Title: On random circuits and their uses in compilation

Speakers: Earl Campbell

Series: Perimeter Institute Quantum Discussions

Date: October 28, 2020 - 11:00 AM

URL: http://pirsa.org/20100062

Abstract: I will review work by myself and others in recent years on the use of randomization in quantum circuit optimization. I will present general results showing that any deterministic compiler for an approximate synthesis problem can be lifted to a better random compiler. I will discuss the subtle issue of what "better" means and how it is sensitive to the metric and computation task at hand. I will then review specific randomized algorithms for quantum simulations, including randomized Trotter (Su & Childs) and my group's work on the qDRIFT and SPARSTO algorithms. The qDRIFT algorithm is of particular interest as it gave the first proof that Hamiltonian simulation is possible with a gate complexity that is independent of the number of terms in the Hamiltonian. Since quantum chemistry Hamiltonians have a very large (~N^4) number of terms, randomization is especially useful in that setting. I will conclude by commenting on a recent Caltech paper with interesting results on the derandomization of random algorithms! Some of the relevant preprints include:

https://arxiv.org/abs/1910.06255

https://arxiv.org/abs/1811.08017

https://arxiv.org/abs/1612.02689

Pirsa: 20100062 Page 1/48



Earl Campbell

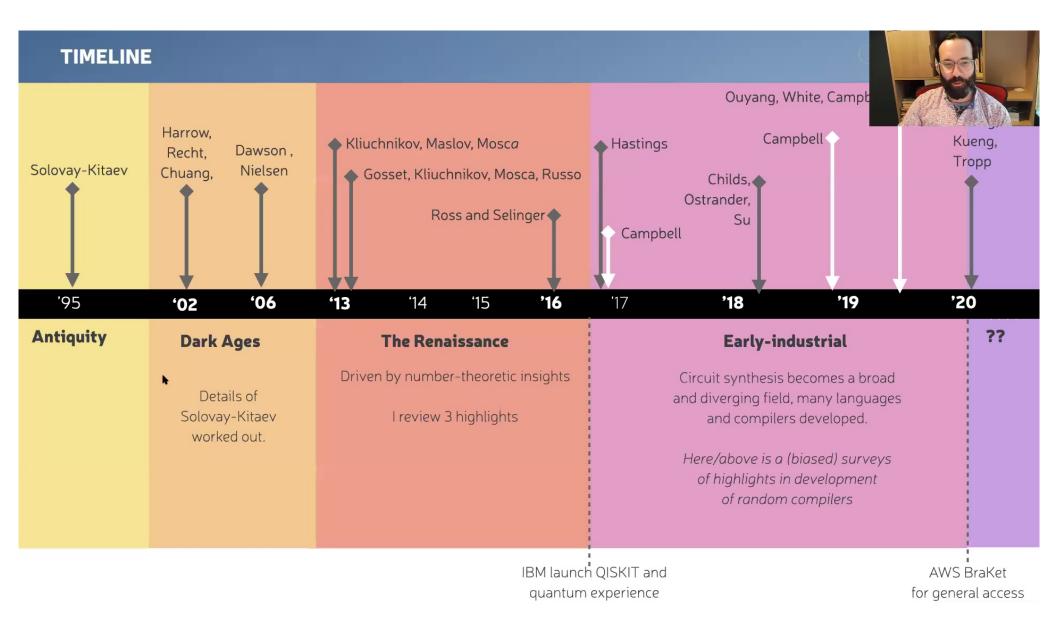
On random quantum circuits and their uses in compilation

an overview of work by myself and others

All work done at University of Sheffield talk includes work with collaborators: Yingkai Ouyang and David White

Currently a contractor for AWS Center for Quantum Computing,

Pirsa: 20100062 Page 2/48



Pirsa: 20100062 Page 3/48





Pirsa: 20100062 Page 4/48



Gate set ${\cal G}$

A collection of unitaries used to build circuits

e.g. from
$$\mathcal{G} = \{A, B, C\}$$
 we can build $ABC, ABBC, CBC$, etc

Pirsa: 20100062 Page 5/48



Gate set \mathcal{G}

A collection of unitaries used to build circuits

e.g. from
$$\mathcal{G} = \{A, B, C\}$$
 we can build $ABC, ABBC, CBC$, etc

Universality - Informal statement

 \mathcal{G} is **universal** if it can implement any unitary (upto finite precision)

Universality - Formal statement

 ${\mathcal G}$ is **universal** if for any target unitary V and $\epsilon>0$ there exists a finite circuit $U\in\langle{\mathcal G}\rangle$ such that $d(U,V)\leq\epsilon$

Example

Clifford+T or Clifford+Toffoli



Cost model $\mathfrak{C}:\mathcal{G}
ightarrow \mathbb{R}_+$

Each elementary gate given a positive valued "cost" This induces a circuit cost

$$\text{if} \quad U = \prod_i G_i \quad \text{then} \quad \mathfrak{C}(U) = \sum_i \mathfrak{C}(G_i)$$

Example

Uniform cost model:

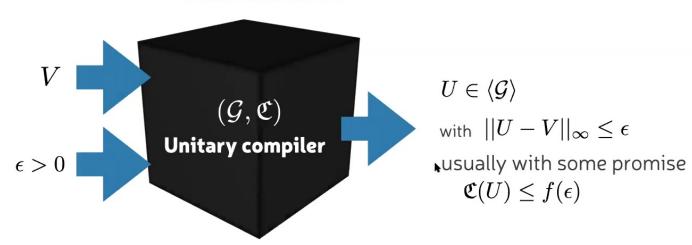
$$\mathfrak{C}(G)=1$$
 for all $G\in\mathcal{G}$

Magic state cost model / T-count:

$$\mathfrak{C}(T)=1$$
 and $\mathfrak{C}(C)=0$ for all C in the Clifford group.







