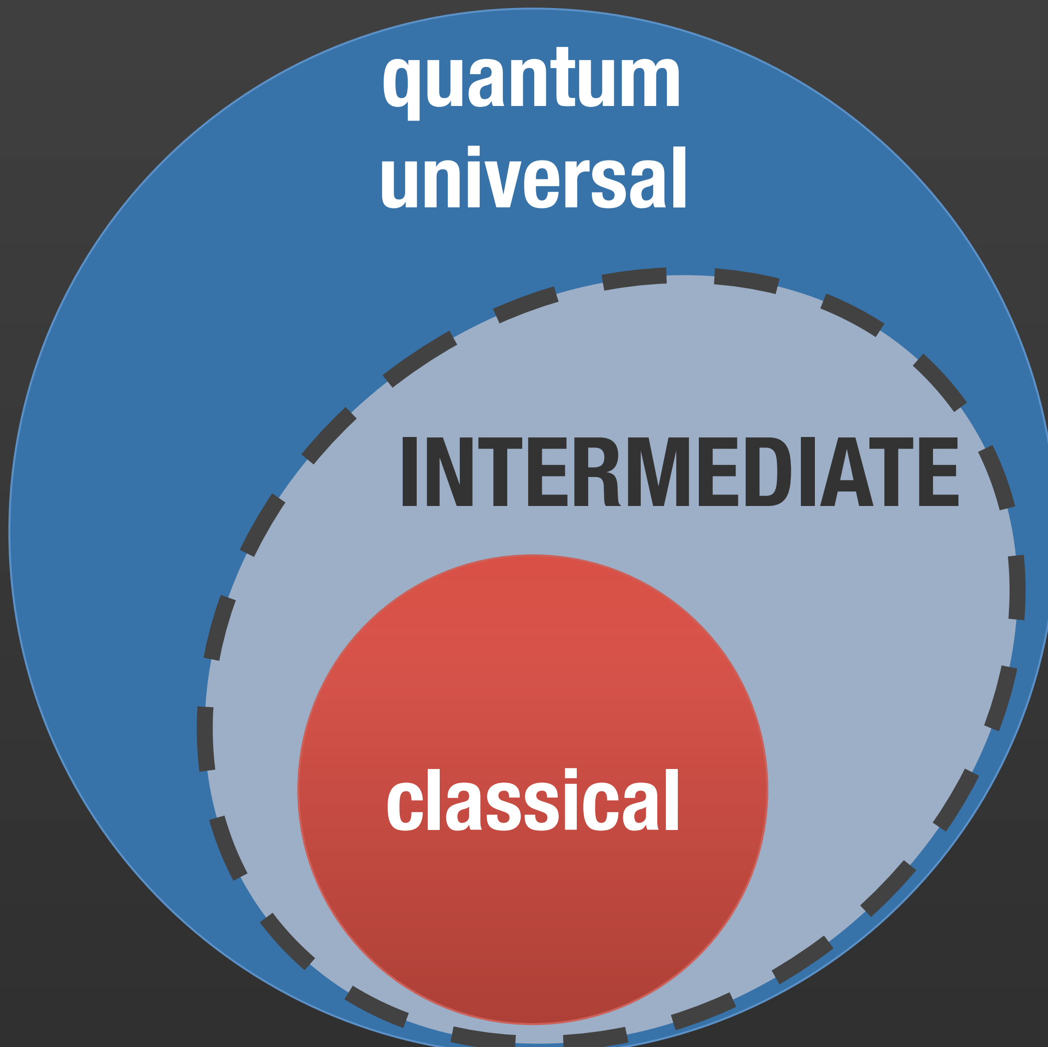
The computational power of normalizer circuits (over ∞ Abelian groups)

Juan Bermejo-Vega
Maarten Van den Nest, Cedric Yen-Yu Lin.
Max Planck Institute of Quantum Optics, MIT.

