Joint Center for Quantum Information and Computer Science

University of Maryland 1856

Is there an advantage of quantum learning?

Dominik Hangleiter

Quantum Workshop NCSU, January 22, 2020

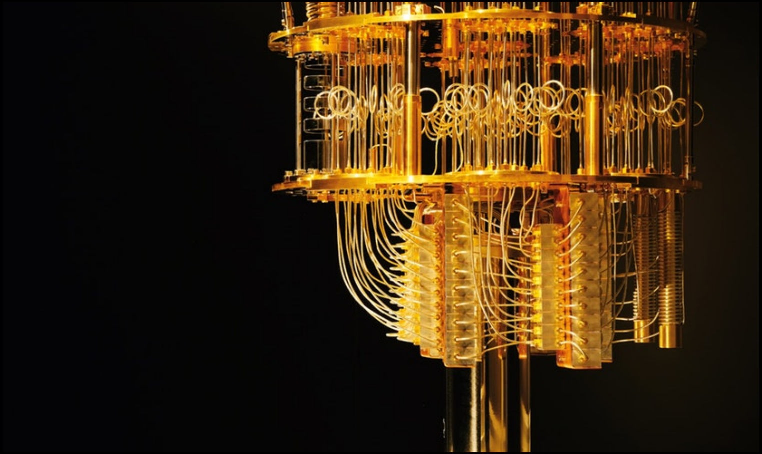
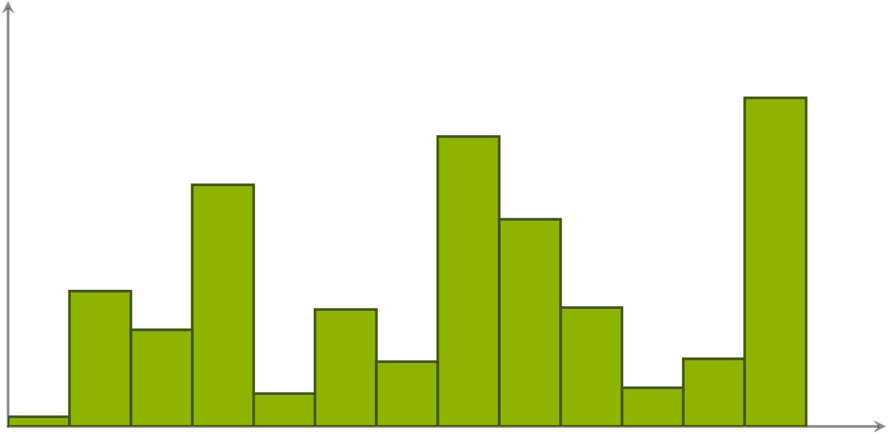


Image Ref.: Graham Carlow/IBM

vs.



Machine learning

Image Ref.: Wikipedia – Katze (CC0)

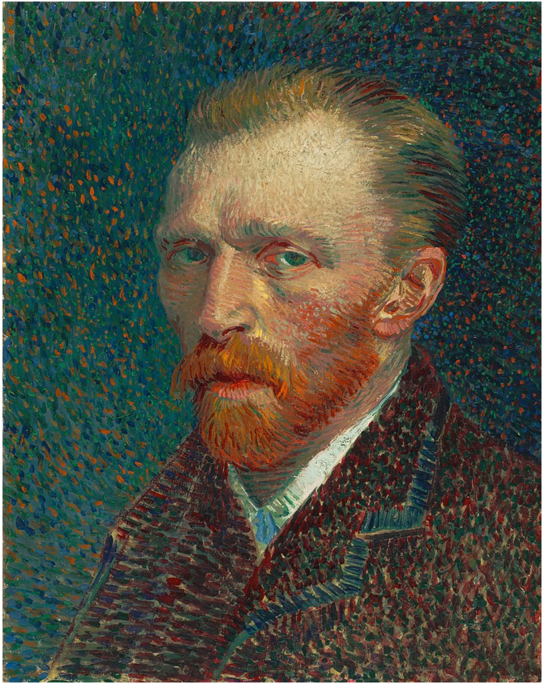
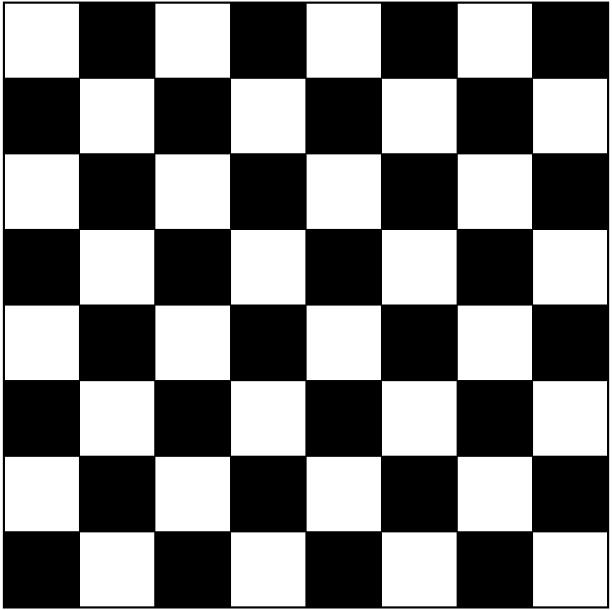


Image Ref.: Wikipedia – Vincent Van Gogh (CC0)



Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning

oracle

learner

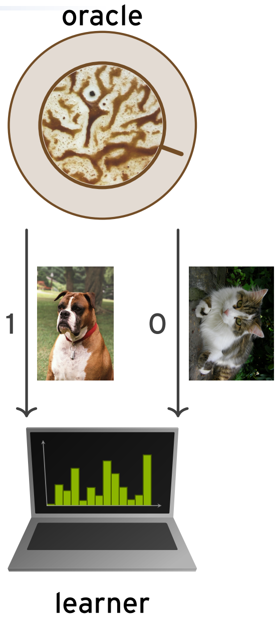
Image Refs.: Wikipedia – Hund, Katze, Van Gogh, Kaffeesatz (CC0), QC: Graham Carlow/IBM

Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning



Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning

oracle

Distribution on {images} $\times \{0, 1\}$.

→

→ ?

