



---

# Quantum Algorithms

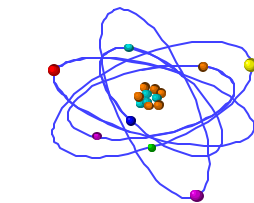
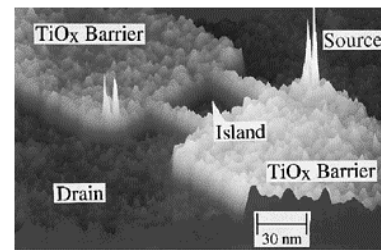
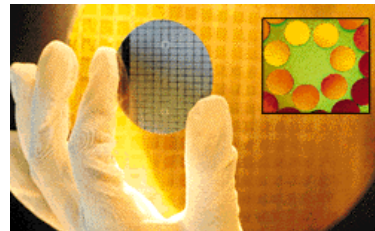
Artur Ekert  
University of Oxford

# Motivation

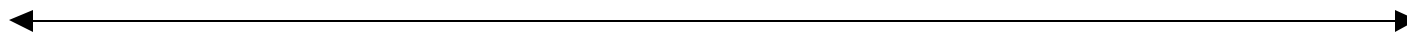
1. Faster => smaller => shrinking computer



1m



1nm



2. Computational complexity

New quantum algorithms can turn some difficult problems into easy ones

3. Quantum computation = multi-particle quantum interference

Understanding/testing the foundations of QM

# Outline

---

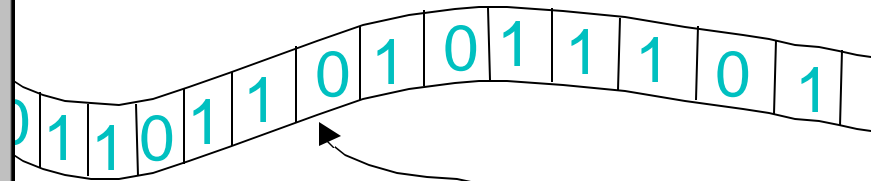
- Reasonable models of computation
  - » Finite alphabets, finite set of rules, efficient physical representation of data
- Deterministic, probabilistic and quantum computation
- Sequential computation
  - » Quantum computers = interferometry
- Beyond sequential models

# What is computation?



I can formalise computation it in terms of actions of an abstract machine...

Finite alphabet  $\Sigma = \{0,1\}$



Finite set of internal states of the head

$Q = \{q_0, q_1, q_2, \dots, q_f\}$

Finite set of rules:  $\Sigma \times Q \rightarrow \Sigma \times Q \times \{\leftarrow, 0, \rightarrow\}$

Computation:  $(x \in \Sigma^*, q_0) \rightarrow (y \in \Sigma^*, q_f)$

# Models & Physics

---

---

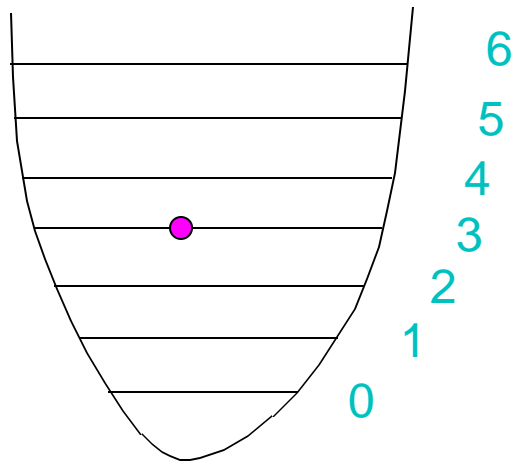
Any reasonable model of computation must be:

