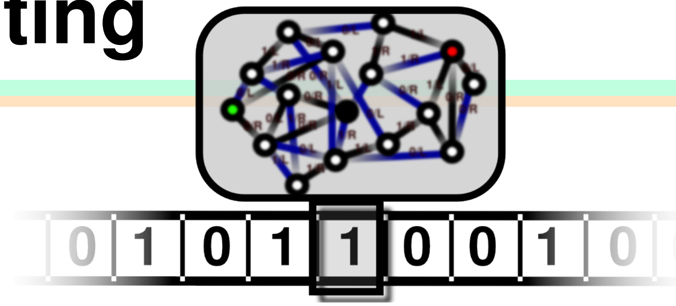
Building Quantum Computers

Produced with pdflatex and inkscape

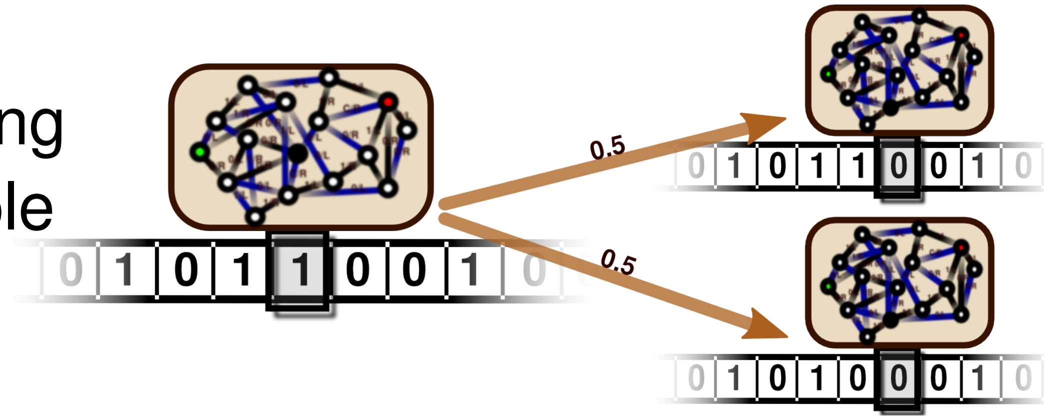
- Why quantum compute?
- How does it work?
- Why is it difficult?
- How much can we do today?
- What are the prospects?

E. “Manny” Knill: knill@boulder.nist.gov

Models of Computing

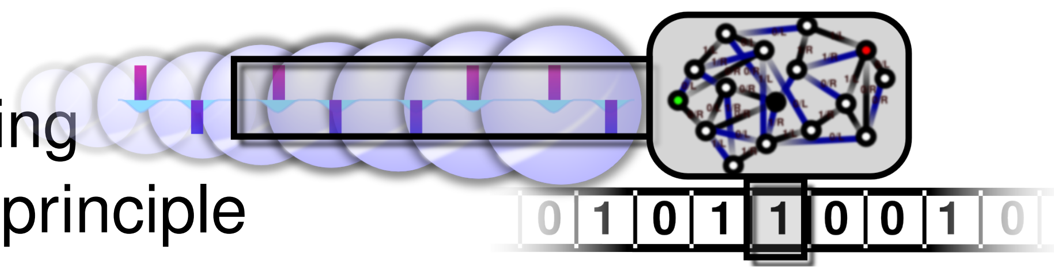


- Classical (deterministic) computing.



- Probabilistic computing

$$= \begin{cases} \text{classical computing} \\ + \text{ mixture principle} \\ + \text{ coin flip} \end{cases}$$

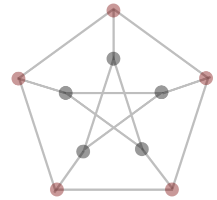


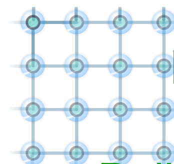
- Quantum computing

$$= \begin{cases} \text{classical computing} \\ + \text{ superposition principle} \\ + \text{ an interference gate} \end{cases}$$

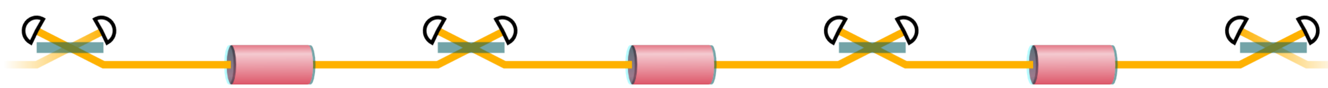
Why Quantum Compute?

- Algorithmic speedups.
  - Efficient quantum factoring. $N=pq$ Shor '94 [1]
  - Quadratic speedups of combinatorial search and Monte Carlo algorithms. Grover '95 [2], . . .





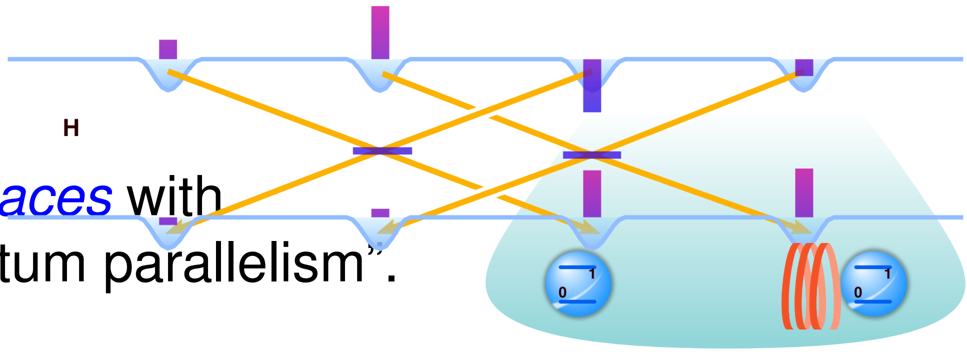
  - Efficient physics simulations. Feynman '82 [3], . . .
  - Quadratic improvements in measurement precision. Bollinger&al. '96 [4], . . .
- Cryptographic protocols.
  - Remove distance limitations of quantum key exchange. Briegel&al. '98 [5]
  - Quantum digital signatures. Gottesman&Chuang '01 [6]
  - Extensions of classical crypto to quantum information.



- Tests of quantum mechanics.
  - Validity of the superposition principle.
  - Ability to preserve many-system "entanglement".

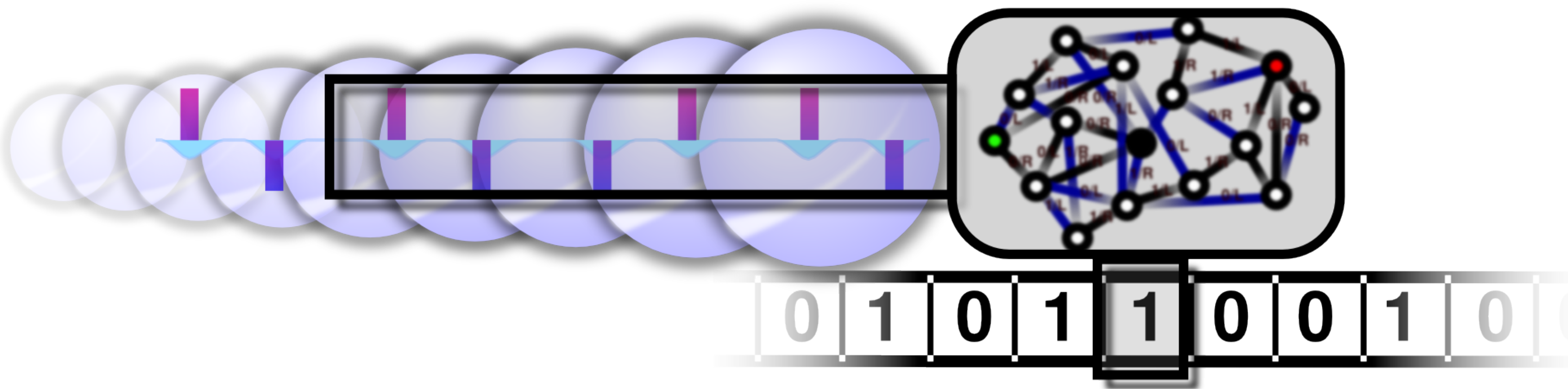
Preview

- QCs control
  - *wavefunctions* on
  - efficiently realized *configuration spaces* with
  - *interference* gates exploiting “quantum parallelism”.



Quantum Computers

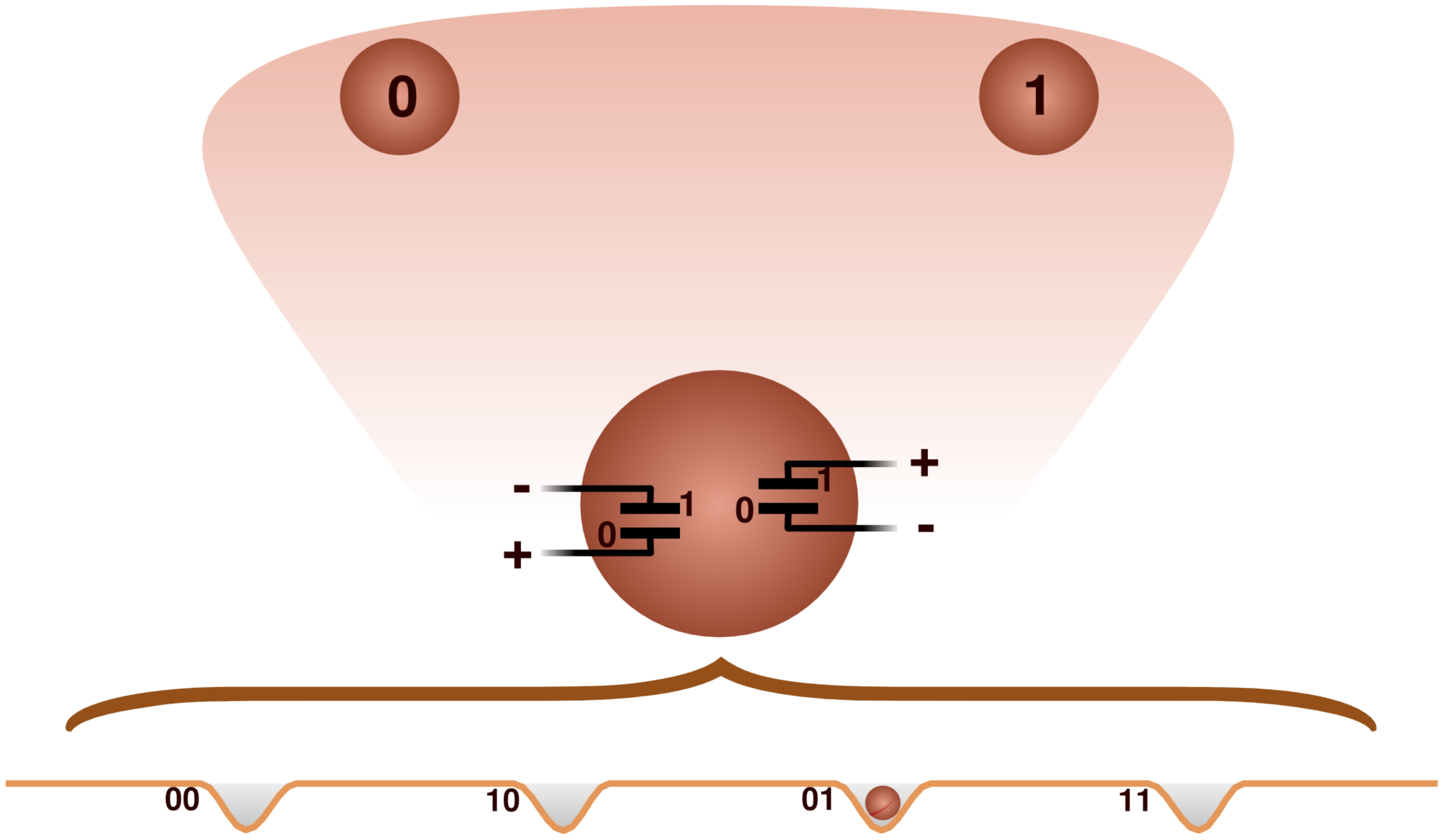
- Classical computer + quantum state machine.
  - Advanced programming constructs provided classically.