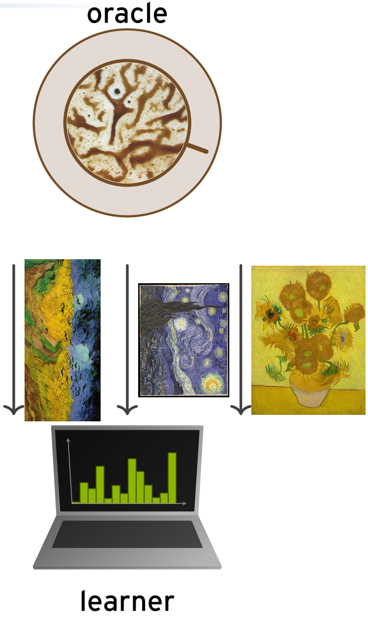
learner

Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning

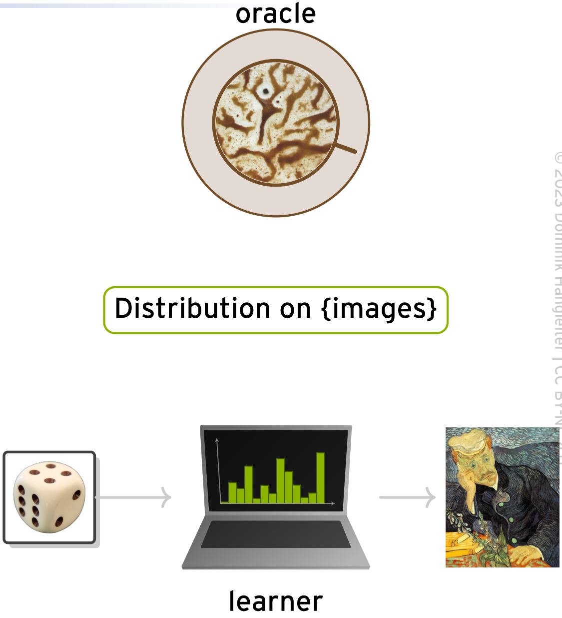


Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning



Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning

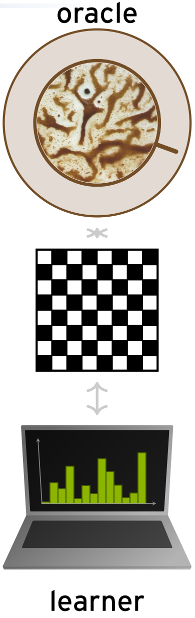


Image Refs.: Wikipedia – Hund, Katze, Van Gogh, Kaffeesatz (CC0), QC: Graham Carlow/IBM

Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning

oracle

Distribution on moves,
conditioned on environ. configs.

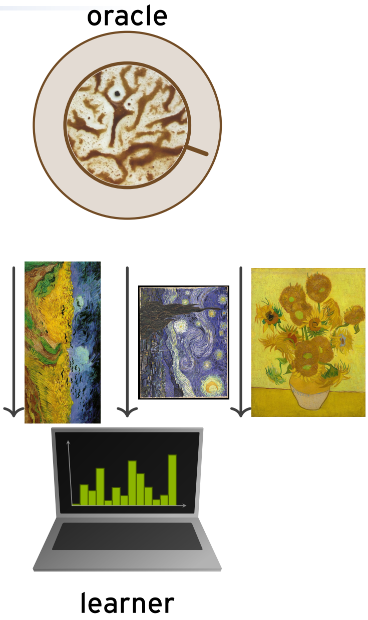
learner

Machine learning and distribution learning

Supervised learning

Unsupervised learning

Reinforcement learning



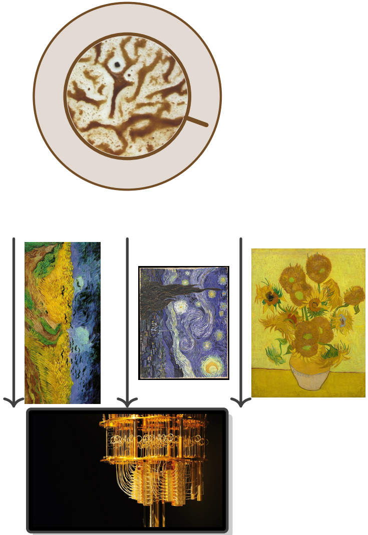
Machine learning and distribution learning

Supervised learning

Unsupervised learning

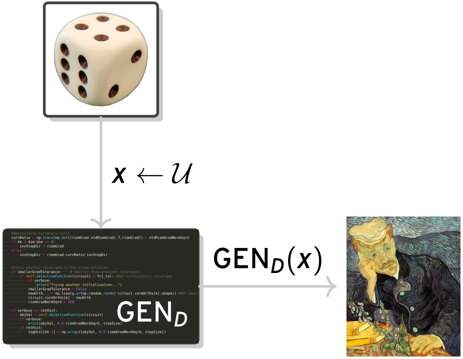
Reinforcement learning

oracle

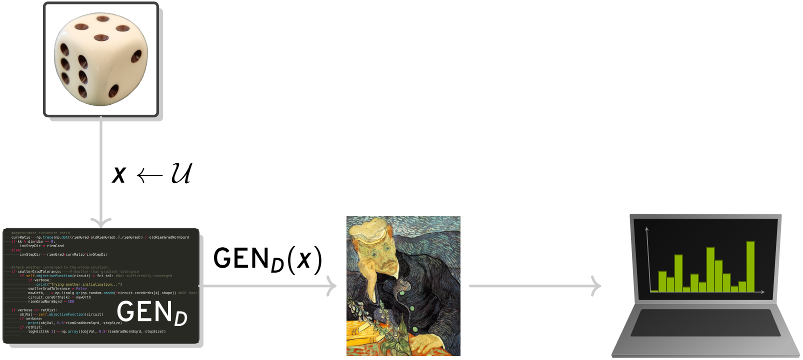


quantum learner

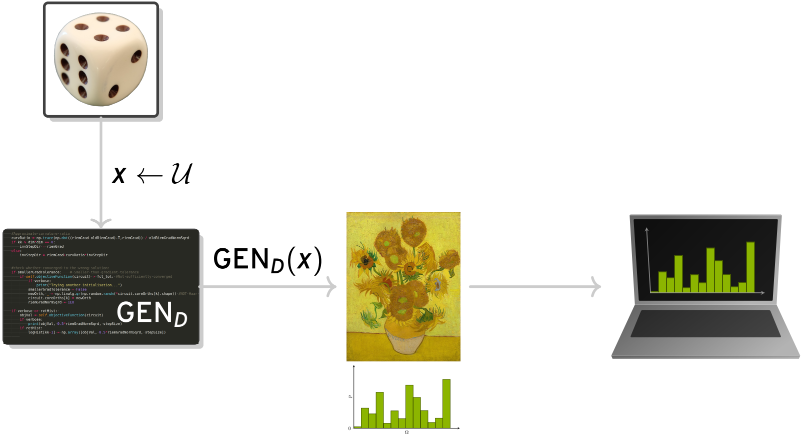
Unsupervised learning: generator vs. evaluator learning