- **Physically possible**
- **Efficient in its use of physical resources**

# Physical representations of symbols

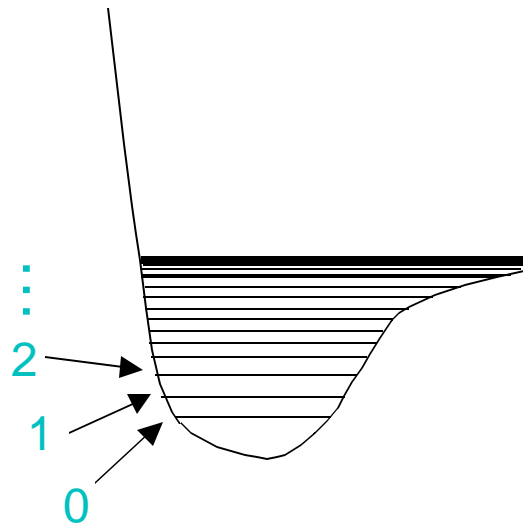
unary encoding - inefficient

binary encoding - efficient



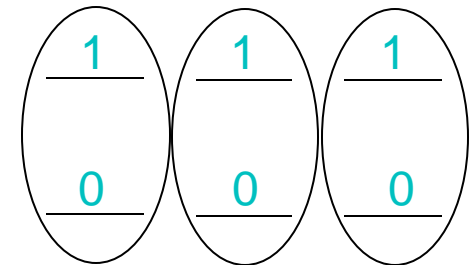
$$E \propto n$$

$$dE = \text{const}$$



$$E = \text{const}$$

$$dE \propto 1/n$$



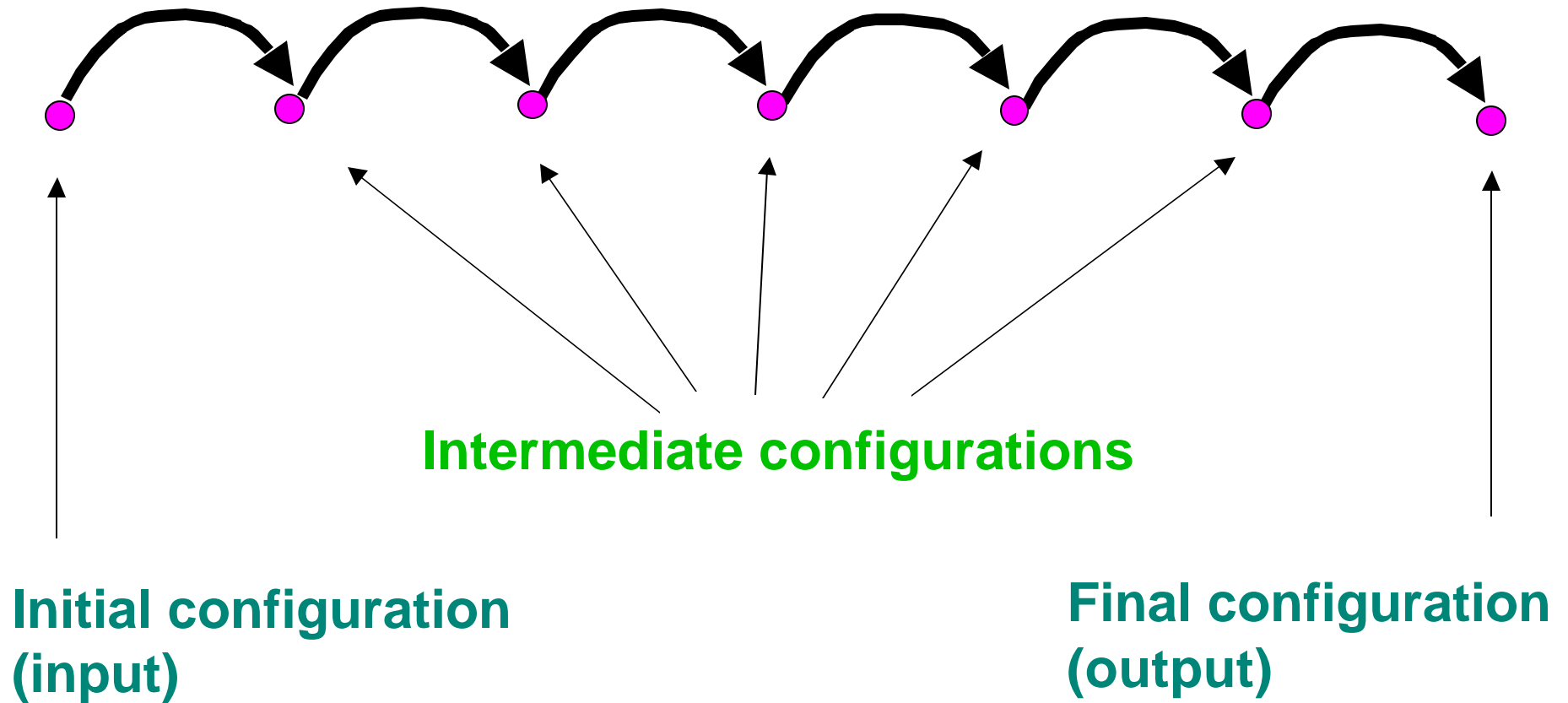
$$E \propto \log n$$

$$dE = \text{const}$$

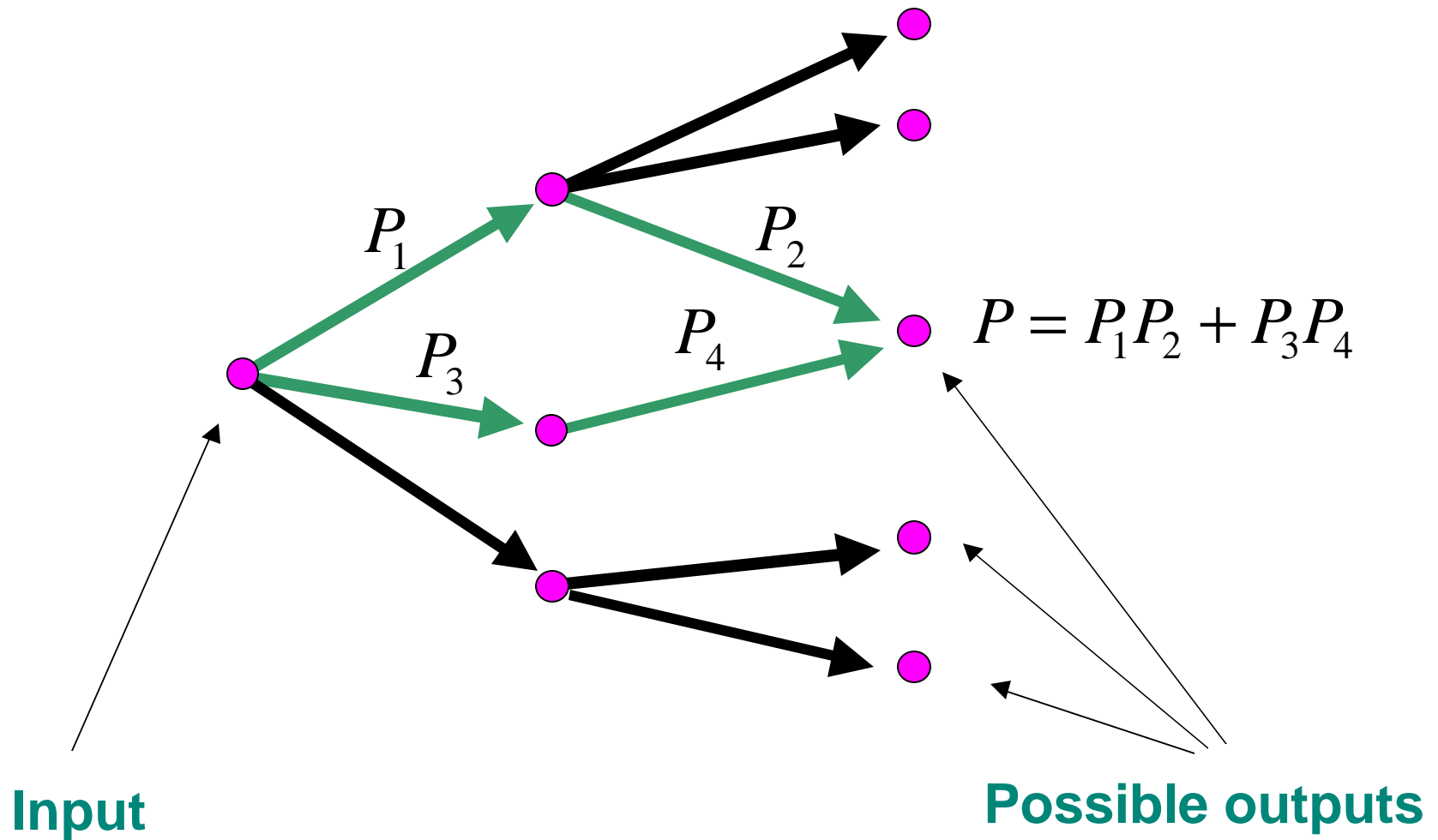
# Deterministic computation

---

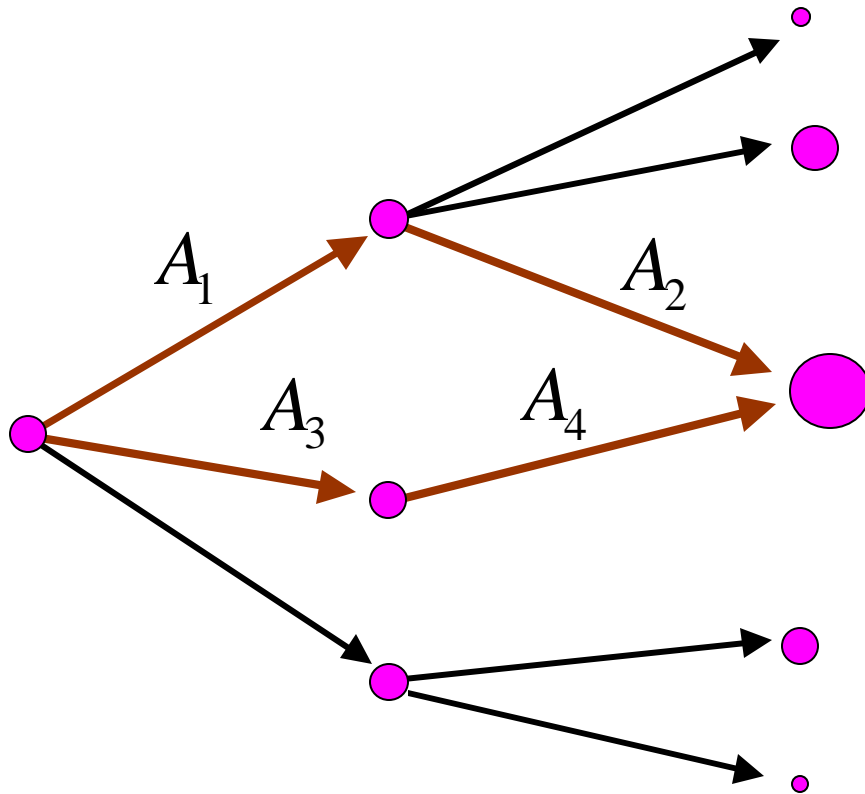
---



# Probabilistic computation



# Quantum computation

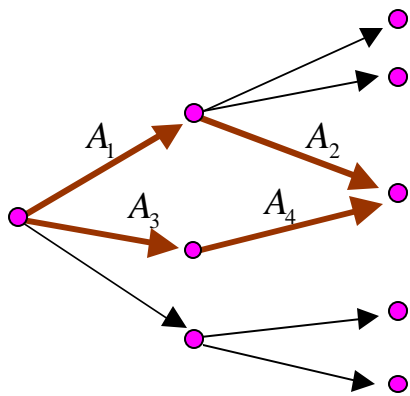


$$A = A_1 A_2 + A_3 A_4$$

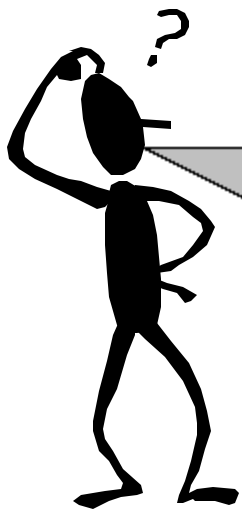
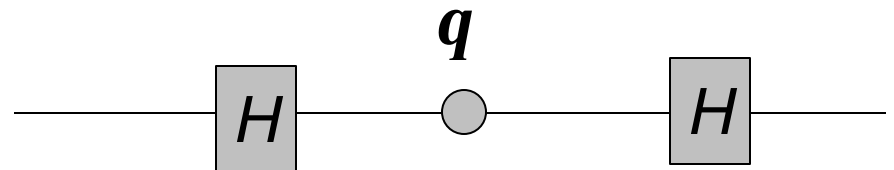
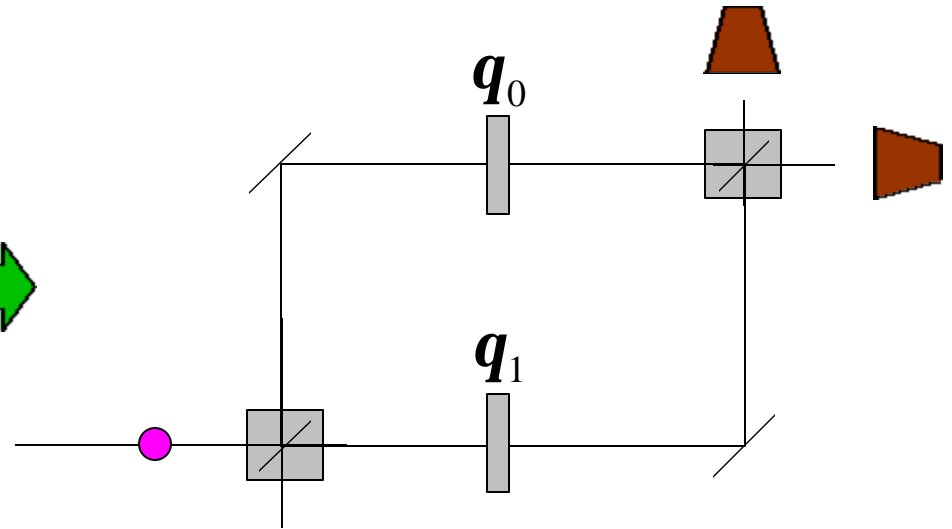
$$\begin{aligned} P &= |A_1 A_2 + A_3 A_4|^2 \\ &= |A_1 A_2|^2 + |A_3 A_4|^2 \\ &\quad + 2 \operatorname{Re}(A_1 A_2 A_3^* A_4^*) \end{aligned}$$

