COFI Advanced Instrumentation and Analysis Techniques School

December 9-17, 2023

Principles (and future) of **Quantum Computing**

Jens Koch | Northwestern University

logistics

Quantum Simulation for High-Energy Physics

Christian W. Bauer,^{1,*} Zohreh Davoudi⁽⁰⁾,^{2,†} A. Baha Balantekin,³ Tanmoy Bhattacharya,⁴ Marcela Carena,^{5,6,7,8} Wibe A. de Jong,¹ Patrick Draper,⁹ Aida El-Khadra,⁹ Nate Gemelke,¹⁰ Masanori Hanada,¹¹ Dmitri Kharzeev,^{12,13} Henry Lamm,⁵ Ying-Ying Li,^{14,15} Junyu Liu⁽⁰⁾,^{16,17} Mikhail Lukin,¹⁸ Yannick Meurice,¹⁹ Christopher Monroe,^{20,21,22,23} Benjamin Nachman,¹ Guido Pagano,²⁴ John Preskill,²⁵ Enrico Rinaldi,^{26,27,28} Alessandro Roggero,^{29,30} David I. Santiago,^{31,32} Martin J. Savage,³³ Irfan Siddiqi,^{31,32,34} George Siopsis,³⁵ David Van Zanten,⁵ Nathan Wiebe,^{36,37} Yukari Yamauchi,² Kübra Yeter-Aydeniz,³⁸ and Silvia Zorzetti⁶ ¹ Physics Division, Lawrence Berkelev National Laboratory, Berkelev, California 94720, USA ²Department of Physics, Maryland Center for Fundamental Physics, and the NSF Institute for Robust Quantum Simulation, University of Maryland, College Park, Maryland 20742, USA Department of Physics, University of Wisconsin, Madison, Wisconsin 53706, USA T-2, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA ⁵ Fermi National Accelerator Laboratory, Batavia, Illinois 60510, USA ⁶Enrico Fermi Institute, University of Chicago, Chicago, Illinois 60637, USA ⁷Kavli Institute for Cosmological Physics, University of Chicago, Chicago, Illinois 60637, USA ⁸ Department of Physics, University of Chicago, Chicago, Illinois 60637, USA ⁹ Department of Physics and Illinois Center for the Advanced Study of the Universe and Illinois Quantum Information Science and Technology Center, University of Illinois, Urbana, Illinois 61801, USA ¹⁰ QuEra Computing Inc, Boston, Massachusetts 02135, USA ¹¹Department of Mathematics, University of Surrey, Guildford, Surrey GU2 7XH, United Kingdom ¹² Center for Nuclear Theory, Department of Physics and Astronomy, Stony Brook University, New York 11794-3800, USA ¹³Department of Physics, Brookhaven National Laboratory, Upton, New York 11973, USA ¹⁴ Peng Huanwu Center for Fundamental Theory, Hefei, Anhui 230026, China ¹⁵ Interdisciplinary Center for Theoretical Study, University of Science and Technology of China, Hefei, Anhui 230026. China ¹⁶ Pritzker School of Molecular Engineering, Chicago Quantum Exchange, and Kadanoff Center for Theoretical Physics, University of Chicago, Illinois 60637, USA ¹⁷ aBraid Co., Harper Court 5235, Chicago, Illinois 60615, USA ¹⁸ Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA ¹⁹ Department of Physics and Astronomy, University of Iowa, Iowa City, Iowa 52242, USA ²⁰Duke Quantum Center, Duke University, Durham, North Carolina 27701, USA ²¹ Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA ²² Department of Physics, Duke University, Durham, North Carolina 27708 ²³ IonO, Inc., College Park, Maryland 20740, USA ²⁴ Physics and Astronomy Department, Rice University, Houston, Texas 77005, USA ²⁵ Institute for Ouantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA ²⁶ Physics Department, University of Michigan, Ann Arbor, Michigan 48109, USA ²⁷ Theoretical Quantum Physics Laboratory, Center for Pioneering Research, RIKEN, Wako, Saitama 351-0198, Japan ²⁸ Interdisciplinary Theoretical and Mathematical Sciences Program (iTHEMS), RIKEN, Wako, Saitama 351-0198, Japan ²⁹ Dipartimento di Fisica, University of Trento, via Sommarive 14, Povo, Trento I–38123, Italy