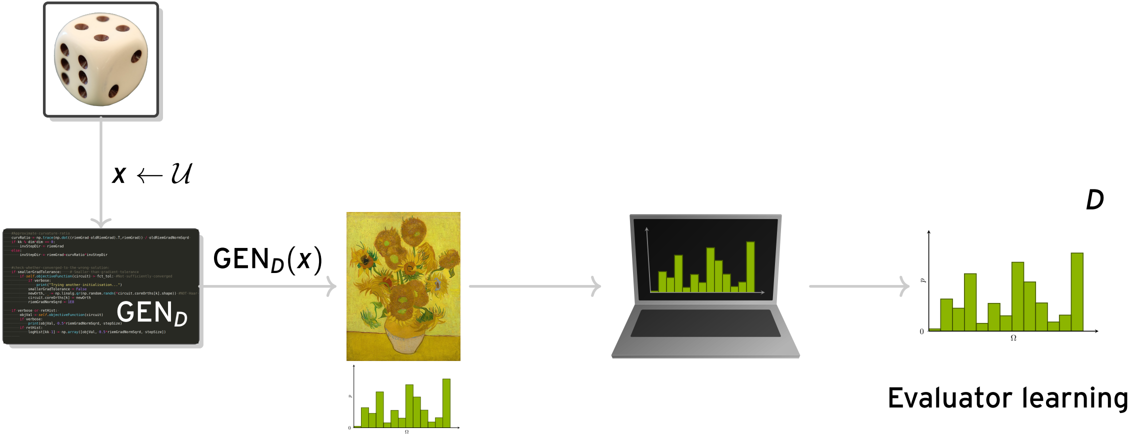
Unsupervised learning: generator vs. evaluator learning



Unsupervised learning: generator vs. evaluator learning



Unsupervised learning: generator vs. evaluator learning



Task: Learn an evaluator EVAL$_D$ of a distribution D.

Unsupervised learning: generator vs. evaluator learning

Task: Learn a generator GEN_D of a distribution D.

The details matter – the case of function learning

Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.

Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

The details matter – the case of function learning

Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.

exact learning

PAC learning

agnostic learning

membership queries

random example queries

quantum example queries

query complexity

sample complexity

computational complexity

no speedup

at most poly speedup

super-poly speedup

Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

The details matter – the case of function learning

Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.

exact learning

PAC learning

agnostic learning

learning framework

membership queries

random example queries

quantum example queries

query complexity

sample complexity

computational complexity

no speedup

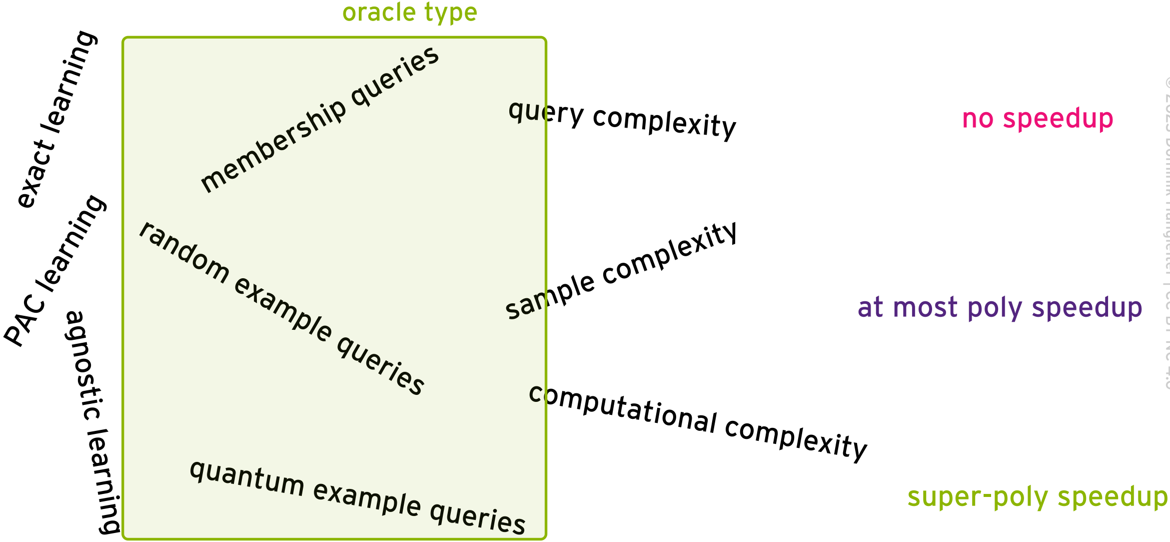
at most poly speedup

super-poly speedup

Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

The details matter – the case of function learning

Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.



Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

The details matter – the case of function learning

Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.

exact learning
membership queries
PAC learning
random example queries
agnostic learning
quantum example queries

complexity

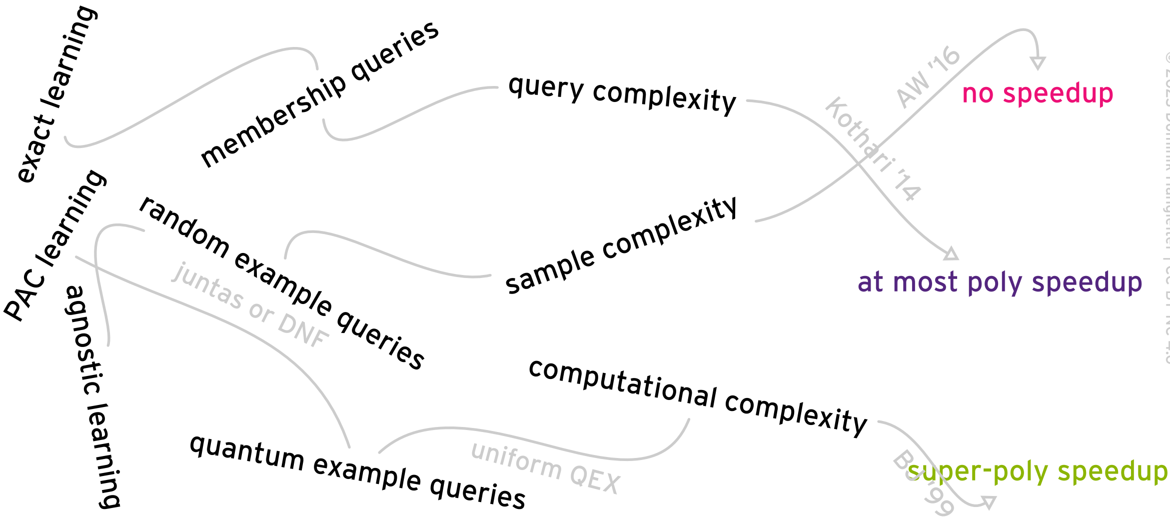
query complexity
sample complexity
computational complexity

no speedup
at most poly speedup
super-poly speedup

Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

The details matter – the case of function learning

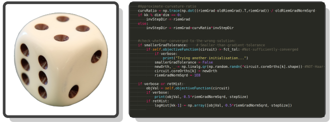
Learning Boolean functions $f : \{0,1\}^n \to \{0,1\}$.