↑  
sensitive to decoherence

# Building quantum computers

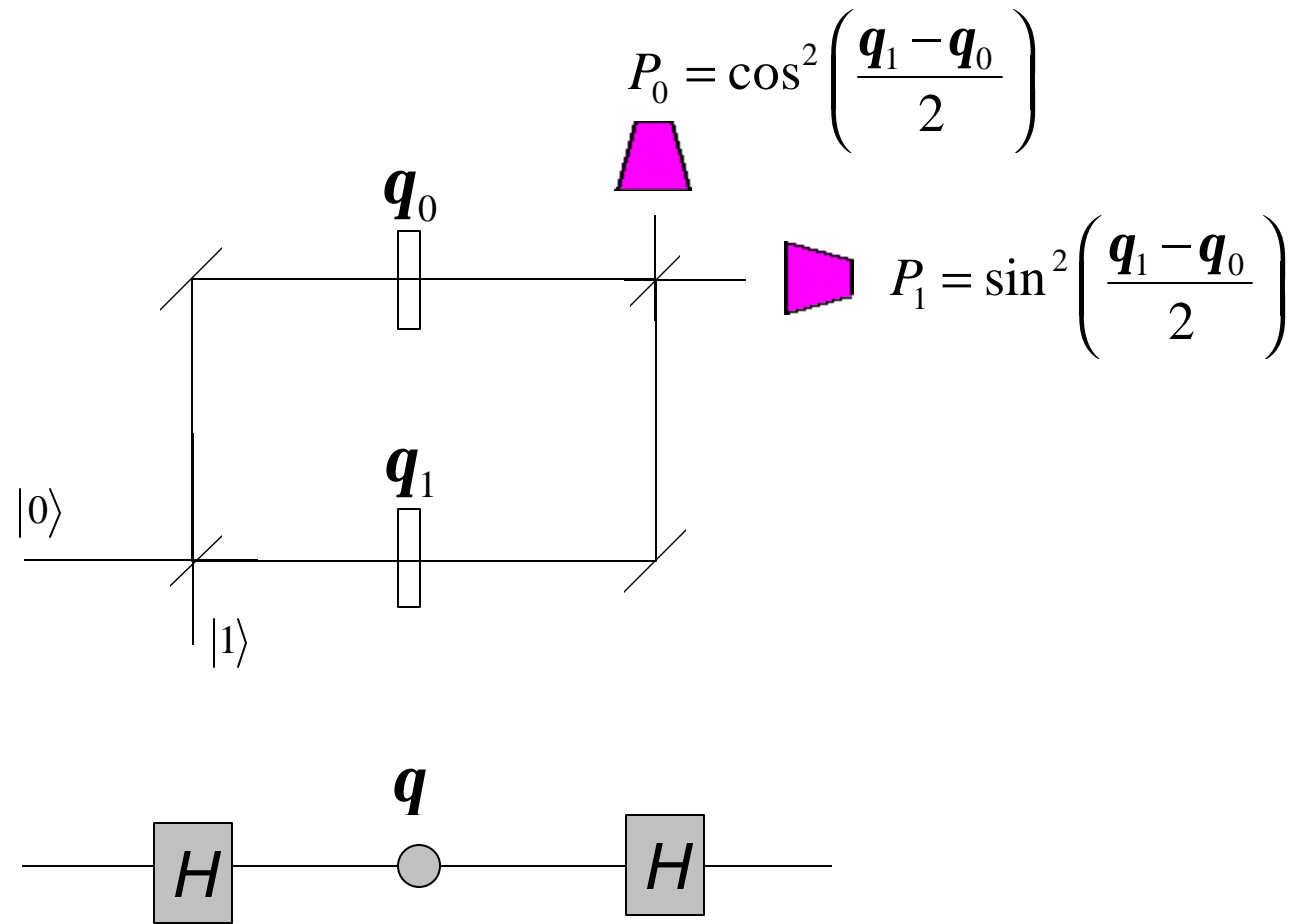


$$A = A_1A_2 + A_3A_4$$
$$P = |A_1A_2 + A_3A_4|^2$$



In fact, there are many ways of implementing quantum interference...

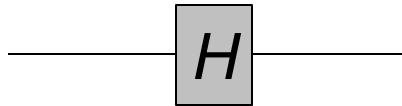
# Quantum interference



# Hadamard & Phase gates

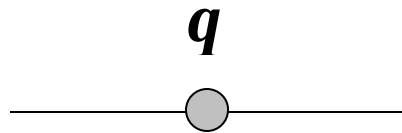
---

---



$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

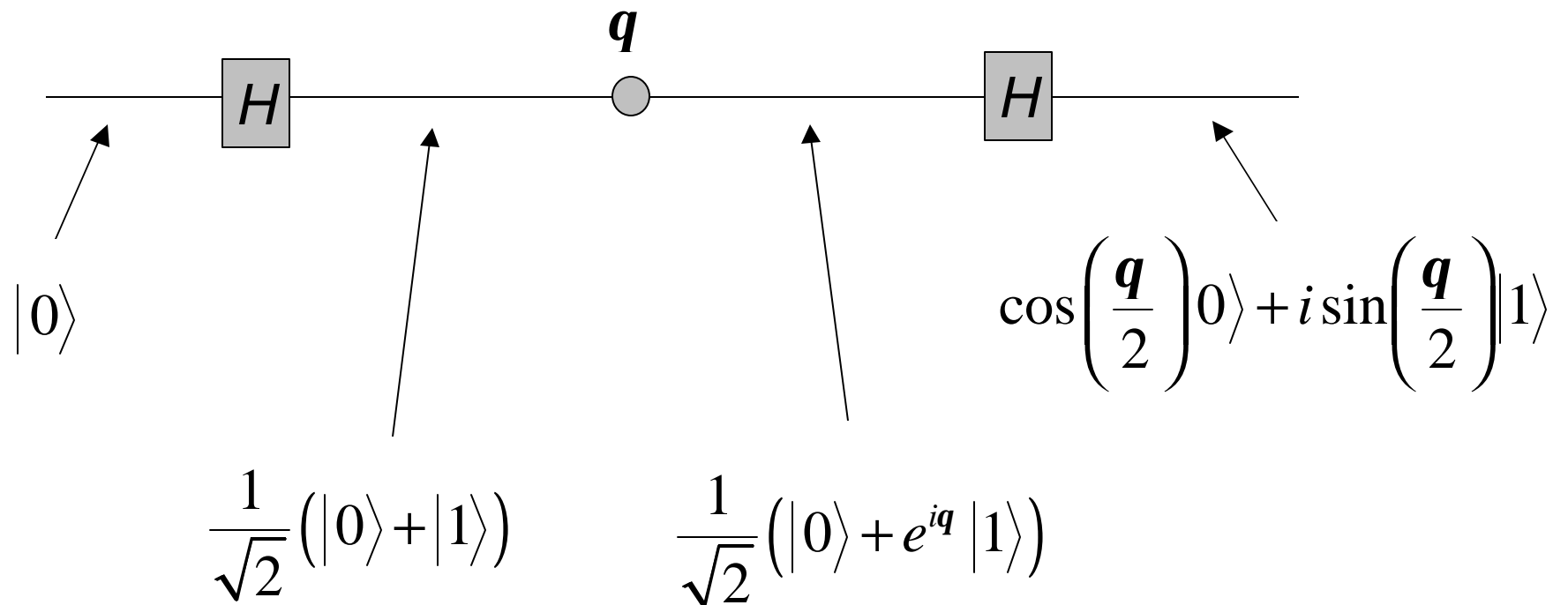
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



