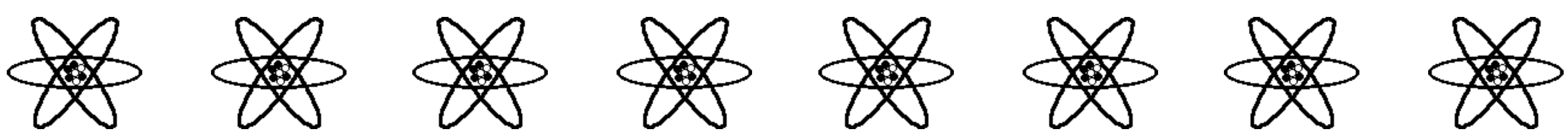
Strange Bits

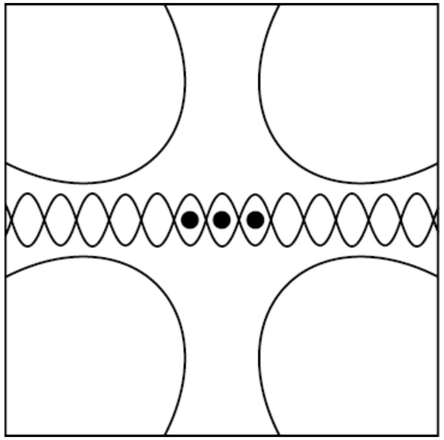
Quantum Computing and the Search for New Quantum Algorithms

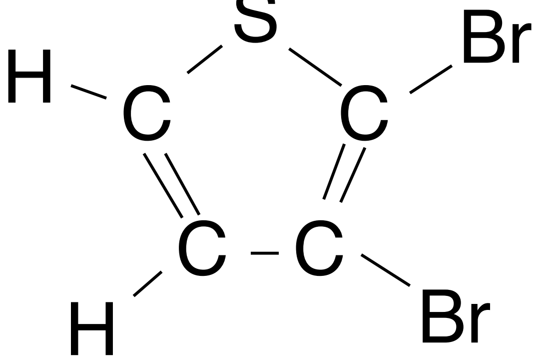
Lee Spector
Professor of Computer Science
School of Cognitive Science
Hampshire College
Amherst, MA
http://hampshire.edu/lspector

What is Quantum Computing?

- Computation with coherent atomic-scale dynamics.
- The behavior of a quantum computer is governed by the laws of quantum mechanics.

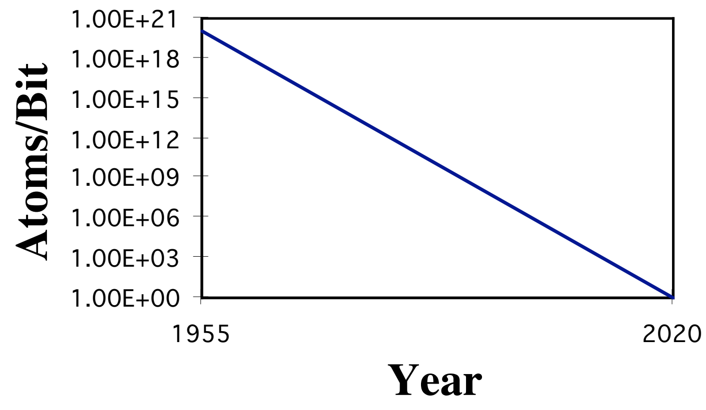






- Ion traps
- Nuclear spins in NMR devices
- Optical systems
- So far: few qubits, impractical
- A lot of current research

Why Bother?



- Moore's Law: the information storable on a given amount of silicon has roughly doubled every 18 months. We hit the quantum level 2010~2020.
- Quantum computation is more powerful than classical computation. More can be computed in less time; the complexity classes are different!

