな2 qubit gateを randomな N.N. qubitsにかける.

D=2 (N qubits)



step1. 横方向で LRC. $O((\sqrt{N})^2)\times\sqrt{N} = O(N^{3/2})$ で t-des.

step2. 縦方向で LRC. 〃 〃 〃

step3. Repeat 1 & 2 $t\log t$ times.

⇒ 全体で t-design!!

# of gates $=$ poly$(t)\times N^{3/2}$.

↳ 一般のD次元へ拡張 : $\mathrm{poly}(t)\times N^{\frac{2}{D}}\times N^{\frac{D-1}{D}} = \mathrm{poly}(t)\times N^{1+\frac{1}{D}}$

($N^{\frac{2}{D}}$ ↑ 各方向の design.) ($N^{\frac{D-1}{D}}$ ↑ "各方向"の本数.)

(ただし, $D = O(\frac{\log N}{\log\log N})$)

⇓

$O(N\log N)$ までは到達可. [HM18]

t 依存性は?
- 少なくとも $t^{11}\log t$.
- t^D になるのか? (論文の書き方が……)

3. まとめ..

情報の scrambling. recovery.

量子情報
- Killer application?
- Q. randomized algorithm?

物理 → 量子(擬似)ランダムネス

- Thermalization (ETH)
- Q. chaos (OTOC)
- Black hole (scrambling)

数学.
- 拡張.

t-design を def したけど, 2-des. で十分なことが多い

1と2の間を知りたい!!

I. VARIOUS DEFINITIONS OF DESIGNS

It is summarized very well in [Low10]. For the frame potential, see [GAE07, Zhu15, RY17].

II. PROPERTIES OF HAAR AND DESIGNS

- Extremely highly entangled [Lub78, Pag93, FK94, HLW06].
- Anti-concentration property [HBVSE18]
- Concentration of measure phenomena [Led01, Mec14]. In the context of quantum information, it is also well-summarized in [PSW06, HLW06]. State and unitary designs also have a "concentration" properties [Low09].
- No existence of exact unitary designs, which form a group, when $d \geq 5$ and $t \geq 4$ [BNRT18].

III. EFFICIENT IMPLEMENTATIONS OF UNITARY DESIGNS

- Up to unitary 2-designs [DLT02, BWV08, WBV08, GAE07, TGR07, DCEL09, HL09b, DJ11, BWV08, WBV08, CLLW16, NHMW17]. The best method based on the Clifford circuits is [CLLW16]. Clifford group on qubits was also shown to be a unitary 3-design but not to be a 4-design [Zhu15, Web16, ZKGG16]. However, as far as I know, no efficient implementations of 3-designs based on Clifford circuits are known (but perhaps straightforward to construct).
- Quantum tensor product expander [HL09a].
- Local random circuits [BHH16, HM18].
- Random diagonal-unitaries in two complementary bases [NHKW17].

IV. APPLICATIONS OF QUANTUM RANDOMNESS

- Quantum computation
  - Any element of an approximate unitary 3-design is useful [BH13]
  - Quantum supremacy by local random circuits [BFNV18] (see also [BHH16] about the proof that the local random circuits form a unitary design)
- Checking the devices that are experimentally implemented
  - Randomised benchmarking [DCEL09, EAŻ05, KLR+08, MGE11, MGE12, Fla17]
- Quantum sensing
  - SIC-POVM [RBKSC04] (a good basis for quantum tomography with a special property)
  - Random *bosonic* states are useful in quantum metrology [OAG+16]
  - Compressed sensing [KRT14, KL15, KZG16]
- Quantum information theory

- Decoupling approach [Dev05, DW04, GPW05, ADHW09, Hay12, DBWR14, SDTR13, HM14]. See especially [DBWR14] and [Dup10].
- A proof technique to construct a counterexample to the additivity conjecture [Has09] (one of the most "shocking" results in quantum information science).
- Data-hiding [TDL01, DLT02]
- Quantum one-time pad [BaO12]

- Fundamental problems in physics
  - Quantum thermodynamics [PSW06, GLTZ06, Rei08, dRAR+11, dRHRW14]
  - Black hole information science [HP07, SS08, Sus11, LSH+13, Sus14, HQRY16, RY17]
  - Strongly correlated many-body physics [BaH13]

[ADHW09] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, *The mother of all protocols : Restructuring quantum information's family tree*, Proc. R. Soc. A **465** (2009), 2537.

[BaH13] F. G. S. L. Brandão and M. Horodecki, *An area law for entanglement from exponential decay of correlations*, Nat. Phys. **9** (2013), no. 11, 721–726.

[BaO12] F. G. S. L. Brandão and J. Oppenheim, *Quantum One-Time Pad in the Presence of an Eavesdropper*, Phys. Rev. Lett. **108** (2012), no. 4, 040504.

[BFNV18] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, *Quantum Supremacy and the Complexity of Random Circuit Sampling*, 2018, arXiv: 1803.04402.