$$|0\rangle \rightarrow |0\rangle$$

$$|1\rangle \rightarrow e^{iq}|1\rangle$$

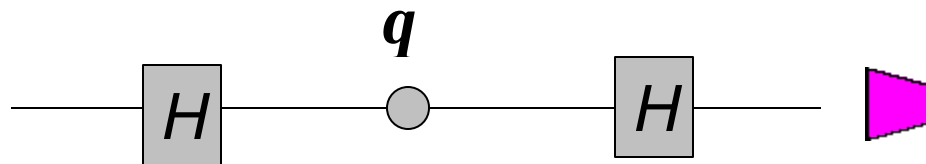
# Any single particle interference



# Gates & Networks = convenient description of experiments

---

---



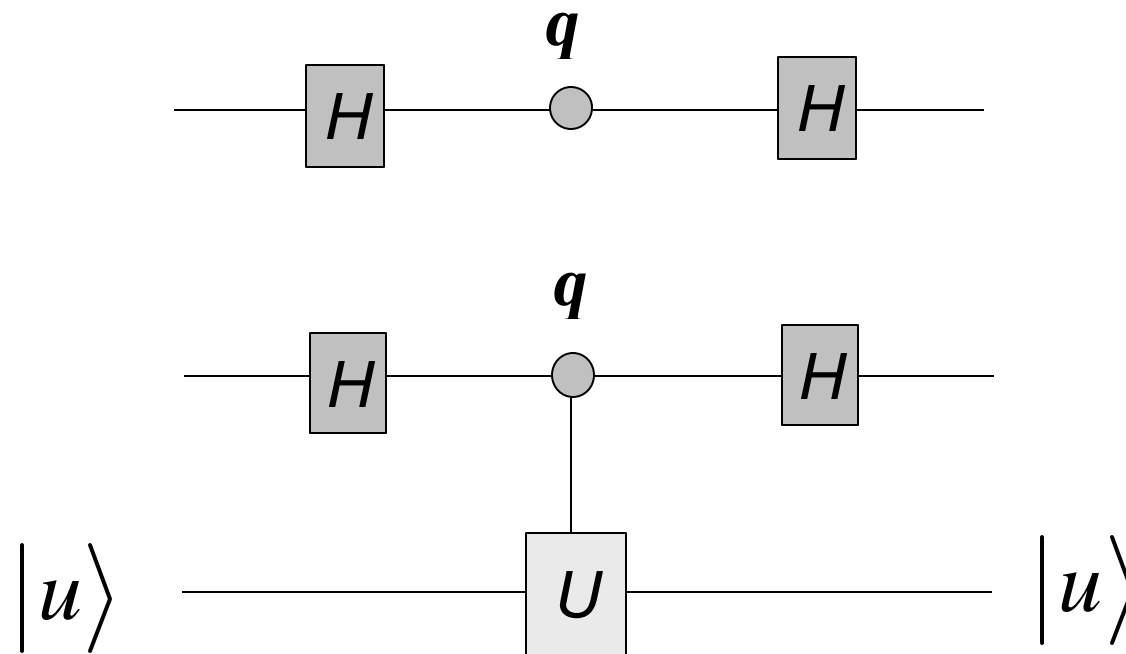
- Mach-Zehnder interferometer
- Cavity QED Ramsey interferometry
- Ramsey interferometry using trapped ions
- Neutron interferometry
- ...

# So far so good, but...

---

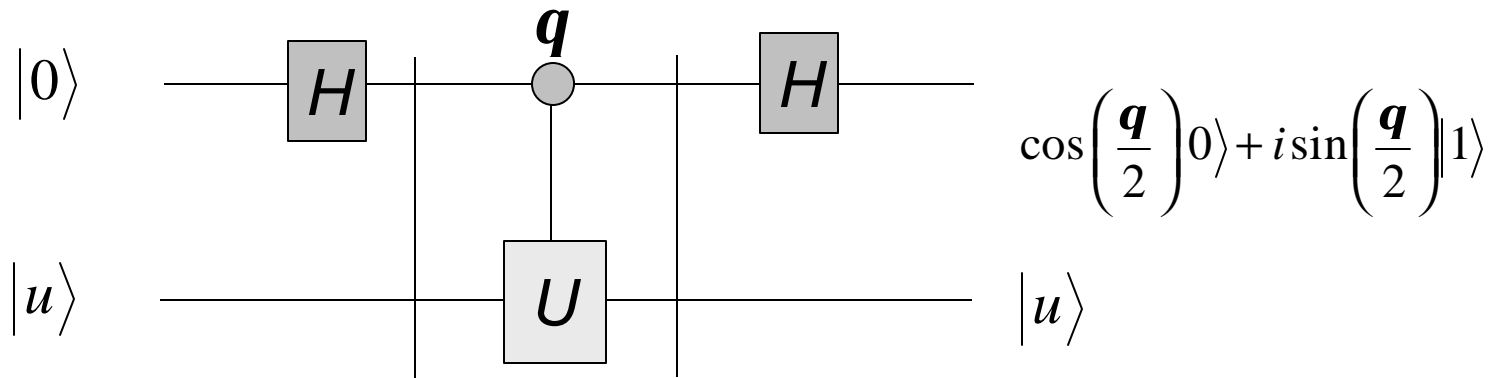
- ...by earlier arguments we need many particles for efficient data storage...
- ...how is interferometry related to conventional computational tasks such as computing functions...

# Quantum interferometry revisited



$$U |u\rangle = e^{iq} |u\rangle$$

# Phases in a new way



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle = \frac{1}{\sqrt{2}}|0\rangle|u\rangle + \frac{1}{\sqrt{2}}|1\rangle|u\rangle$$

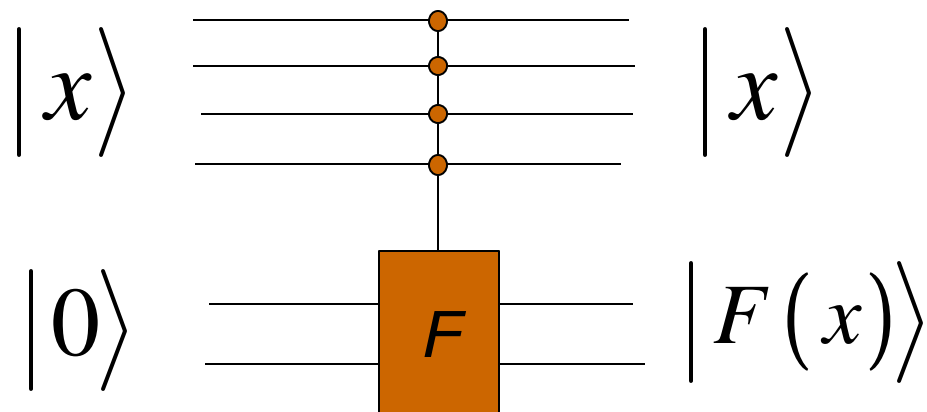
$$\frac{1}{\sqrt{2}}|0\rangle|u\rangle + \frac{1}{\sqrt{2}}|1\rangle U|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{iq}|1\rangle)|u\rangle$$

# Quantum function evaluation

---

---

$$\{0,1\}^n \xrightarrow{f} \{0,1\}^m$$



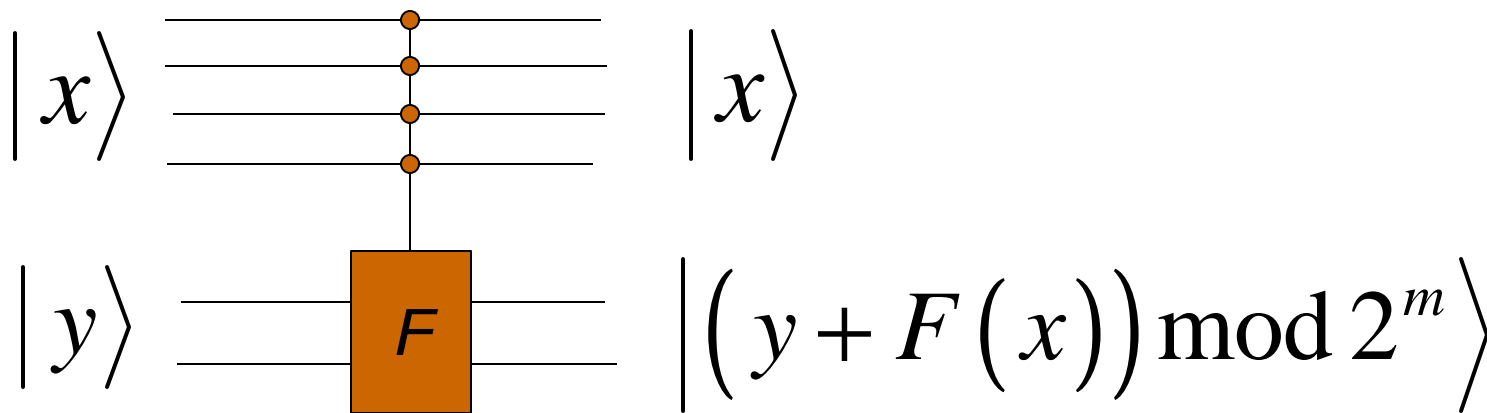
$$|x\rangle|0\rangle \rightarrow |x\rangle|F(x)\rangle$$

