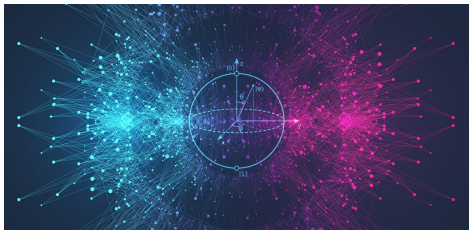
FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion



Introduction to Quantum Algorithms

Quantum Gates
Circle Notation
Basic Quantum Algorithms:
- Oracle functions
- Amplitude Amplification
- Quantum Fourier Transform
- Phase Estimation (phase logic)
- Shor's algorithm
- HHL, QSVM, QAOA, VQE

(Notebooks & instructions on Deepthought2: /lustre/software/qiskit)

Franz Klein
fklein@umd.edu
Dir. Q-Lab / HPC Engineer
ACIGS
Division of Information Technology
University of Maryland

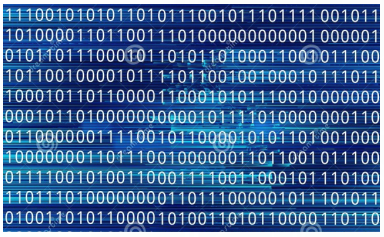
1

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Why Quantum Computing?

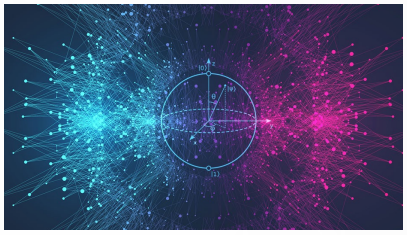
Modern-day digital computers
- ✓ extremely powerful
- ✓ backbone of the Information Age
- ✓ very high precision for arithmetic and algebraic calculations – anything with deterministic outcome

… all based on manipulating long strings of '0' and '1' (bits)



- limited when it comes to probabilistic problems:
  - probability distributions not or barely known or are complicated functions
  - data fitting may yield local minima instead of the global minimum
  - large number of parameters often result in exponential growth of complexity
- Random numbers (obtained via mathematical algorithms) are not completely random
  → large samples of random numbers won't cover the probability space equally
  → cybersecurity keys and encrypted data can, in principle, be decrypted by a third party

Quantum systems
- ➢ inherently probabilistic
- ➢ populate all possible states simultaneously
- ➢ quantum objects superpose (interfere) and can act coherently (entangled)
- ➢ number of states increases exponentially (2^N for N qubits)

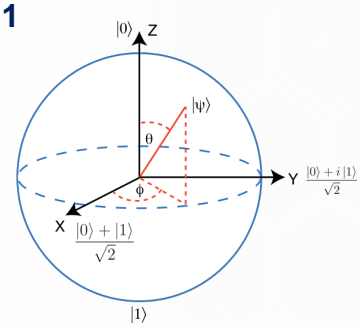


2

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Recall the basics 1

- Qubit is a 2-level quantum system, an *arbitrary* state is represented as linear combination of 2 base states, e.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with complex amplitudes α and β, normalized by $|\alpha|^2 + |\beta|^2 = 1$



- A qubit can point in any *arbitrary* direction on the Bloch Sphere using the angles θ and φ:

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2}\end{pmatrix}$$

- Vector representation: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ (*orthogonal Z-basis with* $\langle 0|1\rangle = 0$)

- Basis transformation: $\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ with $\boldsymbol{HH = 1}$

HAD gate (Hadamard gate)
→ $H|0\rangle$ results in 50-50 mixing of $|0\rangle, |1\rangle$ states
→ *H* also for inverse transf.: $|+\rangle \rightarrow |0\rangle$, $|-\rangle \rightarrow |1\rangle$

to *X-base kets*: $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$; $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

- Pauli gates: $\boldsymbol{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $\boldsymbol{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$, $\boldsymbol{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; Identity (no-op): $\boldsymbol{I} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

X-Gate swaps $|0\rangle \leftrightarrow |1\rangle$ (also called NOT gate)

- Rotation about z-axis (these gates change only the $|1\rangle$ component: relative phase rotation!):

P-Gate: $\boldsymbol{P(\phi)} = \begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix}$; $\boldsymbol{S} = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/2}\end{pmatrix}$; $\boldsymbol{T} = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$

(with $e^{i\phi} = \cos\phi + i\sin\phi$)

3

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Recall the basics 2

- Any state of a qubit (q_a) can be written as superposition: $|q\rangle_a = \alpha_0|0\rangle_a + \alpha_1|1\rangle_a = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}_a$

Coefficients α_0, α_1 are complex numbers, e.g. $\alpha_0 = |\alpha_0|\, e^{i\varphi_0}$ with magnitude, $|\alpha_0|$, and phase, φ_0, $|\alpha_0|^2$ and $|\alpha_1|^2$ are the probabilities that measuring $|q\rangle_a$ will yield the state $|0\rangle_a$ and $|1\rangle_a$, resp.
(index 'a' denotes that these are states of qubit q_a)

- Similarly, any state of different qubit (q'_b) can be written as: $|q'\rangle_b = \beta_0|0\rangle_b + \beta_1|1\rangle_b$
- Qubits q_a and q'_b have in total 4 levels: $\{|0\rangle_a, |1\rangle_a, |0\rangle_b, |1\rangle_b\}$, but we want to describe them as a combined system:
-

$$|q_a\, q'_b\rangle = |q\rangle_a \otimes |q'\rangle_b = \begin{pmatrix}\alpha_0\times\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\\ \alpha_1\times\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix} = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

→ space includes all possible superpositions of these 4 states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
normalization: $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = 1$