[BH13] F. G. S. L. Brandão and M. Horodecki, *Exponential Quantum Speed-ups are Generic*, Q. Inf. Comp. (2013), no. 13, 0901.

[BHH16] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Local Random Quantum Circuits are Approximate Polynomial-Designs*, Commun. Math. Phys. **346** (2016), no. 2, 397–434.

[BNRT18] E. Bannai, G. Navarro, N. Rizo, and P. H. Tiep, *Unitary t-groups*, 2018, arXiv: 1810.02507.

[BWV08] W. G. Brown, Y. S. Weinstein, and L. Viola, *Quantum pseudorandomness from cluster-state quantum computation*, Phys. Rev. A **77** (2008), no. 4, 040303(R).

[CLLW16] R. Cleve, D. Leung, L. Liu, and C. Wang, *Near-linear constructions of exact unitary 2-designs*, Quant. Info. & Comp. **16** (2016), no. 9 & 10, 0721–0756.

[DBWR14] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, *One-shot decoupling*, Commun. Math. Phys. **328** (2014), 251.

[DCEL09] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, Phys. Rev. A **80** (2009), 012304.

[Dev05] I. Devetak, *The private classical capacity and quantum capacity of a quantum channel*, IEEE Trans. Inf. Theory **51** (2005), no. 1, 44–55.

[DJ11] I. T. Diniz and D. Jonathan, *Comment on "Random quantum circuits are approximate 2-designs"*, Commun. Math. Phys. **304** (2011), 281.

[DLT02] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, *Quantum data hiding*, IEEE Trans. Inf. Theory **48** (2002), 580.

[dRAR+11] L. del Rio, J. Aberg, R. Renner, O. Dahlsten, and V. Vedral, *The thermodynamic meaning of negative entropy*, Nature **474** (2011), no. 7349, 61–63.

[dRHRW14] L. del Rio, A. Hutter, R. Renner, and S. Wehner, *Relative thermalization*, 2014, arXiv:1401.7997.

[Dup10] F. Dupuis, *The decoupling approach to quantum information theory*, Ph.D. thesis, Université de Montréal, 2010, arXiv:1004.1641.

[DW04] I. Devetak and A. Winter, *Relating Quantum Privacy and Quantum Coherence: An Operational Approach*, Phys. Rev. Lett. **93** (2004), no. 8, 080501.

[EAŻ05] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators*, J. Opt. B: Quantum semiclass. opt. **7** (2005), S347–S352.

[FK94] S. K. Foong and S. Kanno, *Proof of Page's conjecture on the average entropy of a subsystem*, Phys. Rev. Lett. **72** (1994), no. 8, 1148–1151.

[Fla17] S. Flammia, *Characterization of quantum devices*, `https://www.microsoft.com/en-us/research/wp-content/uploads/2017/09/2017-01-14-Morning-Tutorial-Steve-Flammia-2.pdf`, 2017, Accessed: 2019-3-17.

[GAE07] D. Gross, K. Audenaert, and J. Eisert, *Evenly distributed unitaries: On the structure of unitary designs*, J. of Math. Phys. **48** (2007), no. 5, 052104.

[GLTZ06] S. Goldstein, J. L. Lebowitz, R. Tumulka, and N. Zanghí, *Canonical Typicality*, Phys. Rev. Lett. **96** (2006), no. 5, 050403.

[GPW05] B. Groisman, S. Popescu, and A. Winter, *Quantum, classical, and total amount of correlations in a quantum state*, Phys. Rev. A **72** (2005), no. 3, 032317.

[Has09] M. B. Hastings, *Superadditivity of communication capacity using entangled inputs*, Nature Physics **5** (2009), no. 4, 255–257.

[Hay12] P. Hayden, *Decoupling: A building block for quantum information theory*, `http://qip2011.quantumlah.org/images/QIPtutorial1.pdf`, 2012, Accessed: 2017-3-30.

[HBVSE18] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, *Anticoncentration theorems for schemes showing a quantum speedup*, Quantum **2** (2018), 65.

[HL09a] A. W. Harrow and R. A. Low, *Efficient Quantum Tensor Product Expanders and k-Designs*, Proc. RANDOM'09, Lecture Notes in Computer Science, no. 5687, Springer Berlin Heidelberg, 2009, pp. 548–561.

[HL09b] A. W. Harrow and R. A. Low, *Random quantum circuits are approximate 2-designs*, Commun. Math. Phys. **291** (2009), 257.

[HLW06] P. Hayden, D. W. Leung, and A. Winter, *Aspects of Generic Entanglement*, Commun. Math. Phys. **265** (2006), no. 1, 95–117.

[HM14] C. Hirche and C. Morgan, *Efficient achievability for quantum protocols using decoupling theorems*, Proc. 2014 IEEE Int. Symp. Info. Theory, 2014, p. 536.

[HM18] A. Harrow and S. Mehraban, *Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates*, 2018, arXiv: 1809.06957.