# Quantum function evaluation

---

---

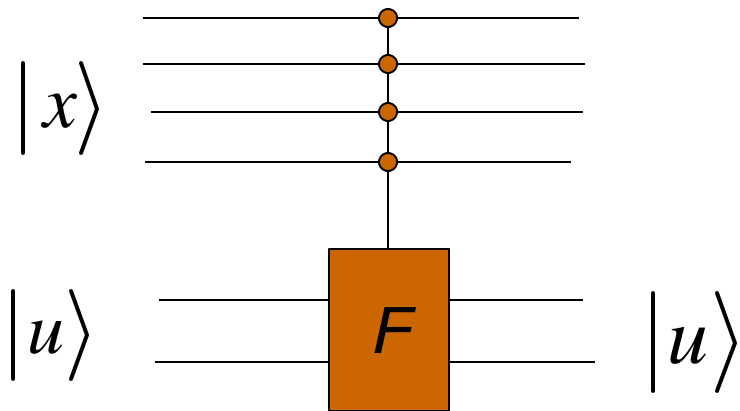
$$\{0,1\}^n \xrightarrow{f} \{0,1\}^m$$



$$|x\rangle|y\rangle \rightarrow |x\rangle|(y + F(x)) \bmod 2^m\rangle$$

# Quantum function evaluation

$$\{0,1\}^n \xrightarrow{f} \{0,1\}^m$$



$$|u\rangle = \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} \exp\left(\frac{2\pi i}{2^m} y\right) |y\rangle$$

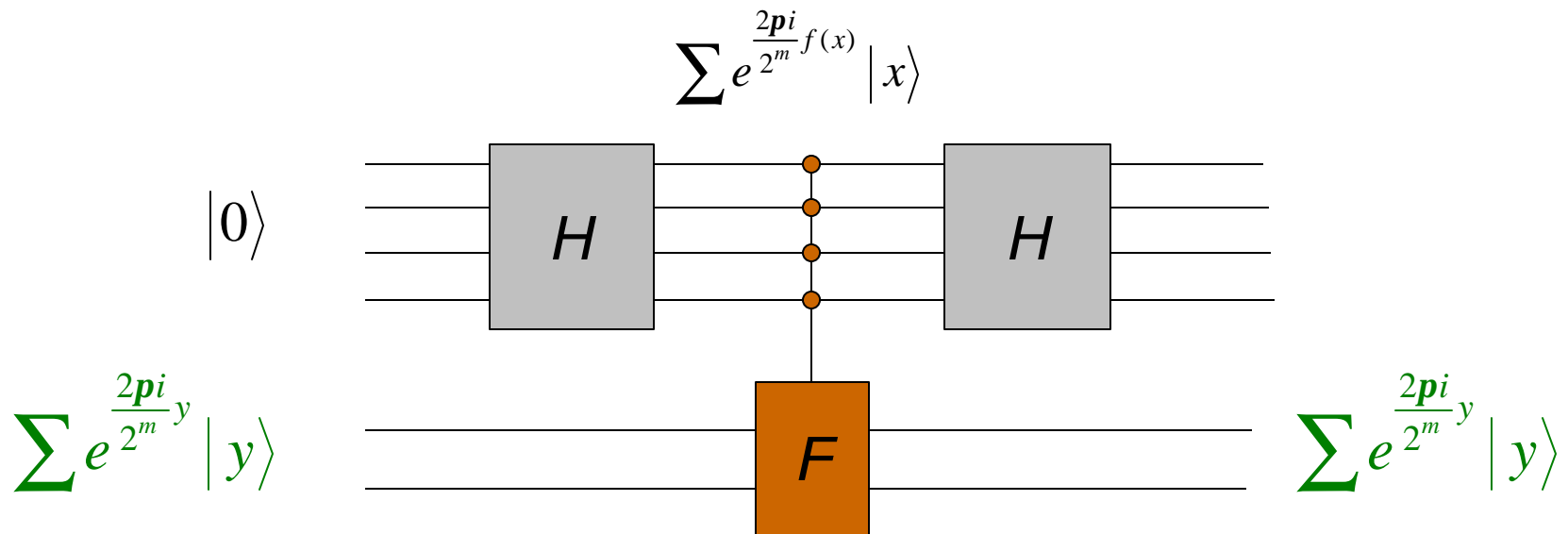
$$|x\rangle|u\rangle \rightarrow \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} \exp\left(\frac{2\pi i}{2^m} y\right) |x\rangle|y + F(x)\rangle$$

$$|x\rangle|u\rangle \rightarrow \exp\left(\frac{2\pi i}{2^m} F(x)\right) |x\rangle|u\rangle$$

$$|x\rangle|y\rangle \rightarrow |x\rangle|(y + F(x)) \bmod 2^m\rangle$$

$$|x\rangle \rightarrow \exp\left(\frac{2\pi i}{2^m} F(x)\right) |x\rangle$$

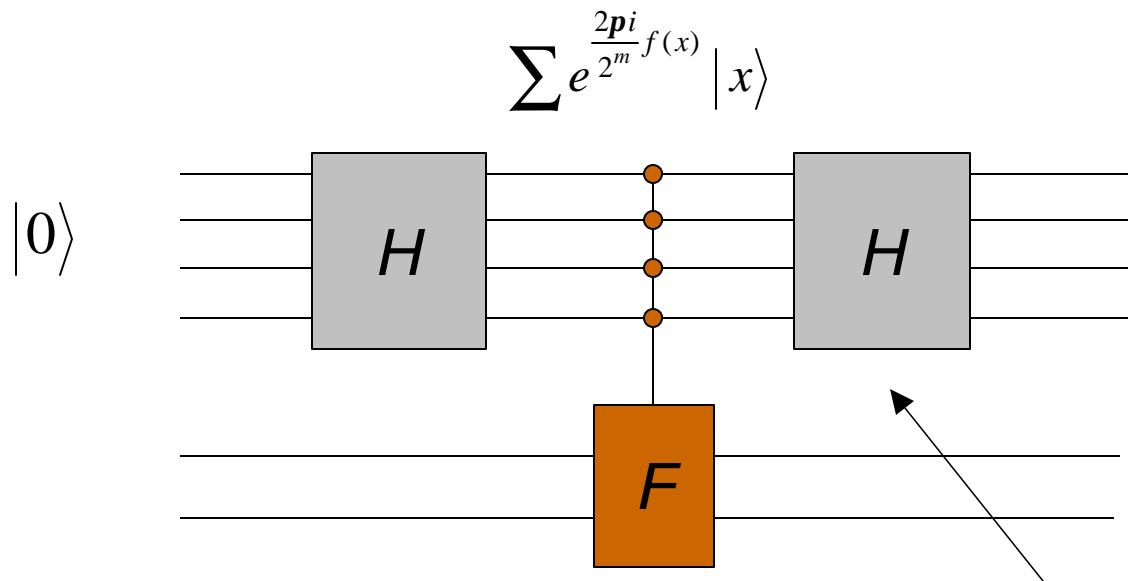
# Quantum Algorithms



$$\{0,1\}^n \xrightarrow{f} \{0,1\}^m$$

(for details see Cleve et al Proc. Roy. Soc. Lond. A, 400 pp. 97-117 (98))

# Quantum Algorithms

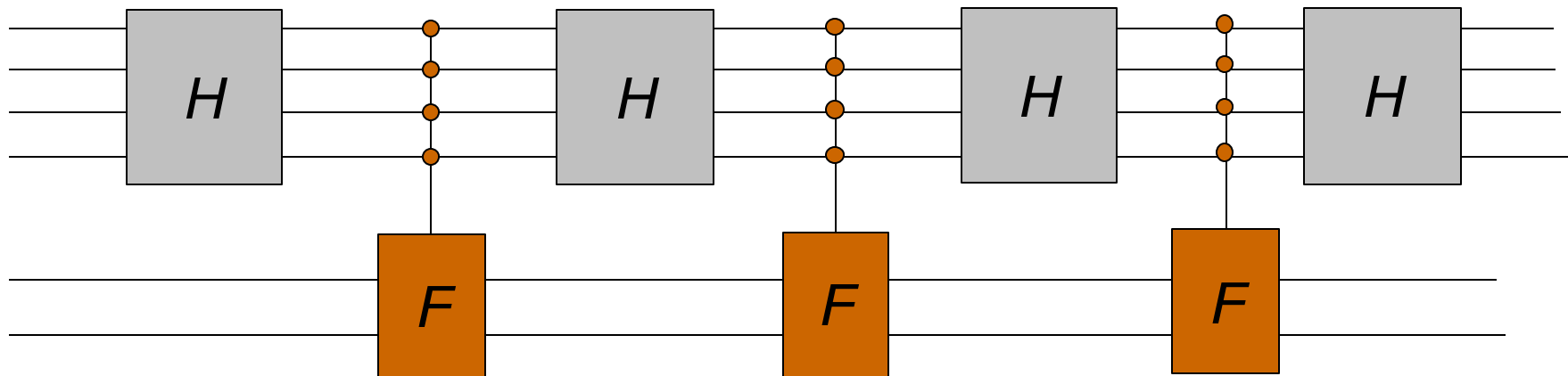


Quantum Fourier Transform

$$x, z = 0, 1, 2 \dots N - 1$$

$$|x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} e^{\frac{2\pi i xz}{N}} |z\rangle$$