- State machine specified by:
  - State space.
  - State-transition operators.
  - Initial state.
  - Readout.

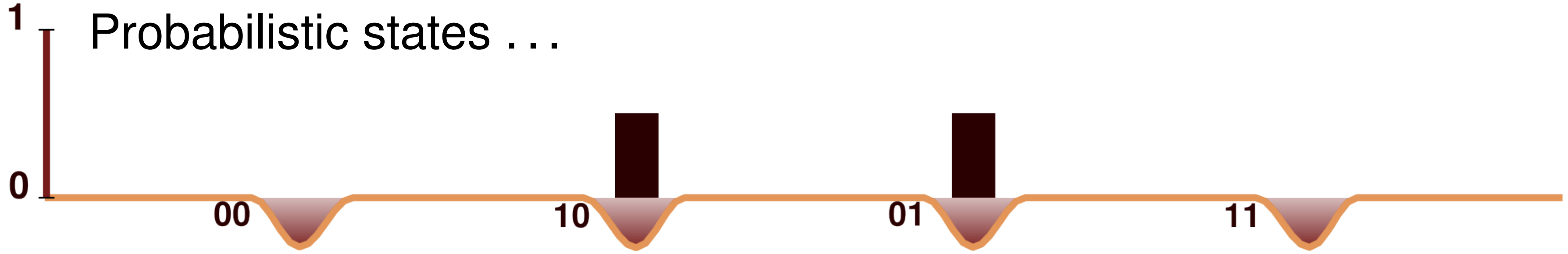
How Does It Work?

Classical states . . .



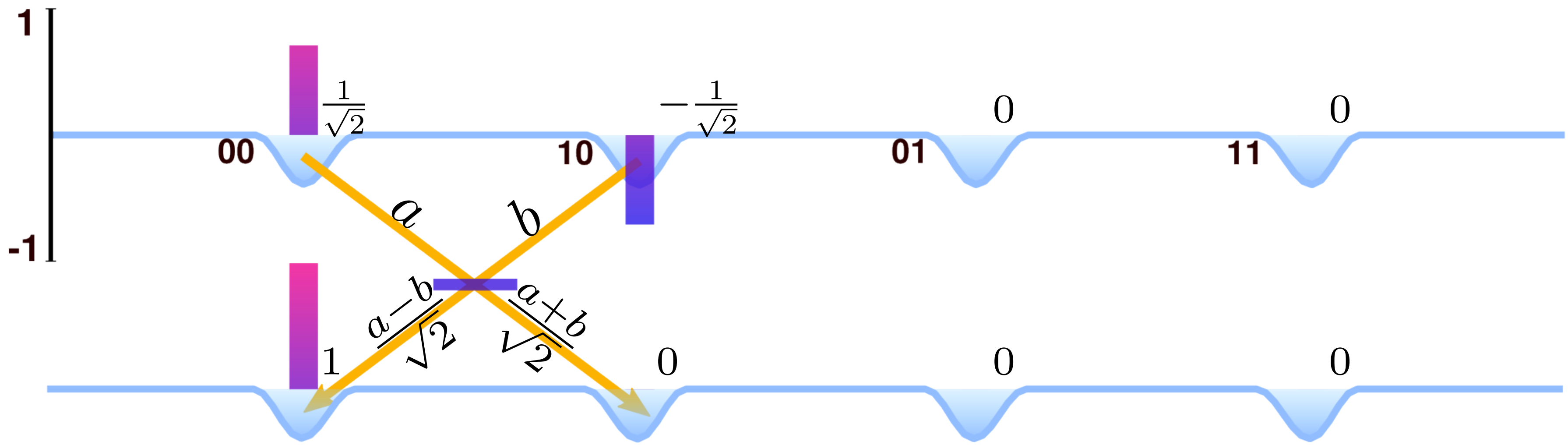
How Does It Work?

Probabilistic states . . .



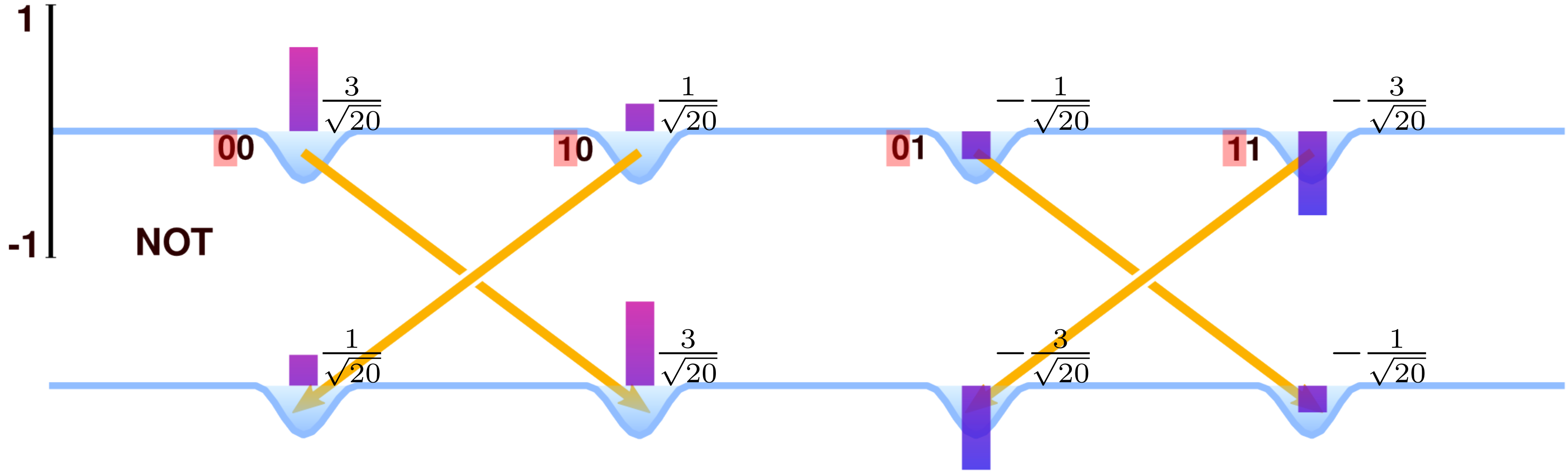
How Does It Work?

Quantum states . . . Interference . . .



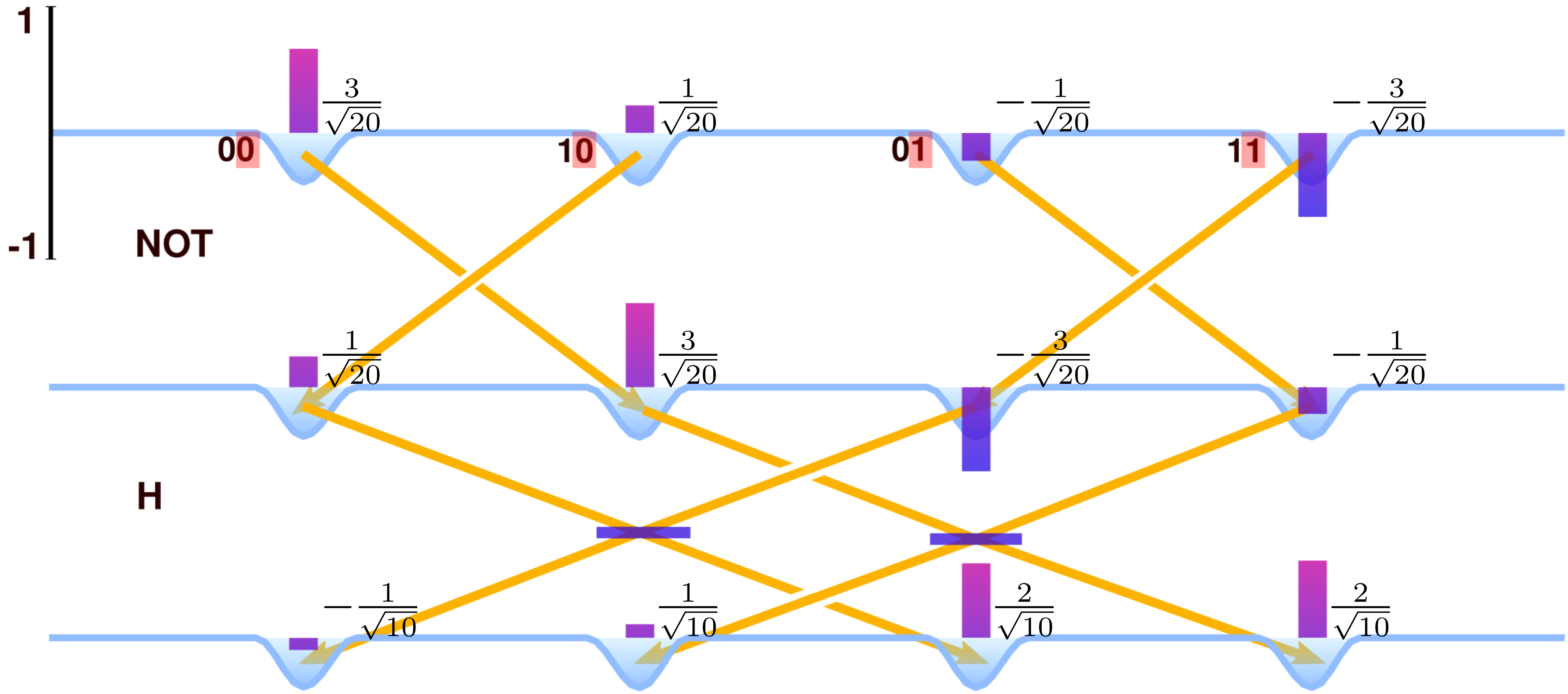
How Does It Work?

Quantum states . . . Interference . . . Q. Parallelism . . .



How Does It Work?