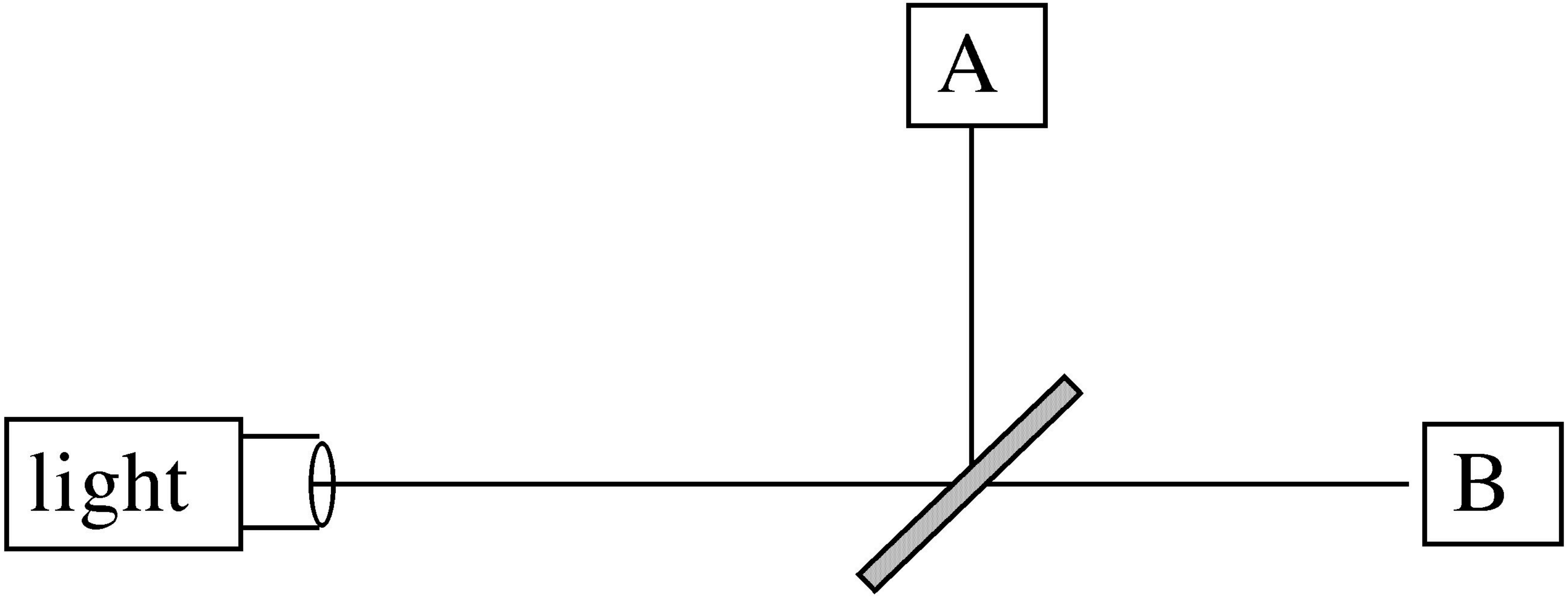
Source of the Power

- In quantum systems ***possibilities count***, even if they never happen!
- Each of exponentially many possibilities can be used to perform a part of a computation ***at the same time***.

Nobody Understands

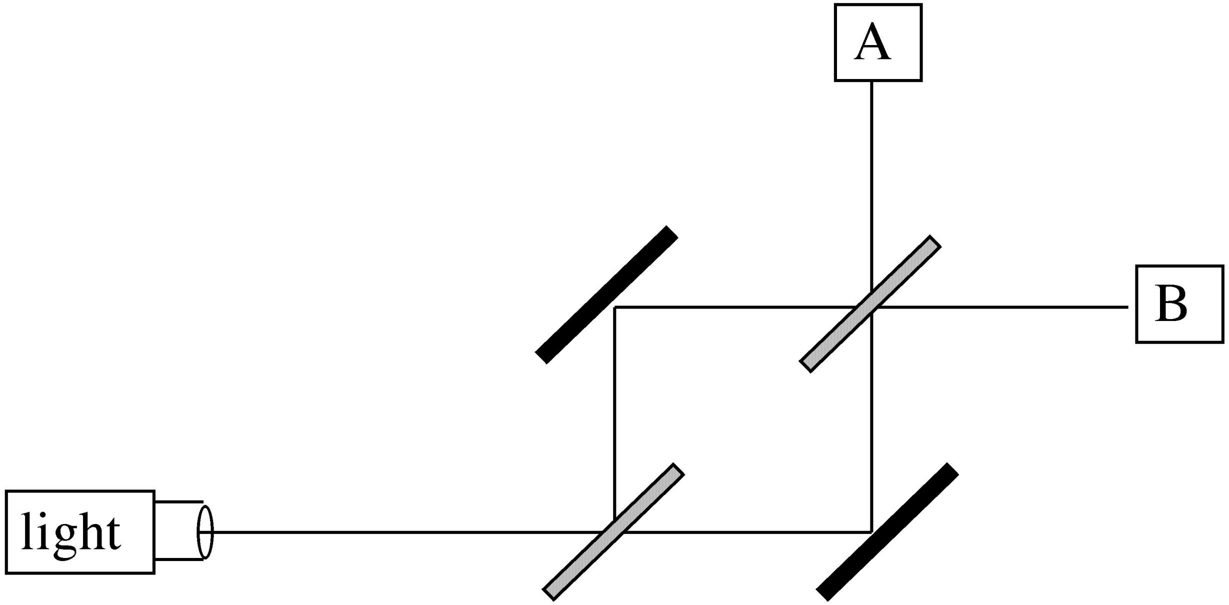
- "Anybody who is not shocked by quantum mechanics hasn't understood it." -Niels Bohr
- "No, you're not going to be able to understand it. ... You see, my physics students don't understand it either. That is because I don't understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with experiment. So I hope you can accept Nature as She is—absurd." -Richard Feynman

Beam Splitter



Half of the photons leaving the light source arrive at detector A; the other half arrive at detector B.

Interferometer



- Equal path lengths, rigid mirrors.
- Only one photon in the apparatus at a time.
- All of the photons leaving the light source arrive at detector B. WHY?

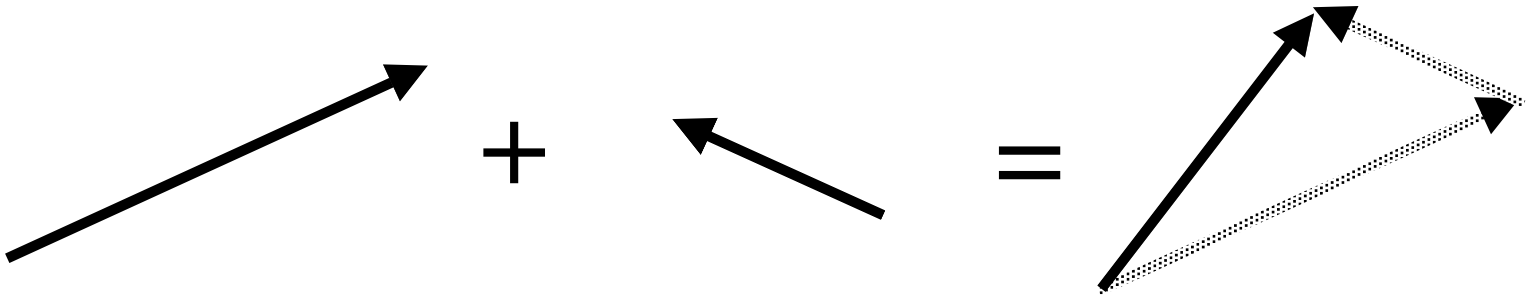
Possibilities Count

- There is an “amplitude” for each possible path that a photon can take.
- The amplitudes can interfere constructively and destructively, even though each photon takes only one path.
- The amplitudes at detector A interfere destructively; those at detector B interfere constructively.