For *efficient* compilers The promise function $f(\epsilon)$ is often polylog $f(\epsilon) \leq A \log(1/\epsilon)^{\gamma}$

An **optimal** compiler will have the lowest possible $\,\mathfrak{C}(U)\,$ and $f(\epsilon)$

Solovay ('97 email claim)-Kitaev ('97 paper)

Consider any universal gate set $\mathcal G$ (generating a group) with uniform cost.

An algorithm to solve the compiling problem using $\mathfrak{C}(U) \leq O(\log(1/\epsilon)^{\gamma})$ where γ is between 3 and 4.

Runtime is efficient in Hilbert space dimension and $\log(1/\epsilon)$



Robert Solovay (1983)



Alexei Kitaev

But what is the constant γ ?

Pirsa: 20100062 Page 9/48

Solovay ('97 email claim)-Kitaev ('97 paper)

Consider any universal gate set \mathcal{G} (generating a group) with uniform cost.

An algorithm to solve the compiling problem using $\mathfrak{C}(U) \leq O(\log(1/\epsilon)^{\gamma})$ where γ is between 3 and 4.

Runtime is efficient in Hilbert space dimension and $\log(1/\epsilon)$

The Solovay-Kitaev algorithm **Dawson and Nielsen QIC 2006**



Michael Nielsen



Christopher Dawson

undergrad thesis



Aram Harrow



Robert Solovay (1983)



Alexei Kitaev

The exponent constant is

$$\gamma = 3.97$$

The prefactor grows with the Hilbert space dimension

Pirsa: 20100062 Page 10/48

Efficient discrete approximations of quantum gates

Harrow, Recht, Chuang

Journal of Mathematical Physics (2002)

Consider any universal gate set \mathcal{G} (generating a group) with uniform cost.

There exists a solution to the compiling problem with $\mathfrak{C}(U) \leq O(\log(1/\epsilon))$ and this is optimal!

No construction algorithm given (except an inefficient brute force search)



Aram Harrow



Ben Recht



Issac Chuang

Pirsa: 20100062 Page 11/48



Theoretically possible

(Harrow, Recht, Chuang)

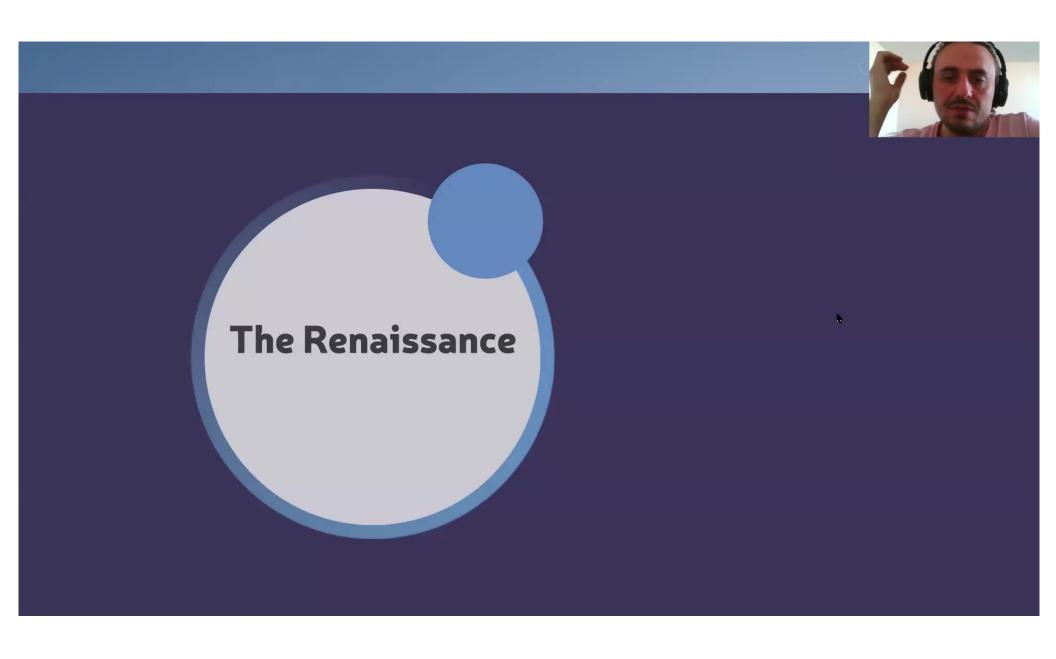
$$\gamma = 1$$

Practically feasible for modest Hilbert space dimension

(Solovay,Kitaev) see also (Harrow and Nielsen,Dawson)

$$\gamma = 3.97$$

Pirsa: 20100062



Pirsa: 20100062 Page 13/48

FOCUS ON SPECIFIC GATE SETS



Progress driven by focusing on a specific gate set important in fault-tolerant quantum computing