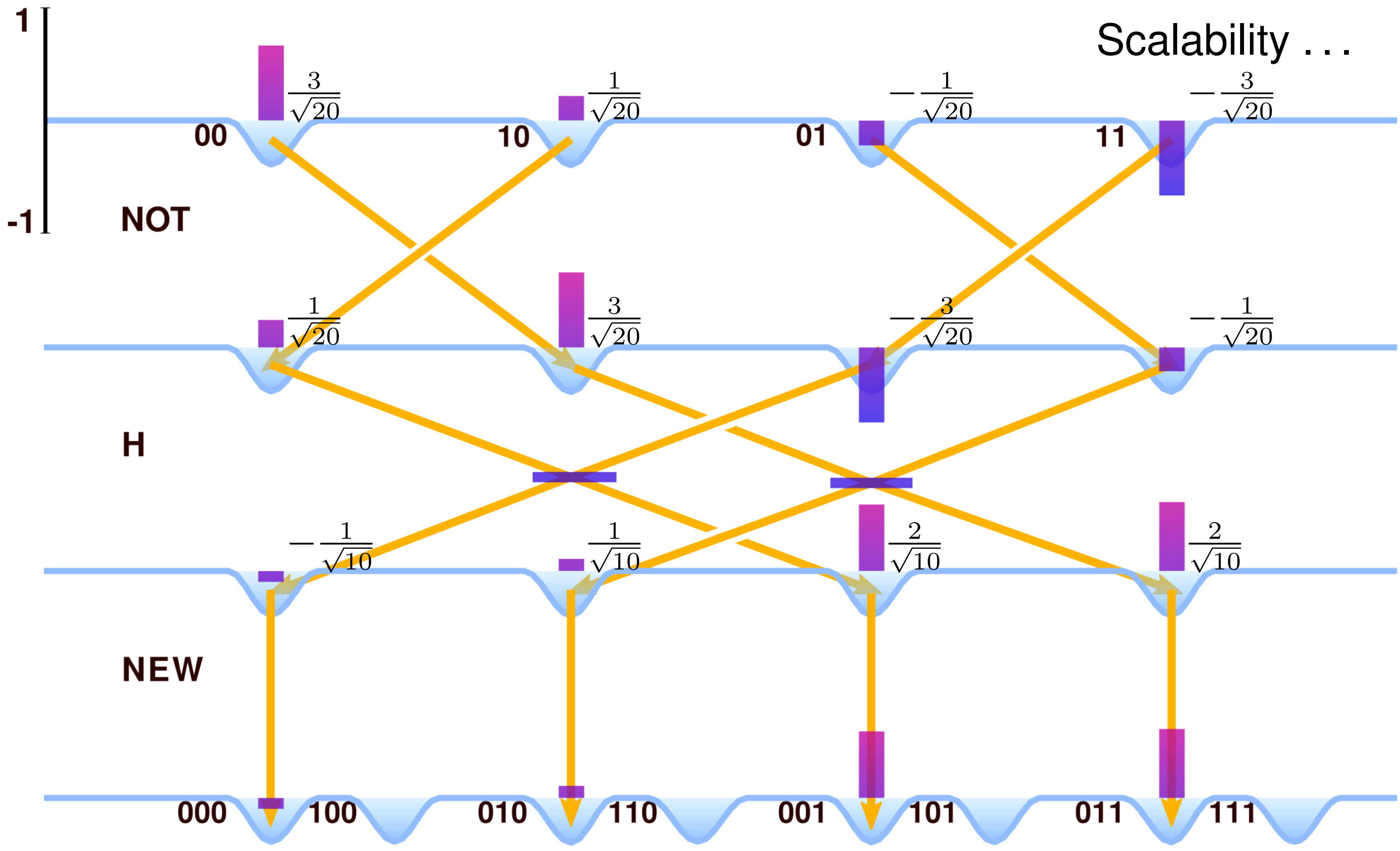
Quantum states . . . Interference . . . Q. Parallelism . . .



How Does It Work?

Quantum states . . . Interference . . . Q. Parallelism . . .

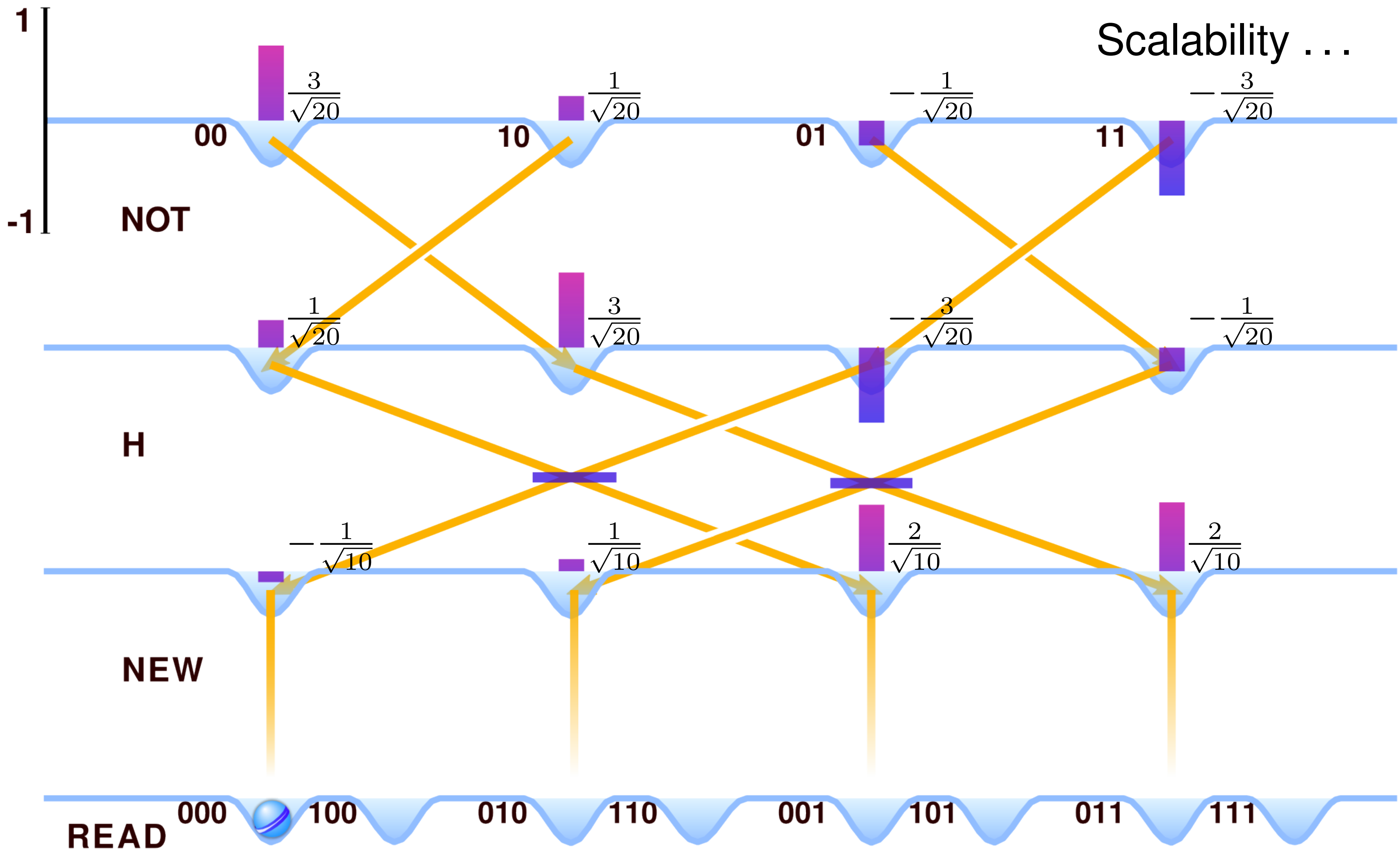
Scalability . . .



How Does It Work?

Quantum states . . . Interference . . . Q. Parallelism . . .

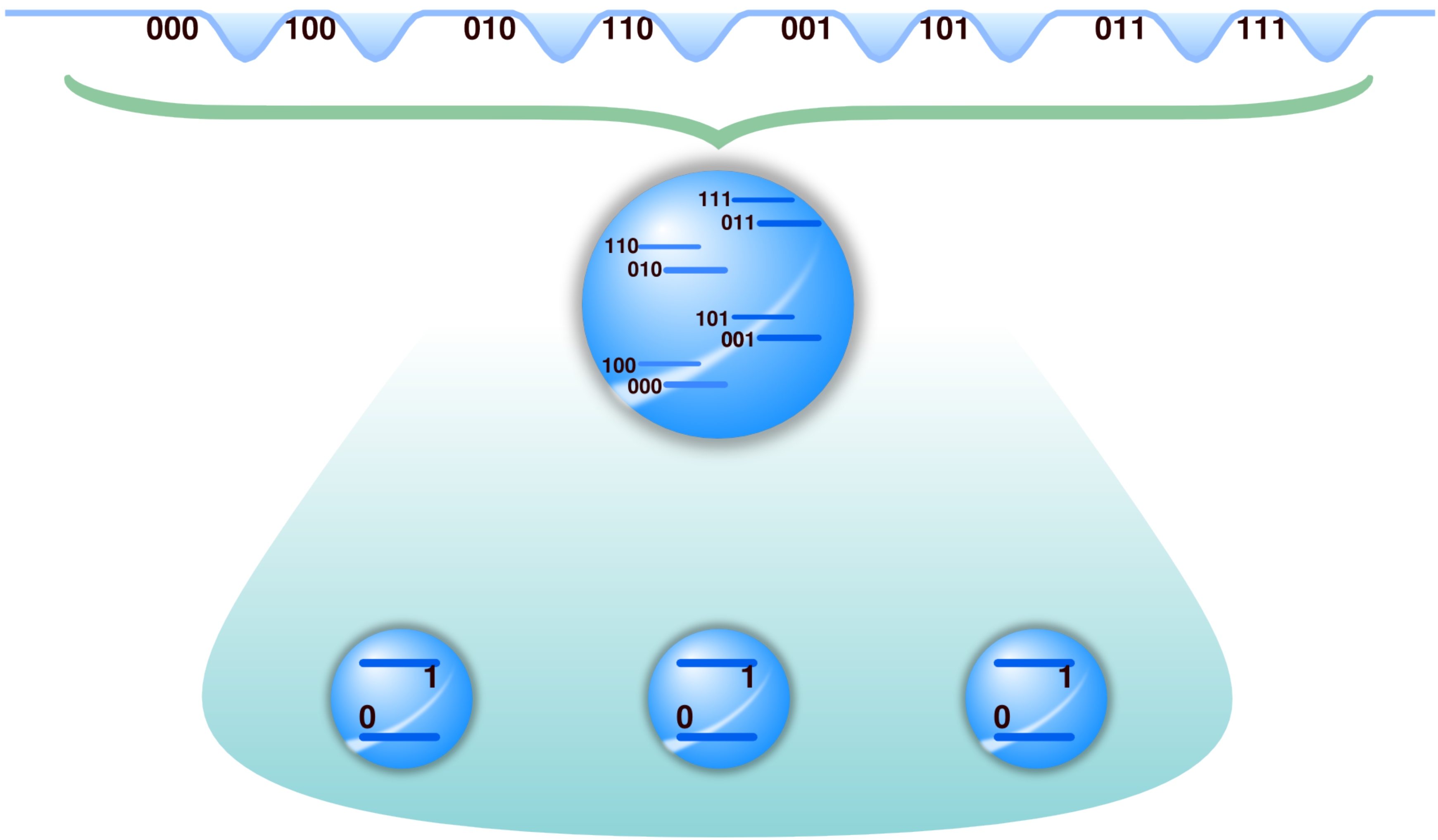
Scalability . . .



How Does It Work?

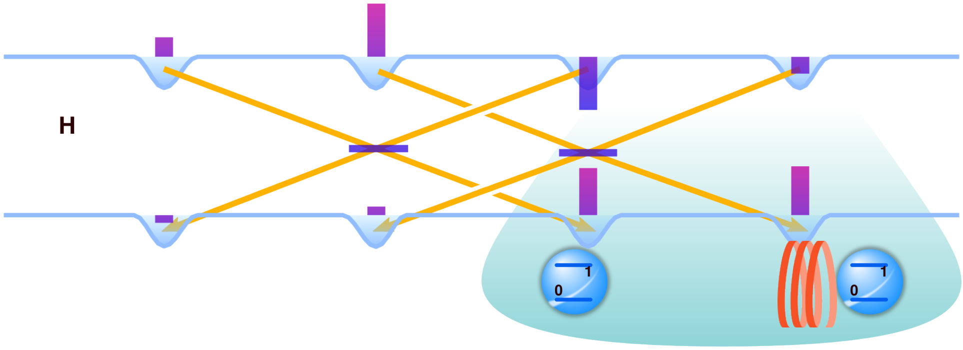
Quantum states . . . Interference . . . Q. Parallelism . . .