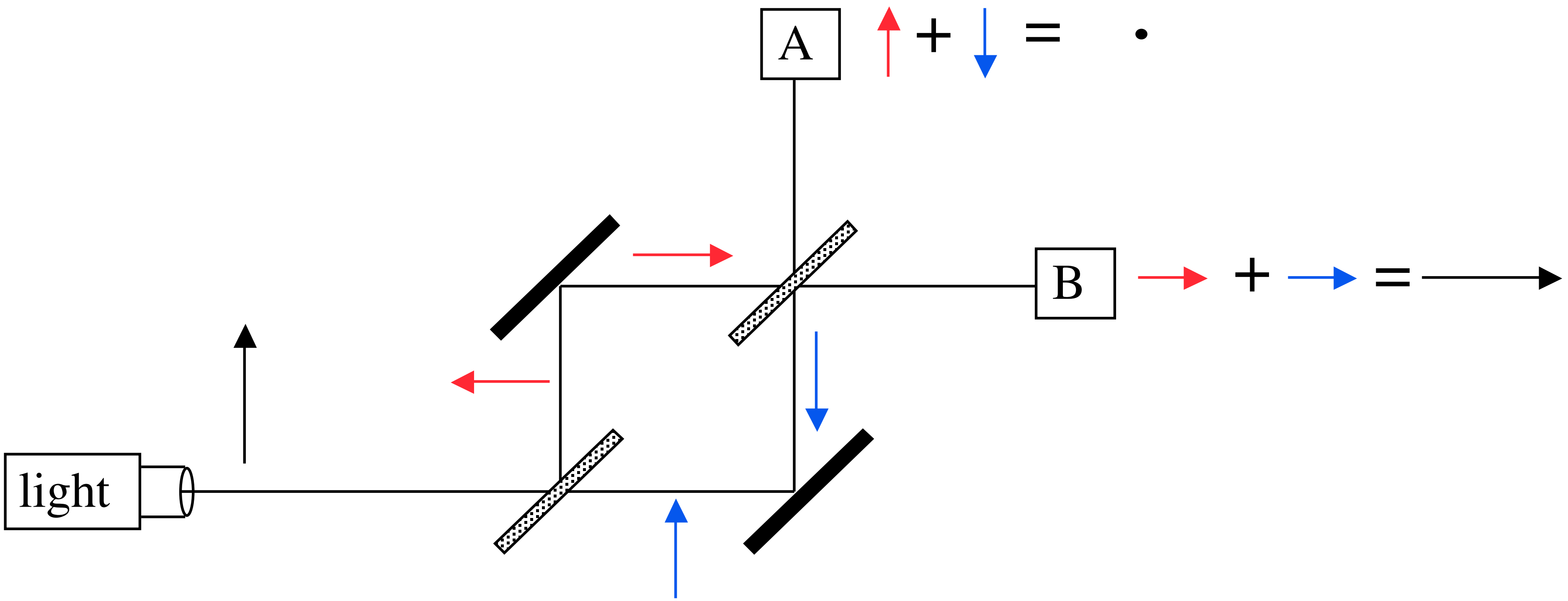
Calculating Interference

- "You will have to brace yourselves for this—not because it is difficult to understand, but because it is absolutely ridiculous: All we do is draw little arrows on a piece of paper—that's all!" —Richard Feynman
- Arrows for each possibility.
- Arrows rotate; speed depends on frequency.
- Arrows flip 180° at mirrors, rotate 90° counter-clockwise when reflected from beam splitters.
- Add arrows and square the length of the result to determine the probability for any possibility.