HHL algorithm & ML relevance

Harrow, Hassadim & Lloyd 2008

$A\vec{x} = \vec{b}$ $\vec{x} = A^{-1}\vec{b}$

Use of HHL in training of deep neural networks offers exponential speedup over classical training











Notation

 $\mathbb{B} = \{0, 1\}, \quad n, m \in \mathbb{N}$



Notation

 $\mathbb{B} = \{0, 1\}, \quad n, m \in \mathbb{N}$



 $\mathbb{B} = \{0, 1\}, \quad n, m \in \mathbb{N}$

 $\begin{array}{ll} \Omega & {\rm sample \ space} \\ & {\rm for \ random \ variable(s)} \end{array}$

a black box* implementing map f

Examples



$f\colon \mathbb{B}^n\times\Omega\to\mathbb{B}^m$

a black box* implementing map f

Examples



$f\colon \mathbb{B}^n\times\Omega\to\mathbb{B}^m$

a black box^{*} implementing map f



 $f\colon \mathbb{B}^n\times\Omega\to\mathbb{B}^m$

Vout

a black box^{*} implementing map *f*

Examples



$f\colon \mathbb{B}^n\times\Omega\to\mathbb{B}^m$

programmable computer

a black box* that can implement** any*** given *f*





classical vs. quantum computer



classical

"uses purely classical physics paradigms for computing"



quantum

"uses concepts specific to quantum physics"

Jozsa & Linden (2003)

For any quantum algorithm operating on pure states, we prove that the presence of **multi-partite entanglement**, with a number of parties that **increases unboundedly with input size**, is **necessary** if the quantum algorithm is to offer an **exponential speed-up over classical computation**.

entanglement

quantum computing hardware



Development Roadmap |



IBM Quantum

	2019 🕑	2020 🥪	2021 🔗	2022 🕑	2023	2024	2025	2026+
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applica- tions with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum softwa	re applications $\mathfrak{Y} \longrightarrow$	Quantum software applicat	ions
							Machine learning Natural science Optimization	
Algorithm Developers		Quantum algorithm and ap	oplication modules	\bigcirc	Quantum Serverless 👌			
		Machine learning Natura	l science Optimization			Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits	\odot	Qiskit Runtime 🛛 🔗					
				Dynamic circuits 🔗	Threaded primitives 👌	Error suppression and mitig	ation	Error correction
System Modularity	Falcon 🔗 27 qubits	Hummingbird 🔗	Eagle 🗸	Osprey 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron 👌 133 qubits x p	Crossbill 408 qubits		



Quantum Computing Market Map

Non exhaustive and in no particular order. Excludes details on control systems, assembly languages, circuit design, etc.



¹ Software offerings can be further classified into SDKs, firmware / enablers, algorithms / applications, simulators etc. but many companies are offering a mixture across the stack ² Many QPU providers are offering full stack services (e.g. Pasqal acquired Qu&Co, Quantinuum was originally CQC prior to merger with HQS, etc.



Ohmic losses energy dissipation, V = RI

interaction with the environment

dramatically reduces quantum effects

Building quantum bits from superconducting circuits











$$=\hbar\omega\left(a^{\dagger}a+\frac{1}{2}\right)$$

$$[\Phi,Q]=i\hbar$$

Т

L





Quantum LC oscillator as a qubit?