# Quantum Algorithms

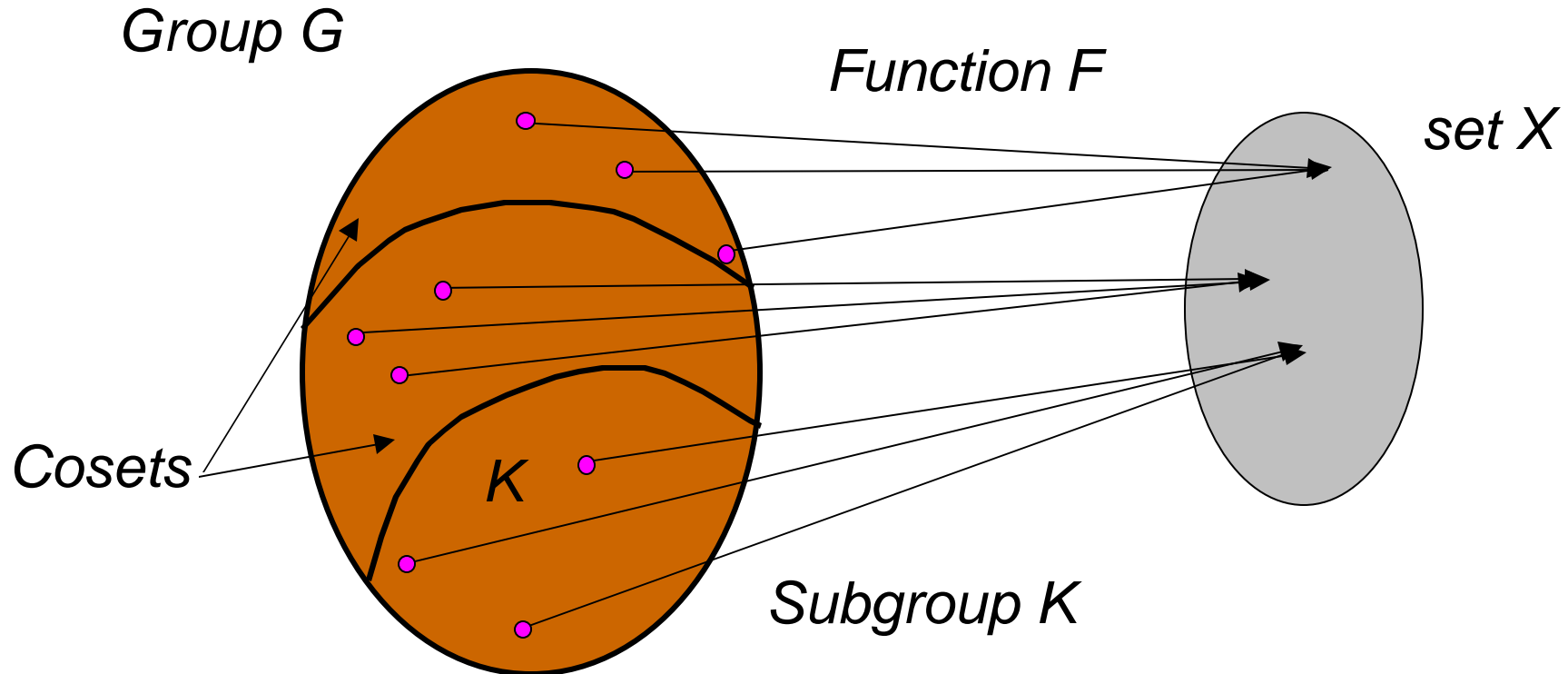


Repeated interference pattern – e.g. for Grover's algorithm

(for details see Cleve et al Proc. Roy. Soc. Lond. A, 400 pp. 97-117 (98))

# Abelian Hidden Subgroups

*Unification – mathematical perspective*



(Brassard and Hoyer / Mosca and Ekert)

# Partial Unification

---

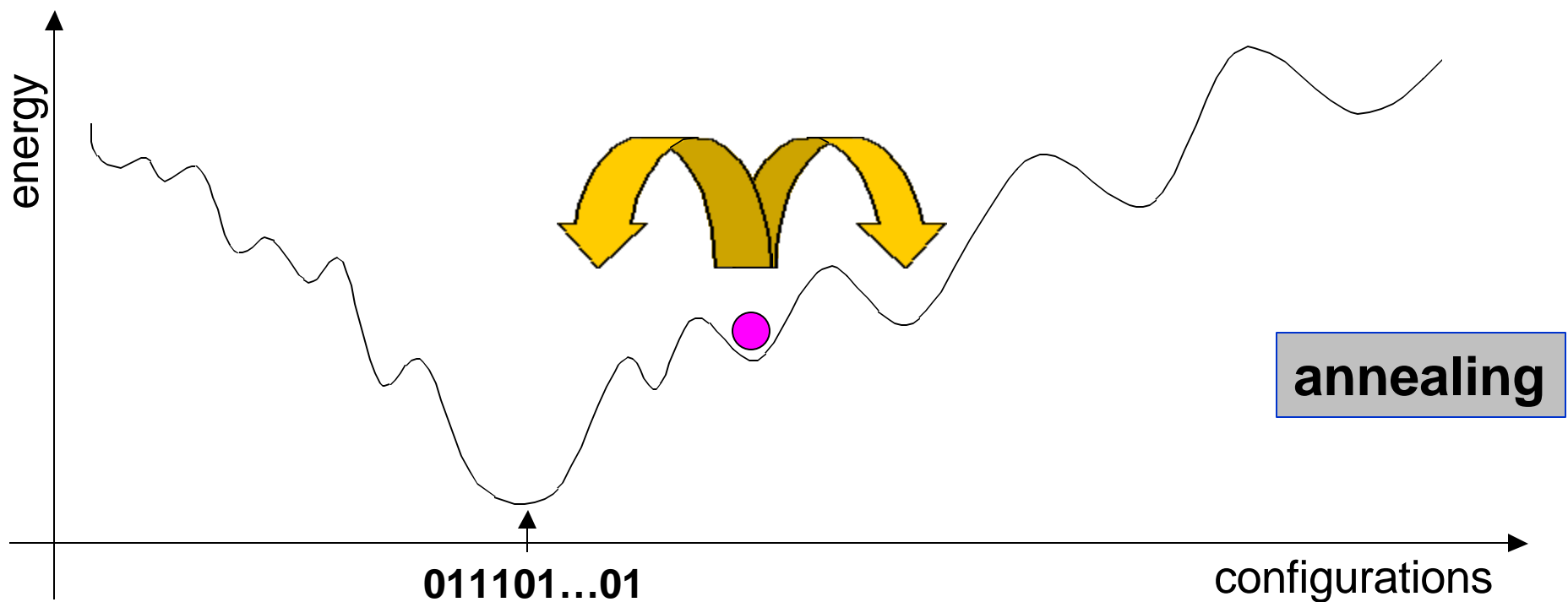
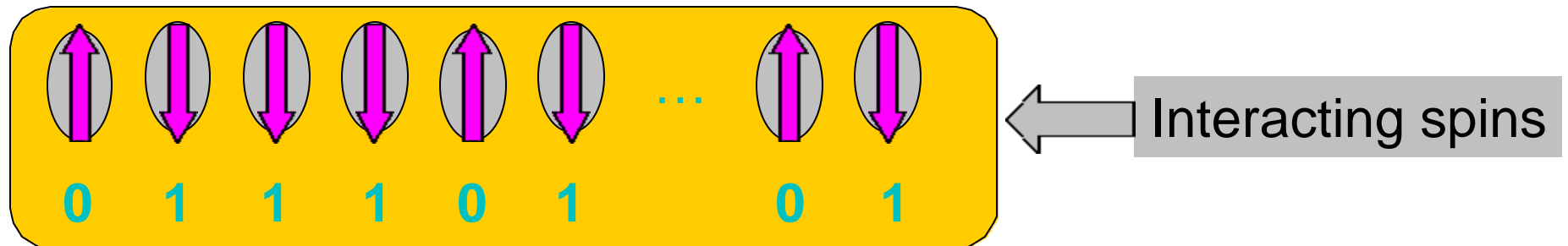
- Hidden subgroup problems
  - » Include all early quantum algorithms (Deutsch, Simon...)...
  - » ...factoring, discrete logarithm, Abelian stabiliser,...
  - » For algorithms that do not belong to this category see, for example, work by John Watrous on solvable groups
- Interferometric structure is common for all sequential quantum algorithms – including quantum search, counting, etc