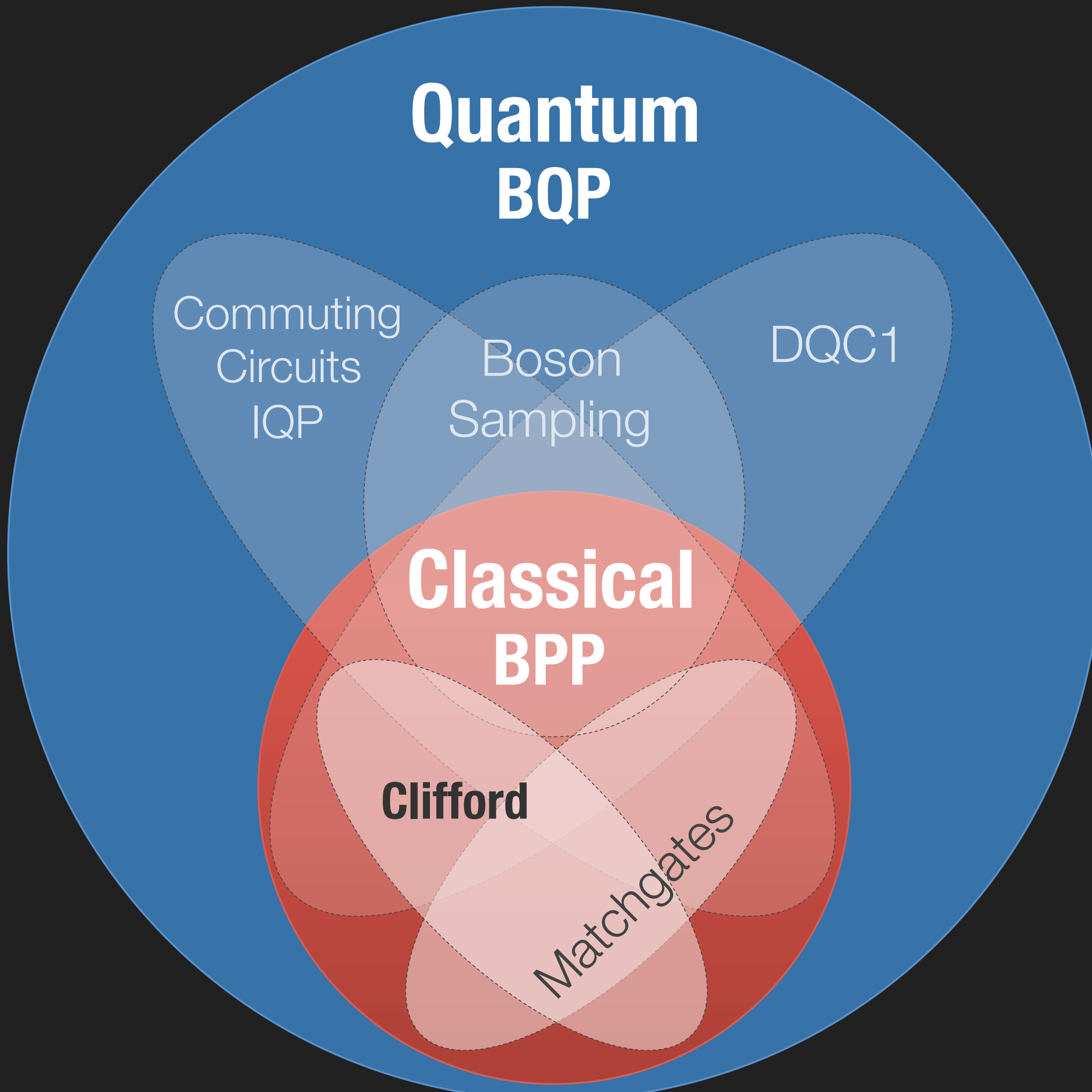
intermediate quantum computer



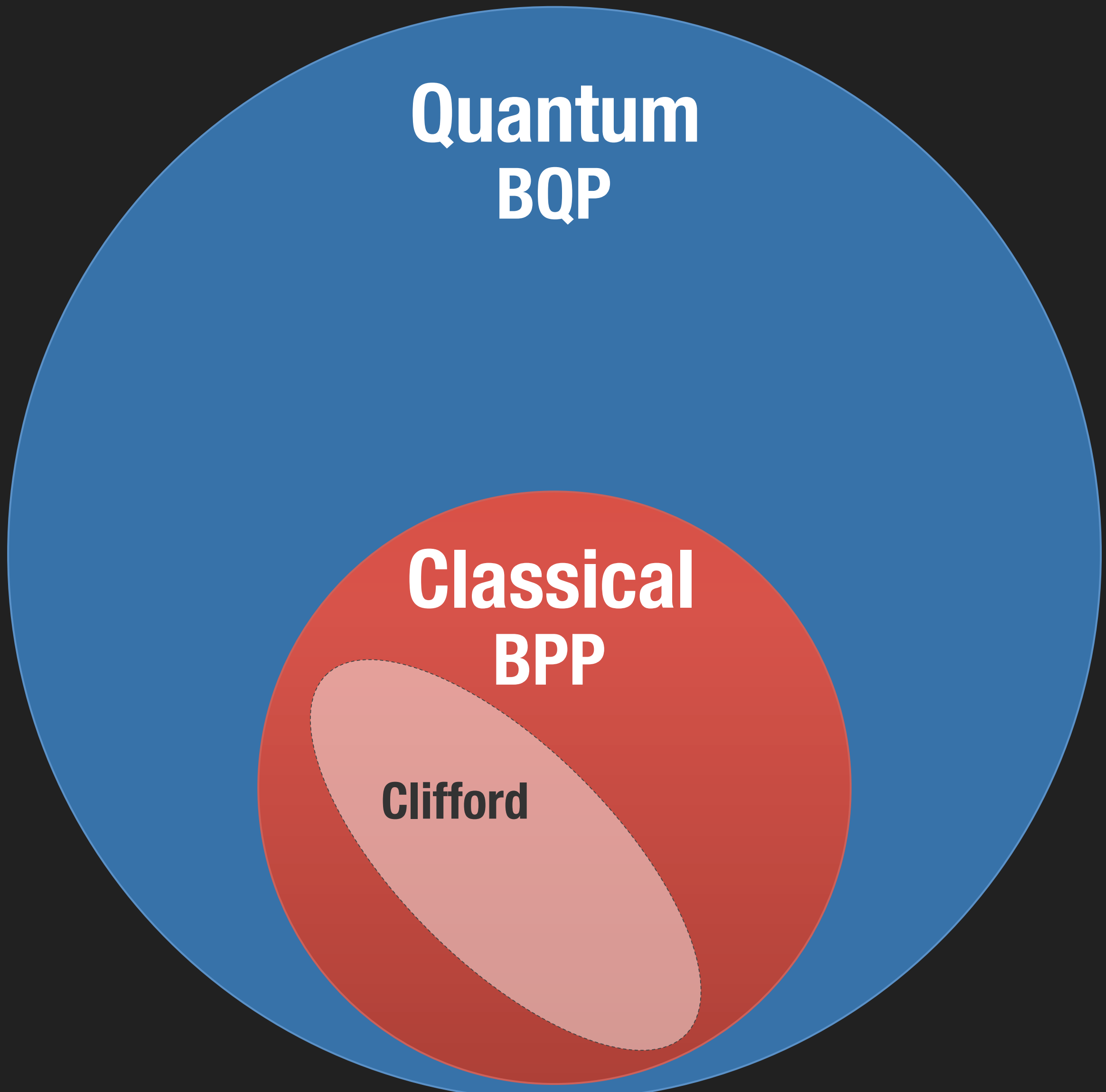
Motivation

how do you find a new quantum algorithm?

