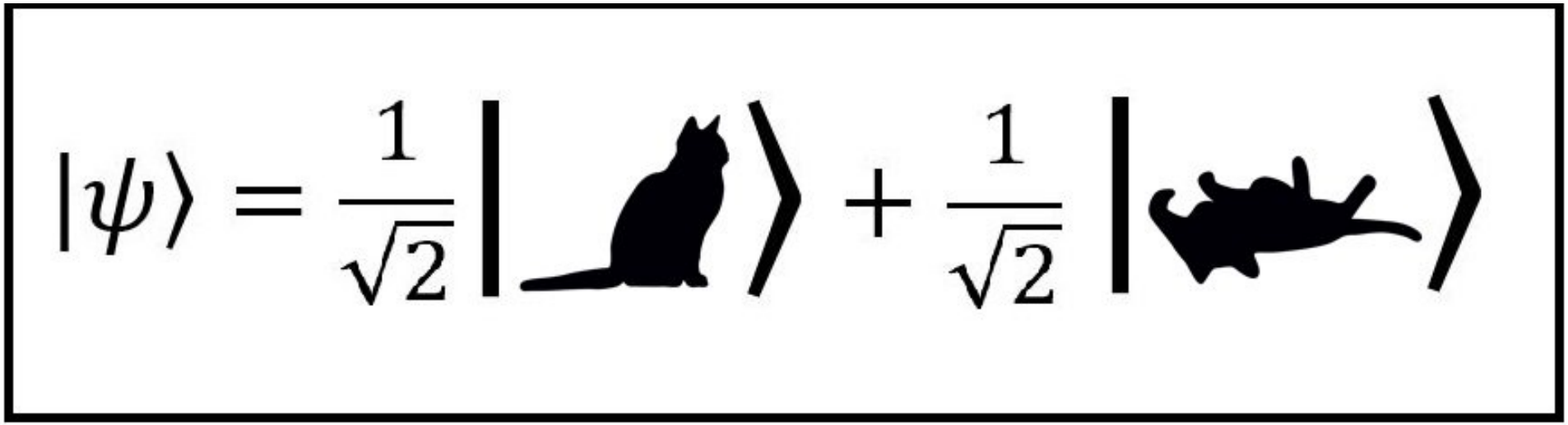
QC for QCs

Jon Crowcroft

http://www.cl.cam.ac.uk/~jac22



Lay intro to Quantum Computing

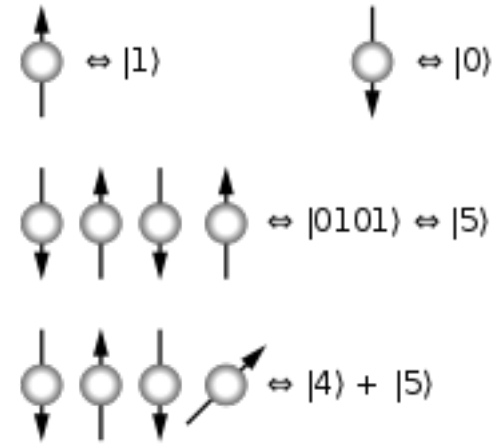
- A piece of my mind?
  - Penrose theory☺
- Can I do it justice?
  - Intended audience e.g. lawyers

