Cover: ‘Microsoft Has Demonstrated the Underlying Physics Required to Create a New Kind of Qubit’, *Microsoft Research*, March 14, 2022, https://www.microsoft.com/en-us/research/blog/microsoft-has-demonstrated-the-underlying-physics-required-to-create-a-new-kind-of-qubit/.

Another peek into

Quantum Computing

Kees van Kempen
<ru@keesvankempen.nl>

May 31, 2022 @ student seminar PMM

Radboud University

Saturday Morning Breakfast Cereal - The Talk. https://www.smbc-comics.com/comic/the-talk-3.

PRESENTATION GOALS

- Motivate the potential of quantum computing (QC)
- Demystify the buzz around QC
- Specifically not:
  - Go deeply into the mathematics
  - Cover every (important) notion of QC
  - Give a lecture on (quantum) information

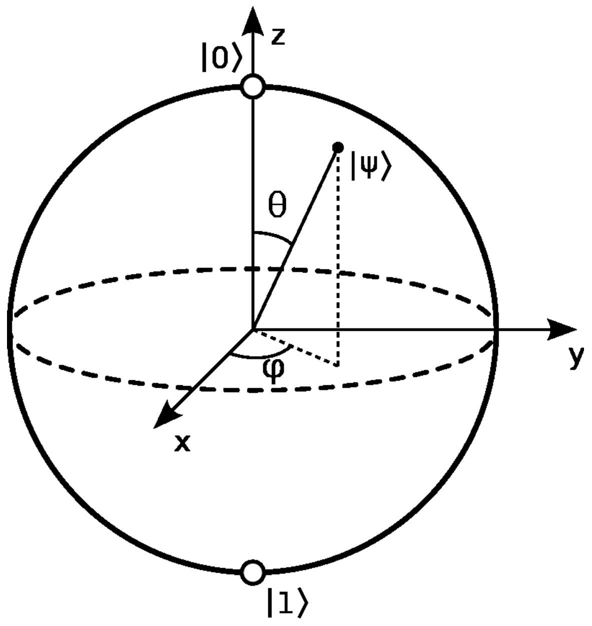
RECAP FROM “QUBITS IN DIAMOND” BY JEROEN (MAY 10, 2022)

- Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$
- $|\langle 0|\psi\rangle|^2 = |\alpha|^2 \qquad |\langle 1|\psi\rangle|^2 = |\beta|^2 \qquad |\alpha|^2 + |\beta|^2 = 1$
- Measurement yields a basis state
- Representation on a Bloch sphere:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

- Manipulation done by unitary operations
  - No heat production -> reversible
- Decoherence and entanglement

- Example: defects in diamonds



QUBITS, AND THEN?

- QCs make use of a combination of quantum mechanical properties
  - n qubits yields 2^n basis states $|b_1\rangle \otimes \cdots \otimes |b_n\rangle$ with $b_i \in \{0, 1\}$ such that a register has state
    $$|\psi\rangle = \sum_i \alpha_i |b_i\rangle \qquad \alpha_i \in \mathbb{C}, \qquad \sum_i |\alpha_i|^2 = 1$$
  - Measurement collapses the states (no-teleportation theorem)
  - We *can* apply unitary operations
  - Cloning of uncollapsed states is impossible (no-cloning theorem)
  - …

- What are these unitary operations in practice?
- What real applications can we design using these ideas?
  - Classical computing can be done, but is uninteresting: requires the same amount of (qu)bits
  - New algorithms!

QUANTUM ALGORITHMS

- Quantum fourier transform (QFT)
  - Classical: discrete fourier transform (DFT)
  - QFT is a unitary operation: $QFT|x\rangle \rightarrow |\tilde{x}\rangle$
  - $O(n^2)$ instead of DFT $O(n2^n)$

- Shor's algorithm
  - Finds prime factors of integers
  - Polynomial runtime instead of exponential
  - Potential danger to encryption (RSA, Diffie-Hellman, Elliptic Curve)
  - Results: factorization of $15 = 5 x 3$ in 2001, factorization of $21 = 7 x 3$ in 2012, attempt at $35 = 7 x 5$ failed in 2019

- Deutsch-Jozsa algorithm

DEUTSCH-JOZSA PROBLEM (1992)