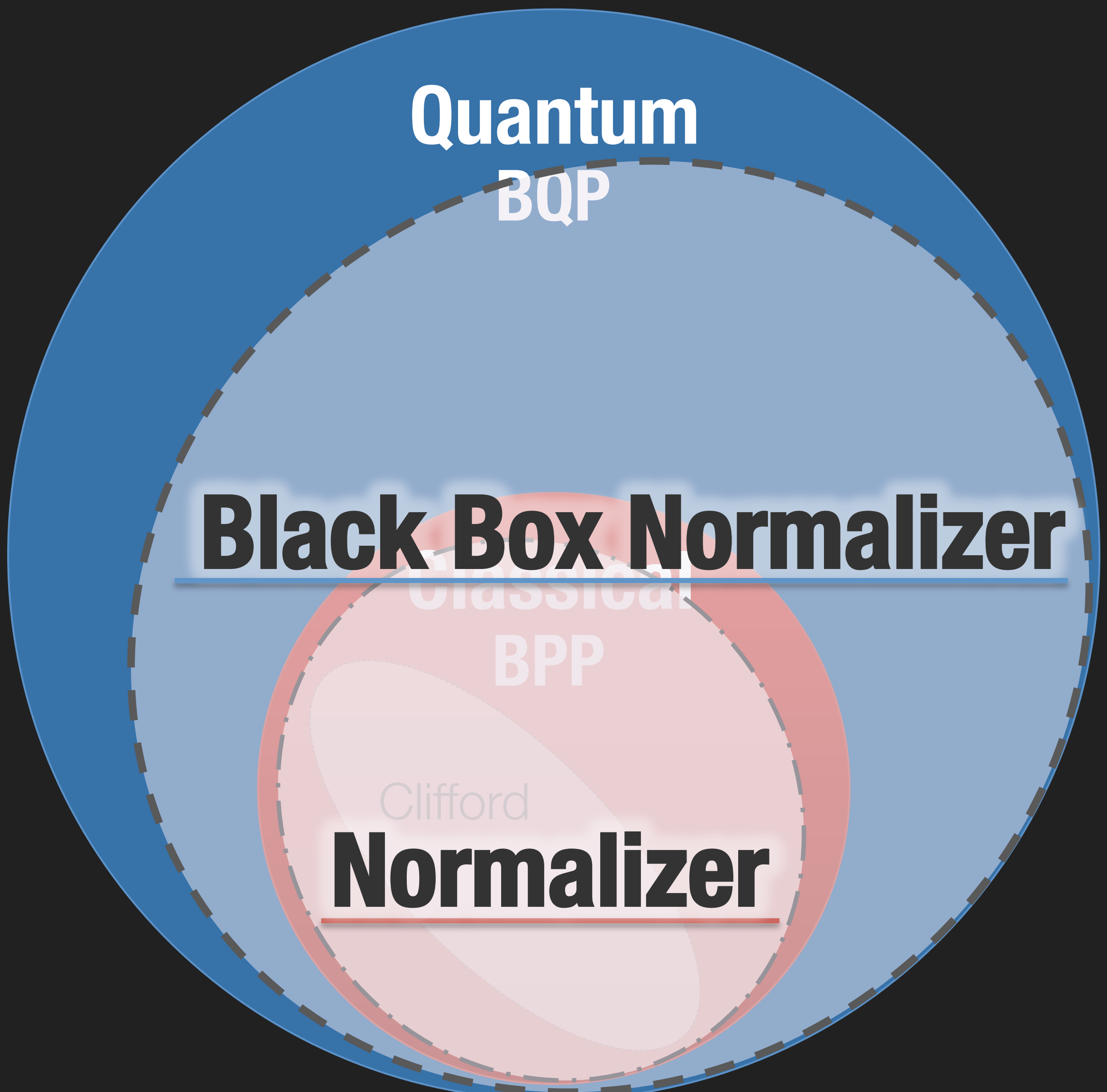
the missing middle



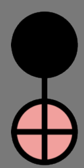
the missing middle



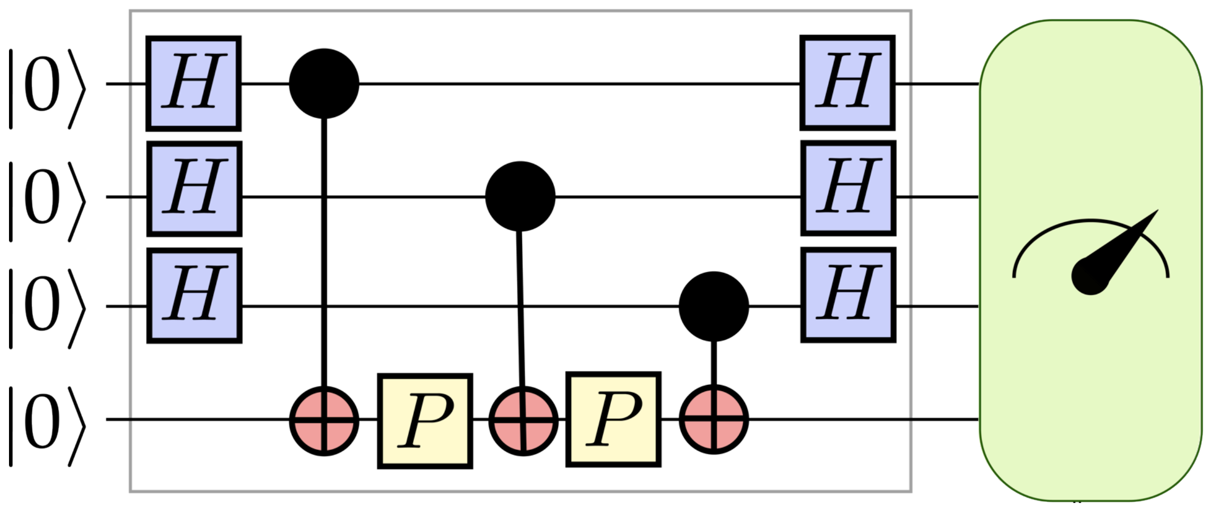
the missing middle



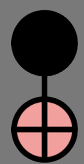
Clifford Circuits



$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

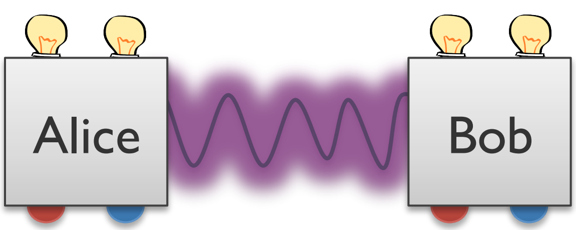


Clifford Circuits



$$\boxed{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \boxed{P} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

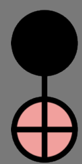
Quantum



Classical

$$\psi = \langle \mathrm{i}^a Z(x) X(y) \rangle$$

Clifford Circuits

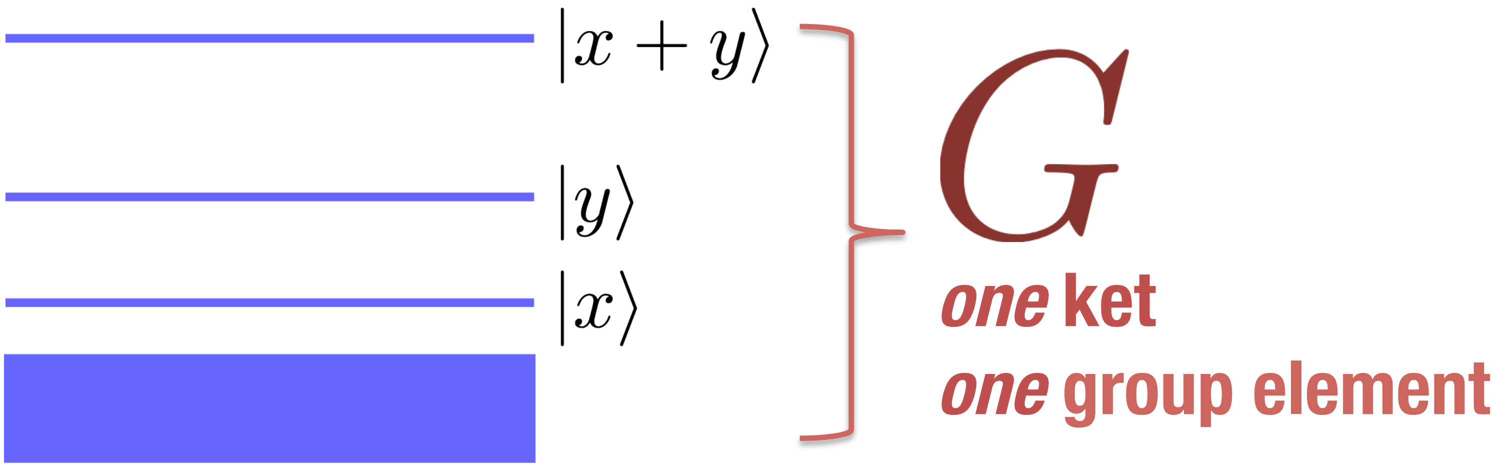


$$\boxed{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \boxed{P} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