From LC oscillator to transmon





Brian Josephson Nobel Prize 1973

Josephson effect

current-phase relation:

phase evolution equation:

$$I = I_0 \sin \varphi$$
$$\frac{d\varphi}{dt} = V \cdot \frac{2\pi}{\Phi_0}$$

Josephson junction

V 1 = 141.4 nm

Bottom SC electrode 1 (Al)

> Top SC electrode 1 (Al)

> > **IBM** Quantum

H 1 = 121.0 nm













quantum computing:

use quantum parallelism and entanglement to beat classical computers

Shor's algorithm

N = p q (p,q prime) period-finding of modular functions

Grover's algorithm

search unsorted database

ed

Harrow-Hassidim-Lloyd (HHL) algorithm

matrix inversion* $\vec{x} = \mathcal{A}^{-1}\vec{b}$

quantum adiabatic algorithm

optimization

digital quantum simulation $i\hbar \frac{d}{dt} |\Psi(t)\rangle = H |\Psi(t)\rangle$

quantumalgorithmzoo.org
quantum parallelism



quantum parallelism



What makes a quantum computer tick?



quantum parallelism



storing quantum states

$$|\Psi\rangle = \alpha_0 |00\cdots 000\rangle$$

$$+ \alpha_1 | 00 \cdots 001 \rangle$$

$$+ \alpha_2 | 00 \cdots 010 \rangle$$

 $+ \alpha_2 | 00 \cdots 011 \rangle$

$$+ \alpha_3 |00 \cdots 011\rangle$$

 $+ \alpha_{2^N} | 1 \cdots 111 \rangle$

- 2^N complex amplitudes
- storage: $2^{N} \times 128$ bits
 - N= 65 qubits



- memory/disk space:
 590 billion GB
- **but**: output only N classical bits

$$\Psi\rangle$$
 — e.g., $01\cdots 101$

quantum parallelism

- can process all possible inputs at once
- not sufficient for quantum speedup
 - measurement only accesses one output state

Circuit elements

Building blocks for superconducting qubits



transmon qubit



 $H = \frac{Q^2}{2C} - E_J \cos(2\pi\Phi/\Phi_0)$

Introduce nonlinearity: replace inductor with

Josephson junction















arbitrary single-qubit gates





 $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

1/f charge noise1/f flux noisecritical current noisedielectric lossphoton shot noisePurcell decaynonequilibrium quasiparticles

. . .

DECOHERENCE / ERRORS

Your qubit ran into a problem that it couldn't handle, and now it needs to restart.

You can search for the error online: HBAR_DIED_A_HORRIBLE_DEATH





error mitigation strategies



reduce noise

(materials science, fabrication, microwave engineering, ...)





intrinsic noise protection (develop circuits that are insensitive to noise)





B active quantum error correction (monitor for errors, apply correction steps when required in feedback loop)



charge noise flux noise

Cooper pair box rf SQUID qubit, 3-junction flux qubit

Cooper pair box

letters to nature

Coherent control of macroscopic quantum states in a single-Cooper-pair box

Y. Nakamura*, Yu. A. Pashkin† & J. S. Tsai*

* NEC Fundamental Research Laboratories, Tsukuba, Ibaraki 305-8051, Japan † CREST, Japan Science and Technology Corporation (JST), Kawaguchi, Saitama 332-0012, Japan

NATURE | VOL 398 | 29 APRIL 1999 | www.nature.com

Physica Scripta. Vol. T76, 165-170, 1998

Quantum Coherence with a Single Cooper Pair

V. Bouchiat,* D. Vion, P. Joyez, D. Esteve and M. H. Devoret

Quantronics group, Service de Physique de l'Etat Condensé CEA-Saclay, F-91191 Gif-sur-Yvette, France

Received October 27, 1997; revised version received January 15, 1998; accepted January 23, 1998

Cooper pair box



Fig. 1. Schematics of the single Cooper box: a superconducting electrode (island) is in contact with a superconducting reservoir though a tunnel junction (grey zone) with capacitance C_j . Excess Cooper pairs tunnel onto the island in response to an electric field applied by means of the gate capacitance C_g and voltage U.