Gate set generated by
$$\mathcal{G} = \{T, CNOT, S, H\}$$

Clifford group

$$\{CNOT, S, H\}$$

$$H = \frac{1}{\sqrt{2}} \left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right)$$

$$S = \left(\begin{array}{cc} 1 & 0 \\ 0 & i \end{array}\right)$$

CNOT 2-qubit control-X

$$\mathfrak{C}(C) = 0$$

non-Clifford element

$$T = \left(\begin{array}{cc} 1 & 0 \\ 0 & \sqrt{i} \end{array}\right)$$

Also called pi over 8 phase gate

$$\mathfrak{C}(T) = 1$$

Pirsa: 20100062 Page 14/48



Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates

Kliuchnikov, Maslov, Mosca, QIC 13 607 (2013) — arXiv:1206.5236

Let $\mathcal G$ be single qubit Clifford+T and $U\in\langle\mathcal G\rangle$ then we can efficiently compute a circuit achieving the optimal T-count. $\mathfrak C(U)$

Proof uses the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$

In bullet points:

- Only single qubit gates
- Only exact synthesis & not all unitaries (no epsilon)
- Efficient
- Optimal



Vadym Kliuchnikov



Dmitri Maslov



Mike Mosca

Pirsa: 20100062 Page 15/48



An algorithm for the T-count

Gosset, Kliuchnikov, Mosca, Russo

preprint arXiv:1308.4134

Let $\mathcal G$ be n-qubit Clifford+T and $U\in\langle\mathcal G
angle$ then we can compute a circuit achieving the optimal T-count $\mathfrak C(U)$ in time $\mathcal O(2^{n\mathfrak C(U)}\mathrm{poly}(n,\mathfrak C(U)))$

Proof uses the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$

In bullet points:

- Any number of qubits!
- Only exact synthesis & not all unitaries (no epsilon)
- Inefficient!
- Optimal





David Gosset



Vincent Russo



Mike Mosca



Optimal ancilla-free Clifford+T approximation of z-rotations

Ross and Selinger

QIC 16 901 (2016) - arXiv:1403.2975

Let $\mathcal G$ be single qubit Clifford+T and $U=\exp(-i\theta Z)$ then for any $\epsilon>0$ we can find approximation V with $d(U,V)\leq\epsilon$ and optimal T-count. $\mathfrak C(V)\leq 4\log(1/\epsilon)+O(\log\log(1/\epsilon))$

In bullet points:

- Only single-qubit Z-axis rotations
- Inexact synthesis
- Efficient!



Practically means 100s of gates rather than 10,000s of gates for Solovay-Kitaev



Convenient command line tool



Neil "Julien" Ross



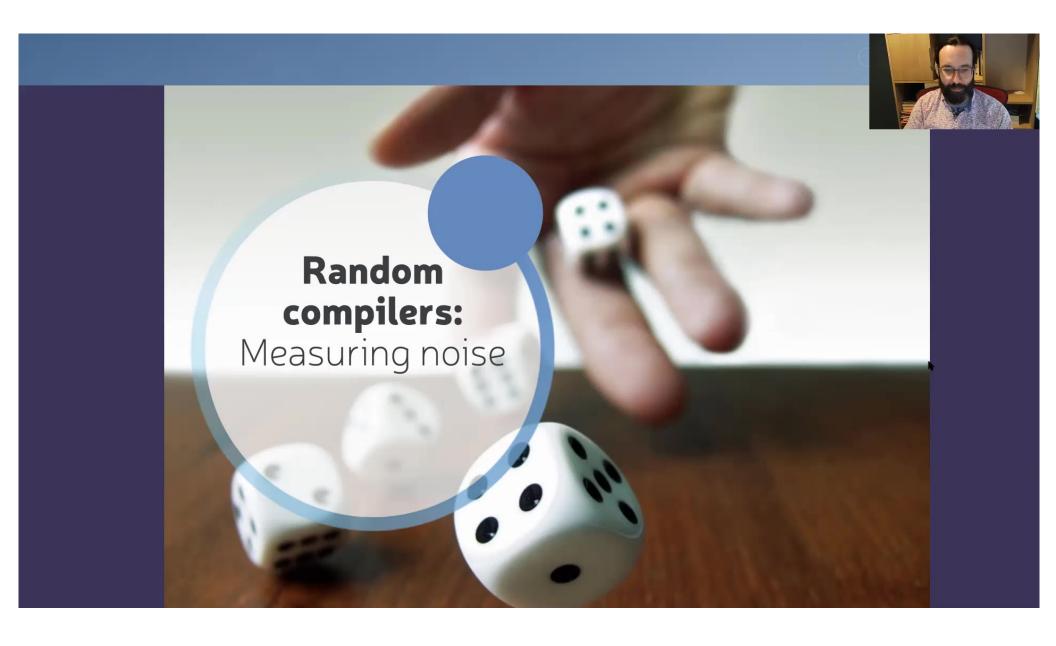
Peter Selinger



Still leaves open:

- .
- Heuristics for many-qubit synthesis
 - · too hard to hope for practical, optimal solutions
- Approaches for specific tasks
 - · e.g. Hamiltonian simulation more on this later
- Benefits of ancilla and measurements
 - · Many nice/partial results but little known regarding optimality.
- Benefits of randomness remainder of this talk

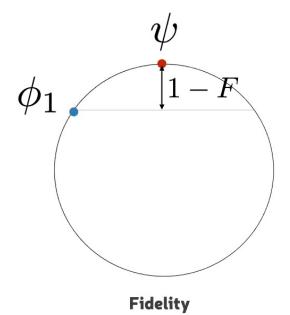
Pirsa: 20100062 Page 18/48



Pirsa: 20100062 Page 19/48

MEASURING ERRORS



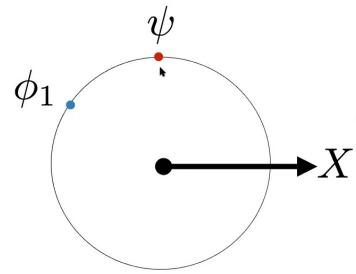


 $F(\phi_1, \psi) = \langle \phi_1 | \psi \rangle \langle \psi | \phi_1 \rangle$

1-norm error
$$||M||_1={
m Tr}[\sqrt{MM^\dagger}]$$
 where $M=|\phi_1\rangle\langle\phi_1|-|\psi\rangle\langle\psi|$

MEASURING ERRORS





Measure some observable X, then

Error in probability of measurement outcomes

 \leq 1-norm error

Not fidelity!!!

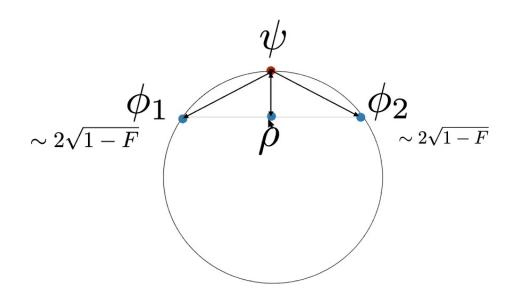
1-norm error $||M||_1=\mathrm{Tr}[\sqrt{MM^\dagger}]$

where $M=|\phi_1\rangle\langle\phi_1|-|\psi\rangle\langle\psi|$

Pirsa: 20100062 Page 21/48

MEASURING ERRORS





$$ho=rac{$$
50% probability $\phi_1}{$ 50% probability ϕ_2

Randomness quadratically reduced 1-norm error!

Although (average) fidelity is unchanged

Pirsa: 20100062 Page 22/48



Random compiling problem

Given a V and $\epsilon>0$ output a probability distribution of circuits, realising

$$\mathcal{E}(
ho) = \sum_i p_i U_i
ho U_i^\dagger$$

such that $d(\mathcal{E},\mathcal{V}) \leq \epsilon$ and minimise $\mathfrak{C}(\mathcal{E})$

Def:
$$\mathcal{U}(\cdot) := U \cdot U^\dagger$$

Pirsa: 20100062 Page 23/48

.



Random compiling problem

Given a V and $\epsilon>0$ output a probability distribution of circuits, realising

$$\mathcal{E}(
ho) = \sum_i p_i U_i
ho U_i^\dagger$$

such that $d(\mathcal{E},\mathcal{V}) \leq \epsilon$ and minimise $\mathfrak{C}(\mathcal{E})$

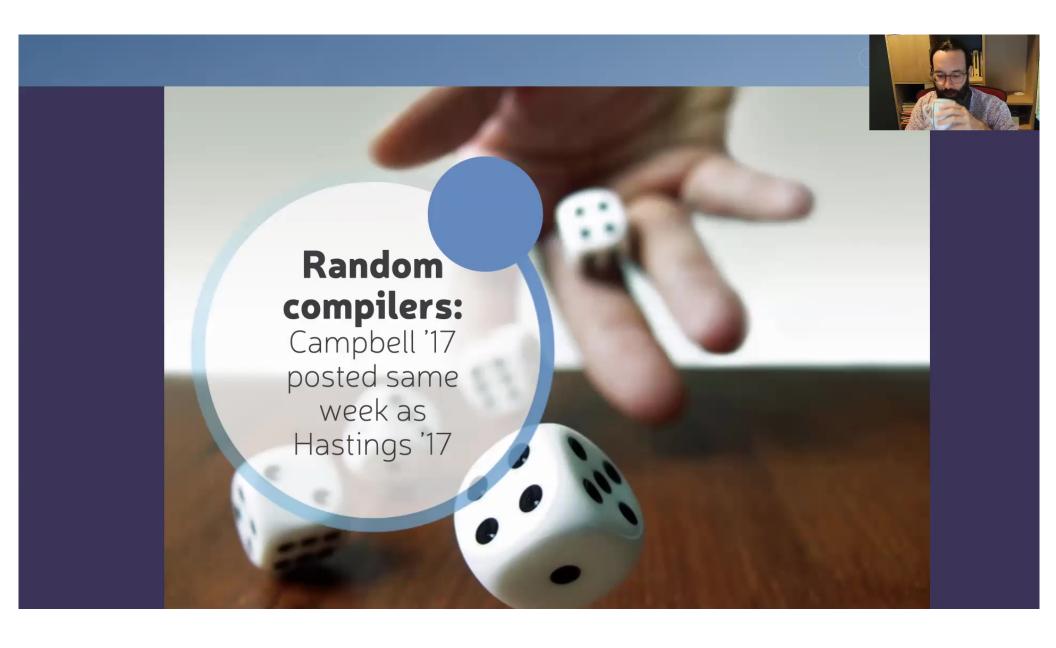
Def:
$$\mathcal{U}(\cdot) := U \cdot U^\dagger$$