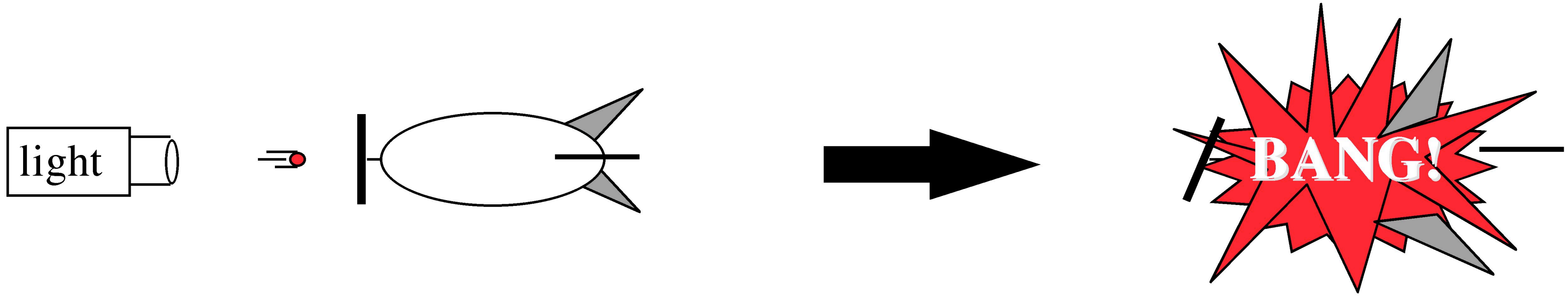
Adding Arrows



Interference in the Interferometer

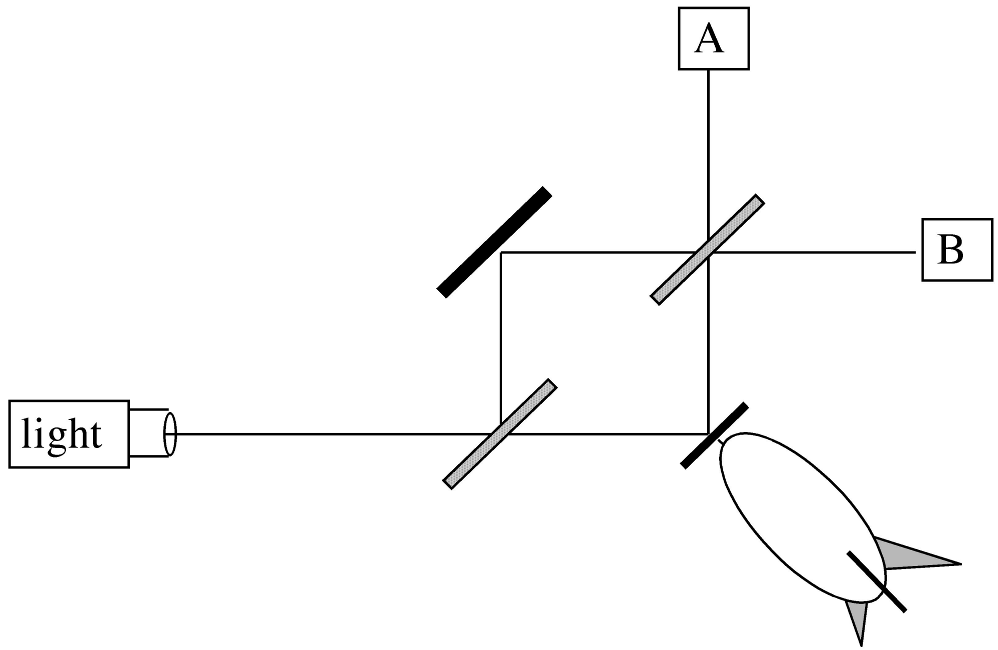


A Photon-Triggered Bomb



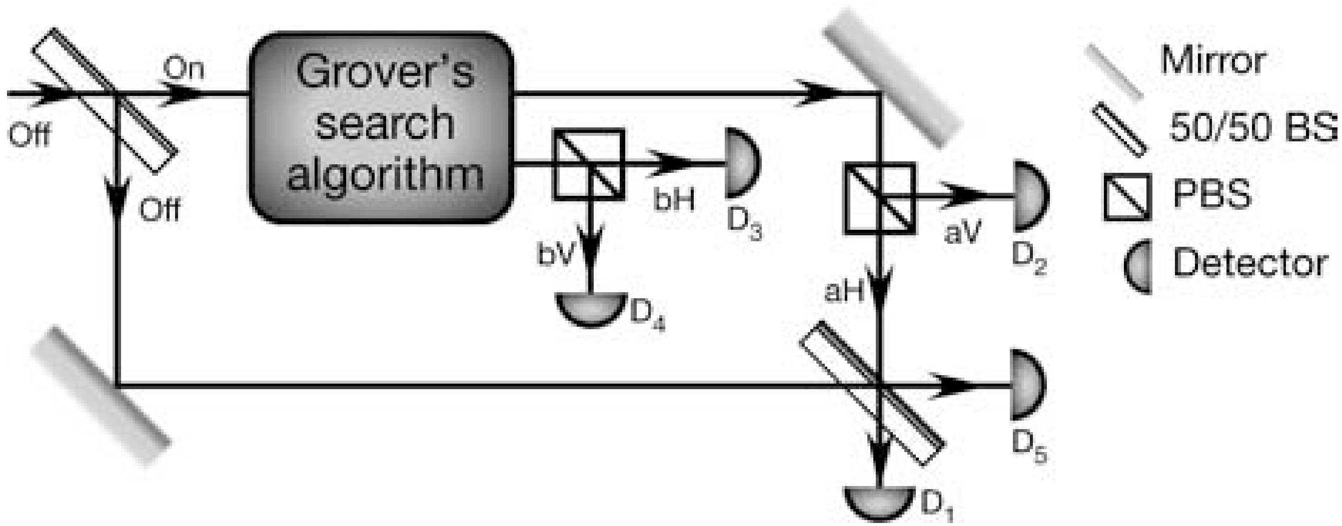
- A mirror is mounted on a plunger on the bomb.
- A single photon hitting the mirror depresses the plunger and explodes the bomb.
- Some plungers are stuck, producing duds.
- How can you find a good, unexploded bomb?

Elitzur-Vaidman Bomb Testing



- Possibilities count!
- Experimentally verified
- Can be enhanced to reduce or eliminate bomb loss [Kwiat, Weinfurter and Kasevich]

Counterfactual Computation



(Hosten et al., *Nature* **439**, 23 Feb 2006)

- Hosten et al.: optical counterfactual computation to conduct a search without running the search algorithm.
- They also used a "chained Zeno effect"—a sequence of interferometers—to boost the inference probability.