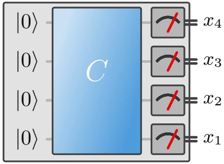
Arunachalam and de Wolf: *A survey of quantum learning theory.* SIGACT news (2017).
Arunachalam and de Wolf: *Optimal quantum sample complexity of learning algorithms.* CCC'17.
Bshouty and Jackson: *Learning DNF over the uniform distribution using a quantum example oracle.* SIAM J. Comp (1999).

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

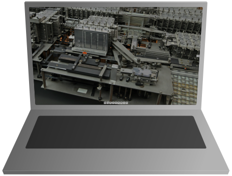
SAMPLE(D)

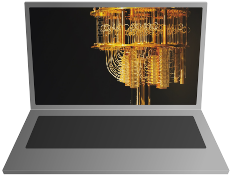
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm



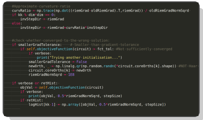


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

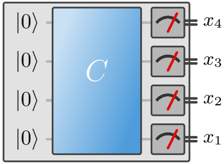
Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

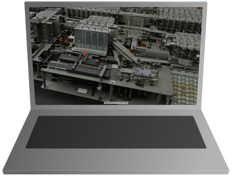
SAMPLE(D)

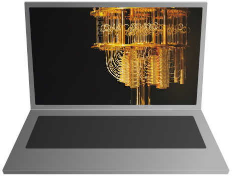
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)} |x\rangle$

Learning algorithm



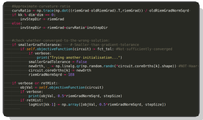


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

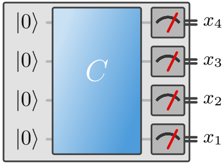
Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

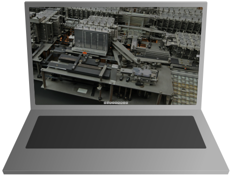
SAMPLE(D)

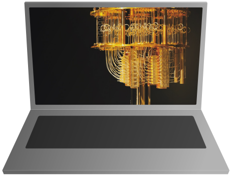
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm

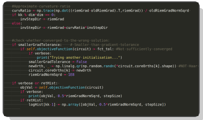




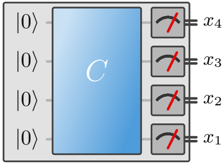
Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

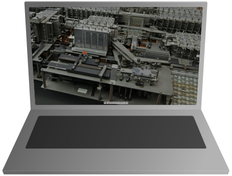
SAMPLE(D)

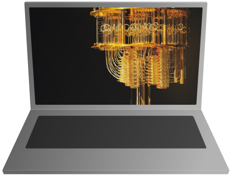
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm



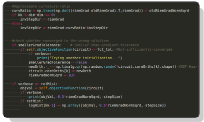


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

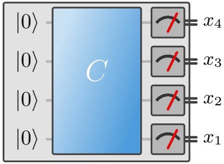
Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

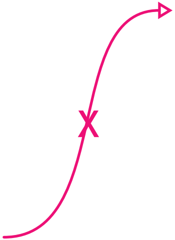
Oracle access

SAMPLE(D)

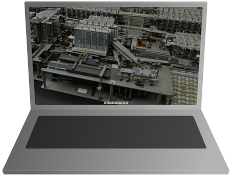
$x \leftarrow D$

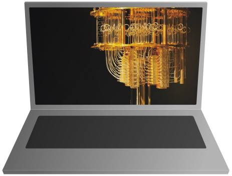
QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$



Learning algorithm



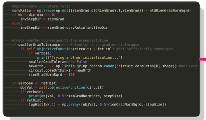


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

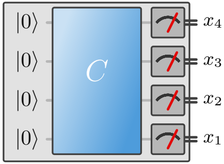
Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

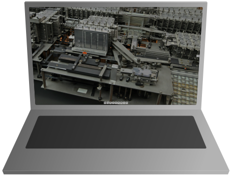
SAMPLE(D)

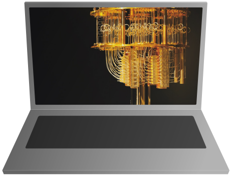
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm



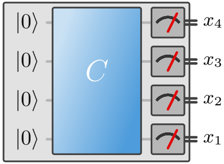


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

Learning settings: classical vs. quantum

Generators

GEN$_D$



QGEN$_D$

Oracle access

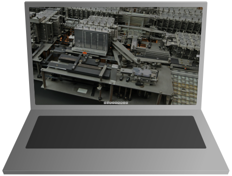
SAMPLE(D)

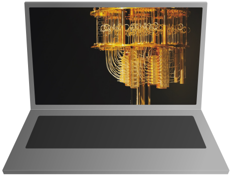
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm





Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Is there a quantum advantage in generator learning?

Generator learning

Task: Learn a generator GEN_D of a distribution D.

A quantum vs. classical separation for distribution learning

Question: Quantum generator-learning advantage?

Is there a class of *efficiently classically generated* discrete distributions which is

- not efficiently classsical PAC generator-learnable, but
- efficiently quantum PAC generator-learnable

w.r.t. the *SAMPLE oracle* and the *KL divergence*?

Coyle *et al.*, NPJ Quant. Inf. (2020).

A quantum vs. classical separation for distribution learning

Question: Quantum generator-learning advantage?

Is there a class of *efficiently classically generated* discrete distributions which is

- not efficiently classsical PAC generator-learnable, but
- efficiently quantum PAC generator-learnable

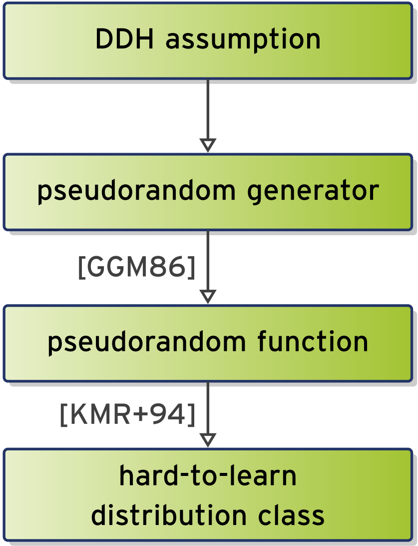
w.r.t. the *SAMPLE oracle* and the *KL divergence*?