- Applying a gate to a single qubit affects all qubits, e.g. *X*-Gate applied to q'_b and identity gate to q_a:

$$I_a \otimes X_b = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}_a \otimes \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}_b = \begin{pmatrix}1\times\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} & 0\times\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\\ 0\times\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} & 1\times\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} = \begin{pmatrix}X & 0\\ 0 & X\end{pmatrix}$$

- Controlled Gates $G(q_t, q_c)$ perform operations on target qubit (q_t) only if the control qubit (q_c) is in state $|1\rangle$, e.g. apply a NOT gate on q'_b if q_a is in state $|1\rangle$, i.e. swap the coefficients of state $|10\rangle$ with $|11\rangle$:

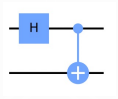
$$CNOT(q'_b, q_a)\begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix} = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_1\\ \alpha_1\beta_0\end{pmatrix} \rightarrow CNOT(q'_b, q_a) = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} = \begin{pmatrix}I & 0\\ 0 & X\end{pmatrix}$$

(*CNOT = CX*)

4

FEARLESS IDEAS
Inspiration | Boldness | Curiosity | Passion

Recall the basics 3



➢ **Entangled states**

- not described by tensor product (i.e. not $|q\rangle_a \otimes |q'\rangle_b$) but correlated states
- **Bell states** created via: $CNOT(q_t, q_c)|+0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; $CNOT(q_t, q_c)|+1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

➢ **More on CNOT(q_t, q_c) = CX(q_t, q_c)**

- if q_c is in $|+\rangle$ state and q_t in $|+\rangle$ or $|-\rangle$ state:

$$CNOT(q_t, q_c)|+-\rangle = CNOT(q_t, q_c)\left[|+\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = CNOT(q_t, q_c)\tfrac{1}{\sqrt{2}}|+0\rangle -$$

$$CNOT(q_t, q_c)\tfrac{1}{\sqrt{2}}|+1\rangle = \tfrac{1}{2}(|00\rangle + |11\rangle) - \tfrac{1}{2}(|01\rangle + |10\rangle) = \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = |--\rangle$$

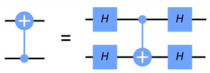
$$CNOT(q_t, q_c)|++\rangle = CNOT(q_t, q_c)\left[|+\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] = |++\rangle$$

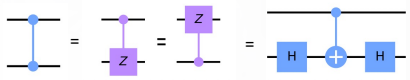
- if q_c is in $|1\rangle$ state and q_t in $|+\rangle$ or $|-\rangle$ state: $CNOT(q_t, q_c)|1+\rangle = |1\rangle \otimes X|+\rangle = |1\rangle \otimes |+\rangle = |1+\rangle$

$$CNOT(q_t, q_c)|1-\rangle = |1\rangle \otimes X|-\rangle = |1\rangle \otimes -|-\rangle = -|1-\rangle$$

- basis transformation (H-Gate) can be used to construct other controlled gates, e.g. **CZ = H CX H**

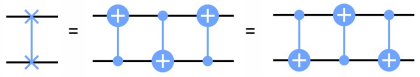
or to exchange target ←→ control qubit:





$$CZ = \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}$$

- qubit swapping q_b ←→ q_a :



- Note: there is **no COPY gate**: it is **not possible to clone qubits**!

5

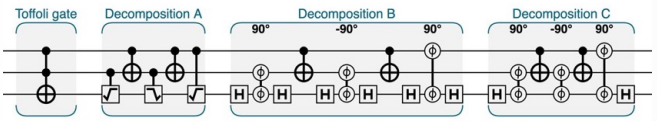
FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

More on Quantum Gates 1

- all **multi-qubit gates** can be written as **product of single- and two-qubit gates**

Toffoli gate (*CCX* or *CCNOT*):

$$CCX = \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & X \end{pmatrix}$$



Note:

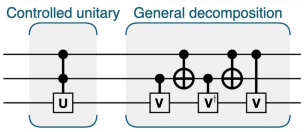
 ***RNOT* gate (*ROOT-NOT* or *SX* gate) with *(RNOT)² = X***

$$RNOT = \tfrac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

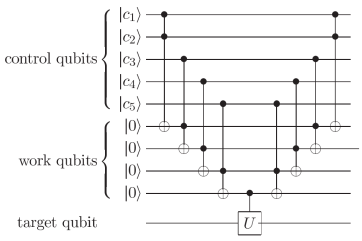
 $= RNOT^{\dagger} = SX^{\dagger}$ is the adjoint gate (adjoint ('dagger') means complex conjugate & transposed)

- in general: $CCU = V\ CX\ V^{\dagger}\ CX\ V$

(any doubly controlled unitary operator can be replaced by this series with $V^2 = U$)



- multi-controlled gate (C^nU):
requires a CXX ladder & CU gate & ladder uncompute



(see Nielsen & Chuang, Chap.4 for n=5: with n-1 work (scratch) qubits)

6

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

More on Quantum Gates 2

- **Rotations**

Note: $P(\varphi)$, $S = P(\pi/4)$, $T = P(\pi/8)$ change the relative phase between $|0\rangle$ and $|1\rangle$ states

General rotation: $U(\vartheta,\varphi,\lambda) = \begin{pmatrix} \cos\left(\frac{\vartheta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\vartheta}{2}\right) \\ e^{i\varphi}\sin\left(\frac{\vartheta}{2}\right) & e^{i(\varphi+\lambda)}\cos\left(\frac{\vartheta}{2}\right) \end{pmatrix}$ so: $P(\varphi) = U(0,\varphi,0)$

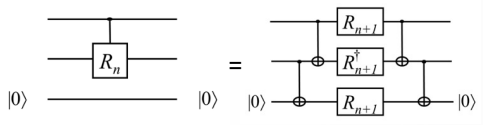
Rotation about x-axis: $R_x(\vartheta) = \begin{pmatrix} \cos\left(\frac{\vartheta}{2}\right) & -i\sin\left(\frac{\vartheta}{2}\right) \\ -i\sin\left(\frac{\vartheta}{2}\right) & \cos\left(\frac{\vartheta}{2}\right) \end{pmatrix} = U\left(\vartheta, -\frac{\pi}{2}, \frac{\pi}{2}\right)$