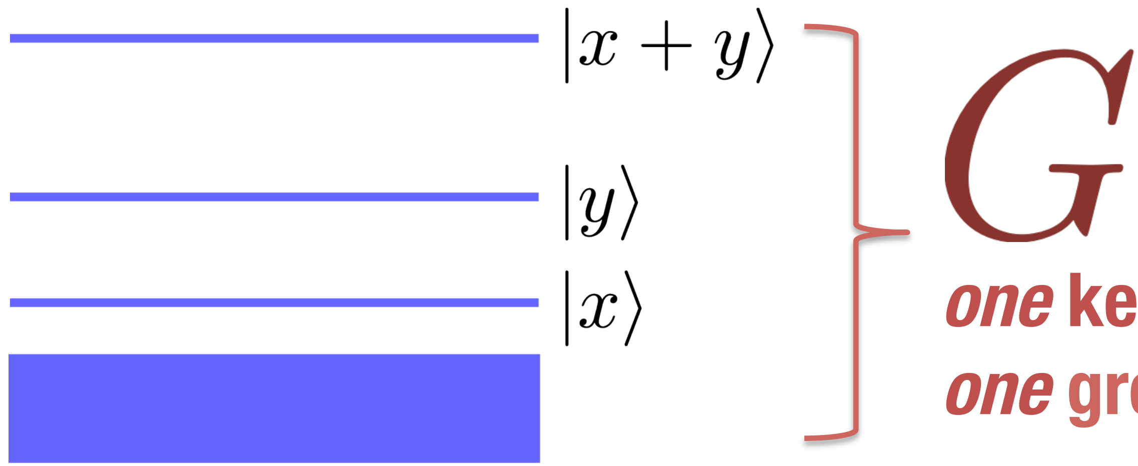
Maximal

Normalizer Circuits:
let’s go beyond qubits

Hilbert space of an (abelian) GROUP



Hilbert space of an (abelian) GROUP



one **ket**

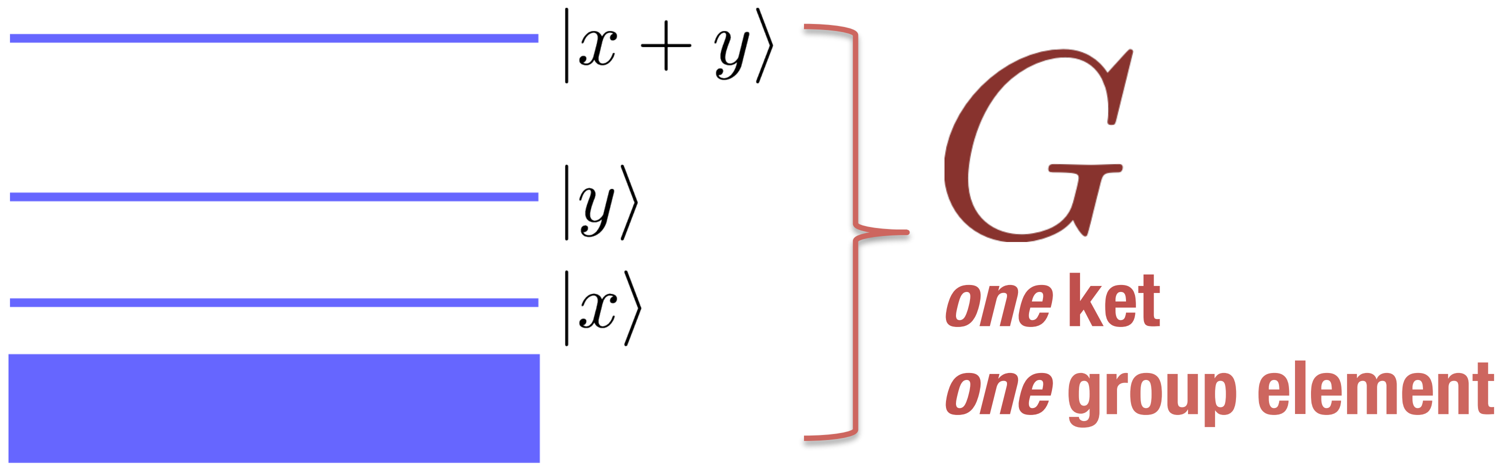
one **group element**

FINITE GROUP

n qubits

$$\mathbb{Z}_2^n \longleftrightarrow |01010\rangle$$

Hilbert space of an (abelian) GROUP



FINITE GROUP

n qubits

$$\mathbb{Z}_2^n \longleftrightarrow |01010\rangle$$

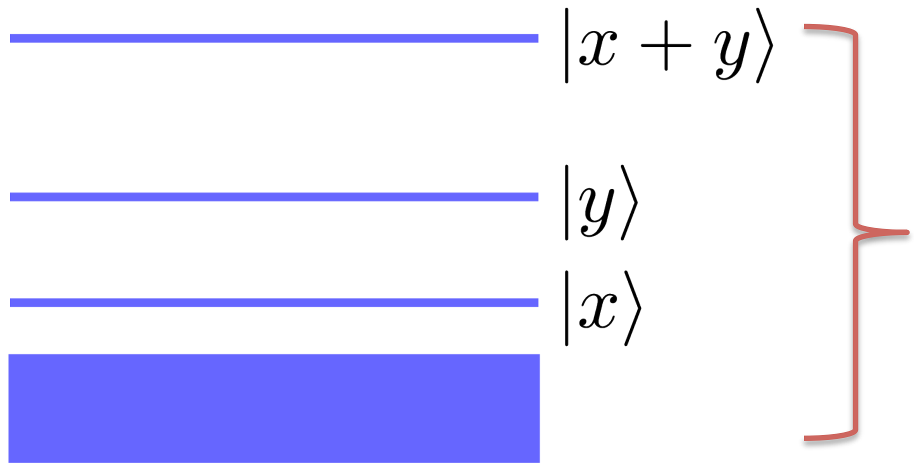
INFINITE GROUP

lattice basis + Fourier basis

$$\mathbb{Z} \longleftrightarrow |0\rangle, |\pm 1\rangle, |\pm 2\rangle, \ldots$$

$$\mathbb{T} \longleftrightarrow |\theta\rangle, \quad \theta \in [0, 2\pi)$$

Hilbert space of an (abelian) GROUP



G

one ket

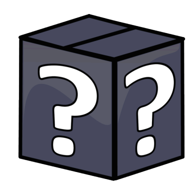
one group element

ELEMENTARY GROUP

$$G = \mathbb{T}^a \times \mathbb{Z}^b \times \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_c}$$