Theorem: Y E S* !

*under the decisional Diffie-Hellman assumption for the group family of quadratic residues

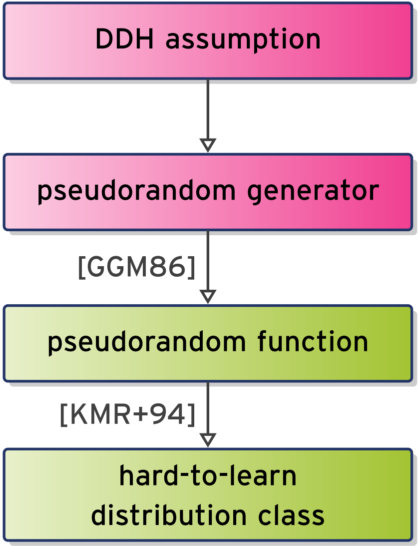
Coyle *et al.*, NPJ Quant. Inf. (2020).

Proof idea: classical hardness and quantum easiness



[KMR+94] Kearns *et al.*, STOC '94 [GGM86] Goldwasser, Goldreich, Micali J. ACM '86 [MZ03] Mosca, Zalka '03

Proof idea: classical hardness and quantum easiness

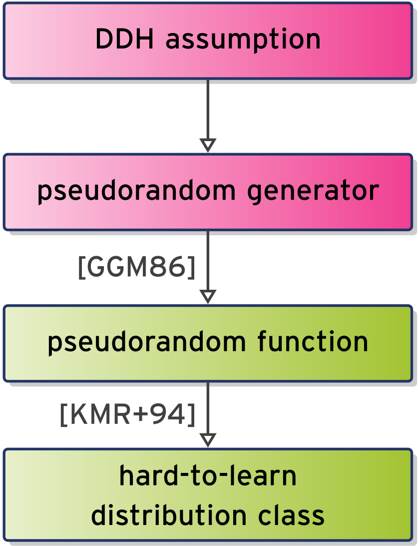


- g generator of $(G, \cdot)$ of order q.
- Think: $\mathbb{Z}_q^*$ and $\text{modexp}_{q,g}(x) = g^x \bmod q$

[KMR+94] Kearns *et al.*, STOC '94
[GGM86] Goldwasser, Goldreich, Micali J. ACM '86 [MZ03] Mosca, Zalka '03

Proof idea: classical hardness and quantum easiness

- g generator of $(G, \cdot)$ of order q.
- Think: $\mathbb{Z}_q^*$ and $\text{modexp}_{q,g}(x) = g^x \bmod q$



Proof idea: classical hardness and quantum easiness

DDH assumption

↓

pseudorandom generator

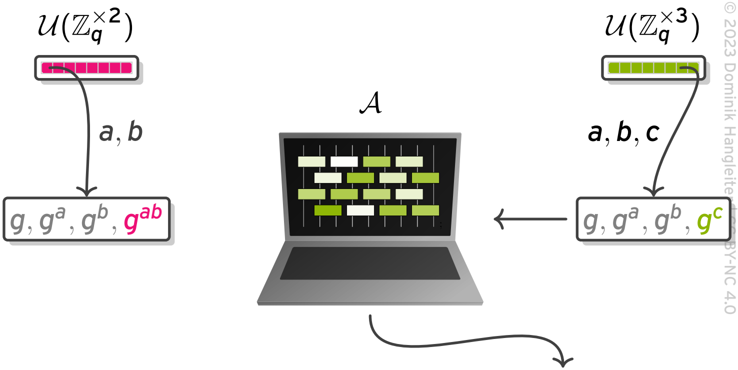
↓ [GGM86]

pseudorandom function

↓ [KMR+94]

hard-to-learn distribution class

- g generator of $(G, \cdot)$ of order q.
- Think: $\mathbb{Z}_q^*$ and $\text{modexp}_{q,g}(x) = g^x \bmod q$



$$\left| \Pr_{a,b \leftarrow \mathcal{U}(\mathbb{Z}_q)}[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1] - \Pr_{a,b,c \leftarrow \mathcal{U}(\mathbb{Z}_q)}[\mathcal{A}(g, g^a, g^b, g^c) = 1] \right|$$

problem size — problem size

[KMR+94] Kearns *et al.*, STOC '94
[GGM86] Goldwasser, Goldreich, Micali J. ACM '86 [MZ03] Mosca, Zalka '03

Proof idea: classical hardness and quantum easiness

DDH assumption

↓

pseudorandom generator

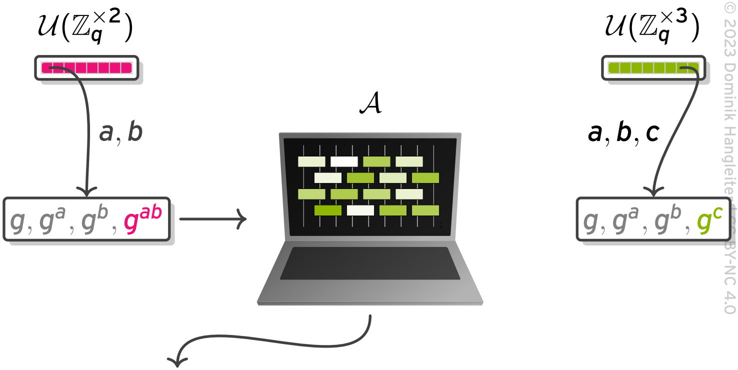
↓ [GGM86]

pseudorandom function

↓ [KMR+94]

hard-to-learn distribution class

- g generator of $(G, \cdot)$ of order q.
- Think: $\mathbb{Z}_q^*$ and $\text{modexp}_{q,g}(x) = g^x \bmod q$



$$\left| \Pr_{a,b \leftarrow \mathcal{U}(\mathbb{Z}_q)}[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1] - \Pr_{a,b,c \leftarrow \mathcal{U}(\mathbb{Z}_q)}[\mathcal{A}(g, g^a, g^b, g^c) = 1] \right|$$

problem size　　problem size

Proof idea: classical hardness and quantum easiness

DDH assumption

↓ quantum adversary

pseudorandom generator

[GGM86] ↓ quantum adversary

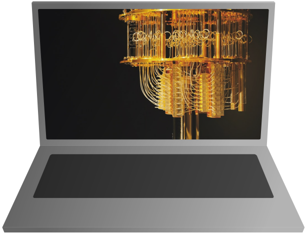
pseudorandom function

[KMR+94] ↓ quantum adversary

hard-to-learn
distribution class

dlog

[MZ03]



[KMR+94] Kearns *et al.*, STOC '94

[GGM86] Goldwasser, Goldreich, Micali J. ACM '86 [MZ03] Mosca, Zalka '03

Proof idea: classical hardness and quantum easiness

DDH assumption

qu

pseudorandom ge

[GGM86]

qu

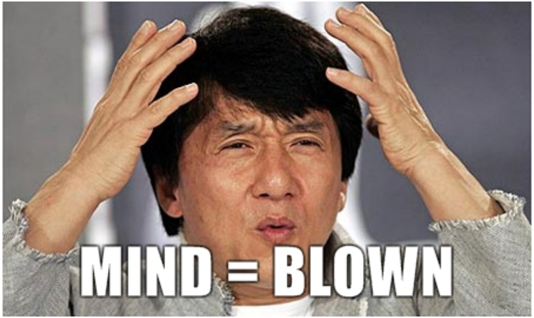
pseudorandom fu

[KMR+94]

qu

hard-to-lear
distribution class

[MZ03]



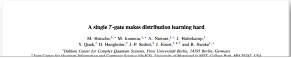
The distribution class can be exactly generator-learned from a single sample!