$T_{\varphi} \approx 1 \,\mathrm{ns}$

V Bouchiat et al., Phys. Scr. **1998**, 165 (1998)

charge noise dephasing







► dephasing $1/T_{\varphi} \sim \left(\frac{\partial \omega_q}{\partial \lambda}\right)^2 S(0)$

Flattening the spectrum

for charge noise protection



increase E_J / E_C

basics of qubit control & readout





Qubit operations and readout

$$\hat{H}_{\rm JC} = \frac{1}{2}\hbar\omega_q\hat{\sigma}_z + \hbar\omega_r\hat{a}^{\dagger}\hat{a} + \hbar g(\hat{a}\hat{\sigma}_+ + \hat{a}^{\dagger}\hat{\sigma}_-)$$

Perturbation theory in $\,g/\Delta\ll 1\,$

(Schrieffer-Wolff transf. / adiabatic elimination)

dispersive regime

$$\hat{H}_{\rm JC}^{\rm eff} = \hbar\omega_r \hat{a}^{\dagger} \hat{a} + \frac{\hbar\omega_q'}{2} \hat{\sigma}_z + \hbar\chi \hat{a}^{\dagger} \hat{a} \hat{\sigma}_z$$

$$=\hbar(\omega_r+\chi\hat{\sigma}_z)\hat{a}^{\dagger}\hat{a}+\frac{\hbar\omega_q'}{2}\hat{\sigma}_z$$

Resonator frequency depends on qubit state!

dispersive readout

$$\hat{H} = \hbar \omega_r \hat{a}^{\dagger} \hat{a} + \hat{H}_{\rm drive}$$



dispersive readout

$$\hat{H}_{\rm JC}^{\rm eff} = \hbar(\omega_r + \chi \hat{\sigma}_z) \hat{a}^{\dagger} \hat{a} + \frac{\hbar \omega_q'}{2} \hat{\sigma}_z$$





1

I

two-qubit gate (example)





time (flux biasing)

two-qubit gate (example)

 ω_r



time (flux biasing)





(flux biasing)



After quarter period: \sqrt{iSWAP} gate



$\sqrt{iSWAP}|01\rangle =$

$$\sqrt{\text{iSWAP}} = \sqrt{\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & i & 0\\ 0 & i & 0 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0\\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$|0\rangle \mapsto \begin{pmatrix} 1\\ 0 \end{pmatrix}, |1\rangle \mapsto \begin{pmatrix} 0\\ 1 \end{pmatrix}$$

$$\sqrt{\text{iSWAP}} = \sqrt{\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & i & 0\\ 0 & i & 0 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0\\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle \quad \mapsto \quad \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$
$$\sqrt{\text{iSWAP}} = \sqrt{\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & i & 0\\ 0 & i & 0 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0\\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\sqrt{\mathrm{iSWAP}}|01\rangle = \mathbf{2}$$

$$|0\rangle \mapsto \begin{pmatrix} 1\\ 0 \end{pmatrix}, |1\rangle \mapsto \begin{pmatrix} 0\\ 1 \end{pmatrix}$$

$$\sqrt{\text{iSWAP}} = \sqrt{\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & i & 0\\ 0 & i & 0 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0\\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\sqrt{\mathrm{iSWAP}}|01\rangle = \mathbf{2}$$

$$|0\rangle \mapsto \begin{pmatrix} 1\\ 0 \end{pmatrix}, |1\rangle \mapsto \begin{pmatrix} 0\\ 1 \end{pmatrix}$$

universal control

For gate based quantum computing: what is a

minimal set of elementary qubit operations

sufficient to carry out an **arbitrary algorithm**?

universal control

- arbitrary single-qubit gates
 (can approximate and decompose into sequence of H, T)
- 2. one 2-qubit entangling gate (like CNOT or \sqrt{i} SWAP)

universal control

U = $2^{n} \times 2^{n}$ unitary

Summary of decomposition chain:



- Iterative reduction of general n-qubit Unitary into n-qubit level-2 Unitaries
- (2) Conversion of n-qubit level-2 unitaries into C^k(U⁽¹⁾) gates (k=n-1), if necessary with the help of Gray codes
- ③ Decompose C^k(U¹¹¹) gale into cascade of TOFFOLIS and one C¹(U⁽¹¹⁾) gale, using h-1 auxiliary qubits
- (2) Express TOFFOLI in terms of CA gates where A²*X. Then, use AXBXC decomposition on CA and C'(U¹¹³) to reduce to CNOTs and Haubit gates.
- S Approximate 1-qubit gates by sequences of H and T gates, using irrational-angle decomposition.