[HP07] P. Hayden and J. Preskill, *Black holes as mirrors: quantum information in random subsystems*, J. High Energy Phys. **2007** (2007), no. 09, 120.

[HQRY16] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, *Chaos in quantum channels*, J. High Energy Phys. **2016** (2016), no. 2, 4.

[KL15] S. Kimmel and Y.-K. Liu, *Quantum compressed sensing using 2-designs*, 2015, arXiv:1510.08887.

[KLR$^+$08] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A **77** (2008), no. 1, 012307.

[KRT14] R. Kueng, H. Rauhut, and U. Terstiege, *Low rank matrix recovery from rank one measurements*, 2014, arXiv:1410.6913.

[KZG16] R. Kueng, H. Zhu, and D. Gross, *Distinguishing quantum states using Clifford orbits*, 2016, arXiv:1609.08595.

[Led01] M. Ledoux, *The Concentration of Measure Phenomenon*, American Mathematical Society Providence, RI, USA, 2001.

[Low09] R. A. Low, *Large deviation bounds for k-designs*, Proc. R. Soc. A **465** (2009), no. 2111, 3289.

[Low10] R. A. Low, *Pseudo-randomness and learning in quantum computation*, Ph.D. thesis, University of Bristol, 2010, arXiv:1006.5227.

[LSH$^+$13] N. Lashkari, D. Stanford, M. Hastings, T. Osborne, and P. Hayden, *Towards the fast scrambling conjecture*, J. High Energy Phys. **2013** (2013), no. 4, 22.

[Lub78] Elihu Lubkin, *Entropy of an n-system from its correlation with a k-reservoir*, J. of Math. Phys. **19** (1978), no. 5, 1028–1031.

[Mec14] E. Meckes, *Concentration of measure and the compact classical matrix groups*, `https://www.math.ias.edu/files/wam/Haar_notes-revised.pdf`, 2014, Accessed: 2017-01-10.

[MGE11] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and Robust Randomized Benchmarking of Quantum Processes*, Phys. Rev. Lett. **106** (2011), no. 18, 180504.

[MGE12] E. Magesan, J. M. Gambetta, and J. Emerson, *Characterizing quantum gates via randomized benchmarking*, Phys. Rev. A **85** (2012), no. 4, 042311.

[NHKW17] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, *Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics*, Phys. Rev. X **7** (2017), no. 2, 021006.

[NHMW17] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, *Unitary 2-designs from random X- and Z-diagonal unitaries*, Journal of Mathematical Physics **58** (2017), no. 5, 052203.

[OAG$^+$16] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, and M. Lewenstein, *Random Bosonic States for Robust Quantum Metrology*, Phys. Rev. X **6** (2016), no. 4, 041044.

[Pag93] D. N. Page, *Average entropy of a subsystem*, Phys. Rev. Lett. **71** (1993), no. 9, 1291–1294.

[PSW06] S. Popescu, A. J. Short, and A. Winter, *Entanglement and the foundations of statistical mechanics*, Nat. Phys. **2** (2006), no. 11, 754–758.

[RBKSC04] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric informationally complete quantum measurements*, J. Math. Phys. **45** (2004), 6.

[Rei08] P. Reimann, *Foundation of Statistical Mechanics under Experimentally Realistic Conditions*, Phys. Rev. Lett. **101** (2008), no. 19, 190403.

[RY17] D. A. Roberts and B. Yoshida, *Chaos and complexity by design*, J. High Energ. Phys. **2017** (2017), no. 4, 121.

[SDTR13] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, *Decoupling with unitary approximate two-designs*, New J. Phys. **15** (2013), 053022.

[SS08] Y. Sekino and L. Susskind, *Fast scramblers*, J. High Energy Phys. **2008** (2008), no. 10, 065.

[Sus11] L. Susskind, *Addendum to Fast Scramblers*, 2011, arXiv: 1101.6048.

[Sus14] L. Susskind, *Computational Complexity and Black Hole Horizons*, 2014.

[TDL01] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, *Locking classical correlations in quantum states*, Phys. Rev. Lett. **86** (2001), 5807.

[TGR07] G. Tóth and J. J. García-Ripoll, *Efficient algorithm for multiqudit twirling for ensemble quantum computation*, Phys. Rev. A **75** (2007), no. 4, 042311.

[WBV08] Y. S. Weinstein, W. G. Brown, and L. Viola, *Parameters of pseudorandom quantum circuits*, Phys. Rev. A **78** (2008), no. 5, 052332.

[Web16] Z. Webb, *The Clifford group forms a unitary 3-design*, Quant. Info. & Comp. **16** (2016), no. 15 & 16, 1379–1400.

[Zhu15] H. Zhu, *Multiqubit Clifford groups are unitary 3-designs*, 2015, arXiv:1510.02619.

[ZKGG16] H. Zhu, R. Kueng, M. Grassl, and D. Gross, *The Clifford group fails gracefully to be a unitary 4-design*, 2016, arXiv:1609.08172.