- Alice iteratively chooses $x \in \{0, \dots, 2^n - 1\}$ $\quad$ ($|\{0,1\}^n| = 2^n$ options)
- Bob chooses one function $f(x) \in \{f_c(x), f_b(x)\}, f: \{0, \dots, 2^n - 1\} \rightarrow \{0,1\}$
  - $f_c(x)$ constant for all x
  - $f_b(x)$ returns 1 for half, 0 for other half
- Each round, Alice chooses x, Bob returns $f(x)$
- Goal: Alice guesses type of $f(x)$

- Classically: worst case, Alice needs to guess $2^{n-1} + 1$ times

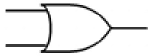
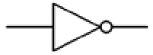
- Quantum:
  - Chuang, Isaac L., en Yoshihisa Yamamoto. 'Simple quantum computer'. *Physical Review A*, vol. 52, nr. 5, November 1995, pp. 3489–96. *APS*, https://doi.org/10.1103/PhysRevA.52.3489.

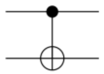
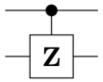
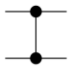
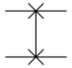
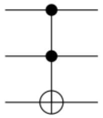
DEUTSCH-JOZSA ALGORITHM SKETCH: 'SIMPLE QUANTUM COMPUTER'

- Alice sends a register $|x\rangle$ of n qubits encoding the 2^n options
- Bob writes $f(x)$ as unitary operation U_f, and applies it yielding a result in another qubit $|y\rangle$
  - Note that $|x\rangle$ is a superposition of all possibilities
  - $|y\rangle$ is now a superposition of zero and one states or of one state only
- Alice measures the sum of states $U_f|x\rangle$ all at once

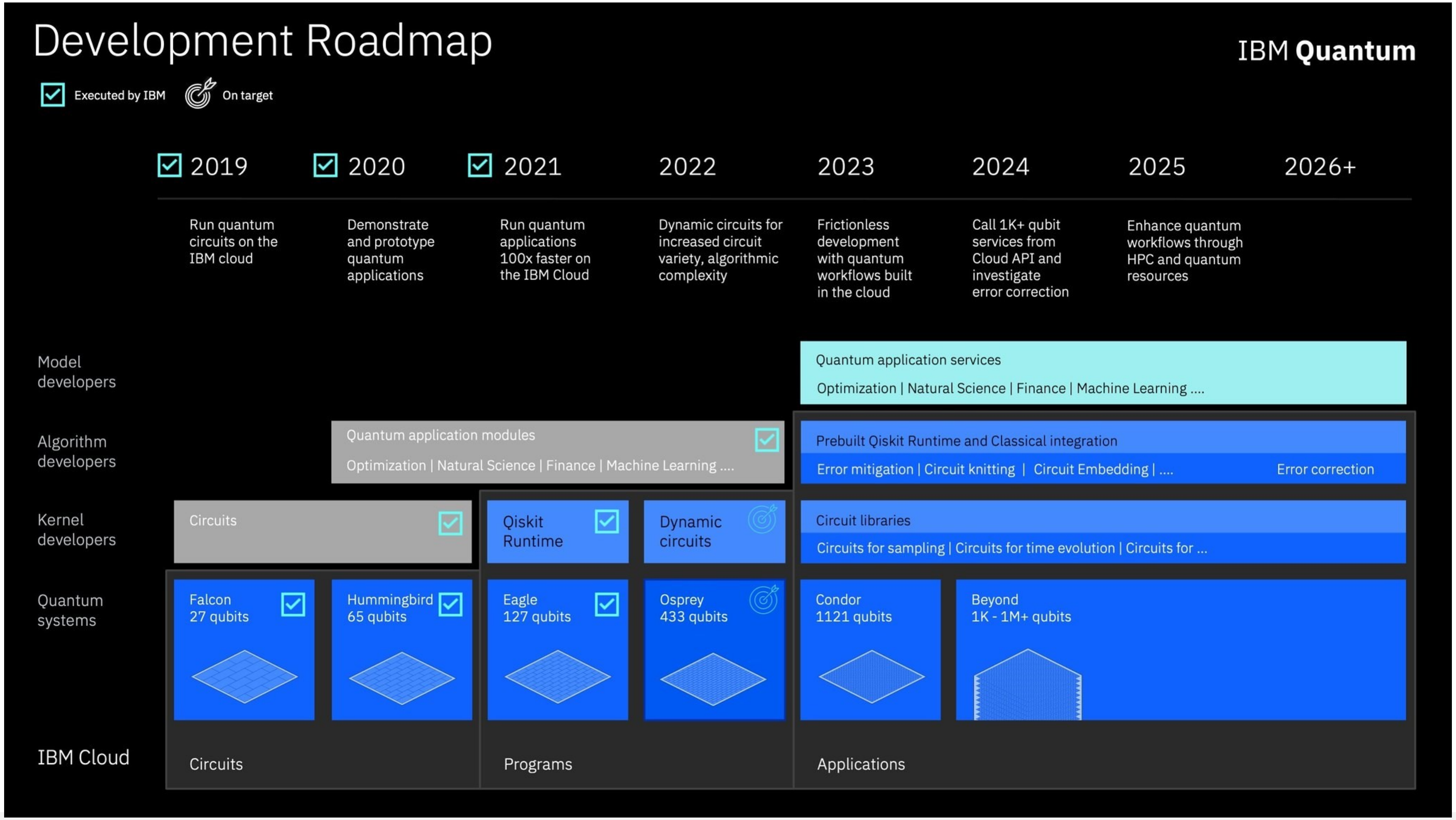
- Setup idea: Chuang, Isaac L., en Yoshihisa Yamamoto. 'Simple quantum computer'. *Physical Review A*, vol. 52, nr. 5, November 1995, pp. 3489–96. *APS*, https://doi.org/10.1103/PhysRevA.52.3489.
  - For the $n = 1$ case: use a photon
  - For larger n: electron spins perhaps
  - "We hope that our work will lead to a future experiment to demonstrate the practicality of quantum computing."
- This is a nice QC problem