Rotation about y-axis: $R_y(\vartheta) = \begin{pmatrix} \cos\left(\frac{\vartheta}{2}\right) & -\sin\left(\frac{\vartheta}{2}\right) \\ \sin\left(\frac{\vartheta}{2}\right) & \cos\left(\frac{\vartheta}{2}\right) \end{pmatrix} = U(\vartheta,0,0)$

Rotation about z-axis: $R_z(\varphi) = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix} = e^{-i\varphi/2}\ U(0,\varphi,0) = e^{-i\varphi/2}\,P(\varphi)$

R_n – Gate: $R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^{n-1}} \end{pmatrix} = P\left(\frac{\pi}{2^{n-1}}\right)$ so: $R_1 = Z$, $R_2 = S$, $R_3 = T$

QFT requires controlled R_n gates for a series of n
→ efficiently decomposed with help of a scratch qubit (needs 4 $CNOT$, 2 R_{n+1}, 1 $R_{n+1}^{\dagger}$)



7

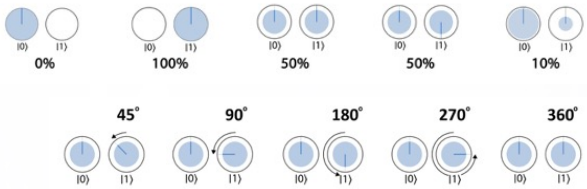
FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Circle Notation 1

(https://www.machinelevel.com/qc/doc/qcengine_workbench.html)

(examples from "Programming Quantum Computers" by E.Johnston, N.Harrigan, M. Gimeno-Segovia, O'Reilly 2019)

- easier to visualize when working with multiple qubits
- 1 circle for each base state: filled area = magnitude, line = phase (recall: $\alpha_0 = |\alpha_0|\, e^{i\varphi_0}$)

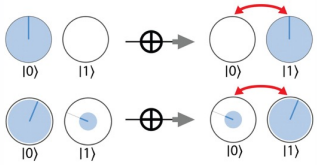


Examples:

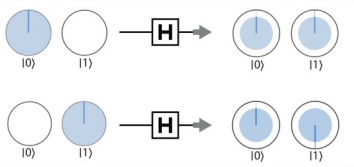
Probability to measure value 1.

Relative phase **(Note: only the relative phase matters)**

- **NOT gate** in circle notation:

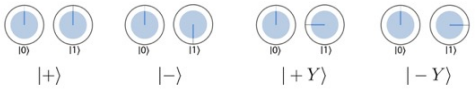


- **Hadamard gate** acting on base states:



- **Phase(45) gate** in circle notation:

- **X and Y base states** (as superpositions of $|0\rangle$, $|1\rangle$):



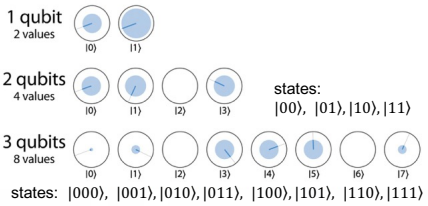
8

FEARLESSLY FORWARD

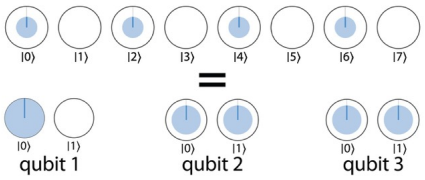
Inspiration | Boldness | Curiosity | Passion

Circle Notation 2

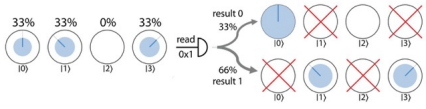
- **multiple-qubits registers**:



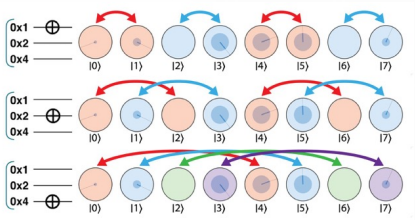
- multiple-qubits register in terms of single-qubit states:



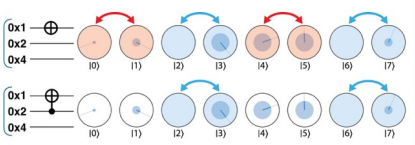
- **reading** qubit 1 in a two-qubit register:



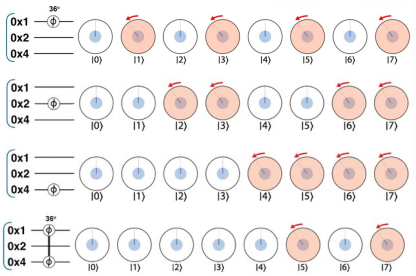
- **NOT gate on single qubits** in a 3-qubit reg.:



- **NOT gate** and **CNOT gate:**



- **single-phase** and **conditional phase rotation:**



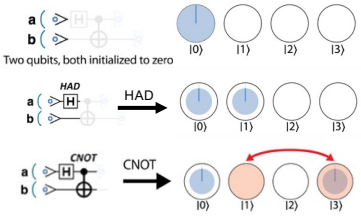
9

FEARLESSLY FORWARD

Inspiration | Boldness | Curiosity | Passion

Circle Notation 3

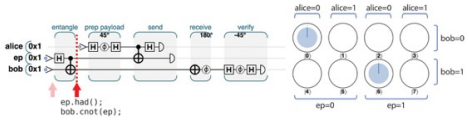
- Example: **Bell pair**



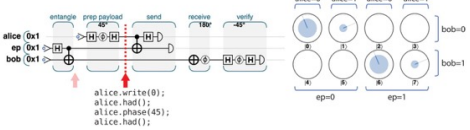
- Example: **Teleportation**

Alice and Bob share a Bell pair,
Alice prepares a payload and links it to her Bell qubit,
Alice measures both of her qubits and send the values to Bob,
Bob performs conditional transformations of his Bell qubit and obtains an exact copy of Alice's payload qubit.