Efficient Scalability . . .

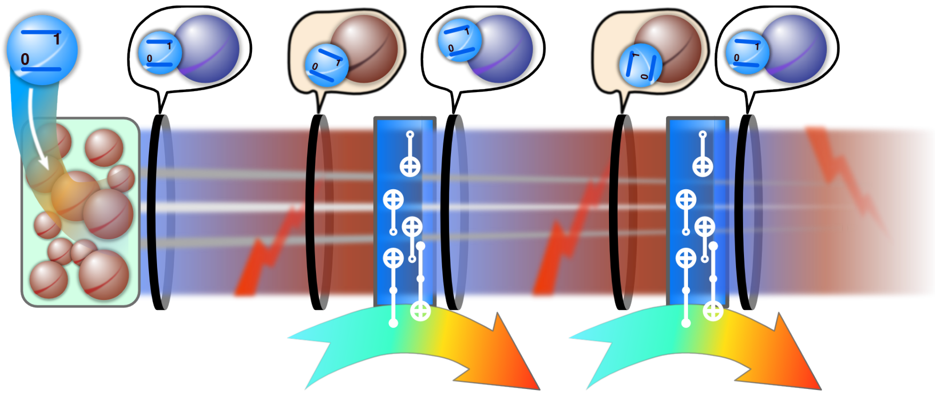


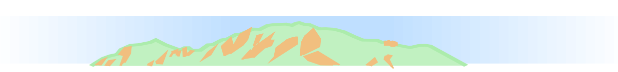
Preview

- QCs:
  - *wavefunctions*
  - *configuration spaces*
  - *interference*



- QCs can be realized in the presence of noise because of
  - the *threshold theorem*, whose implementation requires
  - *quantum error control*, which is based on
  - the *subsystems principle*, the most general way of “encoding” information.





Building QCs: Challenges

- DiVincenzo's requirements: DiVincenzo '00 [7]

  1. Independent QI-carrying quantum systems.
     (Demonstrated, many candidates.)
  2. Initializability of these quantum systems.
     (Demonstrated.)
  3. States are subject to sufficiently low noise.
     (Not demonstrated.)
  4. Universal control.
     (Demonstrated on a few qubits in a few systems.)
  5. Read-out.
     (Demonstrated in a few systems.)

- Challenges:
  - Reducing the effects of quantum noise.
    Low noise requires isolation
    but read-out and gates require strong coupling.
  - Satisfying all requirements in one device.

Decoherence

Definition: *Decoherence* is the loss of phase relationships between amplitudes.

- *Decoherence* often refers to any quantum noise leading to errors.

- Some sources of decoherence:
  - Interactions with the environment.
  - Noise in quantum control fields.
  - Systematic, calibration errors.

> **Fault-Tolerance Threshold Theorem.** *Given: Noisy qubits and gates. If the error rates are sufficiently low, then it is possible to efficiently process quantum information arbitrarily accurately.*

Shor '95 [8, 9], Kitaev '96 [10], Aharonov&Ben-Or '96 [11], Knill&Laflamme&Zurek '96 [12], Gottesman&Preskill '99, Steane '02 [13], Knill '04 [14, 15], Reichardt '04 [16], Aliferis&Gottesman&Preskill '05 [17]

Classical Versus Quantum Error Control

Conceptual difficulties:

- Error control must not “see” stored information.
  - “No cloning” theorem.
  - Nontrivial generalization of repetition codes.
- There is a continuity of error models.
  - Error models have many parameters.
  - Repetition codes are insufficient.

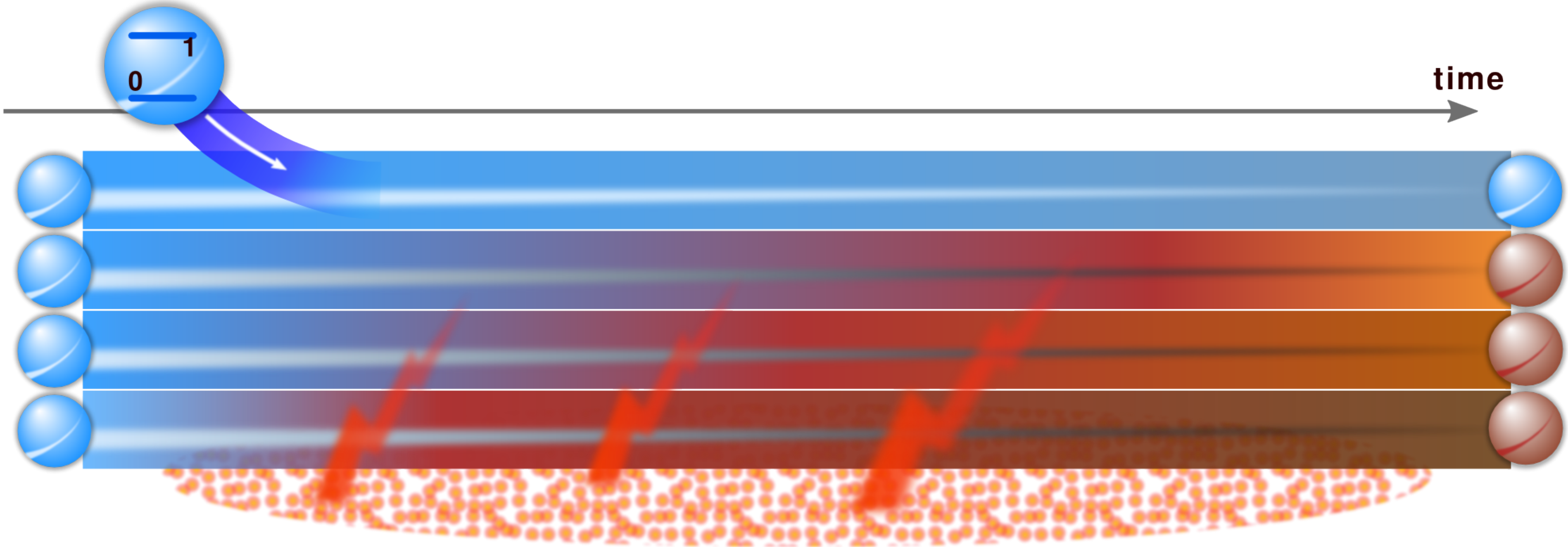
A sample of coping strategies:

- Quantum stabilizer codes generalize classical linear codes.
  Calderbank&al. ’96 [18], Gottesman ’96 [19]
- Adopt the subsystems principle. Knill&Laflamme&Viola ’99[21, 22]

Overcoming Decoherence

- **Goal:** Realize accurate QI in noisy physical systems.
  - Noise must be local in space and time (independence assumptions).

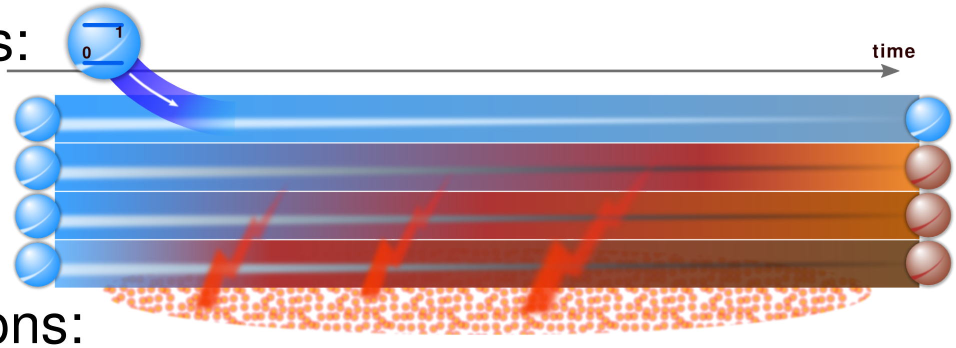
Trivial QI realizations:



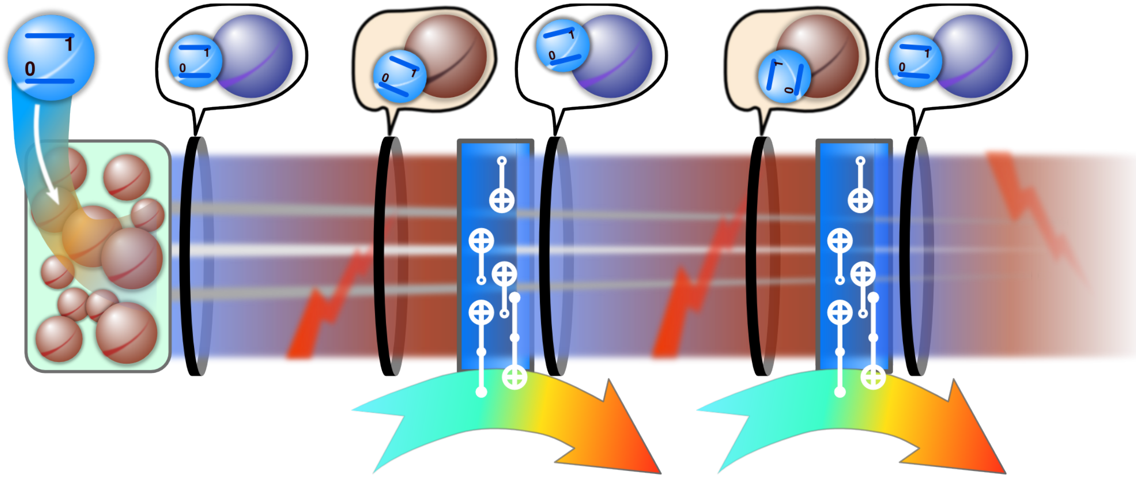
Overcoming Decoherence

- **Goal:** Realize accurate QI in noisy physical systems.
  - Noise must be local in space and time (independence assumptions).