Two Speedups

- Grover's quantum database search algorithm finds an item in an unsorted list of n items in $O(\sqrt{n})$ steps; classical algorithms require $O(n)$.
- Shor's quantum algorithm finds the prime factors of an n-digit number in time $O(n^3)$; the best known classical factoring algorithms require at least time $O(2^{n^{1/3} \log(n)^{2/3}})$.

Factoring a 5,000 Digit Number

Classical computer (1ns/instr, ~today's best algorithm)

- over 5 trillion years (the universe is about 13 billion years old).

Quantum computer (1ns/instr, ~Shor's algorithm)

- just over 2 minutes

QC & the Human Brain

- Penrose's argument

  Brains do X (for X uncomputable)
  Classical computers can't do X
  ∴ Brains aren't classical computers

- First premise is false for all proposed X. For example, brains don't have knowably sound procedures for mathematical proof.

- Would imply brains more powerful than quantum computers; new physics.

Quantum Consciousness?

- Relation to consciousness etc. is much discussed, unclear at best. (Bohm, Penrose, Hameroff, others)
- “[Penrose’s] argument seemed to be that consciousness is a mystery and quantum gravity is another mystery so they must be related.” (Hawking)

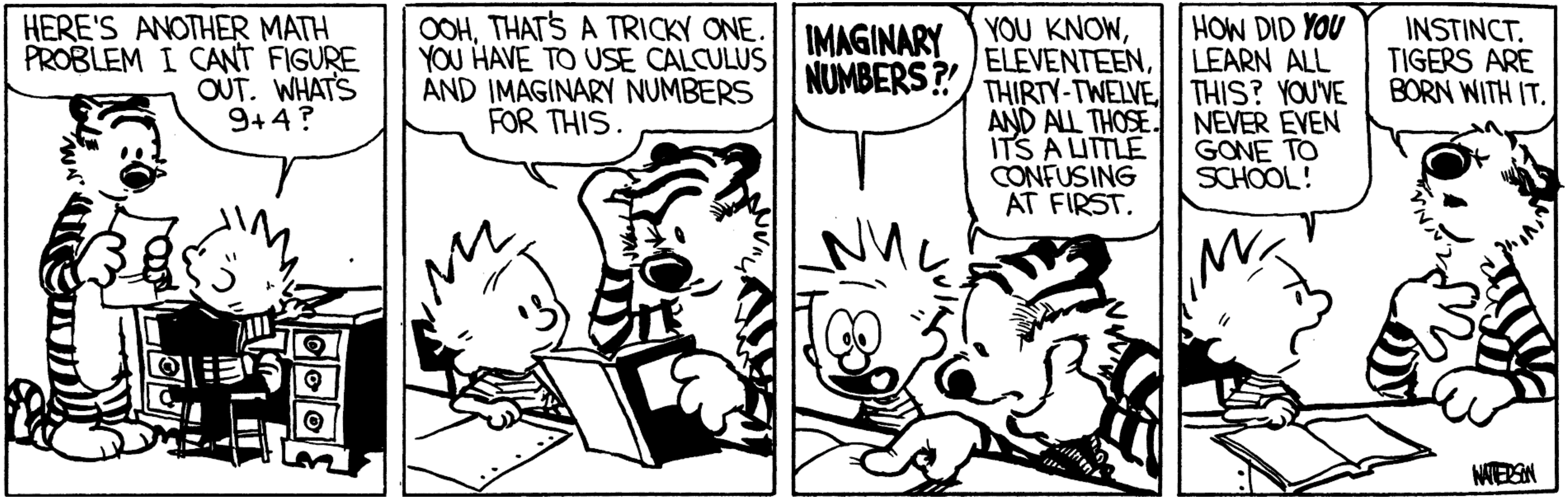
Qubits

- The smallest unit of information in a quantum computer is called a "qubit".
- A qubit may be in the "on" (1) state or in the "off" (0) state or in any superposition of the two!
- We can use 2 complex numbers to represent the state of a qubit on a classical computer.

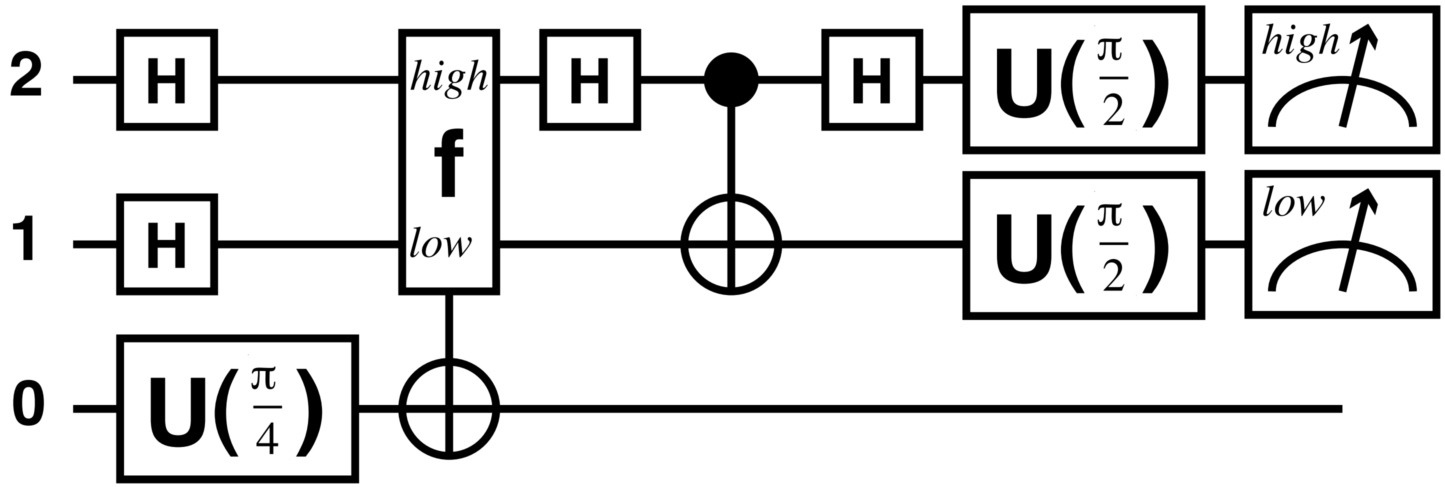
Entanglement

- Qubits in a multi-qubit system are not independent—they can become "entangled."
- To represent the state of *n* qubits one usually uses 2^n complex number amplitudes.