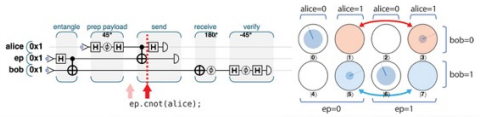
Step 1: create an entangled pair (ep – bob):



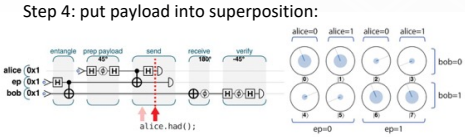
Step 2: Alice prepares the payload:



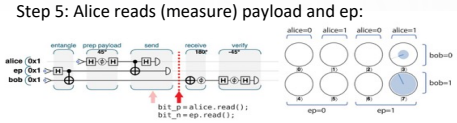
Teleportation (cont.)
Step 3: link payload with entangled pair:



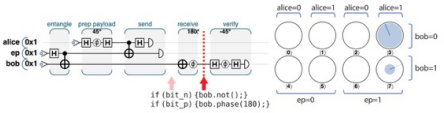
Step 4: put payload into superposition:



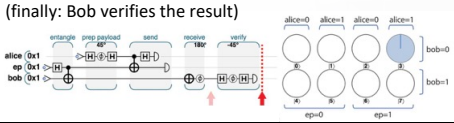
Step 5: Alice reads (measure) payload and ep:



Step 6: Bob conditionally transforms his entangled qubit:



(finally: Bob verifies the result)



10

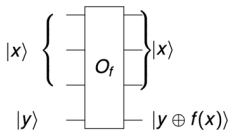
FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Basic Quantum Algorithms 1

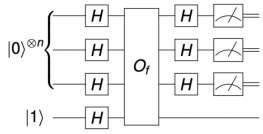
A) Oracle functions

➢ speedup based on superposition (interference) instead of testing each case

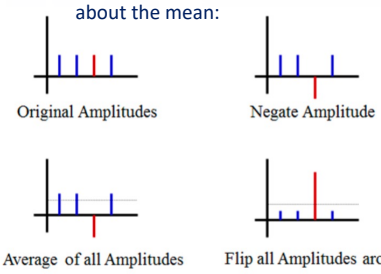
(1985 first quantum algorithm by D. Deutsch, generalized in collab. with Jozsa:
Consider a circuit (oracle) that implements a comparator function, and we are asked whether the function is constant (returns the same value for all inputs) or balanced (returns 1 on one input and 0 on another).

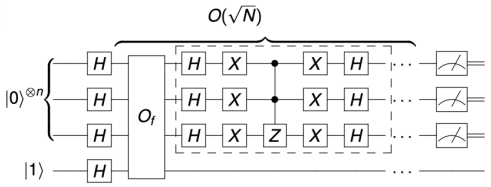


Implemented as (n+1)-qubit circuit:



➢ **Grover's algorithm**: search for a specific element in an unsorted list
- oracle function based on inversion about the mean:



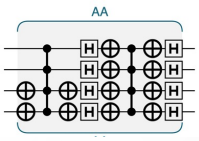


11

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

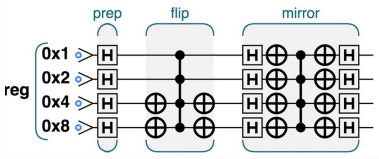
Basic Quantum Algorithms 2

B) Amplitude Amplification (AA or QAA)
(generalization of Grover's algorithm)



➢ **convert phase differences into within a quantum register into detectable variations in magnitudes**

E.g. all values in a 4-qubit register have same magnitudes but one has a different phase. → How to select this value?



➢ apply a sequence of "flip + mirror" operations:
- flip allow to target a value of the register
- mirror converts phase difference into magnitude difference

Probability fluctuates in AA iterations:

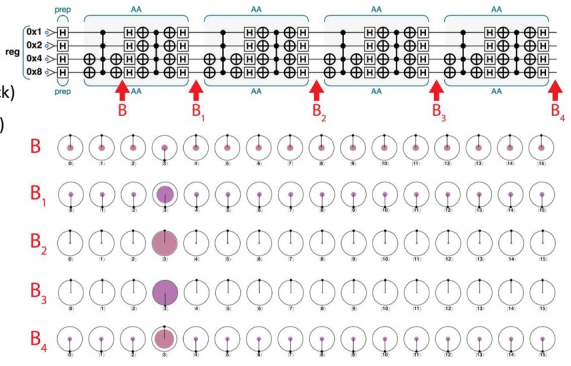
1 iter.: 47.3% prob. (all phases flipped)

2 iter.: 90.8% prob. (all phases flipped back)

3 iter.: 96.1% prob. (marked value flipped)

4 iter.: 58.2% prob. (all others flipped)

…



➢ optimal number of iterations

$$N_{AA} \approx \frac{\pi}{4}\sqrt{\frac{2^n}{m}}$$

(*n*=number of qubits, *m*=number of marked (flipped) values)