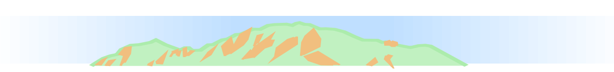
Trivial QI realizations:



General QI realizations:

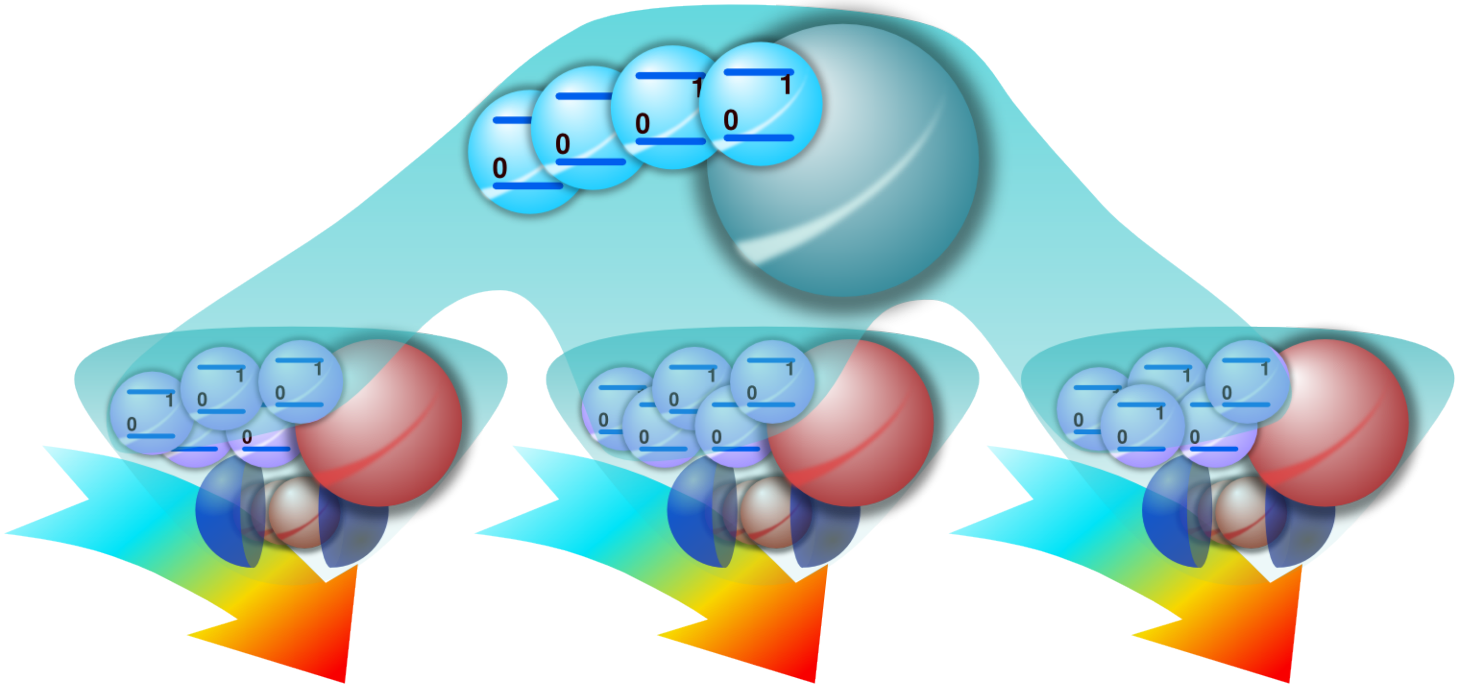


- Information should never be “decoded”.
- The subsystems principle applies to and enhances classical information theory.



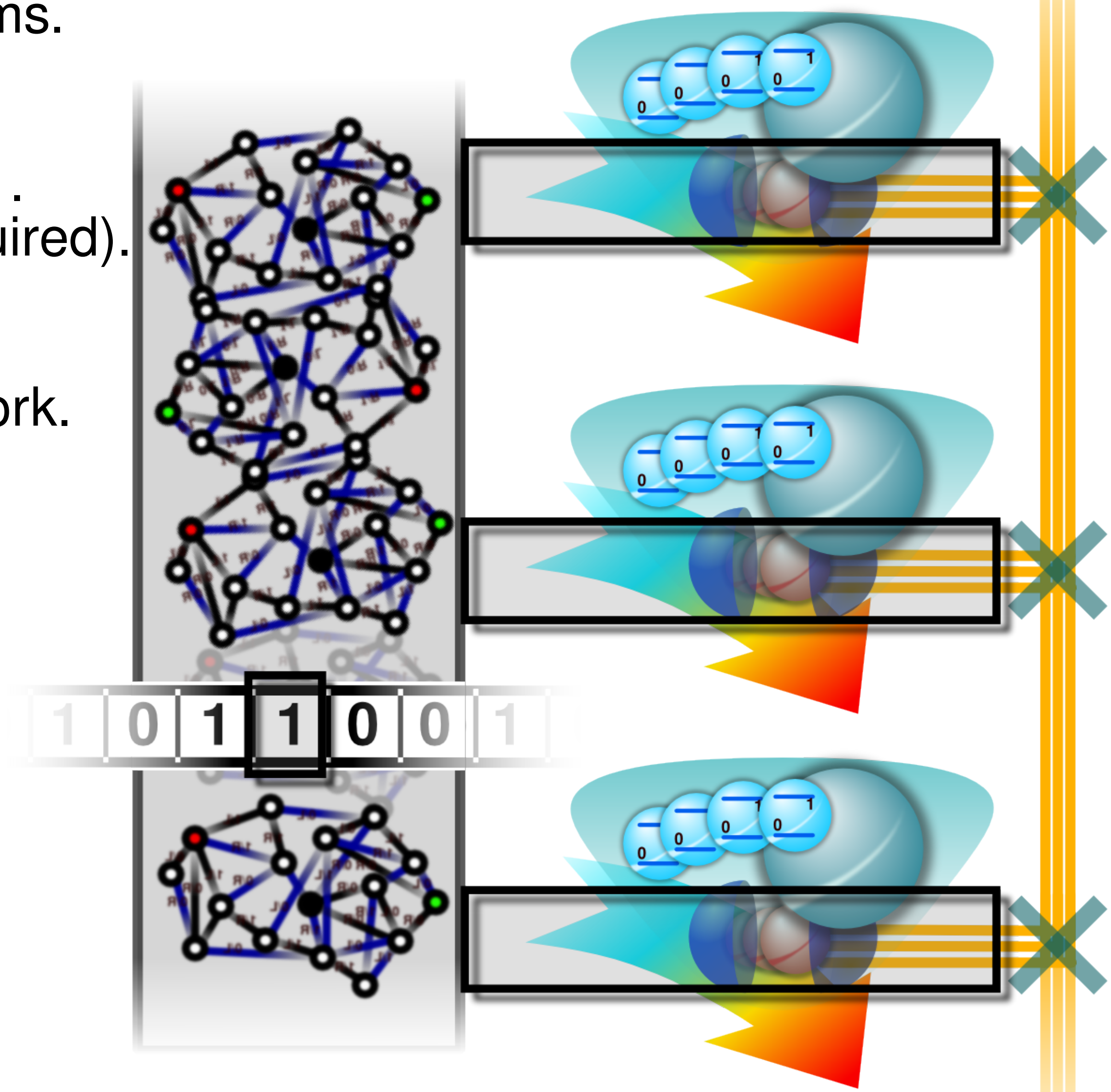
A Path to Large-Scale QCs

- Well defined physical quantum systems.
- Protectable quantum subsystems.
- Error entropy sink.
- Concatenation may help.



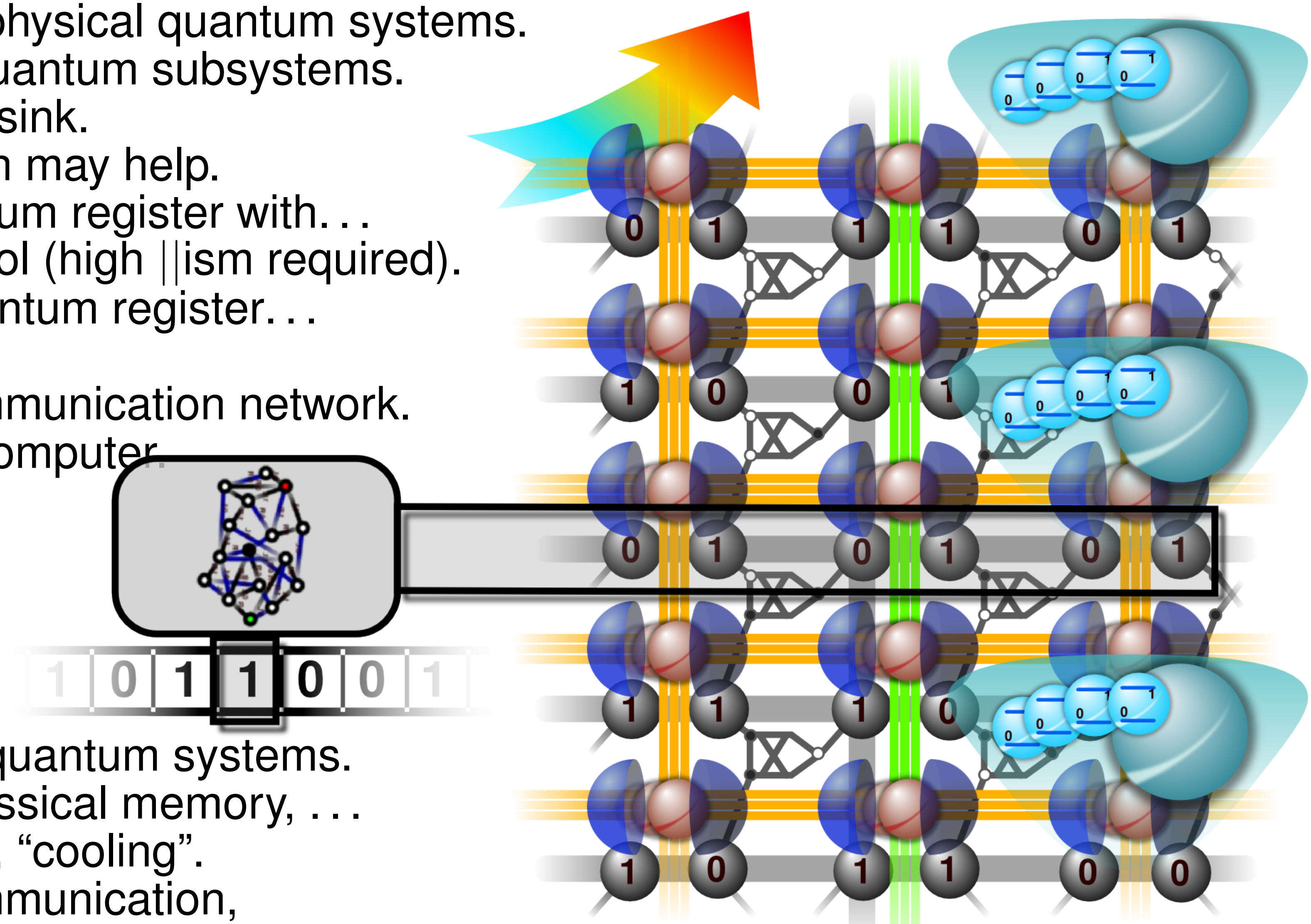
A Path to Large-Scale QCs

- Well defined physical quantum systems.
- Protectable quantum subsystems.
- Error entropy sink.
- Concatenation may help.
- A small quantum register with. . .
  external control (high ||ism required).
- Replicate quantum register. . .
  and control.
- Quantum communication network.
  ⇒ quantum computer.