What distance we use matters!

Diamond norm distance

$$d_{\diamond}(\mathcal{E},\mathcal{U}) := \frac{1}{2}||\mathcal{E} - \mathcal{U}||_{\diamond} = \frac{1}{2} \max_{\rho} \frac{||(\mathcal{E} \otimes \mathbb{I})(\rho) - (\mathcal{U} \otimes \mathbb{I})(\rho)||_{1}}{||\rho||_{1}}$$
 where $||X||_{1} := \text{Tr}[\sqrt{X^{\dagger}X}]$ is the Schatten 1-norm

Pirsa: 20100062 Page 24/48



Pirsa: 20100062 Page 25/48



Shorter gate sequences for quantum computing by mixing unitaries

Earl Campbell

Phys. Rev. A 95, 042306 (2017) — arXiv:1612.02689

Turning Gate Synthesis Errors into Incoherent Errors

Matthew B. Hastings^{1, 2}

Station Q, Microsoft Research, Santa Barbara, CA 93106-6105, USA
 Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA 98052, USA

Using error correcting codes and fault tolerant techniques, it is possible, at least in theory, to produce logical qubits with significantly lower error rates than the underlying physical qubits. Suppose, however, that the gates that act on these logical qubits are only approximation of the desired gate. This can arise, for example, in synthesizing a single qubit unitary from a set of Clifford and T gates; for a generic such unitary, any finite sequence of gates only approximates the desired target. In this case, errors in the gate can add coherently so that, roughly, the error ϵ in the unitary of each gate must scale as $\epsilon \lesssim 1/N$, where N is the number of gates. If, however, one has the option of synthesizing one of several unitaries near the desired target, and if an average of these options is closer to the target, we give some elementary bounds showing cases in which the errors can be made to add incoherently by averaging over random choices, so that, roughly, one needs $\epsilon \lesssim 1/\sqrt{N}$. We remark on one particular application to distilling magic states where this effect happens automatically in the usual circuits.

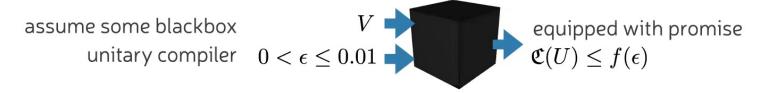
Pirsa: 20100062 Page 26/48

THE RESULT



Preamble

Let ${\mathcal G}$ be a universal gate set with cost measure ${\mathfrak C}$



Theorem

...then there exists a random sequence
$${\cal E}(
ho)=\sum_j p_j U_j
ho U_j^\dagger$$

with $d_{\diamond}(\mathcal{V}, \mathcal{E}) \leq 10\epsilon^2$ and cost $\mathfrak{C}(\mathcal{E}) \leq f(\epsilon)$

2nd Theorem (paraphrased)

For single qubit axial rotations: the assumptions can be relaxed and inequalities tightened slightly.

Pirsa: 20100062 Page 27/48

THE RESULT



"same cost gets you better error suppression"

Theorem

...then there exists a random sequence
$$~{\cal E}(
ho) = \sum_j p_j U_j
ho U_j^\dagger$$

with
$$d_{\diamond}(\mathcal{V}, \mathcal{E}) \leq 10\epsilon^2$$
 and cost $\mathfrak{C}(\mathcal{E}) \leq f(\epsilon)$

"same error suppression for lower cost?"

Corollary

if the unitary cost is polylog $\mathfrak{C}(U) \leq f(\epsilon) = A \log_2 (1/\epsilon)^{\gamma}$

...then there exists a random circuit $\mathcal{E}(
ho) = \sum_j p_j U_j
ho U_j^\dagger$

with $d_{\diamond}(\mathcal{V},\mathcal{E}) \leq \epsilon$ and cost $\mathfrak{C}(\mathcal{E}) \leq C^{\gamma} f(\epsilon) \sim (1/2)^{\gamma} f(\epsilon)$

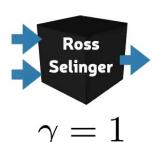
$$C = \left(\frac{1}{2}\right) \left(1 + \frac{\log(A)}{\log(1/\epsilon)}\right) \to_{\epsilon \to 0} \left(\frac{1}{2}\right)$$