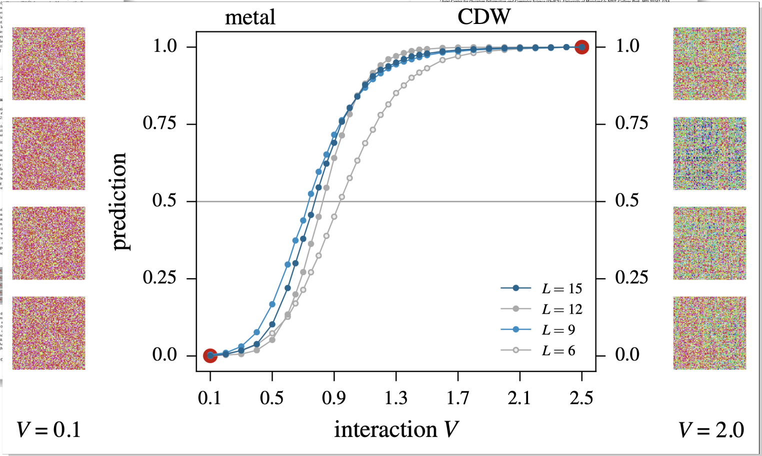
[KMR+94] Kearns *et al.*, STOC '94
[GGM86] Goldwasser, Goldreich, Micali J. ACM '86 [MZ03] Mosca, Zalka '03

A more generic setting

Relevant distributions

Relevant distributions

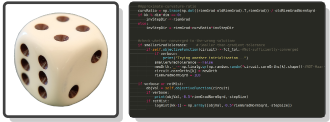




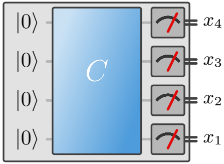
[Broecker *et al.*, 2017]

Learning settings: classical vs. quantum

Generators



GEN_D



QGEN_D

Oracle access

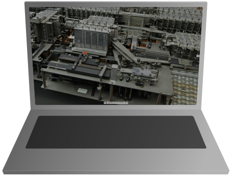
SAMPLE(D)

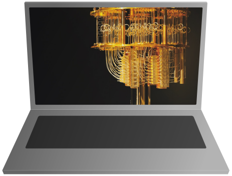
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm



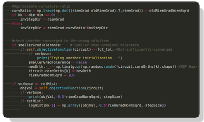


Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

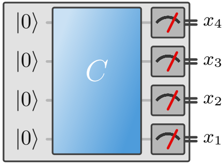
Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

Learning settings: classical vs. quantum

Generators



GEN$_D$



QGEN$_D$

Oracle access

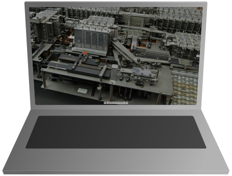
SAMPLE(D)

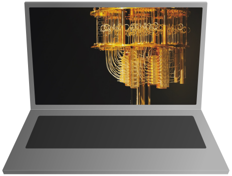
$x \leftarrow D$

QSAMPLE(D)

$\sum_x \sqrt{D(x)}|x\rangle$

Learning algorithm

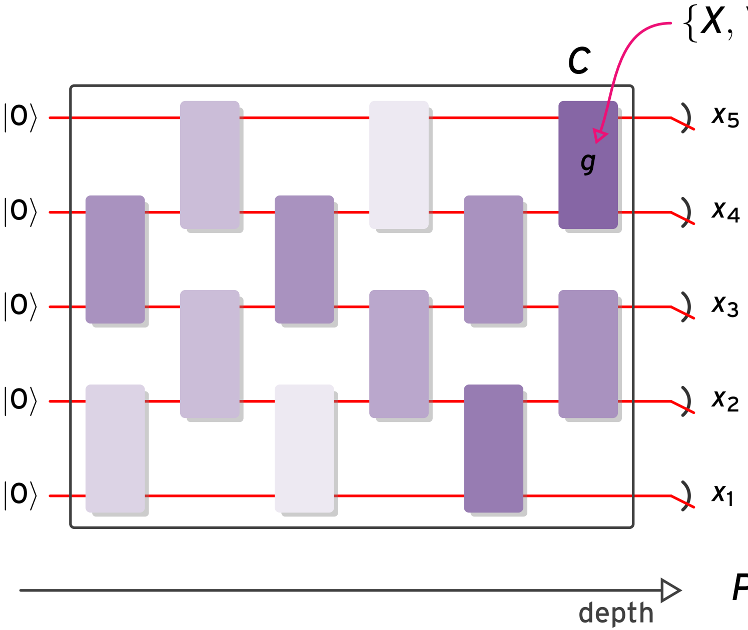




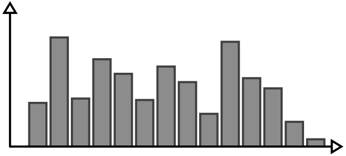
Excellent discussion: Bshouty and Jackson, SIAM J. Comput. (1998)