A Path to Large-Scale QCs

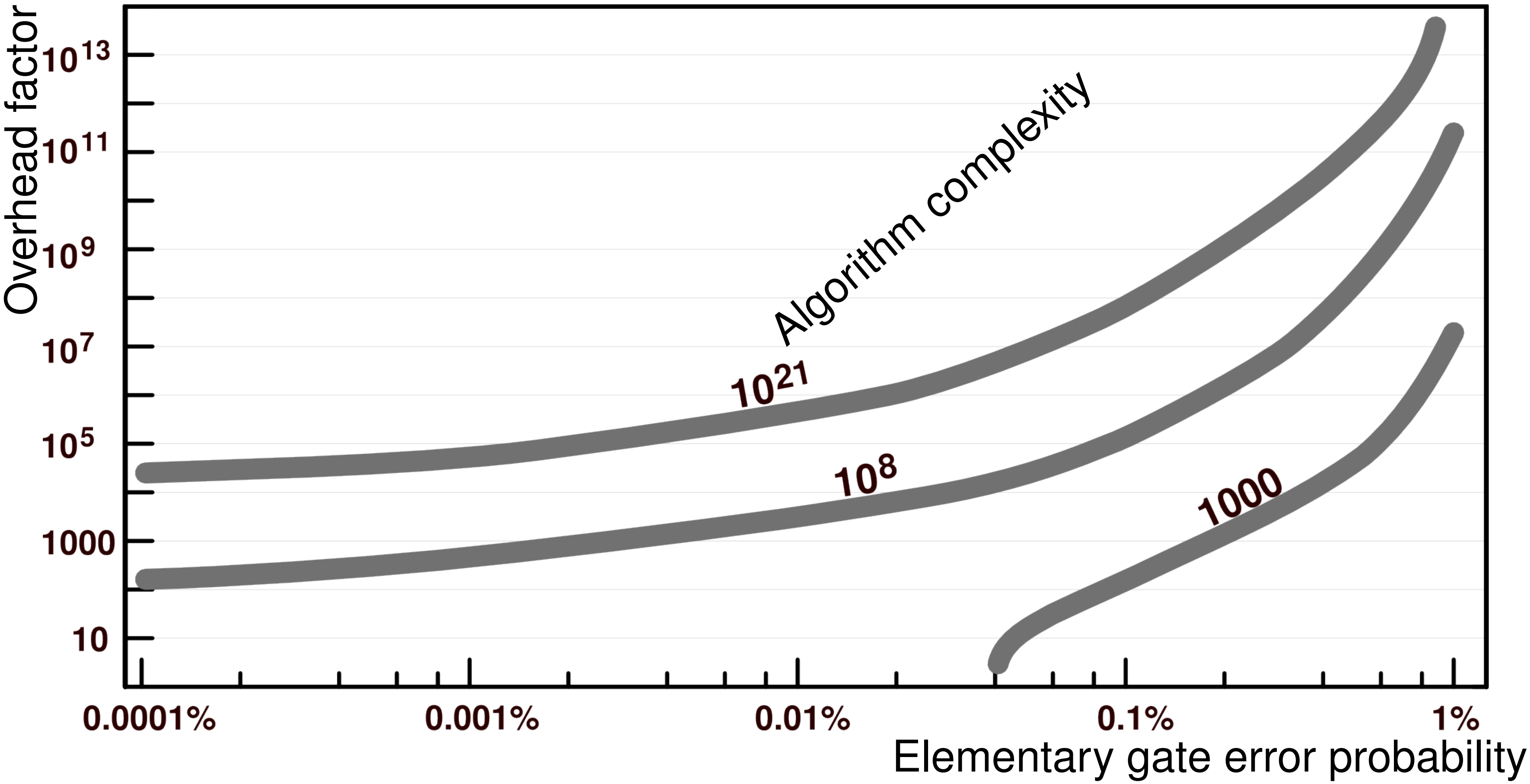
- Well defined physical quantum systems.
- Protectable quantum subsystems.
- Error entropy sink.
- Concatenation may help.
- A small quantum register with. . .
  external control (high ||ism required).
- Replicate quantum register. . .
  and control.
- Quantum communication network.
  ⇒ quantum computer.



- High density quantum systems.
- Integrated classical memory, . . .
  gates, control, “cooling”.
- Quantum communication,
  state prep. factories.
- Interface to classical control.

Goal: Physical computation is quantum, minimal overhead for FTQC over FTCC.

Resource Requirements



- Schematic resource overheads, depending on algorithm complexity and gate error.

Loosely based on Knill '05 [15]

Error Guidelines?

- How low error rates should be depends on:
  - Error parameters/error model.
  - Error tradeoffs for different gates/operations.
  - Architectural constraints.
  - How much resource overhead is acceptable.
  - The specific computation to be implemented.
  - …

- Rough error guidelines for practical scalability:

Gottesman&Preskill ’98, ’00 [27, 28]

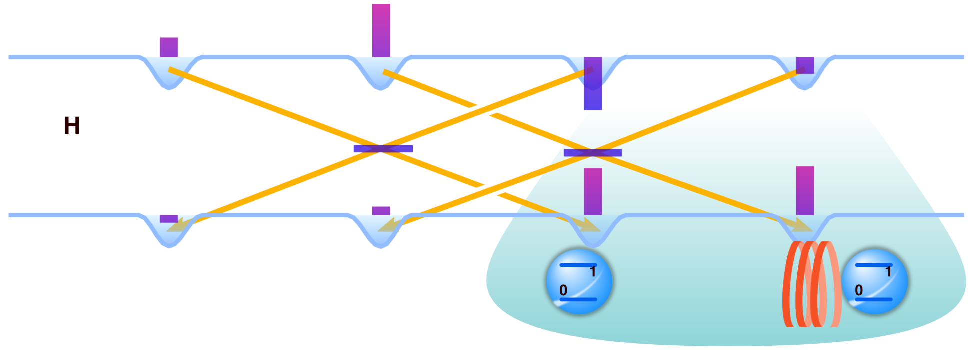
$<10^{-4}$
per gate

$<10^{-2}$
per preparation

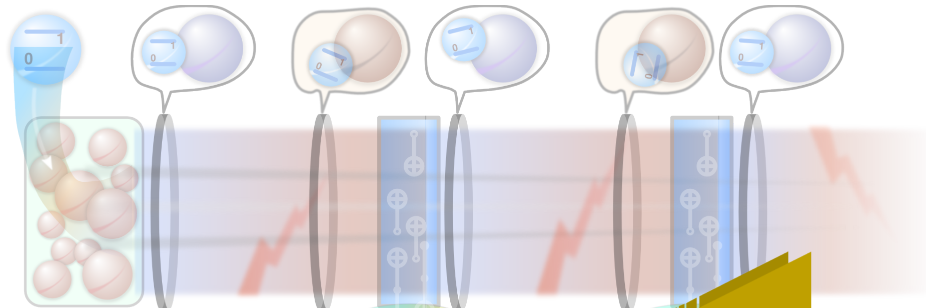
$<10^{-2}$
per measurement

Preview

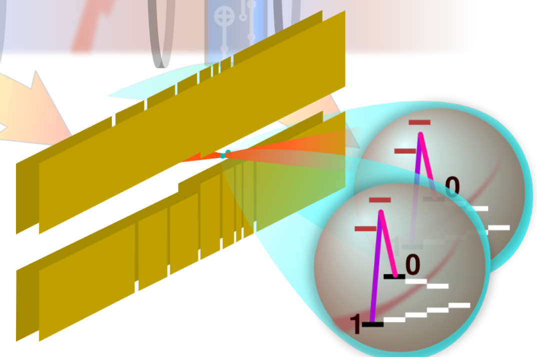
- QCs:
  - *wavefunctions*
  - *configuration spaces*
  - *interference*



- QCs can be realized:
  - *threshold theorem*
  - *quantum error control*
  - *subsystems principle*



- Experimental QC is close to achieving
  - *two-qubit registers*, with
  - *ion trap* devices being the current front runners, but
  - many other systems catching up rapidly.
  - *Decoherence* and *technology integration* are among the challenges.

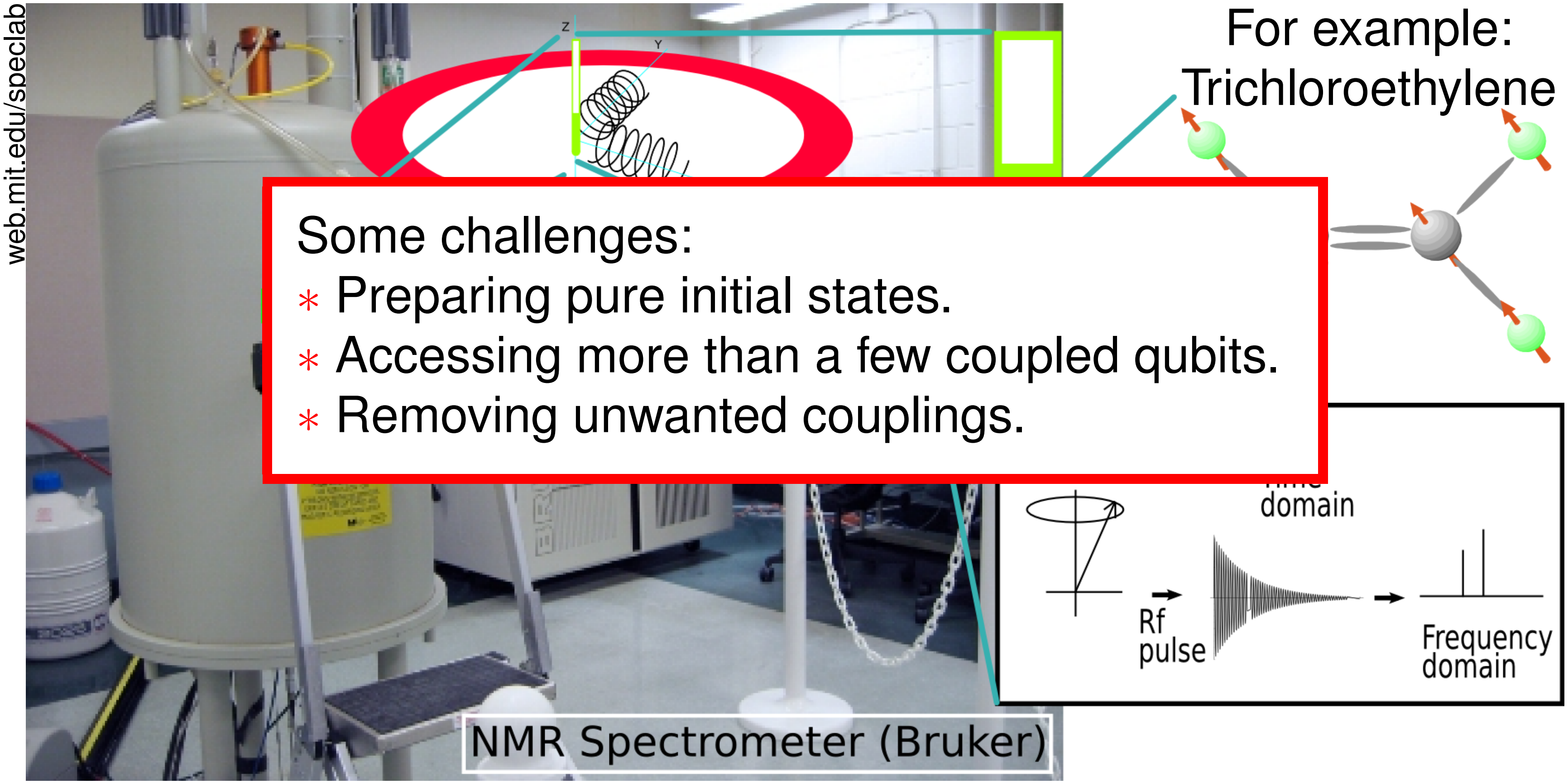


Available and Required QC Resources

- Available resources:
  - Approaching 2 computationally useful qubits.
  - For exploring quantum control:
    Up to ~ 8 qubits and ~ 16 control steps.
- Required resources:

Application	Order of minimum useful	
	qubits	gates
Secret key exchange, short distance	10^0	10^0
Secret key exchange, long distance	10^1	10^1
Factoring, other number theory algorithms	10^3	10^{10}
Unstructured search, optimization	10^2	10^8
Physics simulation	?	?