Pirsa: 20100062 Page 28/48

APPLICATIONS TO SPECIFIC BLACK BOXES



WE SAVE ~ 2^{γ}



For single qubit Clifford+T gate set and T-count cost metric

Resource saving 2X

	optimal unitary	random compiling
$\epsilon = 10^{-20}$	600	314 or less
$\epsilon = 10^{-10}$	300	165 or less
$\epsilon = 10^{-5}$	150	90 or less

Pirsa: 20100062 Page 29/48

APPLICATIONS TO SPECIFIC BLACK BOXES



WE SAVE ~ 2^{γ}



For single qubit Clifford+T gate set

and T-count cost metric

 $\gamma = 1$

Resource saving 2X

	optimal unitary	random compiling
$\epsilon = 10^{-20}$	600	314 or less
$\epsilon = 10^{-10}$	300	165 or less
$\epsilon = 10^{-5}$	150	90 or less



 $\gamma \sim 3.97$

For any gate-set / cost metric

Resource saving $\,2^{3.97}\sim15.7\,$

Still a good option for T-gate synthesis over a modest number of qubits (more than 1, less than ~10)

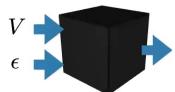
Pirsa: 20100062 Page 30/48

SKETCH



ALGORTIHM SKETCH

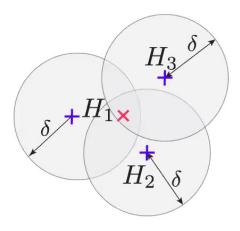
assume some blackbox unitary compiler



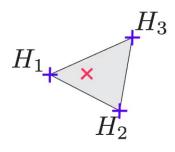
 $\,U\,\,$ equipped with promise

$$\mathfrak{C}(U) \leq f(\epsilon)$$

1) Use black-box to find a net of solutions "nearby" to target

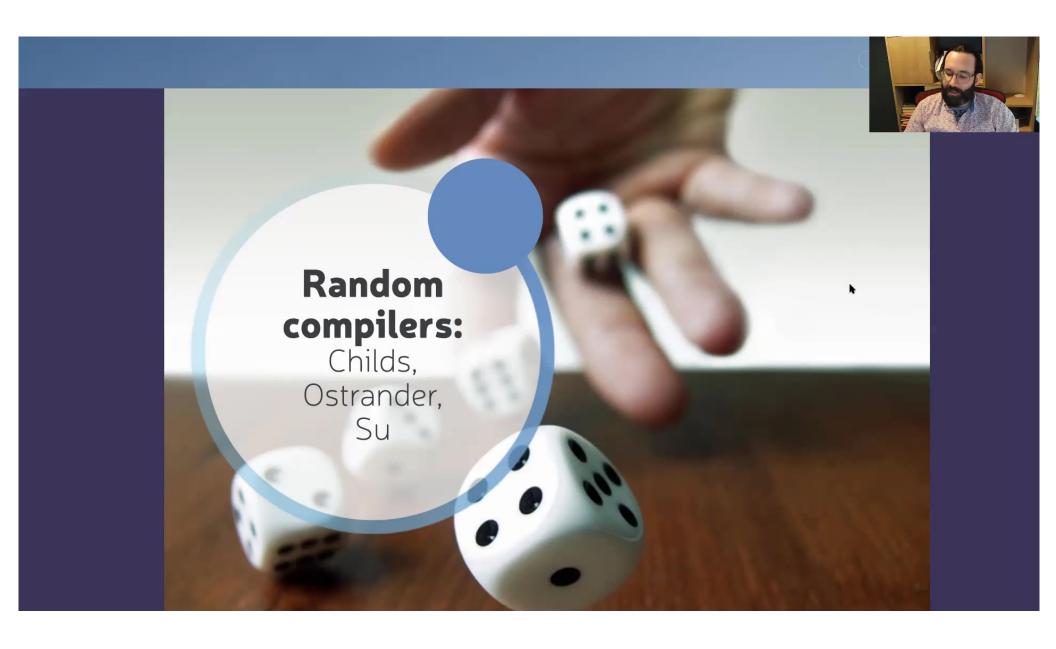


2) Lift to find "nearby" Hamiltonian generators



3) Solve to find probability weights assigned to each circuit

$$\sum_{j} p_{j} H_{j} = H_{\text{target}}$$



Pirsa: 20100062 Page 32/48



Faster Quantum simulation by randomisation

Childs, Ostrander, Su Quantum 3, 182 (2019). — arXiv:1805.08385

Task: Hamiltonian simulation

Given Hamiltonian with fixed decomposition

$$H = \sum_{j=1}^L c_j H_j$$
 with $||H_j|| = 1$

Approximate $U=\exp(iHt)$ for some t

Using gate set $\mathcal{G} = \{\exp(iH_j au)\}$ and cost model is number of such gates