BLACK BOX GROUP

$\mathbf{Z}_N^{\times} \overset{?}{\cong}$

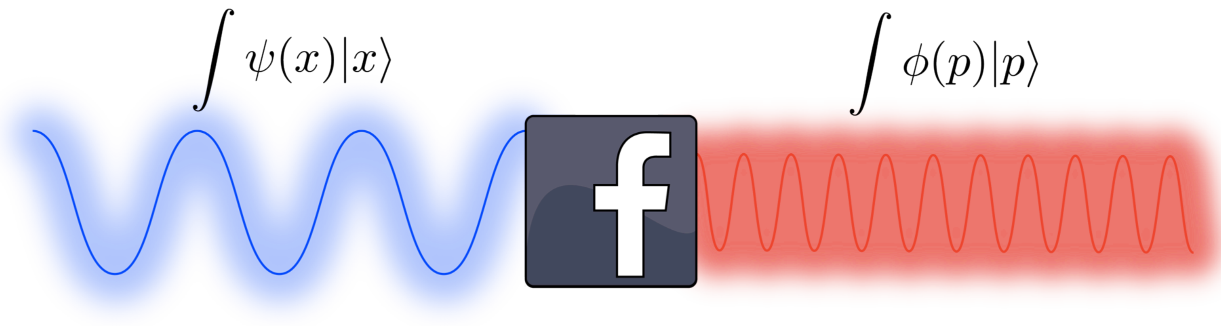


Normalizer Circuits

1

Quantum Fourier Transform

(Quantum) Fourier transform



DISCRETE Fourier Transform	$x, p \in \mathbb{Z}_d$	$\|p\rangle = \sum_{0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} p x} \|x\rangle$
Fourier SERIES	$x \in \mathbb{T}$	$\|p\rangle = \int_{\mathbb{T}} \mathrm{d}x \mathrm{e}^{-2\pi \mathrm{i} p x} \|x\rangle$
DISCRETE-TIME Fourier transform	$p \in \mathbb{Z}$	$\|x\rangle = \sum_{x \in \mathbb{Z}} \mathrm{e}^{2\pi \mathrm{i} p x} \|p\rangle$

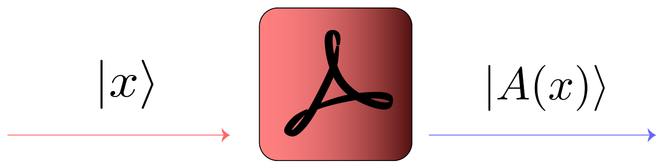
ALL NORMALIZER GATES

QUANTUM FOURIER TRANSFORM

LINEAR MAP GATE

QUADRATIC PHASE GATE

LINEAR MAP GATE



$$A(x+y) = A(x) + A(y)$$

QUADRATIC PHASE GATE

$$Q(x+y) = Q(x)Q(y)B(x,y)$$

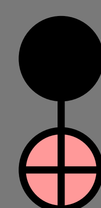
ALL NORMALIZER GATES

QUANTUM FOURIER TRANSFORM

LINEAR MAP GATE

QUADRATIC PHASE GATE

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$G = \mathbb{Z}_2^n$$

MAIN RESULT

MAIN RESULT

many quantum algorithms
are normalizer circuits
with black boxes

NORMALIZER CIRCUITS CAN

NORMALIZER CIRCUITS CAN

factorize (break RSA)

Shor 94

$\mathbb{Z} \times \mathbf{Z}_N^{\times}$

NORMALIZER CIRCUITS CAN

factorize (break RSA)

Shor 94
$\mathbb{Z} \times \mathbf{Z}_N^\times$

find discrete logarithms
(break DH, elliptic curve)

Shor 94
$\mathbb{Z}_{p'}^2 \times \mathbf{Z}_p^\times$

Proos-Zalka 04
$\mathbb{Z}^2 \times \mathbf{E}$

NORMALIZER CIRCUITS CAN

factorize (break RSA)

Shor 94
$\mathbb{Z} \times \mathbf{Z}_N^\times$

find discrete logarithms (break DH, elliptic curve)

Shor 94
$\mathbb{Z}_{p'}^2 \times \mathbf{Z}_p^\times$

Proos-Zalka 04
$\mathbb{Z}^2 \times \mathbf{E}$

solve Abelian hidden subgroup problems

Simon 94, Kitaev 95
Boneh-Lipton 95

NORMALIZER CIRCUITS CAN

factorize (break RSA)

Shor 94

$\mathbb{Z} \times \mathbf{Z}_N^\times$

find discrete logarithms (break DH, elliptic curve)