NMR QC



Some challenges:

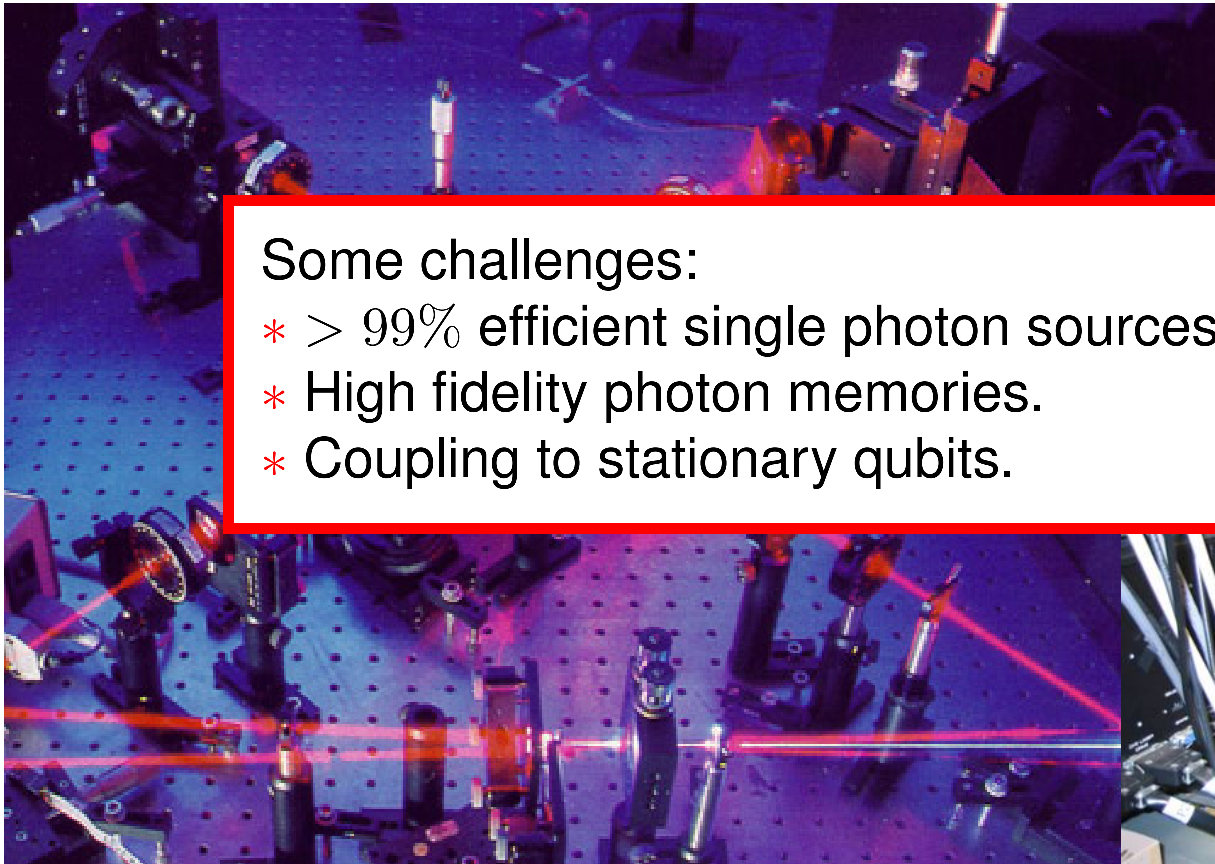
- ∗ Preparing pure initial states.
- ∗ Accessing more than a few coupled qubits.
- ∗ Removing unwanted couplings.

- ≈ 10 qubits, ≈ 20 two-qubit gates are realizable.
- Errors per two-qubit gate are $\gtrsim 1\%$.
- Not realistically scalable due to lack of “purity”. ...scalable in theory.

Reviews: Cory&al. ’00 [29], Laflamme&al. ’02 [30]

Photonic QC, Postselected

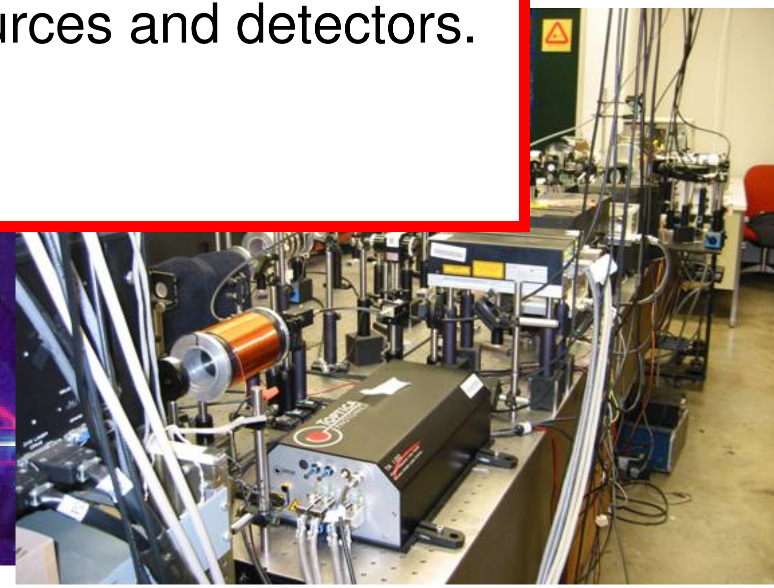
www.quantum.at



Quantum teleportation,
Bouwmeester&al., U. Wien

Some challenges:
* $>99\%$ efficient single photon sources and detectors.
* High fidelity photon memories.
* Coupling to stationary qubits.

s lab, FIU



http://www.fiu.edu/yifuzhu

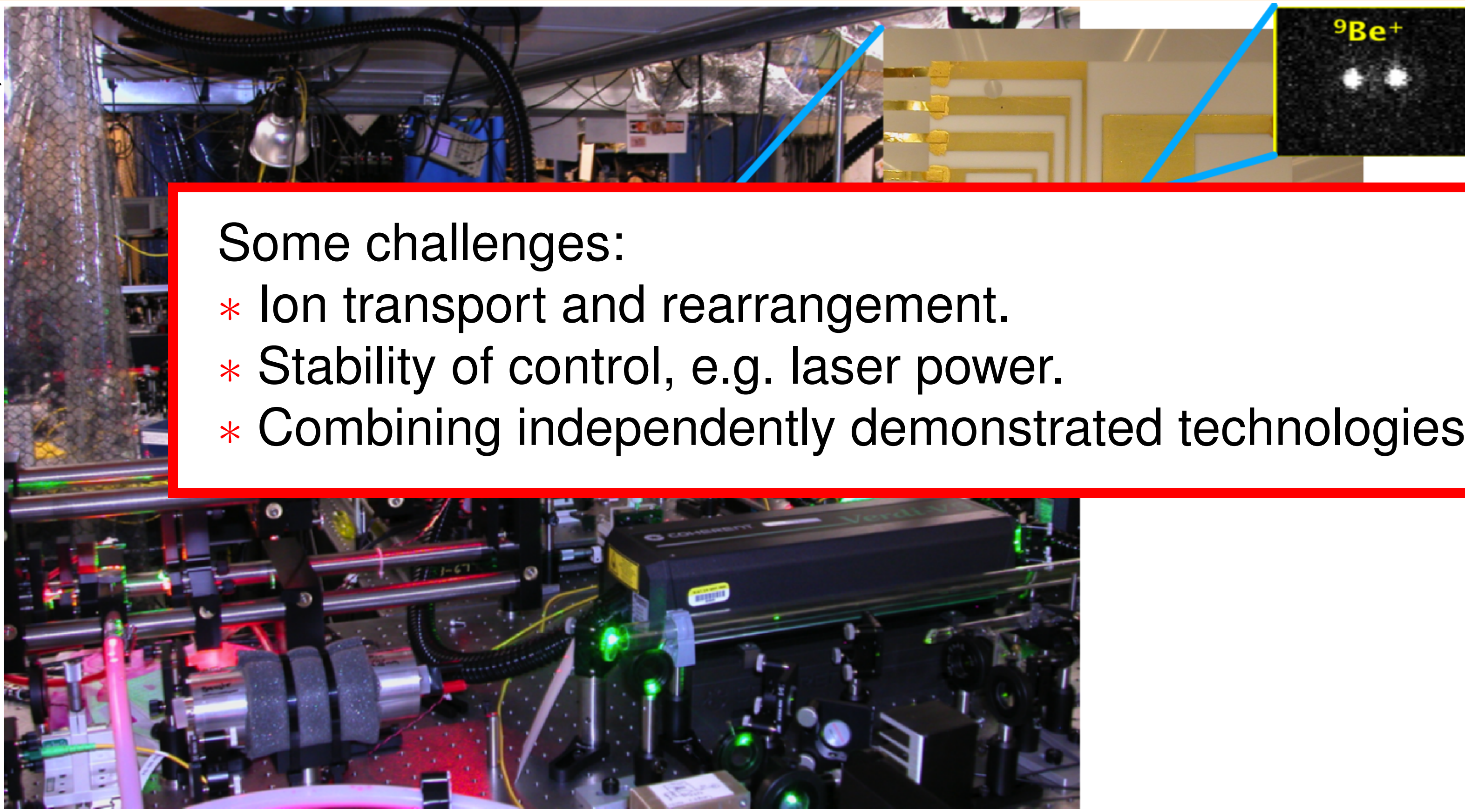
- ≈ 5 qubits, ≈ 3 two-qubit gates are realizable.
- Error per two-qubit gate $\gtrsim 3\%$ plus $>50\%$ loss.
- Not realistically scalable due to lack of determinism.

Review: Kok&al. '07 [31]

...optical QC is scalable in principle.

Ion Trap QC

Joe Britton, NIST



Some challenges:

* Ion transport and rearrangement.
* Stability of control, e.g. laser power.
* Combining independently demonstrated technologies.