Why Complex?


HERE'S ANOTHER MATH PROBLEM I CAN'T FIGURE OUT. WHAT'S 9+4?
OOH, THAT'S A TRICKY ONE. YOU HAVE TO USE CALCULUS AND IMAGINARY NUMBERS FOR THIS.
IMAGINARY NUMBERS?!
YOU KNOW, ELEVENTEEN, THIRTY-TWELVE, AND ALL THOSE. IT'S A LITTLE CONFUSING AT FIRST.
HOW DID YOU LEARN ALL THIS? YOU'VE NEVER EVEN GONE TO SCHOOL!
INSTINCT. TIGERS ARE BORN WITH IT.
WATTERSON

Grover's Algorithm

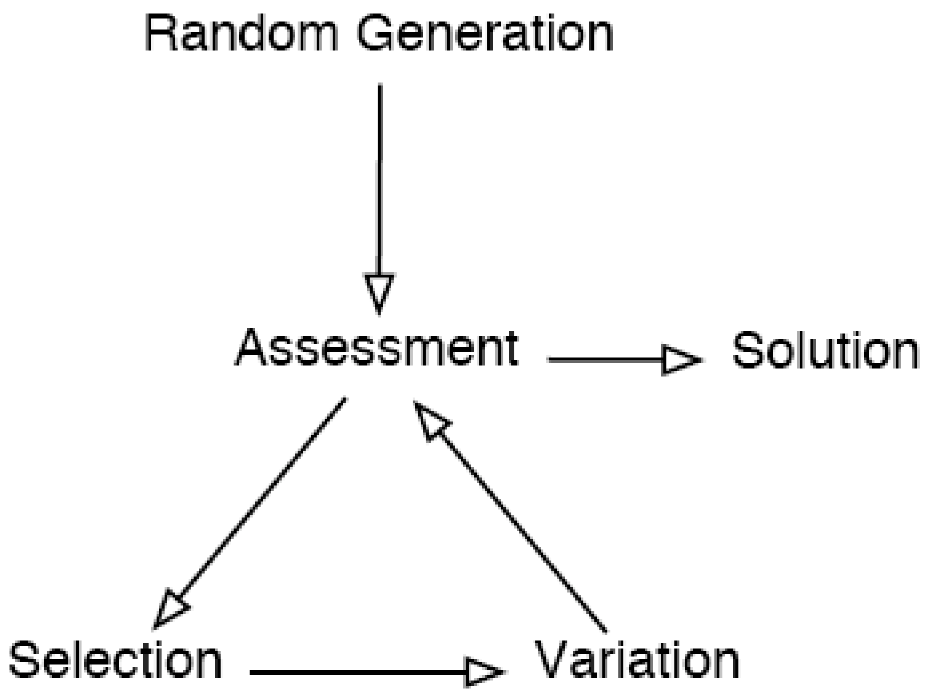


- Version for a 4-item database.
- Start in the state 000.

What Else?

- New quantum algorithms may support new applications and/or help to answer open theoretical questions.
- But discovery of new quantum algorithms is hard!
- Automated discovery of new and useful quantum algorithms.