Quantum Mechanics

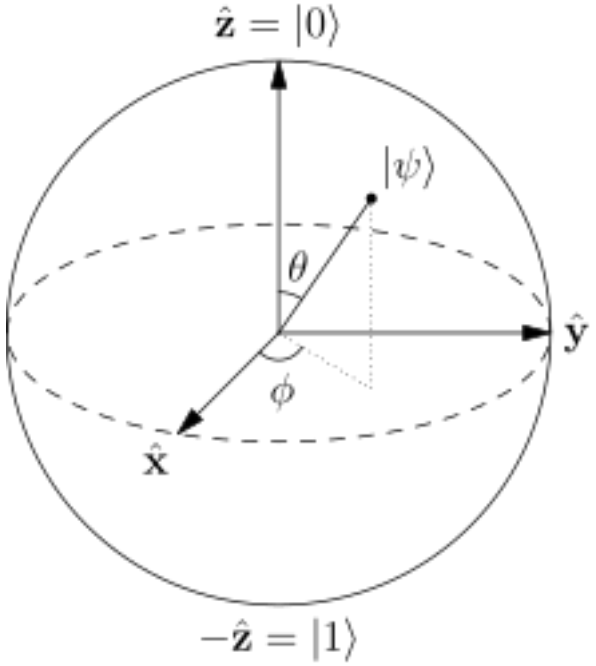
- Ultraviolet Catastrophe
  - Planck/Black body radiation & infinite energy..
- Continuous (waves&particles)
  - Young's slits experiment
    - Wave "self interferes"
    - But if we see which slit particle goes through
      - Doesn't any more!
  - Copenhagen probabilty/Feynmn path integral
- Uncertainty
  - Heisenberg – observer effect
- Spooky (action at distance/entanglement)
  - Einstein

Superposition

- More than just set of states
  - Superset of states
  - Phase & normalisation



qubits can be in a superposition of all the clasically allowed states



A metaphor

QKD

- Is a thing but isn’t QC
  - Just uses one quantum property
  - Tamper evidence
  - Also used in quantum blockchain, for example
- Also one of the things that will save us from QC / Shor

QC resources

- Qubits v. classical bits
  - Entangled story
- QC programs/circuits v. ALUs
  - Iteration is sequence of superposed states
  - Unitary gates operate on whole state
  - Circuits quite problem specific
- Output is the challenge
  - Measurement projects vector/superposed state
  - onto orthonormal basis
  - Final value probably ok

Contrast with classical

- Memory&processor same binary gates
  - Eckart/von Neumann stored program computer
- CPU/ALU: Circuits for common instructions
  - Arithmentic, logic, sequence/control
  - Sequential instruction fetch&execute (mostly)
  - With recursion/iteration
  - Very general (turing machines☺)

Stored Program v. Switched Program

- QC is more like one of the earliest computers
  - Bletchley's Colussus – Switched Program
  - Instead of code&data in store,
  - data input to a sequence of switch configurations
- QC "program" =circuit made of gate types
- QC "data" =sequence of Qubit distributions

QC "programming"

- Is more like CPU design
- programs are like probablistic programming
- See (e.g.) anglican

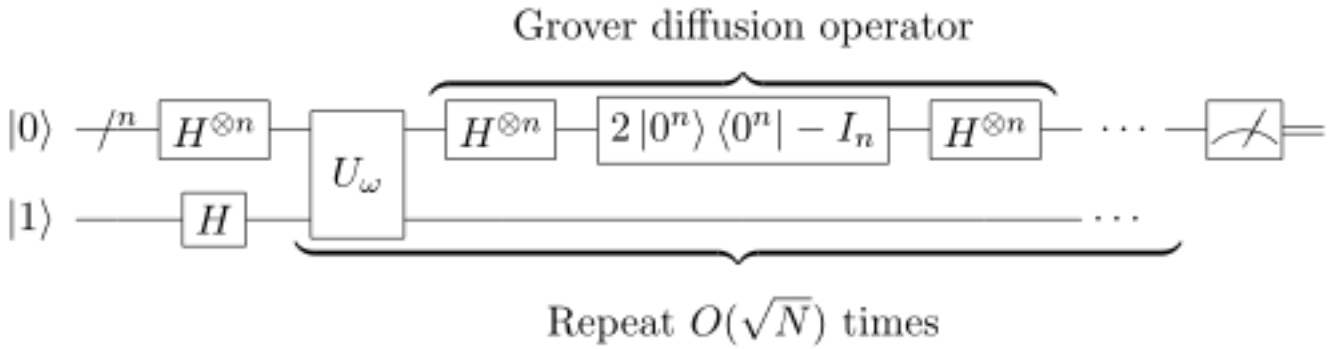
  http://www.robots.ox.ac.uk/~fwood/anglican/language/
- Runtime reminiscent of MCMC