12

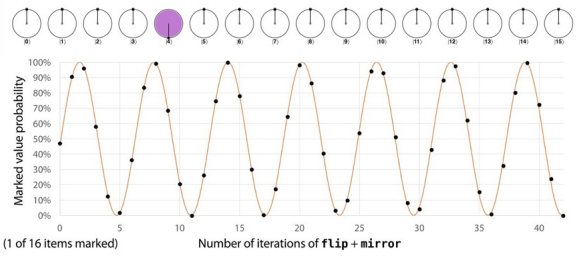
FEARLESSLY FORWARD

Inspiration | Boldness | Curiosity | Passion

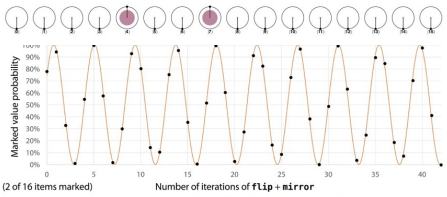
Basic Quantum Algorithms 3

AA probability fluctuations:

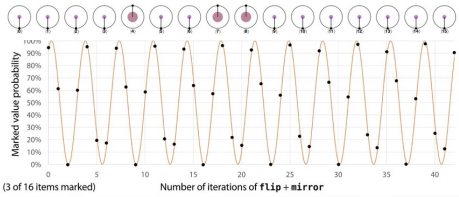
1 marked value
(max. prob. at 9th, 15th, 40th iterations: > 99.9%)



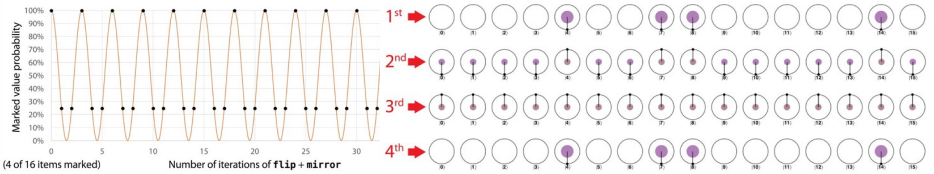
2 marked values:



3 marked values:



4 marked values:



5-7 marked values: fluctuating prob. ; 8 marked values: constant prob. at 50%

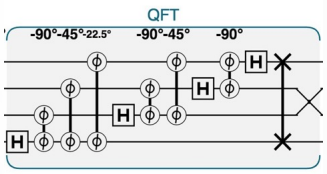
13

FEARLESSLY FORWARD

Inspiration | Boldness | Curiosity | Passion

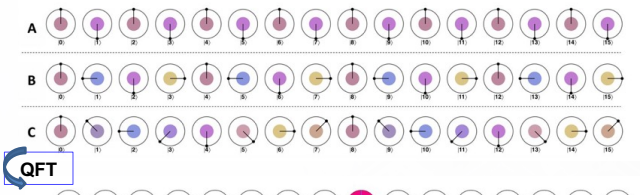
Basic Quantum Algorithms 4

C) Quantum Fourier transform (QFT)



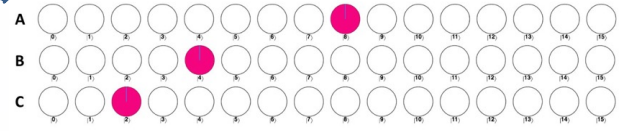
- **access hidden patterns stored in phases and/or magnitudes of a quantum register**
- allows for reading out the frequency with which values vary; the mirror-image peaks whenever the phase shifts by 180° (precision relative to twice the number of qubits)
- more complex signals produce a superposition of frequency values → rerun QFT multiple times

E.g. suppose a 4-qubit register contains one of these 3 states

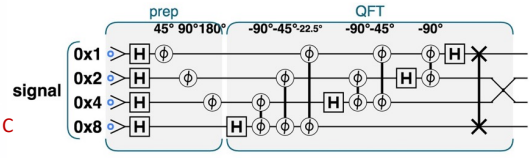


QFT

then applying QFT would result in single non-zero values
(state A: 8 full cycles,
state B: 4 full cycles,
state C: 2 full cycles)



Input data: e.g. 4-qubit signal preparation for state C



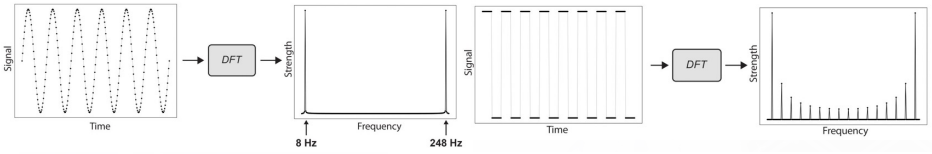
14

FEARLESSLY FORWARD

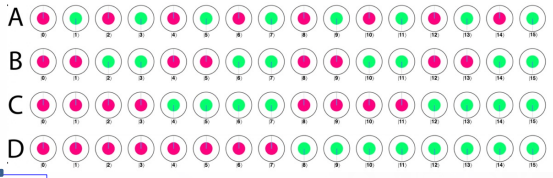
Inspiration | Boldness | Curiosity | Passion

Basic Quantum Algorithms 5

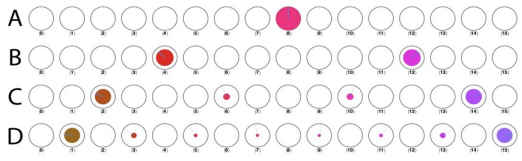
QFT is practically a Discrete Fourier Transform (like FFT), but all possible solutions appear simultaneously



E.g. suppose a 4-qubit register contains one of these 4 states
(note: all values have phase=0 or 180°)

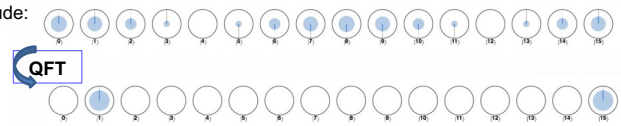


QFT



QFT results in a superposition of discrete frequencies with different weights
→ requires multiple readouts to access the values

- in many cases oscillations are encoded as variations of magnitude:



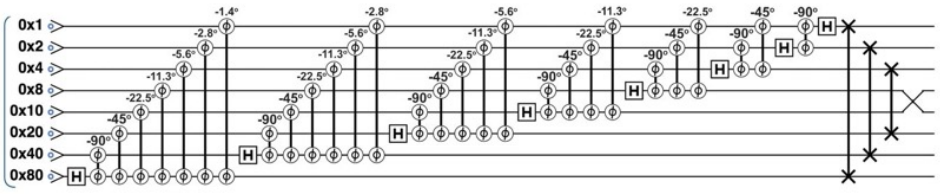
15

FEARLESSLY FORWARD

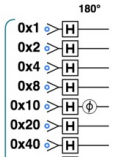
Inspiration | Boldness | Curiosity | Passion

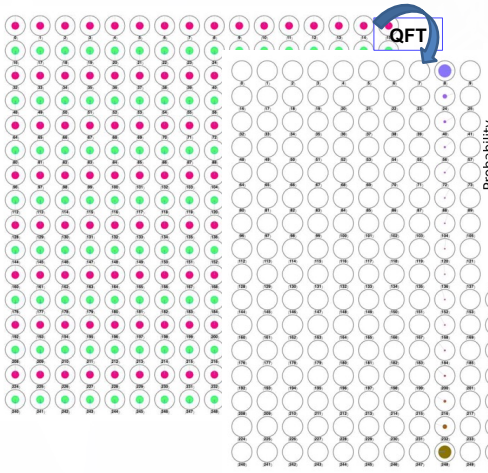
Basic Quantum Algorithms 6

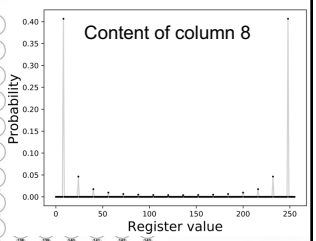
- increased precision when using more qubits (e.g. 8-qubit signal):



e.g. input signal: (uniform except phase of 5th qubit flipped)







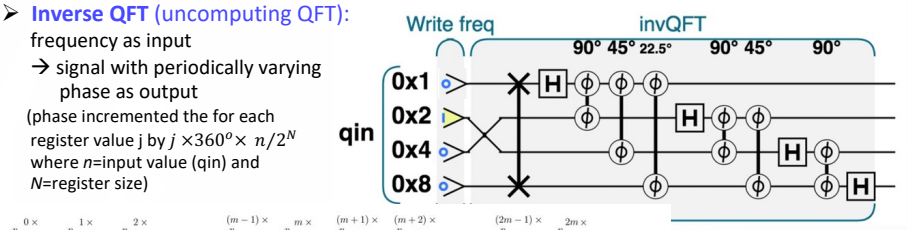
16

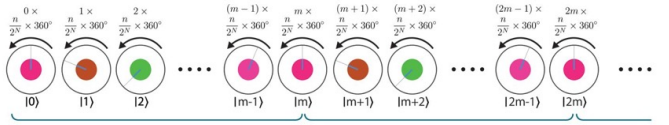
FEARLESSLY FORWARD

Inspiration | Boldness | Curiosity | Passion

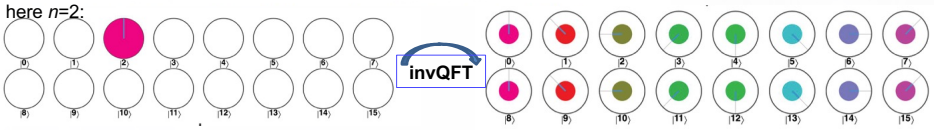
Basic Quantum Algorithms 7

- **Inverse QFT** (uncomputing QFT):
  frequency as input
  → signal with periodically varying phase as output
  (phase incremented the for each register value j by $j \times 360^o \times n/2^N$ where *n*=input value (qin) and *N*=register size)

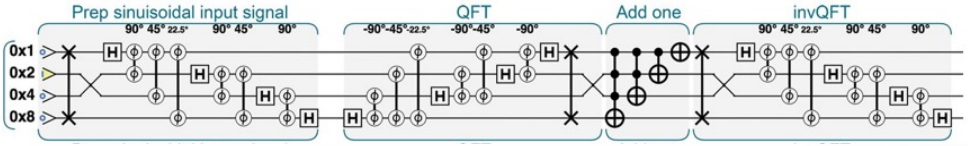




here *n*=2:



Note: invQFT – QFT sequence is used to modify frequencies, e.g.



17

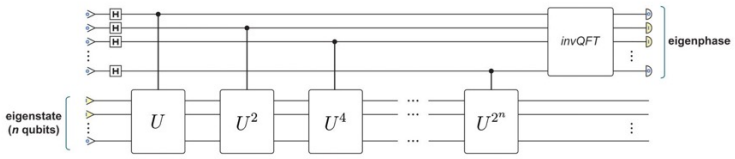
FEARLESSLY FORWARD

Inspiration | Boldness | Curiosity | Passion

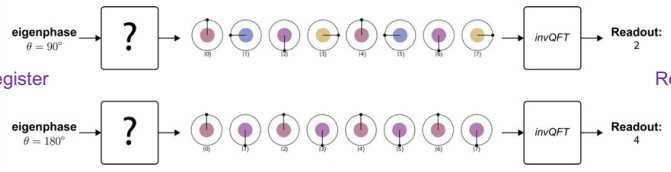
Basic Quantum Algorithms 8

D) Quantum Phase Estimation (QPE)

- **returns the superposition of all eigen-phases of an operator *U***



e.g.
3-qubit register

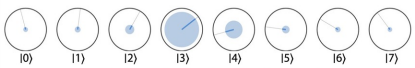


Readout: $j \times \frac{360^o}{N}$

Notes:

- repeated execution allows for resolution beyond the register size!

e.g. when output like:



- encode a frequency value in the through conditional rotation

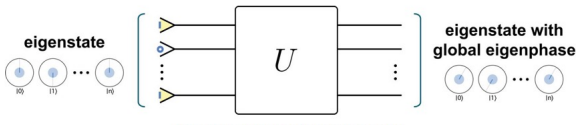


Figure 8-7. Simple suggestion for phase estimation

18

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

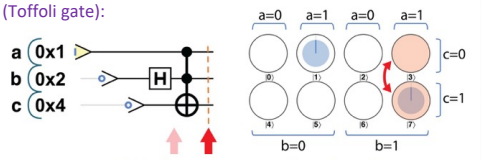
Note to Phase Logic

- Quantum Computing implements two methods of algebraic and logic operations:

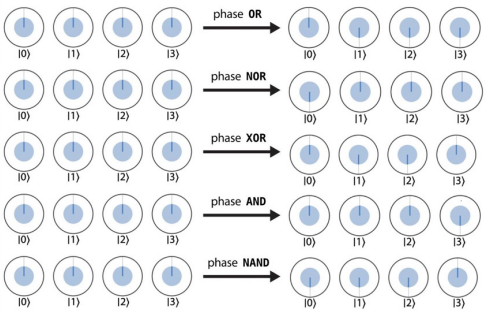
- based on magnitudes
  (standard method)

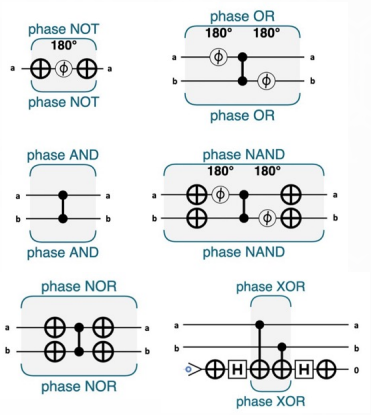
QPE QAA

e.g. AND operation
(Toffoli gate):



- based on phases





19

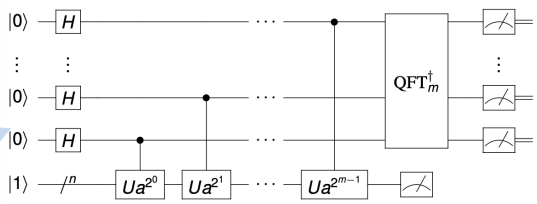
FEARLESS IDEAS
Inspiration | Boldness | Curiosity | Passion

Basic Quantum Algorithms 9

E) Shor's algorithm

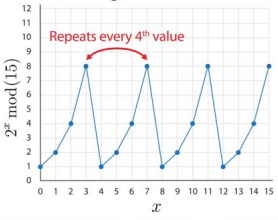
- hybrid (quantum & classical) algorithm for factorizing integers
- basic idea: measure a periodic sequence

Steps:
1. Given N, check that N is not a prime or power of a prime. If it is, stop.
2. Choose $1 < a < N$ at random
3. If $b = gcd(a,N) > 1$, output b and stop
4. Find the order of a mod N, that is: $x > 0$ such that $a^x \equiv 1 \bmod N$
5. If x is odd, go to 2
6. Compute $y = a^{x/2} + 1 \bmod N$; $z = a^{x/2} - 1 \bmod N$
7. If $y = 0$, go to 2; If $z = 0$, take $x = x/2$ and go to 5
8. Compute $p = gcd(y,N)$ and $q = gcd(z,N)$; at least one of them will be a non-trivial factor of N

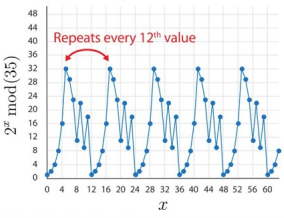


Step 4: period finding via invQFT: $x \pm 1$ are good candidates as factors (if this doesn't work, try secondary maxima)

Factoring 15



Factoring 35



20

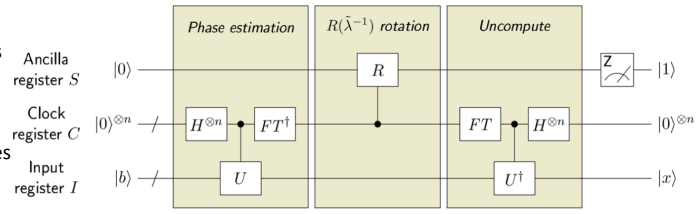
FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Basic Quantum Algorithms 10

E) HHL Algorithm (Harrow, Hassidim, Lloyd 2009)

- solving linear systems of equations using QPE

Main steps:
1. determine eigenvalues (QPE)
2. invert eigenvalues and rotate
3. uncompute eigenvalues (inverse QPE)

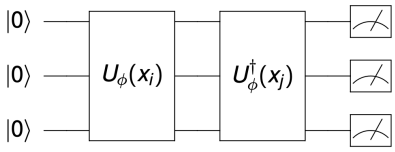


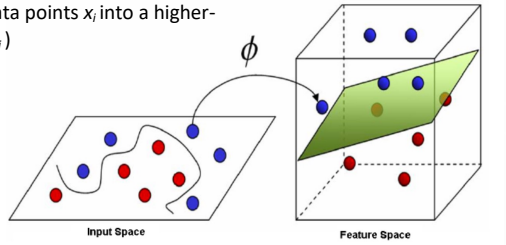
F) Quantum Support Vector Machine (QSVM)

- main idea: find a hyperplane that separates data from two different classes with the maximum possible margin
- improve classification by embedding the data points x_i into a higher-dimensional space using a feature map $\phi(x_i)$

→ compute Kernel estimators $\phi(x_i) \cdot \phi(x_j)$

(Havlíček, Córcoles, Temme 2019)