Figure Refs. Dice, coffee grounds: Wikipedia (CC0), QC: Graham Carlow/IBM

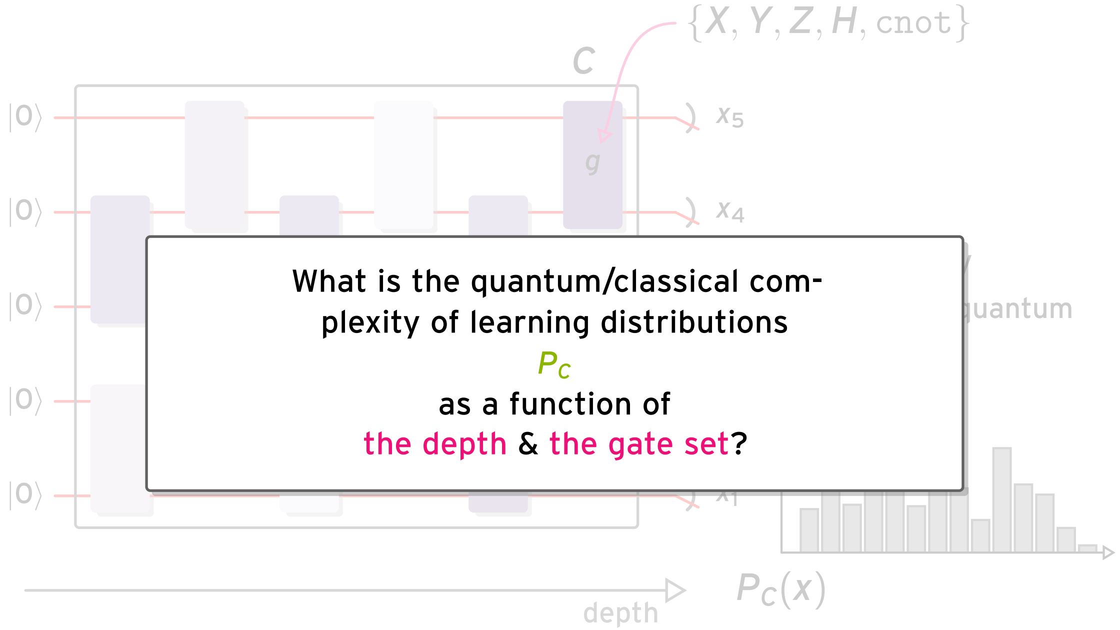
Output distributions of quantum circuits



- expressivity
- efficiently quantum generated



Output distributions of quantum circuits



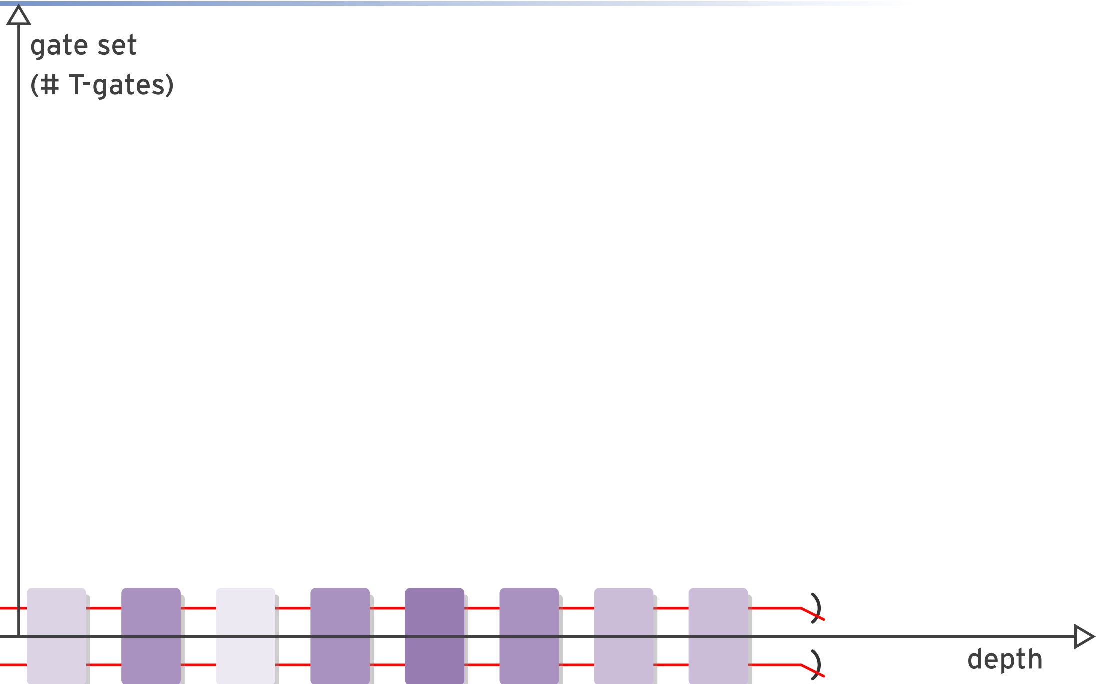
What is the quantum/classical complexity of learning distributions

P_C

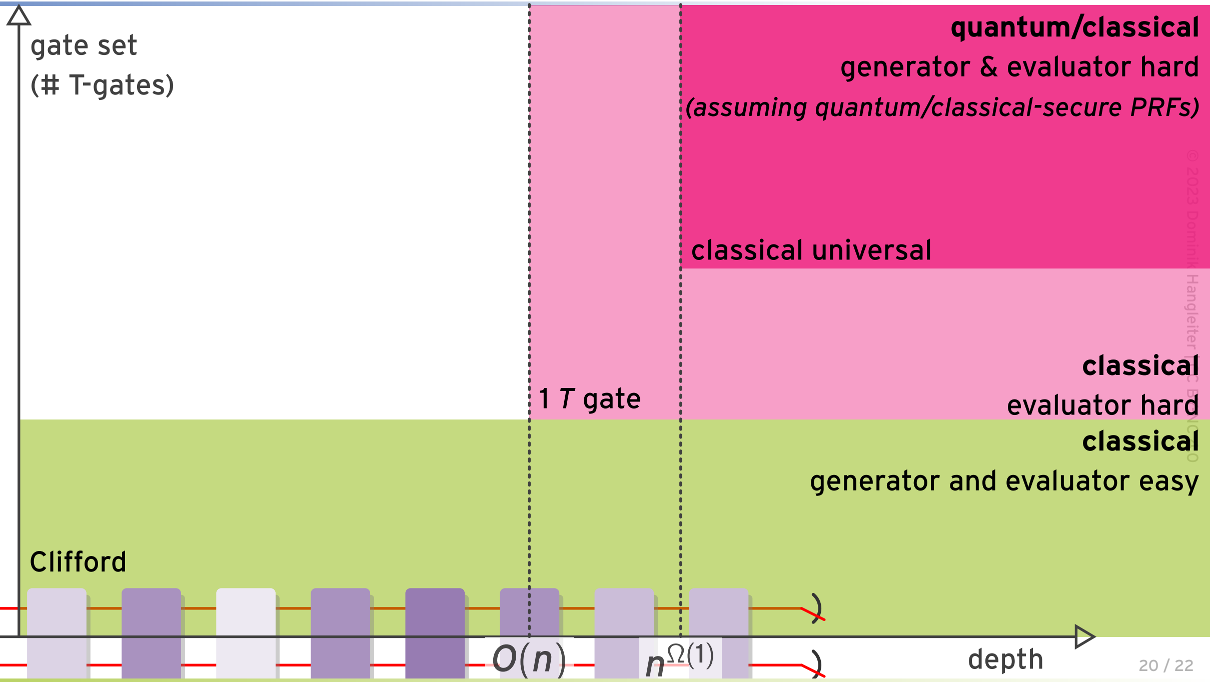
as a function of

the depth & the gate set?