Shor 94

$\mathbb{Z}_{p'}^2 \times \mathbf{Z}_p^\times$

Proos-Zalka 04

$\mathbb{Z}^2 \times \mathbf{E}$

solve Abelian hidden subgroup problems

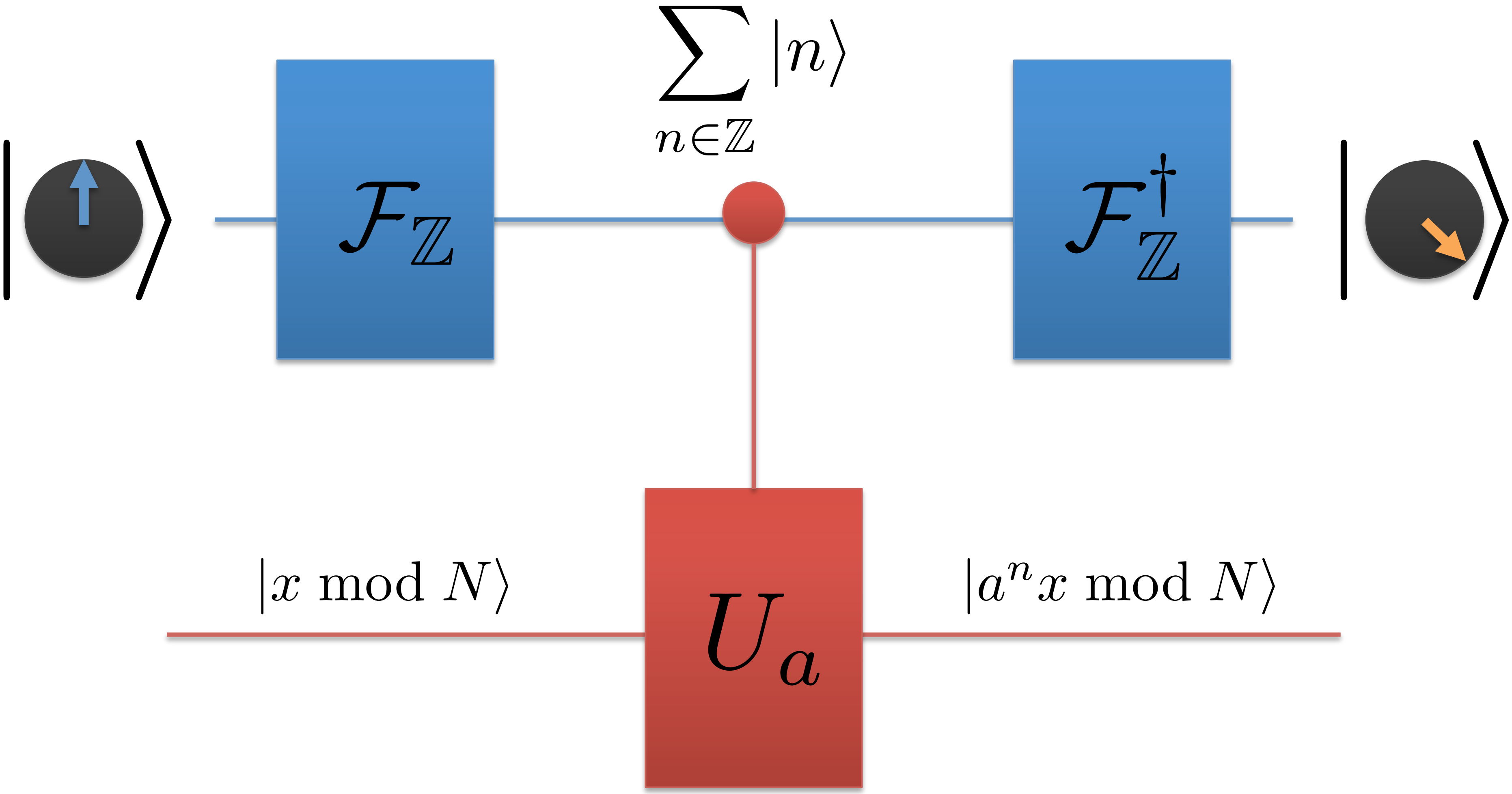
Simon 94, Kitaev 95
Boneh-Lipton 95

$F \times \mathbf{B}$

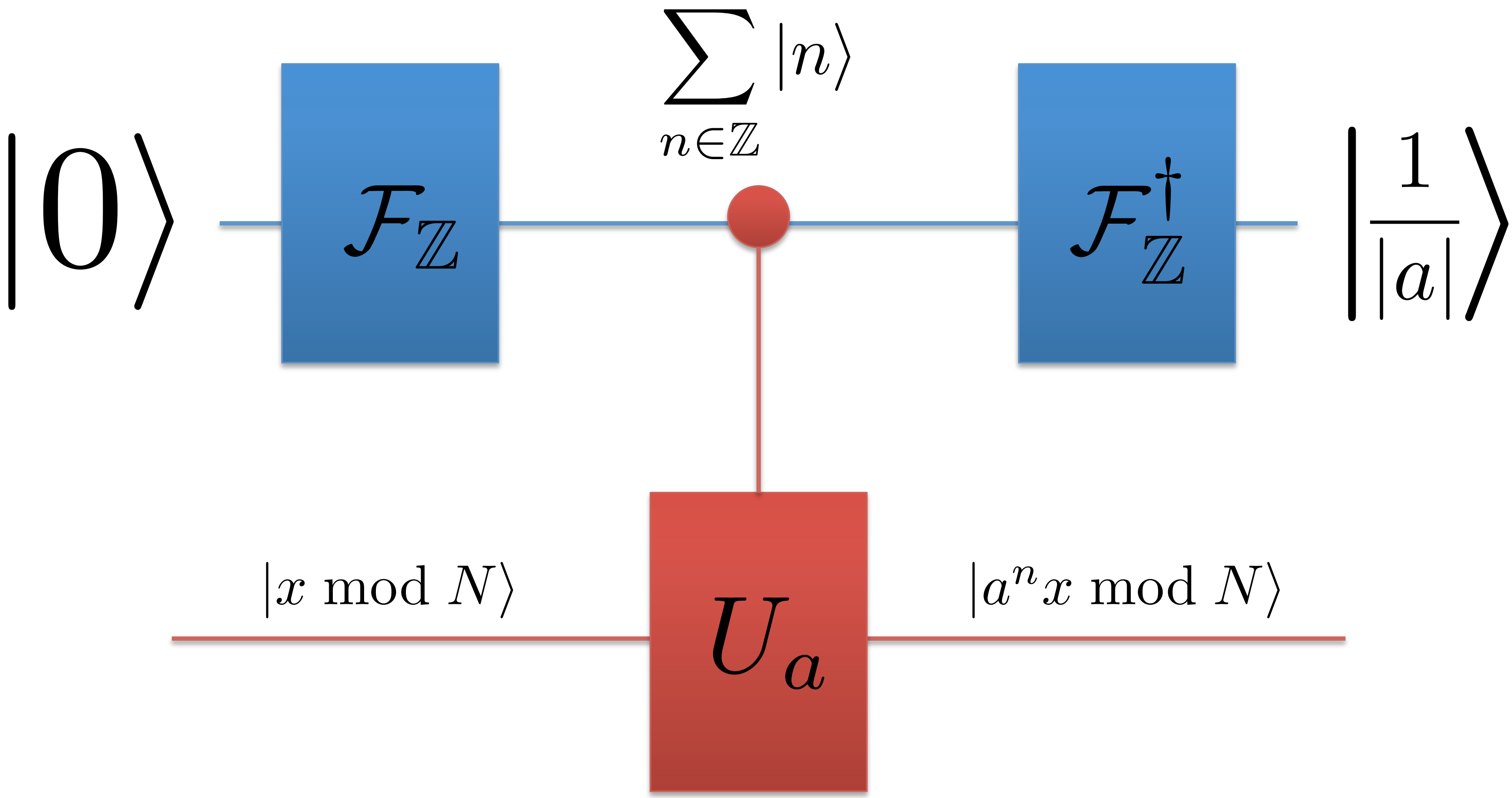
be classically simulated (if no black box)

$\mathbb{T}^a \times \mathbb{Z}^b \times \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_c}$