TOFFOLI gate decomposition





who's the qubit? bosonic-qubit architectures

who's the qubit?

SCHEME 1: The qubit is the qubit (duh!) (Google, IBM, Rigetti etc.)

SCHEME 2: The qubit is a linear cavity mode Yale, FNAL-SQMS, Schuster





- Fock state encoding
- bosonic codes
- cat states
- GKP states

$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$







$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



NEXT: load an excitation into mode 2 $(\pi \text{ pulse on mode 2})$

$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



$$\hat{H} = \sum_{j} \omega_j \hat{a}_j^{\dagger} \hat{a}_j + \sum_{j} \chi_j \hat{a}_j^{\dagger} \hat{a}_j \hat{\sigma}_z + \frac{\omega_q'}{2} \hat{\sigma}_z$$



quantum optimal control





N. Khaneja, ..., S. J. Glaser, Optimal Control of Coupled Spin Dynamics: Design of NMR Pulse Sequences by Gradient Ascent Algorithms

J. Magn. Reson. 172, 296-305 (2005)

robust quantum control



Crosstalk-Robust Quantum Control in Multimode Bosonic Systems

Xinyuan You,^{1, *} Yunwei Lu,² Taeyoon Kim,^{1,2,3} Doğa Murat Kürkçüoğlu,¹ Shaojiang Zhu,¹ David van Zanten,¹ Tanay Roy,¹ Yao Lu,¹ Srivatsan Chakram,⁴ Anna Grassellino,¹ Alexander Romanenko,¹ Jens Koch,^{2,3} and Silvia Zorzetti^{1,†}

 ¹Superconducting Quantum Materials and Systems Center, Fermi National Accelerator Laboratory (FNAL), Batavia, IL 60510, USA
 ²Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208, USA
 ³Center for Applied Physics and Superconducting Technologies, Northwestern University, Evanston, IL 60208, USA
 ⁴Department of Physics and Astronomy, Rutgers University, Piscataway, NJ 08854, USA



programmable computer

a black box* that can implement** any*** given *f*

* a "device" obeying the laws of physics ** with input & output sizes $n, m \leq N_0$ *** output is provided in finite time NAND: $\mathbb{B}^2 \to \mathbb{B}^1$

random: $\Omega \to \mathbb{B}^1$

bubble sort: $\mathbb{B}^{64 \cdot 100} \to \mathbb{B}^{64 \cdot 100}$

PFD: $\mathbb{B}^{1024} \rightarrow \mathbb{B}^{1024 \cdot 2}$ prime factor decomposition

assessing performance

COMPUTER 1

NAND: $\mathbb{B}^2 \to \mathbb{B}^1$	
random: $\Omega \to \mathbb{B}^1$	
bubble sort: $\mathbb{B}^{64 \cdot 100} \to \mathbb{B}^{64 \cdot 100}$	
$PFD \colon \mathbb{B}^{1024} \to \mathbb{B}^{1024 \cdot 2}$	

COMPUTER 2

$\mathrm{NAND} \colon \mathbb{B}^2 \to \mathbb{B}^1$	
random: $\Omega \to \mathbb{B}^1$	
bubble sort: $\mathbb{B}^{64 \cdot 100} \to \mathbb{B}^{64 \cdot 100}$	
$\operatorname{PFD} \colon \mathbb{B}^{1024} \to \mathbb{B}^{1024 \cdot 2}$	
•••	

Quantum computation: Shor's algorithm



96