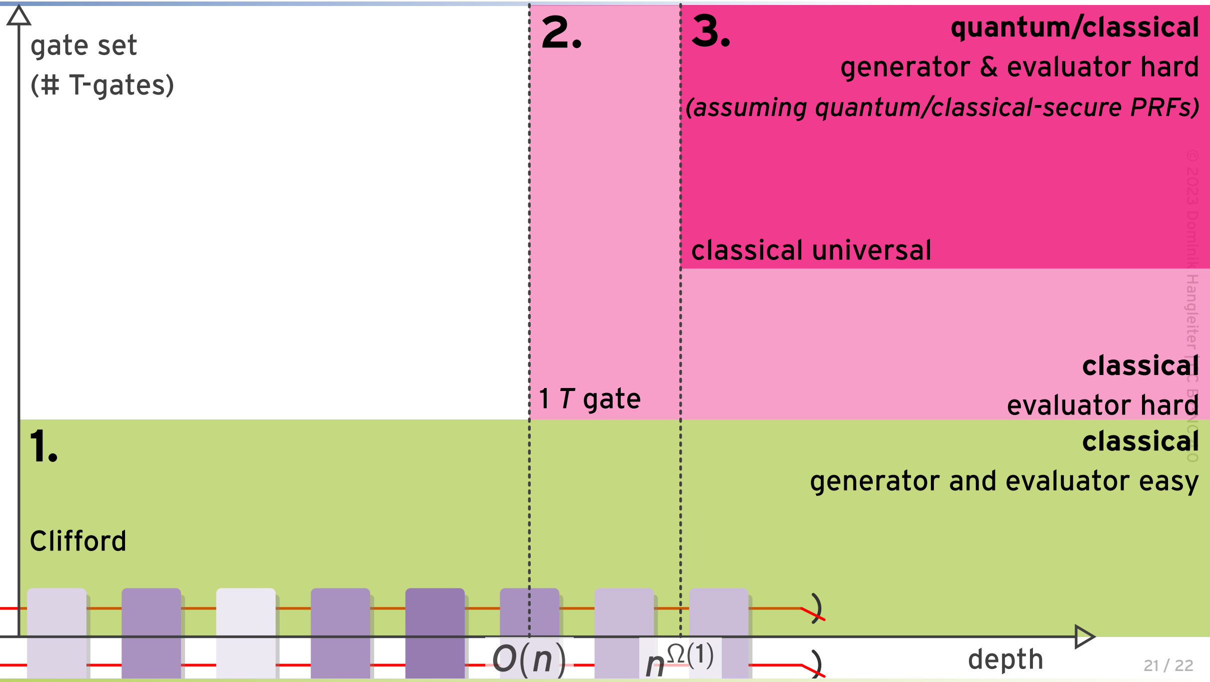
Our results



Our results


gate set
(# T-gates)
quantum/classical
generator & evaluator hard
(assuming quantum/classical-secure PRFs)
classical universal
1 T gate
classical
evaluator hard
classical
generator and evaluator easy
Clifford
$O(n)$
$n^{\Omega(1)}$
depth

Our results: Proof idea



Our results: Proof idea

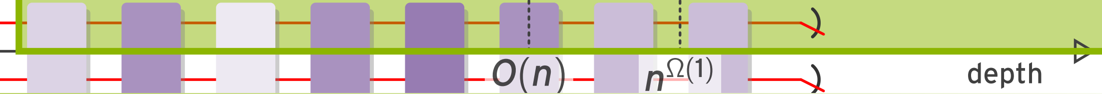
$$\forall \text{ Cliffords } C : P_C(x) = \begin{cases} 2^{-n} & \text{if } x = Rb + t,\ b \in \mathbb{F}_2^m \\ 0 & \text{else} \end{cases}$$

- Sample $O(n)$ strings $x_0, \ldots, x_k \leftarrow P_C$
- Find a basis of span(R) using Gaussian elmination with $y_i = x_0 + x_i$.

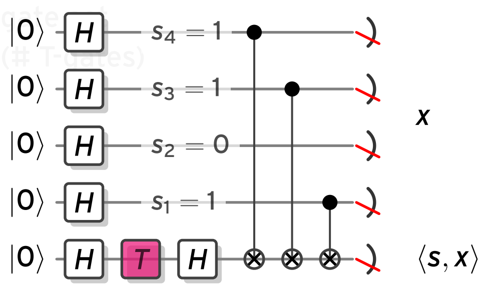
1. **classical**

generator and evaluator easy

Clifford



Our results: Proof idea



2.

3. **quantum/classical**
generator & evaluator hard
(assuming quantum/classical-secure PRFs)

classical universal

classical
evaluator hard

$$P_C(y) = \begin{cases} (1 - \sin^2(\frac{\pi}{8}))/2^n & \text{if } y = (x, \langle s, x \rangle) \\ \sin^2(\frac{\pi}{8})/2^n & \text{if } y = (x, \overline{\langle s, x \rangle}) \end{cases}$$

→ An efficient evaluator would be able to efficiently solve the **learning parity with noise** problem.

Our results: Proof idea

3. **quantum/classical**
generator & evaluator hard
(assuming quantum/classical-secure PRFs)

classical universal

Theorem 17 [KMRRSS94] Polynomial-size classical circuits are hard to learn with respect to a generator or an evaluator if a pseudorandom function (PRF) exists.

⟶ Quantum circuits can implement classical circuits.

[KMRRSS94] Kearns, Mansour, Ron *et al.*, On the learnability of discrete distributions (1994).

Discussion

SUMMARY

- Assessing the power of quantum learning is intricate!

OUTLOOK

- Learnability of low-depth circuits.
- Learnability of quantum samples.
- Is there an advantage for a relevant problem, e.g., learning *mixtures of Gaussians*?

Discussion

SUMMARY

- Assessing the power of quantum learning is intricate!

OUTLOOK

- Learnability of low-depth circuits.
- Learnability of quantum samples.
- Is there an advantage for a relevant problem, e.g., learning *mixtures of Gaussians*?

Discussion

arXiv:2007.14451
arXiv:2207.03140

SUMMARY

- Assessing the power of quantum learning is intricate!

OUTLOOK

- Learnability of low-depth circuits.
- Learnability of quantum samples.
- Is there an advantage for a relevant problem, e.g., learning *mixtures of Gaussians*?

THANK YOU!