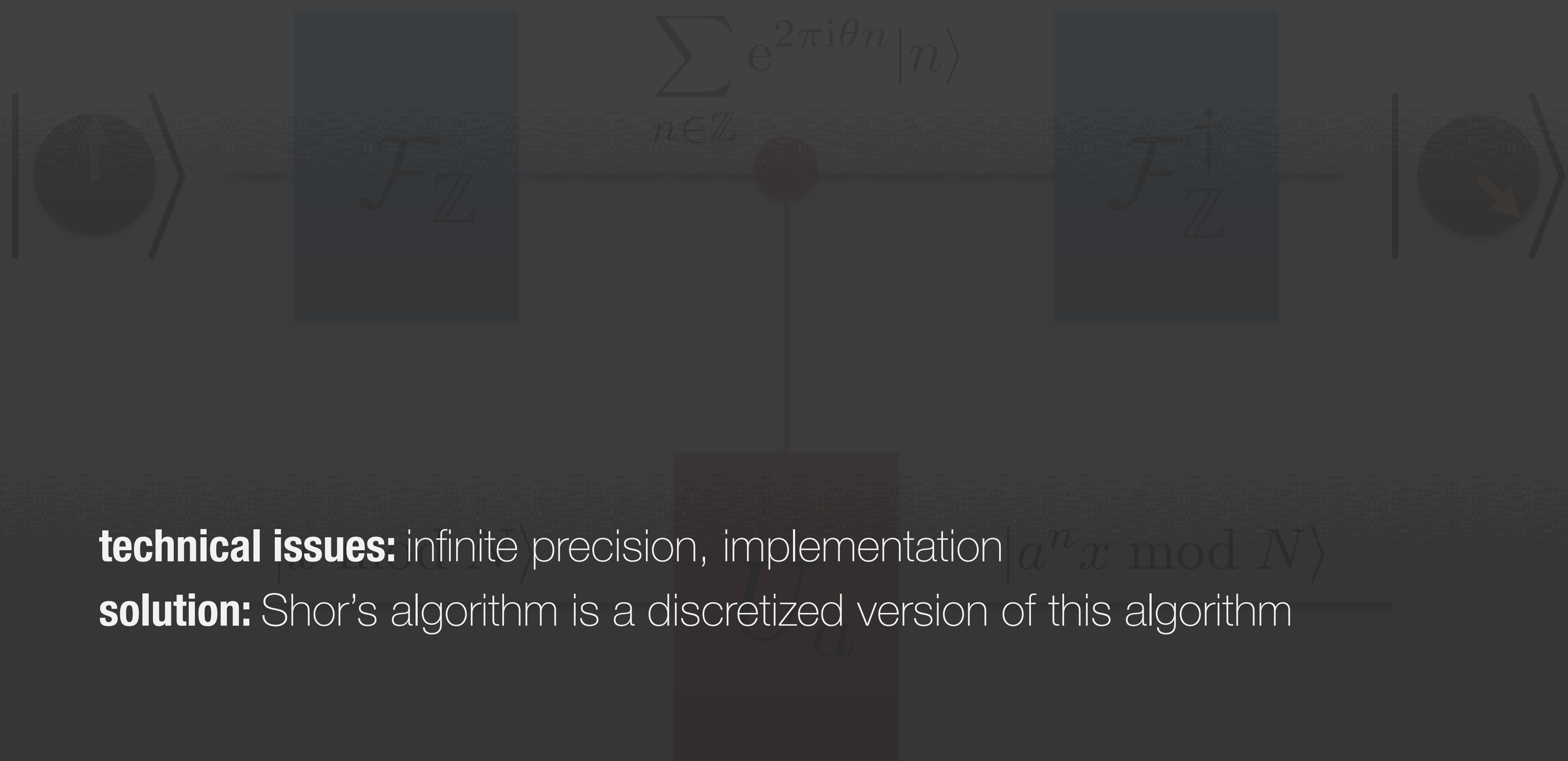
SHOR's ALGORITHM



SHOR's ALGORITHM



SHOR'S ALGORITHM



technical issues: infinite precision, implementation

solution: Shor's algorithm is a discretized version of this algorithm

Applications

Applications

a no-go theorem

decomposing black box groups

is **complete**

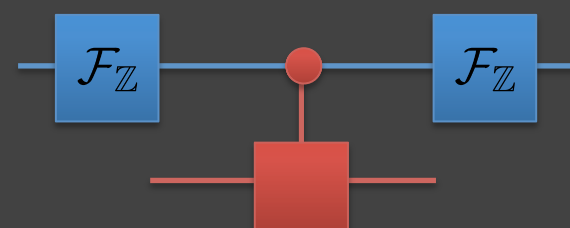
Cheung-Mosca 01

$\stackrel{?}{\cong} \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$

insight for algorithm design

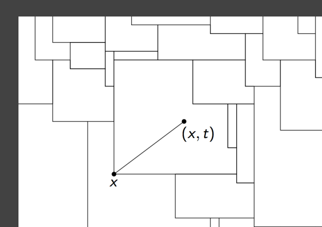
infinite Fourier transforms

aren't better than **2**



room for progress

algorithms for **infrastructures**



Hallgren
Sarvepalli
Wocjan
Fontein

simulation techniques

infinite stabilizer groups

$$\{\xi(\mu, g) Z(\mu) X(g)\}$$

Pauli X $X(g)|h\rangle = |g+h\rangle$

Pauli Z $Z(\mu)|h\rangle = \chi_\mu(h)|h\rangle$

normal forms

$$\xi(g) = e^{\pi i (g^T M g + C \cdot g)}$$

mixed integer linear equations

$$Ax + By = c$$

$$x \in \mathbf{Z}^m, y \in \mathbf{R}^n$$

Conclusions

a link between Clifford and Factoring

famous quantum algorithms are normalizer circuits

a better understanding of intermediate quantum devices
can lead to new insights in quantum algorithm design

THANKS!