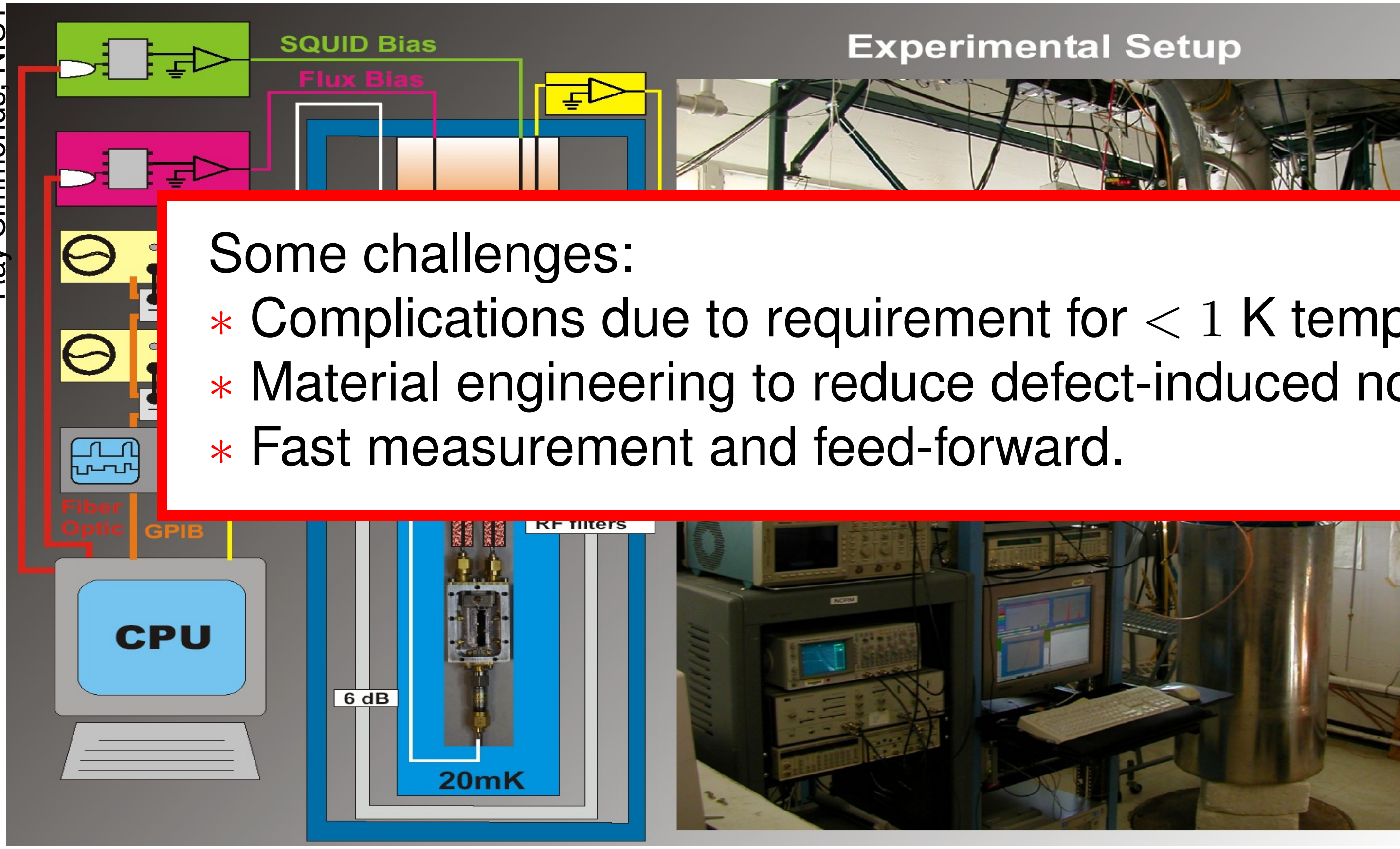
NIST

- Up to 8 qubits (2 routinely), $\gtrsim 5$ gates are realizable.
- $\lesssim 1\%$ achieved for two-qubit gate error.
- Currently closest to realistic scalability.

Reviews: Wineland&al. ’98 [32], Kielpinski ’08 [33]

Superconducting QC

Ray Simmonds, NIST



R. Simmond's lab, NIST

Some challenges:
* Complications due to requirement for < 1 K temperatures.
* Material engineering to reduce defect-induced noise.
* Fast measurement and feed-forward.

- Approaching 2 qubits, $\gtrsim 2$ gates.
- $\approx 15\%$ achieved for two-qubit gate error.
- Should be scalable with sufficient engineering.

Review: Devoret&al. '04 [34]

Experimental QC: Summary

System	Physical qubits	Number of qubits	Number of gates	Error per gate	Scal-able?
NMR	Nuclear spins in a molecule	$\lesssim 10$	$\lesssim 20$	$\gtrsim 1\%$	No
Photonic	Polarization of photons	$\lesssim 5$	$\lesssim 4$	$\gtrsim 3\%$ $> 50\%$	No
Ion trap	Energy levels of trapped ions	$\lesssim 8$	$\lesssim 4$	$\sim 1\%$ $\sim 10\%$	Yes
Superconducting	Collective states of superconducting circuits	< 2	$\lesssim 2$	$>15\%?$	Yes?
Cold atom	Energy levels of trapped atoms	< 2	$\lesssim 2$	?	?
Atomic impurities	Localized states of impurities	< 3	$\lesssim 4?$	?	?
Quantum dot	Localized states at dots	≈ 1	?	?	?
Topological	Delocalized states associated with excitations	0	0	??	??

. . . as of 2008.

Evaluating and Comparing Quantum Devices

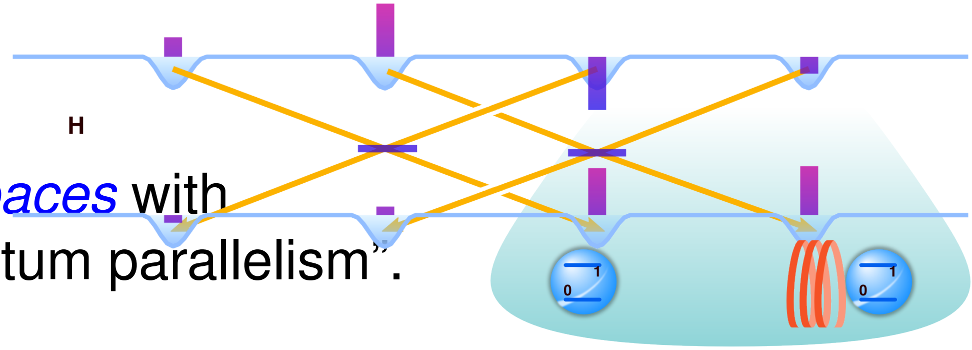
- How much quantum computing has been demonstrated?
  - How to measure "number of qubits used"?
  - How to measure "number of gates realized"?

- Log Quantum Speedup (LQS):

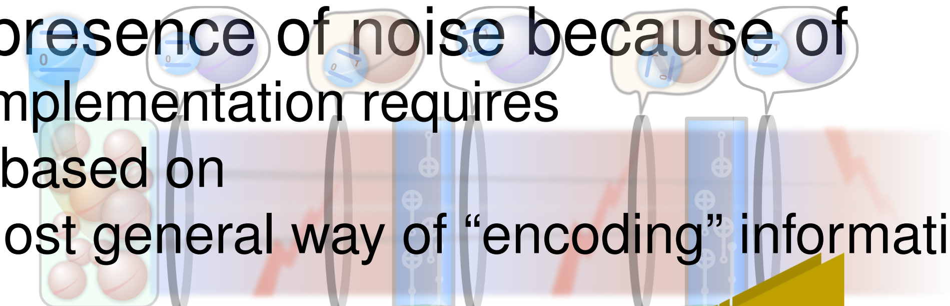
  L_2QS of 1.58 (implicitly) demonstrated with ion qubits on "unique quantum search with random target".

  Schaetz&al. '04 [37], Brickman&al. '05 [38]

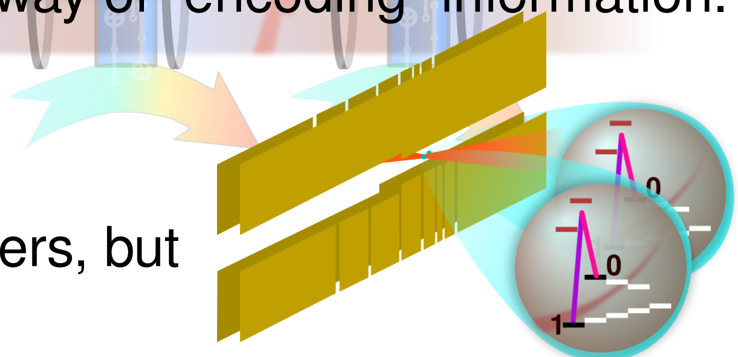
Summary and Prospects



- QCs control
  - *wavefunctions* on
  - efficiently realized *configuration spaces* with
  - *interference* gates exploiting “quantum parallelism”.



- QCs can be realized in the presence of noise because of
  - the *threshold theorem*, whose implementation requires
  - *quantum error control*, which is based on
  - the *subsystems principle*, the most general way of “encoding” information.



- Experimental QC is close to achieving
  - *two-qubit registers*, with
  - *ion trap* devices being the current front runners, but
  - many other systems catching up rapidly.
  - *Decoherence* and *technology integration* are among the challenges.

Quantum computing or new physics!

Contents

References

[1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[2] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, New York, 1996. ACM press.

[3] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[4] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen. Optimal frequency measurements with maximally correlated states. *Phys. Rev. A*, 54:R4649–R4652, 1996.

[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters for communication. quant-ph/9803056, 1998.

[6] D. Gottesman and I. Chuang. Quantum digital signatures. arXiv:quant-ph/0105032, 2001.

[7] D.P. DiVincenzo. The physical implementation of quantum computation. *Fort. Phys.*, 48:771–783, 2000.

[8] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493–2496, 1995.

[9] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS)*, pages 56–65, Los Alamitos, California, 1996. IEEE press.

[10] A. Yu. Kitaev. Quantum computations: Algorithms and error correction. *Russian Math. Surveys*, 52:1191–1249, 1997.

[11] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 176–188, New York, New York, 1996. ACM Press.

[12] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279:342–345, 1998.

[13] A. M. Steane. Overhead and noise threshold of fault-tolerant quantum error correction. *Phys. Rev. A*, 68:042322/1–19, 2003.

[14] E. Knill. Fault-tolerant postselected quantum computation: Threshold analysis. quant-ph/0404104, 2004.

[15] E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434:39–44, 2005.

[16] B. W. Reichardt. Improved ancilla preparation scheme increases fault tolerant threshold. quant-ph/0406025, 2004.

[17] P. Aliferis and D. W. Leung. Fault-tolerant quantum computation with graph states. quant-ph/0503130, 2005.

[18] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78:405–408, 1997.

[19] D. Gottesman. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

[20] G. K. Brennen, D. Song, and C. J. Williams. Quantum computer architecture using nonlocal interactions. *Phys. Rev. A*, 67:050302/1–4, 2003. quant-ph/0301012.

[21] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[22] E. Knill. Protected realizations of quantum information. *Phys. Rev. A*, 74:042301/1–11, 2006.

[23] D. Gottesman. Fault-tolerant quantum computation with local gates. *J. Mod. Optics*, 47:333–345, 2000.

[24] K. M. Svore, D. P. DiVincenzo, and B. M. Terhal. Noise threshold for a fault-tolerant two-dimensional lattice architecture. *Quantum Inf. and Comp.*, 7:297–318, 2007.

[25] P. Gács. Reliable cellular automata with self-organization. *J. Stat. Phys.*, 103:45–267, 2001.

[26] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. quant-ph/9906129, 1999.

[27] J. Preskill. Reliable quantum computers. *Proc. R. Soc. Lond. A*, 454:385–410, 1998.

[28] D. Gottesman and J. Preskill. Unpublished analysis of the accuracy threshold., 1999.

[29] D.G. Cory, R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemariam, Y.S. Weinstein, and W.H. Zurek. NMR based quantum information processing: Achievements and prospects. *Fort. Phys.*, 48:875–907, 2000.

[30] R. Laflamme, E. Knill, D. Cory, E. M. Fortunato, T. Havel, C. Miquel, R. Martinez, C. Negrevergne, G. Ortiz, M. A. Pravia, S. Sinha, R. Somma, and L. Viola. Introduction to NMR quantum information processing. *LA Science*, 27(LAUR-02-6132):226–259, 2002. quant-ph/0207172.

[31] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79:135–174, 2007.

[32] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. Nat. Inst. St. Tech.*, 103:259–328, 1998.

[33] D. Kielpinski. Ion-trap quantum information processing: Experimental status. arXiv:0805.2450, 2008.

[34] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting qubits: A short review. quant-ph/0411174, 2004.

[35] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme. Symmetrised characterisation of noisy quantum processes. *Science*, 317:1893–1896, 2007.

[36] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. arXiv:0707.1032, 2007.

[37] T. Schaetz, M. D. Barrett, D. Leibfried, J. Chiaverini, J. Britton, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland. Quantum dense coding with atomic qubits. *Phys. Rev. Lett.*, 93:040505/1–4, 2004.

[38] K.-A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslaurier, and C. Monroe. Implementation of Grover's quantum search algorithm in a scalable system. *Phys. Rev. A*, 72:050306/1–4, 2005.