21

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

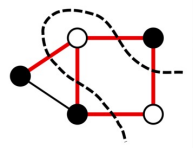
Basic Quantum Algorithms 11

G) Quantum Approximate Optimization Algorithm (QAOA)

- obtain approximate solutions of the problem of minimizing $C(x) = \sum_a w_a C_a(x)$ where x is n-bit string, w_a are real weights and C_a are boolean functions

(Farhi, Goldstone and Gutmann, 2014)

e.g. Max-Cut problem (dividing the vertices of a graph into two sets such that the number of edges with extremes in both sets is the maximum possible)

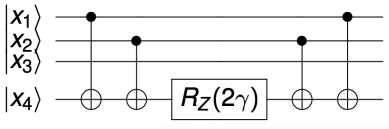


Steps:
1. Choose a value for p and some initial angles β, γ
2. Prepare the state $|\beta, \gamma\rangle$
3. Estimate the energy $E(\beta, \gamma) = \langle \beta, \gamma | H_f | \beta, \gamma \rangle$
4. Vary β and γ in order to minimize $E(\beta,\gamma)$
5. If the stopping criterium is met, stop; else, go to 2

(QAOA is a hybrid algorithms, only step 2 is carried out on a quantum computer)

For Max-Cut C_a is of the form $x_i \oplus x_j$, so the Hamiltonian is given by: $\frac{1}{2} I - \frac{1}{2} Z_1 Z_2$

(e.g. for a 4-qubit register $|\beta, \gamma\rangle = e^{-i\beta\gamma Z_1 Z_2 Z_4} |x_1 .. x_4\rangle$)



- Minimizing C(x) corresponds to finding the ground state of $H_f = \sum_a w_a H_a$ with $C_a = \langle x | H_a | x \rangle$

x	$\frac{1}{2}I - \frac{1}{2}Z$	$\overline{x}$	$\frac{1}{2}I + \frac{1}{2}Z$
$x_1 \oplus x_2$	$\frac{1}{2}I - \frac{1}{2}Z_1Z_2$	$\bigoplus_{j=1}^k x_j$	$\frac{1}{2}I - \frac{1}{2}Z_1Z_2 \dots Z_k$
$x_1 \wedge x_2$	$\frac{1}{4}I - \frac{1}{4}(Z_1 + Z_2 - Z_1Z_2)$	$\bigwedge_{j=1}^k x_j$	$\frac{1}{2^k}\prod_j (I - Z_j)$
$x_1 \vee x_2$	$\frac{3}{4}I - \frac{1}{4}(Z_1 + Z_2 + Z_1Z_2)$	$\bigvee_{j=1}^k x_j$	$I - \frac{1}{2^k}\prod_j (I + Z_j)$
$\overline{x_1 x_2}$	$\frac{3}{4}I + \frac{1}{4}(Z_1 + Z_2 - Z_1Z_2)$	$x_1 \Rightarrow x_2$	$\frac{3}{4}I + \frac{1}{4}(Z_1 - Z_2 + Z_1Z_2)$

Mapping (S. Hadfield, 2018)

22

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Basic Quantum Algorithms 12

H) Variational Quantum Eigensolver (VQE)

➢ solve minimization problem by mapping it to Hamiltonian and using the variational theorem

Consider a general Hamiltonian H_f (with a polynomial number of terms), for which we approximate its ground state:

Instead of the parametrized state $|\beta, \gamma\rangle$ of QAOA we use

- an initial state $|\psi\rangle$ that is easy to prepare (it could be just $|0\rangle$)
- a parametrized unitary $U(\theta)$ that is called a **variational form**

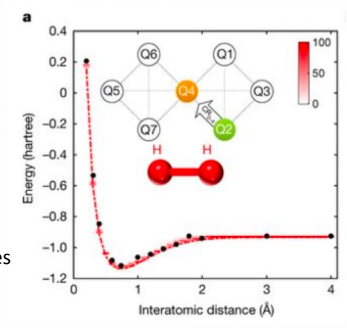
We create an ansatz: $|\psi(\theta)\rangle = U(\theta)\,|\psi\rangle$

and try to minimize its energy with respect to H_f by varying the parameters

Steps (only step 2 is carried out on a quantum computer):

1. Choose an initial state $|\psi\rangle$, a variational form $U(\theta)$ and some initial vector θ
2. Prepare the state $|\psi(\theta)\rangle = U(\theta)\,|\psi\rangle$
3. Estimate the energy $E(\theta) = \langle\psi(\theta)|\, Hf\, |\psi(\theta)\rangle$
4. Vary θ in order to minimize $E(\theta)$
5. If the stopping criterium is met, stop; else, go to 2

VQE has been used to estimate ground states of several molecules and has been applied to many minimization problems.



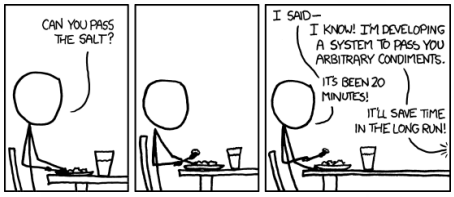
Kandala et al, Nature 549, 242 (2017)

23

FEARLESSLY FORWARD
Inspiration | Boldness | Curiosity | Passion

Last page (already …)

- Many topics were not covered: QPCA, VQC, QGAN, …
- I guess I will split this workshop into 2 parts:
  "Quantum Circuits" and "Quantum Algorithms"
- Topics of this workshop are evolving rapidly – implementations in Qiskit have been changing weekly
- Class notes and Jupyter notebooks unfinished (sorry I didn't have enough time! everything takes longer than expected …)



Upcoming workshops:

HPC introductory series: **Introduction to Parallel Computing on HPC** (4/26/22 2-5pm)

QLab series: **Practical Quantum Computing** (mid of May)

Quantum Circuits (late May)

Quantum Algorithms (early June)

… hopefully with better notebooks and examples …

24