Copyright statement

jbermejovega at gmail dot com

APPENDIX

and a joke

two normalizer circuits walk inside a bar
and they **order “finding”**

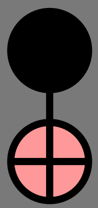
Clifford is Normalizer

Fourier

automorphism gate

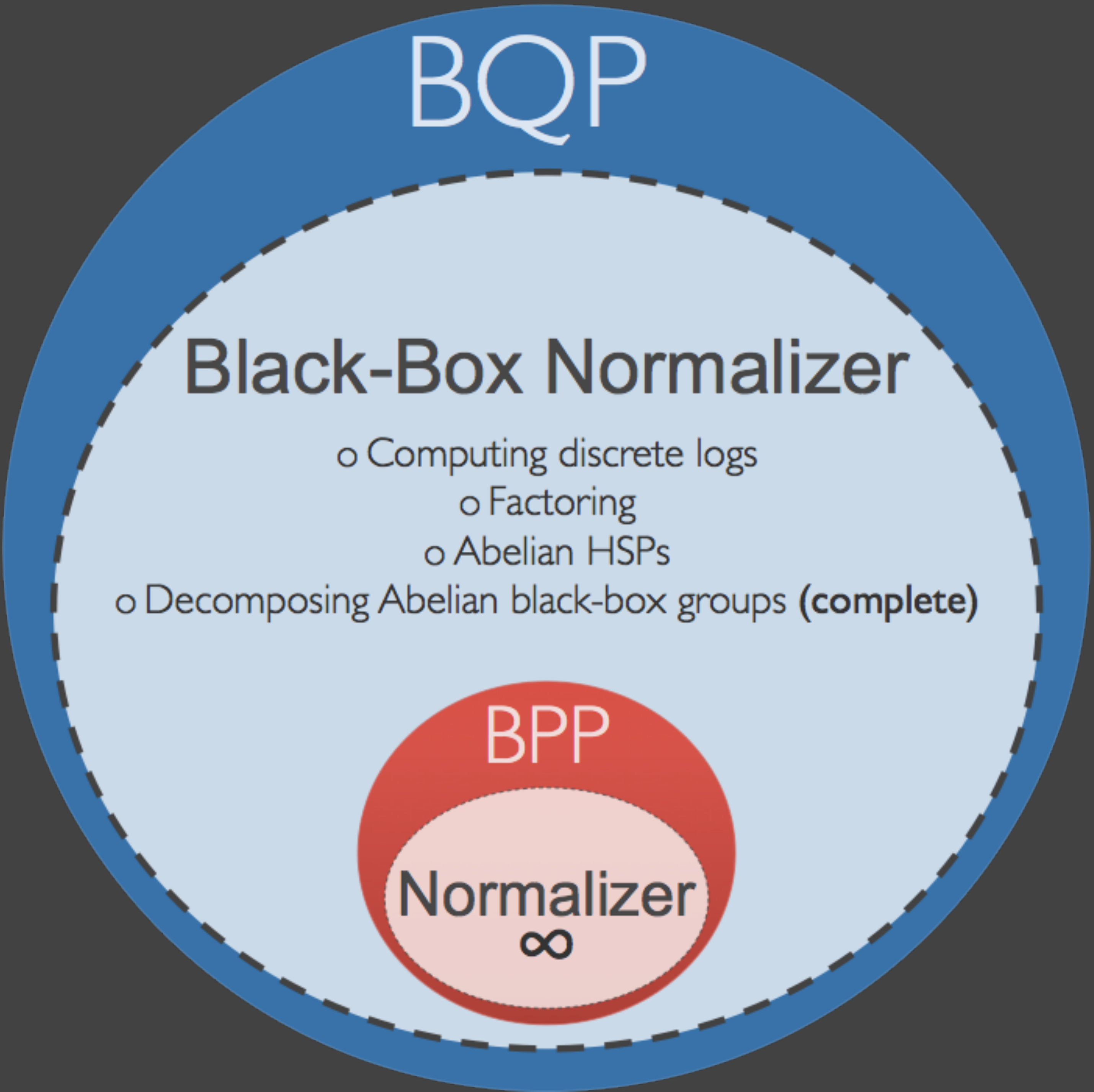
quadratic phase gate

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$G = \mathbb{Z}_2^n$$


BQP
Black-Box Normalizer
o Computing discrete logs
o Factoring
o Abelian HSPs
o Decomposing Abelian black-box groups **(complete)**
BPP
Normalizer
∞

new techniques for proof

infinite stabilizer groups

$$\{\xi(\mu, g) Z(\mu) X(g)\}$$

normal forms

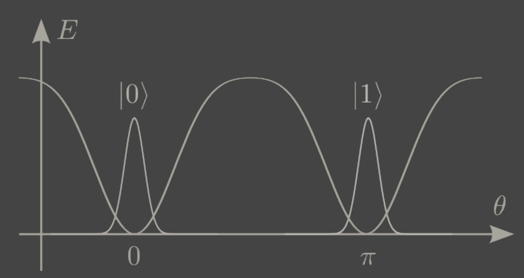
$$\xi(g) = e^{\pi i (g^T M g + C \cdot g)}$$

mixed integer linear equations

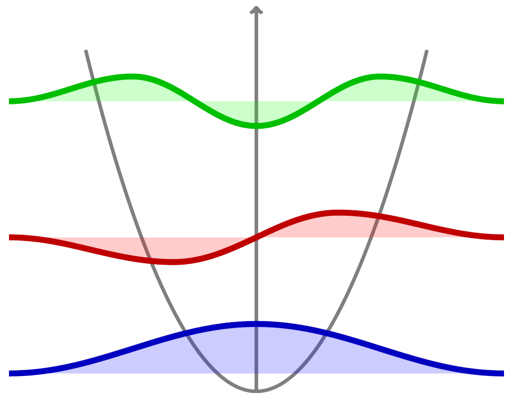
$$A x + B y = c$$

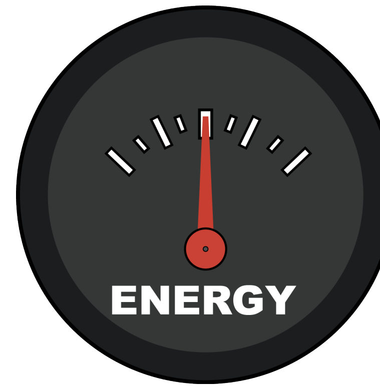
$$x \in \mathbf{Z}^m, y \in \mathbf{R}^n$$

sampling techniques



Types of simulations



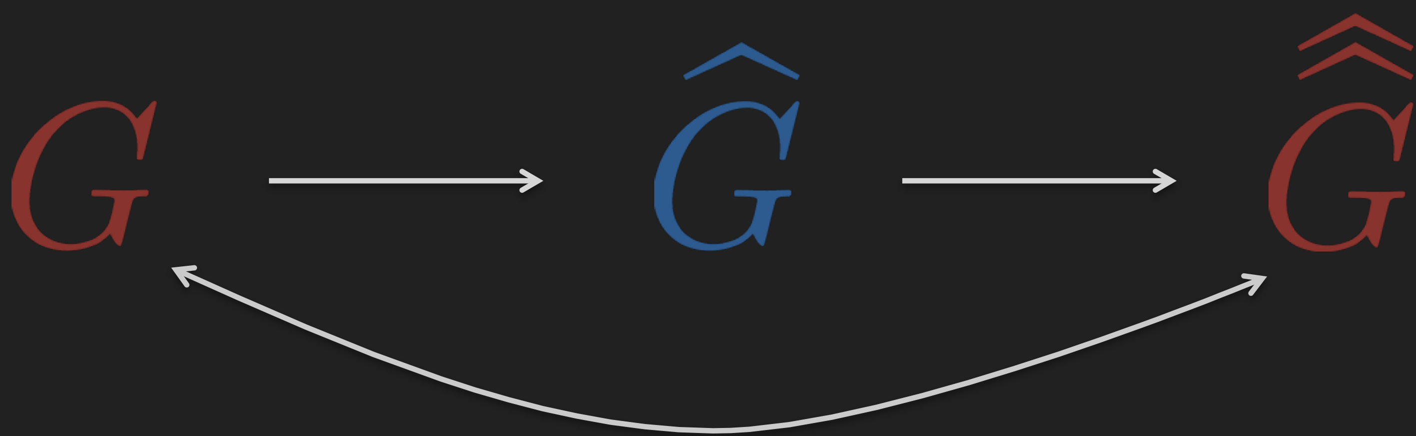


$$|\psi(x)|^2 \qquad \psi(x) \qquad \langle \psi | O | \psi \rangle$$

Probabilistic

Deterministic

G must fullfill Pontryagin's duality



$$\chi(g) = g(\chi)$$