When H_i are Pauli operators further synthesis possible by Ross-Selinger



Andrew Childs



Aaron Ostrander



Yuan Su

Pirsa: 20100062 Page 33/48



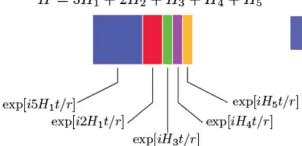
Old (deterministic) solution

Trotter-Suzuki Product Formulae

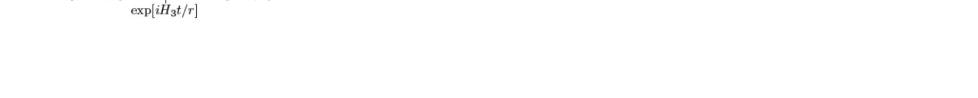
1st order
$$\exp(iHt) pprox \left(\prod_{j=1}^L \exp(iH_j t/r) \right)^r$$

e.g. One 1st order step

 $H = 5H_1 + 2H_2 + H_3 + H_4 + H_5$







Pirsa: 20100062 Page 34/48

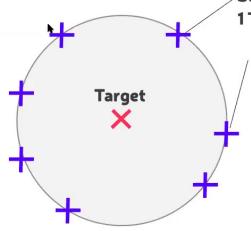






Each permutation has same error bound.





Some permutation of 1 Trotter step

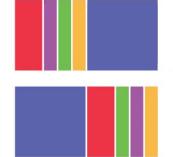
Another permutation of 1 Trotter step

Target unitary is surrounded by many different nearby solutions that we can randomly selected from

Can use Campbell/Hastings results!

Pirsa: 20100062





Each permutation has same error bound.



Target

Some permutation of 1 Trotter step

Another permutation of 1 Trotter step

Target unitary is surrounded by many different nearby solutions that we can randomly selected from

Can use Campbell/Hastings results!

Ten deterministic first order steps



Ten randomised first order steps (each choice must be i.i.d)



Gate complexity to obtain ϵ error

$$G_{\rm det} = O(L^4 t^2/\epsilon)$$

$$G_{
m rand} = O(L^{2.5}t^{1.5}/\epsilon^{0.5})$$

RANDOM PERMUTATIONS



Paper contains theorem statements & proofs showing improvement

Numerical results for 1D Heisenberg Spin chain with a random magnetic field

r = Number of Trotter steps, so lower is better

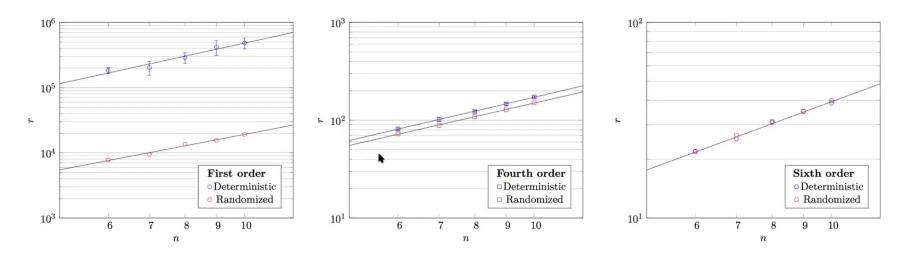


Figure 1: Comparison of the values of r between deterministic and randomized product formulas. Error bars are omitted when they are negligibly small on the plot. Straight lines show power-law fits to the data.

Pirsa: 20100062 Page 37/48



Pirsa: 20100062 Page 38/48



Task: Hamiltonian simulation

Given Hamiltonian with fixed decomposition

$$H = \sum_{j=1}^L c_j H_j$$
 with $||H_j|| = 1$

Approximate $U=\exp(iHt)$ for some t

Using gate set $\, \mathcal{G} = \{ \exp(i H_j au) \}\,$ and cost model is number of such gates

When H_j are Pauli operators further synthesis possible by Ross-Selinger

BUT, what if L **is <u>very large</u>** (e.g. quantum chemistry $L=O(N^4)$) then standard Trotter approaches have large complexity

QDRIFT



A random compiler for fast Hamiltonian simulation Earl Campbell

Phys. Rev. Lett. 123 070503 (2019)

Hamiltonian & assumptions

$$H = \sum_{j=1}^{L} c_j H_j$$

w.l.o.g

$$||H_j|| = 1$$

$$c_j \ge 0$$

letting

$$\lambda = \sum_{j} c_{j}$$

qDRIFT = quantum drift

With probability

$$p_j = c_j/\lambda$$

Do $\exp(i\lambda t H_j/G)$

and repeat $\,G\,$ times

so sequence looks visually like



Results

Gate complexity

$$G_{qDRIFT} = 2\lambda^2 t^2 / \epsilon$$

No L dependence

PROOF SKETCH



Given
$$H = \sum_{j=1}^L c_j H_j$$
 and $\mathcal{L}(
ho) = i[H,
ho]$

Want the unitary "channel" $\exp(\mathcal{L}t) = \mathbb{I} + t\mathcal{L} + O(t^2)$ [*]

Define
$$\mathcal{L}_j(
ho)=i[H_j,
ho]$$
 so that $\mathcal{L}=\sum_j c_j\mathcal{L}_j$

Randomly selecting 1 gate (and forgetting) gives the channel $\mathcal{E} = \sum_{i} p_{j} \exp(au \mathcal{L}_{j})$

Setting
$$p_j = \frac{c_j}{\lambda}$$
 we have $\mathcal{E} = \frac{1}{\lambda} \sum_j c_j \exp(\tau \mathcal{L}_j) = \mathbb{I} + \sum_j \frac{c_j \tau}{\lambda} \mathcal{L}_j + \dots$ [**]

Setting $au=\lambda t$ then [*] and [**] match to 1st order

One 1 gate per "step" so no L dependence. Do some carefully bounding of higher order effects and done.