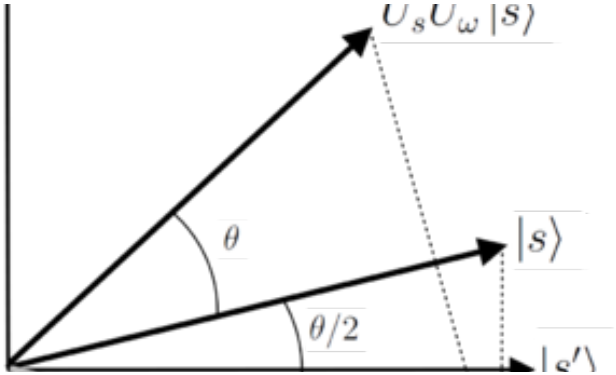
  https://en.wikipedia.org/wiki/Markov_chain_Monte_Carlo
  - Quantum "path integral" equivalent to the multi-dimensional integral
  - Quantum circuit equivalent to sampling mechanism in mcmc

Some “algorithms” then

- Grover
  - database search
- Shor
  - Faster factoriser
- Deutsch–Jozsa
  - Exact oracle
- QC emulation
  - mcmc

Grover

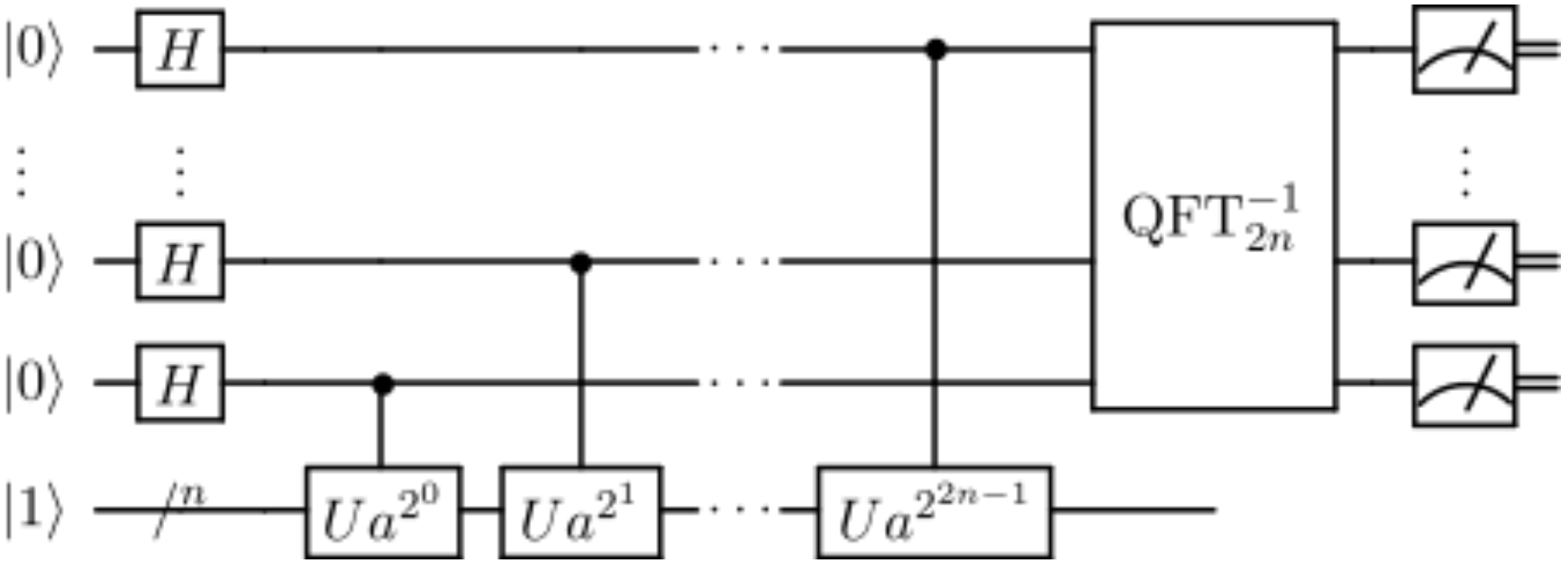

Grover diffusion operator
$|0\rangle$
$|1\rangle$
$/^n$
$H^{\otimes n}$
H
U_ω
$H^{\otimes n}$
$2\,|0^n\rangle\langle 0^n| - I_n$
$H^{\otimes n}$
Repeat $O(\sqrt{N})$ times