# Wacky ideas for the future

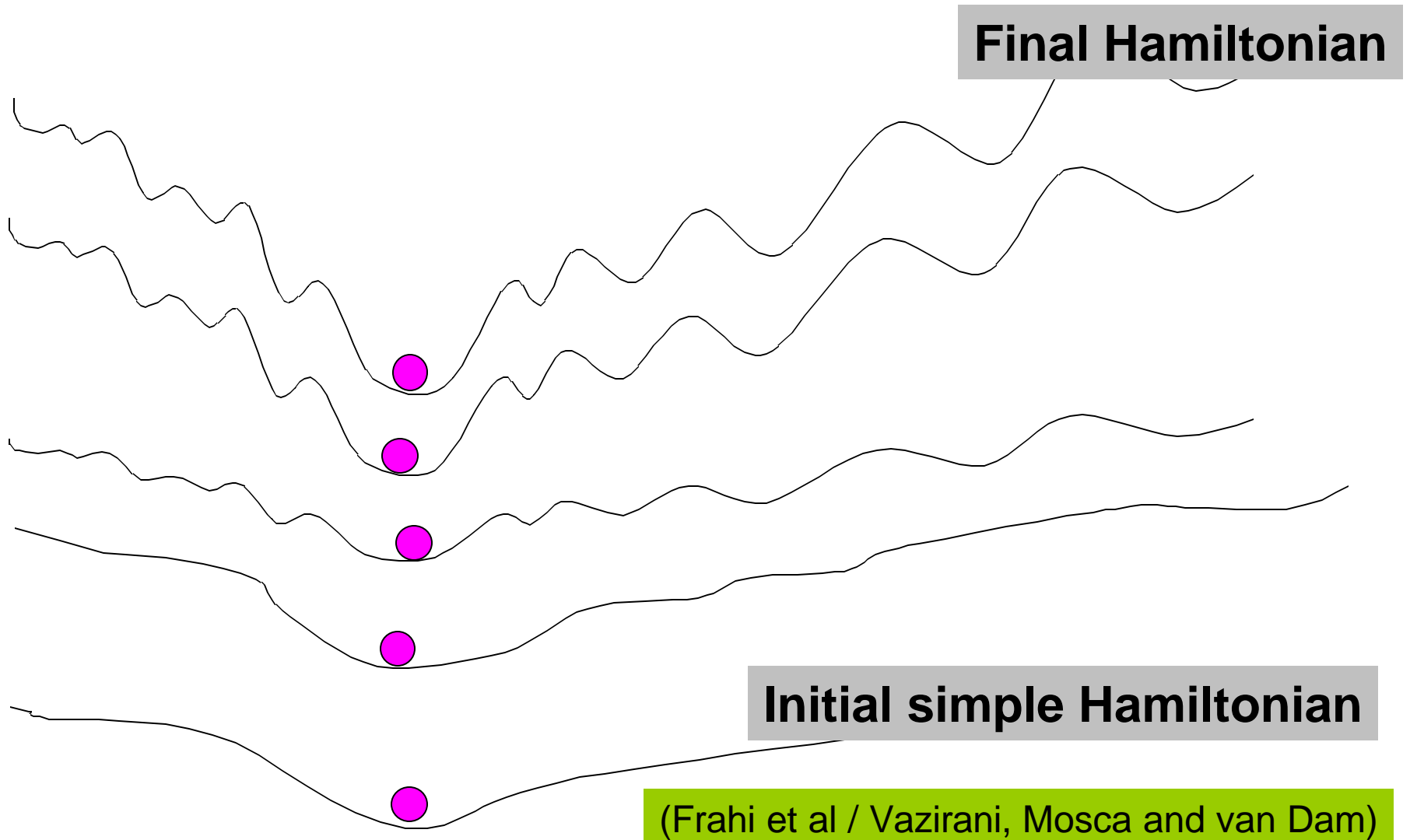
---

- Particle statistics in interferometers, additional selection rules ?
- Beyond sequential models – quantum annealing?
- Holonomic, geometric, and topological quantum computation?
- Discover (rather than invent) quantum computation in Nature?

# Beyond sequential models



# Adiabatic Annealing

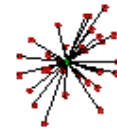


# Classical annealing in action

---

Quantum state estimation

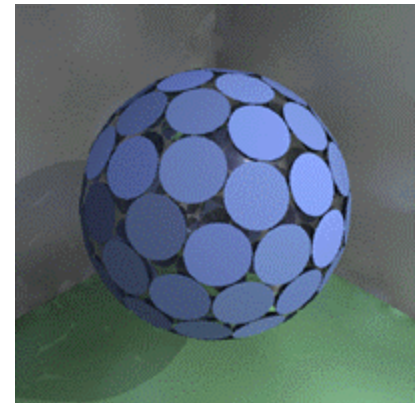
$$|\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle \dots \otimes |\Psi\rangle$$



Optimal POVM (in symmetric subspace)

$$\sum P_r = 1 \quad P_r = \left( |\mathbf{j}_r\rangle \langle \mathbf{j}_r| \right)^{\otimes N}$$

Where the Bloch vectors of  $|\mathbf{j}_r\rangle$   
are uniformly distributed on the sphere



# Stabilising quantum computation

- Projections on symmetric subspaces (Deutsch 93)

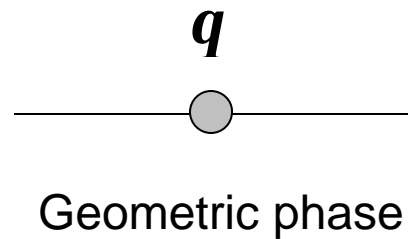
$$\begin{aligned} & |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle \otimes \dots \otimes |\Psi\rangle \\ & |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi'\rangle \otimes \dots \otimes |\Psi\rangle \end{aligned}$$

- Decoherence free subspaces (Palma et al 95)
- Quantum error correcting codes (Shor 95,...)
- ...

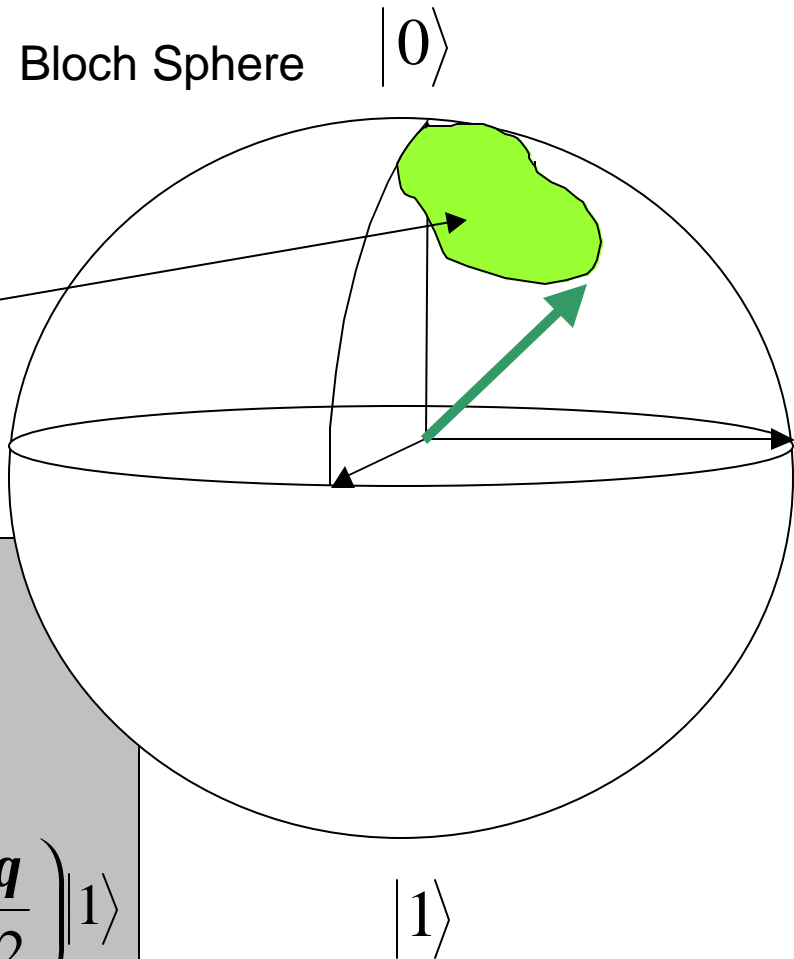
- Geometric/holonomic computation

- » J.A. Jones, A.K. Ekert, G. Castagnoli, V. Vedral Nature 407, 869 (1999)
- » P.Zanardi et al Phys. Lett. A264, 94 (1999)
- » ...