Genetic Algorithms



Genetic Programming

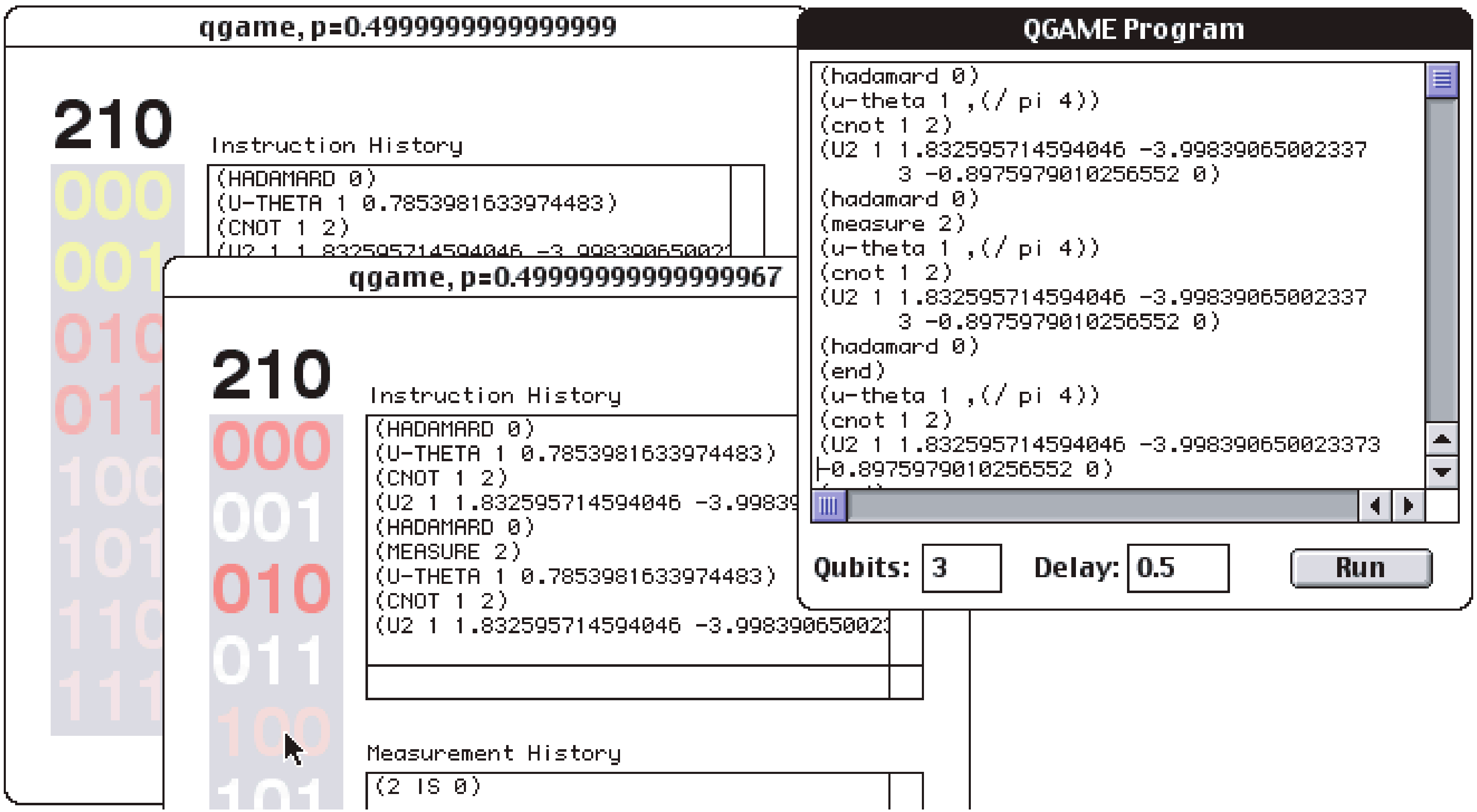
- Genetic algorithm in which the candidate solutions are executable computer programs.
- Candidate solutions are assessed, at least in part, by executing them.

Evolving Quantum Programs

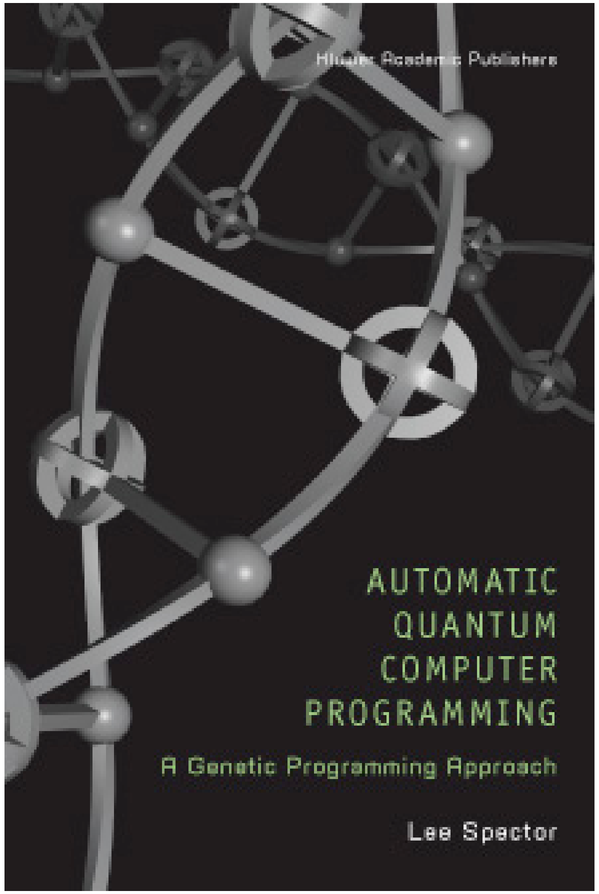
- Evolve:
  - gate arrays
  - programs that produce gate arrays
  - hybrid classical/quantum algorithms
  - input states or parameters
- Genome representation:
  - QGAME program
  - program (in any language) that generates a QGAME program
  - array of numbers

QGAME

Quantum Gate And Measurement Emulator
http://hampshire.edu/lspector/qgame.html



Human-Competitive Results in *Automatic Quantum Computer Programming: A Genetic Programming Approach*



2004. Springer (Kluwer Academic Publishers). ISBN 1-4020-7894-3.
http://hampshire.edu/lspector/aqcp/

“Human-Competitive” Criteria

(B) The result is equal to or better than a result that was accepted as a new scientific result at the time when it was published in a peer-reviewed scientific journal.

(D) The result is publishable in its own right as a new scientific result independent of the fact that the result was mechanically created.

These results were the basis for a Gold Medal in the *Human-Competitive Results* competition at the 2004 *Genetic and Evolutionary Computation Conference*.

1-bit Deutsch-Jozsa (XOR) problem

- Determine whether the behavior of a black-box quantum oracle satisfies the XOR property using only one call to the oracle.
- Result produced by genetic programming with PushGP.