TOWARDS A UNIVERSAL QUANTUM COMPUTER

Logic Gate	Symbol	Description	Boolean
AND		Output is at logic 1 when, and only when all its inputs are at logic 1,otherwise the output is at logic 0.	X = A•B
OR		Output is at logic 1 when one or more are at logic 1.If all inputs are at logic 0,output is at logic 0.	X = A+B
NAND		Output is at logic 0 when,and only when all its inputs are at logic 1,otherwise the output is at logic 1	$X = \overline{A \cdot B}$
NOR		Output is at logic 0 when one or more of its inputs are at logic 1.If all the inputs are at logic 0,the output is at logic 1.	$X = \overline{A+B}$
XOR		Output is at logic 1 when one and Only one of its inputs is at logic 1. Otherwise is it logic 0.	$X = A \oplus B$
XNOR		Output is at logic 0 when one and only one of its inputs is at logic1.Otherwise it is logic 1. Similar to XOR but inverted.	$X = \overline{A \oplus B}$
NOT		Output is at logic 0 when its only input is at logic 1, and at logic 1 when its only input is at logic 0.That's why it is called and INVERTER	$X = \overline{A}$

Operator	Gate(s)		Matrix
Pauli-X (X)	X	$\oplus$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	S		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

QUANTUM REVOLUTION?



TAKE-HOME MESSAGE

- Quantum computing has a good theoretical fundation, but is in its infancy in practice
- Quantum computing solves problems differently than normal computing

- Further reading tips:
  - The given example: Chuang, Isaac L., en Yoshihisa Yamamoto. ‘Simple quantum computer’. *Physical Review A*, vol. 52, nr. 5, November 1995, pp. 3489–96. *APS*, https://doi.org/10.1103/PhysRevA.52.3489.
  - A review by a physicist: Steane, Andrew. ‘Quantum computing’. *Reports on Progress in Physics*, vol. 61, nr. 2, February 1998, pp. 117–73. *DOI.org (Crossref)*, https://doi.org/10.1088/0034-4885/61/2/002.
  - A proper course on quantum computing: de Wolf, Ronald. ‘Quantum Computing: Lecture Notes’. January 11, 2022. https://homepages.cwi.nl/~rdewolf/#LectureNotes. <- Is this familiar, Floris?