$U_s U_\omega\,|s\rangle$
θ
$|s\rangle$
$\theta/2$
$|s'\rangle$

Contrast with classical

- Find a record with key=value in a list
- Iterate - complexity O(n)
- Think – find a book in a pile of books not in order

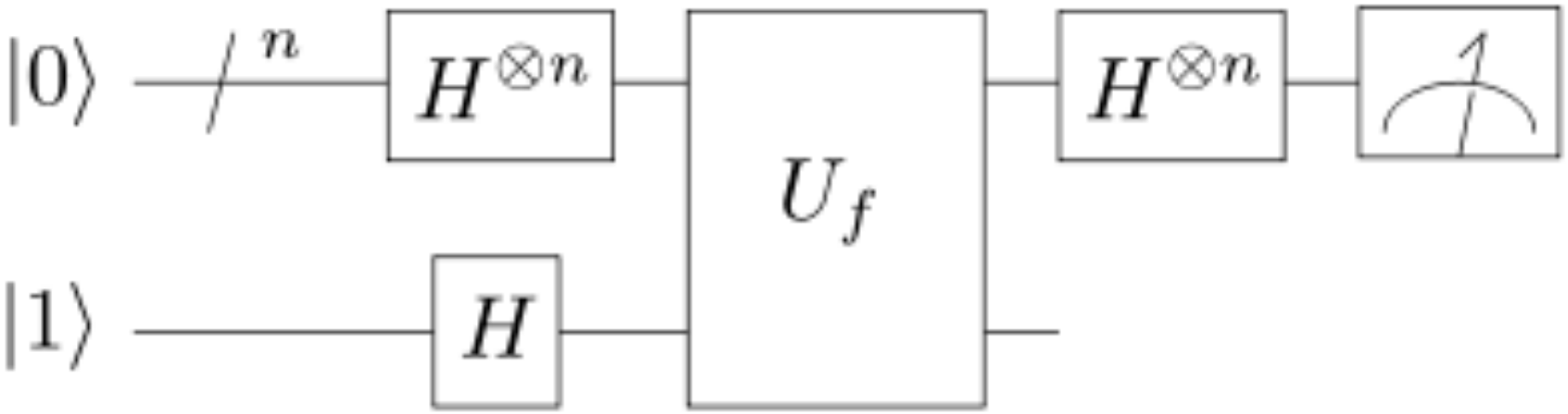
Shor


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|1\rangle$
H
H
H
$/n$
Ua^{2^0}
Ua^{2^1}
$Ua^{2^{2n-1}}$
QFT_{2n}^{-1}

Contrast with classical

- Find prime factors of a large number N
  - e.g. in range 1 to 2^256 (10^90)
  - Isn't known in polynomial time
  - i.e. as range of gets bigger, time gets longer,faster than n^k for any k at all…(as far as we know)
  - Don't try this at home
  - Sieve / search

Deutchse-Jozsa



Exact oracle

- Deterministic algorithm to compute:
  - If f(x) is constant or balanced for all x,
  - In one iteration
- Classically,
  - needs 2^n iterations of f(x) if x is n bits

D-Wave

- 100 q-bit, but only for quantum annealing
- Finds minimum of a function by qunatum fluctations – more like analog computing

Uncertainty

- Decoherence
- Affordability
- Algorithmically
- Intractability

What might this mean…

- If QC is realized…and affordable
  1. Is crypto dead? – Not really c.f. https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography
  2. Are impossible problems then tractable? Not really
  3. Are some problems more practical? Yes
- When might we expect a QC (QC World)?
  - Hard to say, as it isn't just an engineering pb. https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing

Consequence of QC

- If we replace PKI with QKD, may need to devise new mechanism for signatures
- Some direct QC implementation of probabilistic programing or bayes model inferencing may become much more efficient

QC&A

- Questions….?
- Peace of mind?

- Acknowledgements to
  - Anuj Dewar(Cambridge) for slideware
  - Wikipedia for graphical materials