QDRIFT

 $\lambda = 426.61$

30

25

20

10²

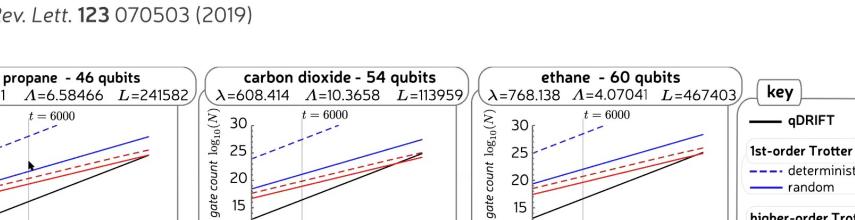
104

Log gate count $\log_{10}(N)$

A random compiler for fast Hamiltonian simulation

Earl Campbell

Phys. Rev. Lett. 123 070503 (2019)



108

20

15

10²

104

106

Time (s/Hr)

108

--- deterministic

random

higher-order Trotter --- deterministic

random

Caveats:

ullet bound in terms of $\Lambda=\max(c_j)$ would be nice to redo in terms of tighter "commutator" bounds;

106

Time (s/Hr)

Works well for chemistry, but not spin chain Hamiltonians;

20

15

10²

104

Error in terms of diamond norm

106

Time (s/Hr)

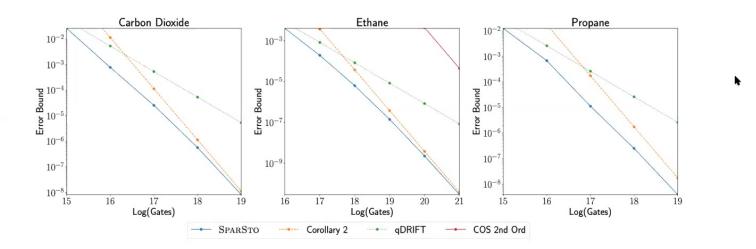
108

Pirsa: 20100062 Page 42/48

SPARSTO

Compilation by stochastic Hamiltonian sparsification

Ouyang, White, Campbell *Quantum* 4 235 (2020)



SPARSTO: Sparsify the Hamiltonian to reduce effective **L** interpolating between qDRIFT and 2nd order Trotter with some improvements in-between



Yingkai Ouyang



David White

Pirsa: 20100062 Page 43/48

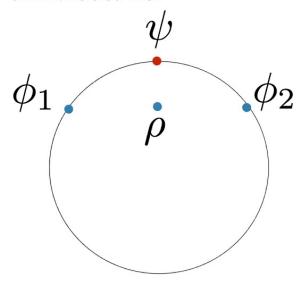


DERANDOMIZED

Quantum simulation via randomized product formulas: Low gate complexity with accuracy guarantees

Chen, (Robert) Huang, Kueng and Tropp

arXiv:2008.11751



Given a randomised algorithm (e.g. qDRIFT or SPARSTO) with some mixed state/channel, how good are the individual samples?



?

Chi-Fang Chen



(Robert) Huang



Richard Kueng



Joel Tropp

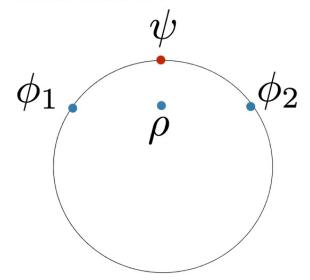
Pirsa: 20100062 Page 45/48

DERANDOMIZED

Quantum simulation via randomized product formulas: Low gate complexity with accuracy guarantees

Chen, (Robert) Huang, Kueng and Tropp

arXiv:2008.11751



Given a randomised algorithm (e.g. qDRIFT or SPARSTO) with some mixed state/channel, how good are the individual samples?

Derandomized qDRIFT: with prob δ the sampled **n**-qubit circuit has diamond norm error less than ϵ when we use G gates:

$$G = O(nt^2\lambda^2/\epsilon^2) + O(\log(1/\delta)t^2\lambda^2/\epsilon^2)$$

Compare
$$G_{qDRIFT}=2\lambda^2t^2/\epsilon$$



?

Chi-Fang Chen



(Robert) Huang



Richard Kueng



Joel Tropp

OUTLOOK



- Not much in terms of software implementation & experimentation of random protocols,
 especially w.r.t multi-qubit circuits
 - Improved randomised algorithms using convex optimisation.
- Understanding roles of randomness in some cases like phase estimation where we are interested in energy error and not unitary error!
 - Randomness in post-Trotter (e.g. LCU) circuits?
 - Beyond i.i.d probability distributions?

Pirsa: 20100062 Page 47/48



THANK YOU!

Pirsa: 20100062 Page 48/48