# Basic idea – geometric phase



$$\mathbf{g} = \frac{1}{2} \text{AREA}$$



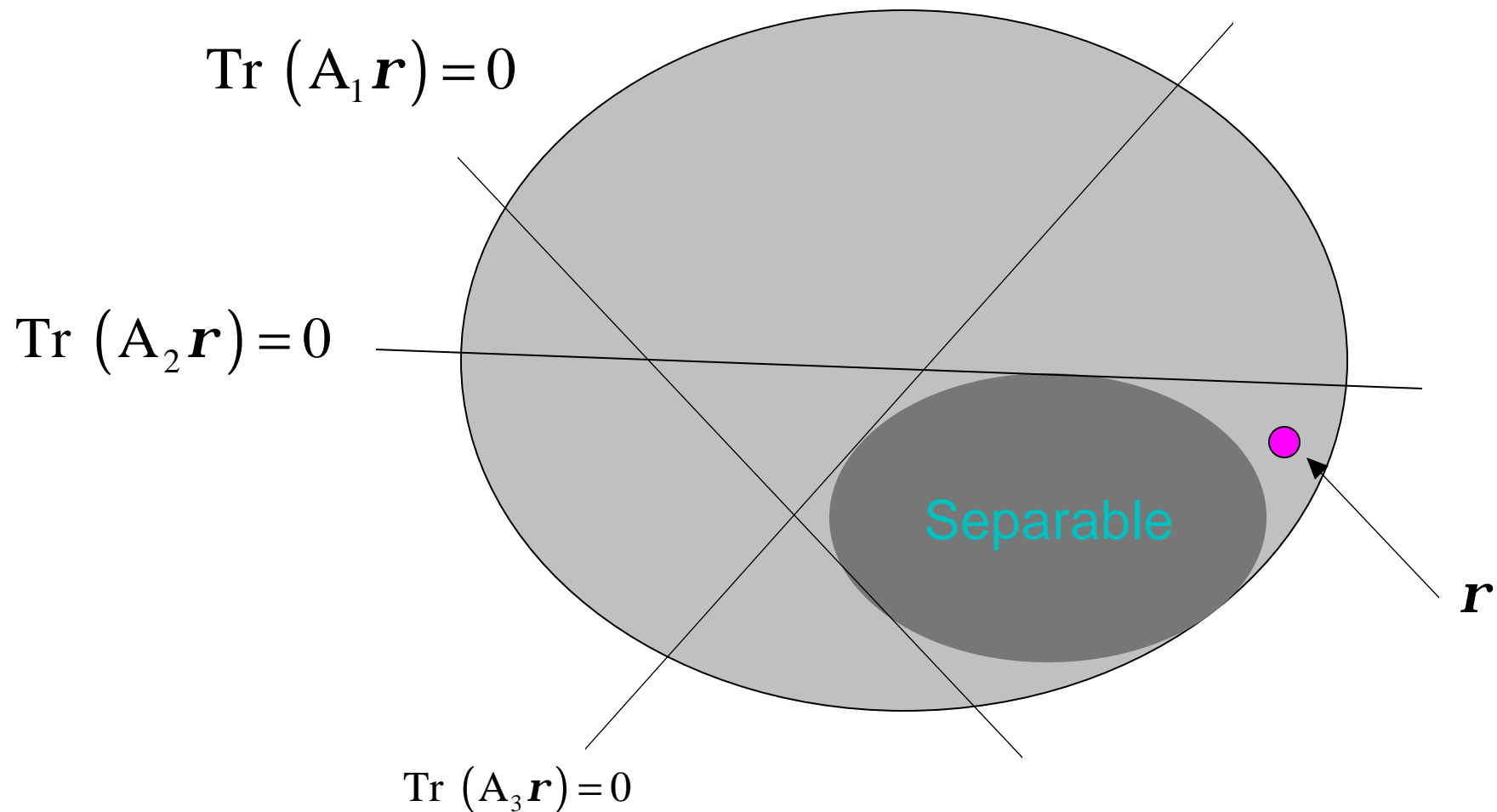
Calculated from:

$$\mathbf{g}(t) = i \int_0^t \langle n(\mathbf{l}) | \frac{\partial}{\partial \mathbf{l}} | n(\mathbf{l}) \rangle \frac{d\mathbf{l}}{dt} dt$$

$$|n(\mathbf{l})\rangle \equiv |n(\mathbf{q}, \mathbf{j})\rangle = \cos\left(\frac{\mathbf{q}}{2}\right) |0\rangle + e^{i\mathbf{j}} \sin\left(\frac{\mathbf{q}}{2}\right) |1\rangle$$

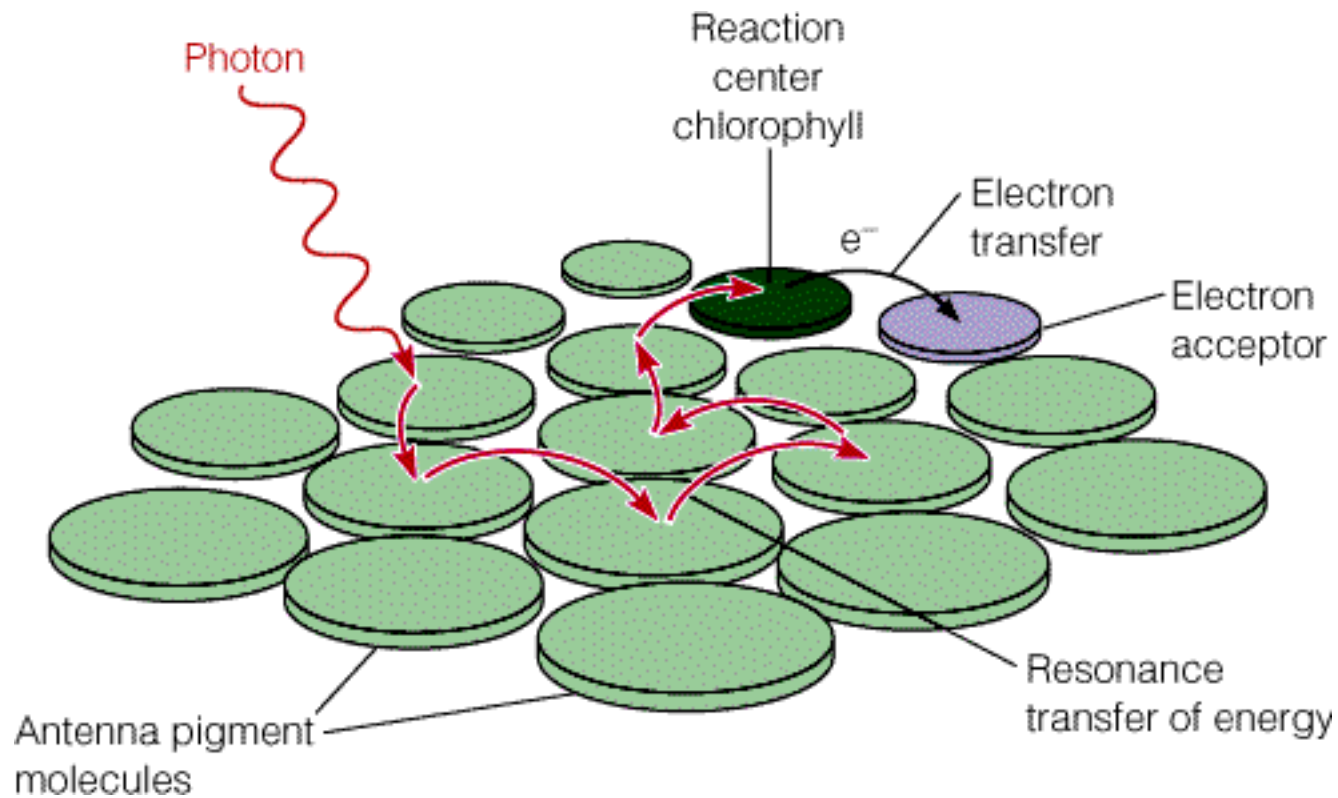
# Inherently quantum algorithms

Decision problem - Entangled or not?



# Coherent quantum phenomena in nature ?

---



# Further Reading

---

---

<http://www.qubit.org>



Oxford Centre for Quantum Computation  
is sponsored by