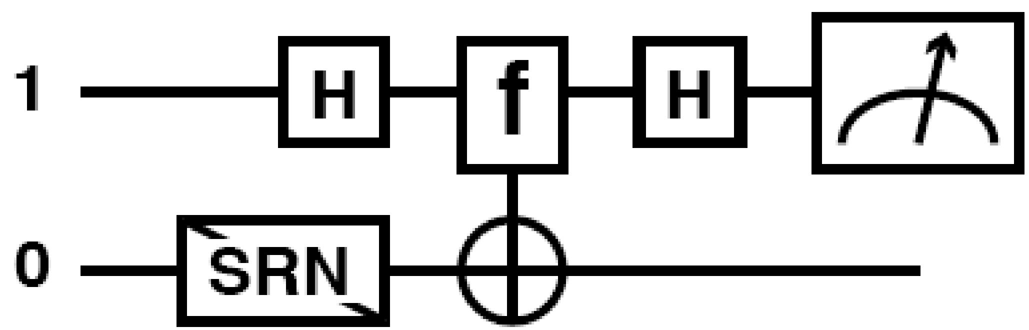


Figure 8.3. Gate array diagram for an evolved solution to the Deutsch-Jozsa (XOR) problem. The "f" gate is the oracle. The "SRN" gate with the diagonal line through it on qubit 0 transposed `Square Root of NOT` gate.

2-bit Grover Database search Problem

- Determine the location of a single marked item in a 4-element quantum database using only one call to the database access function.
- Result produced by genetic programming with PushGP.

(Diagram on next slide)

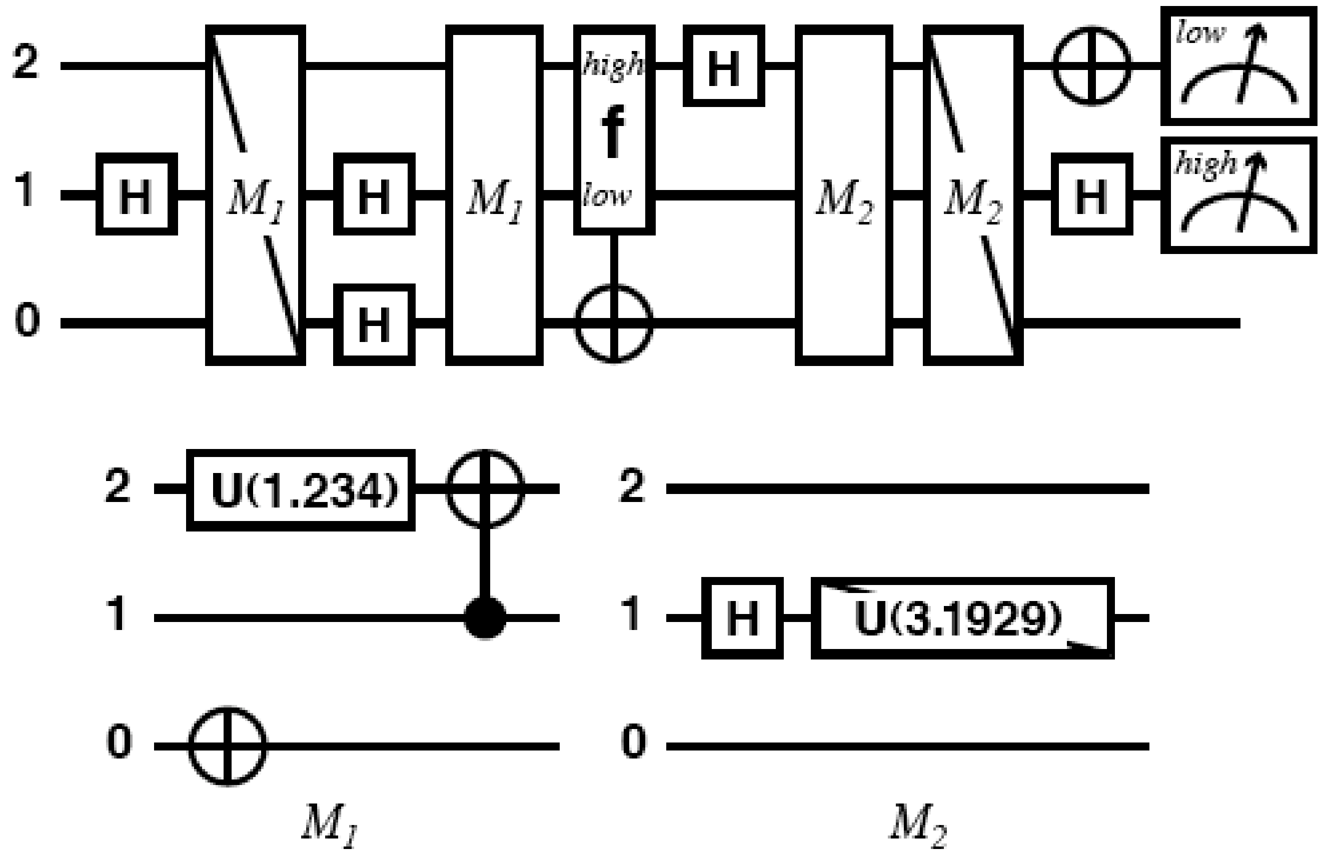


Figure 8.7. A gate array diagram for an evolved version of Grover's database search algorithm for a 4-item database. The full gate array is shown at the top, with M_1 and M_2 standing for the smaller gate arrays shown at the bottom. A diagonal line through a gate symbol indicates that the matrix for the gate is transposed. The "f" gate is the oracle.

1-bit OR Problem

- Determine whether the behavior of a black-box quantum oracle satisfies the OR property using only one call to the oracle, with a probability of error no worse than 0.1.
- Result produced by genetic programming with PushGP.

(Diagram on next slide)

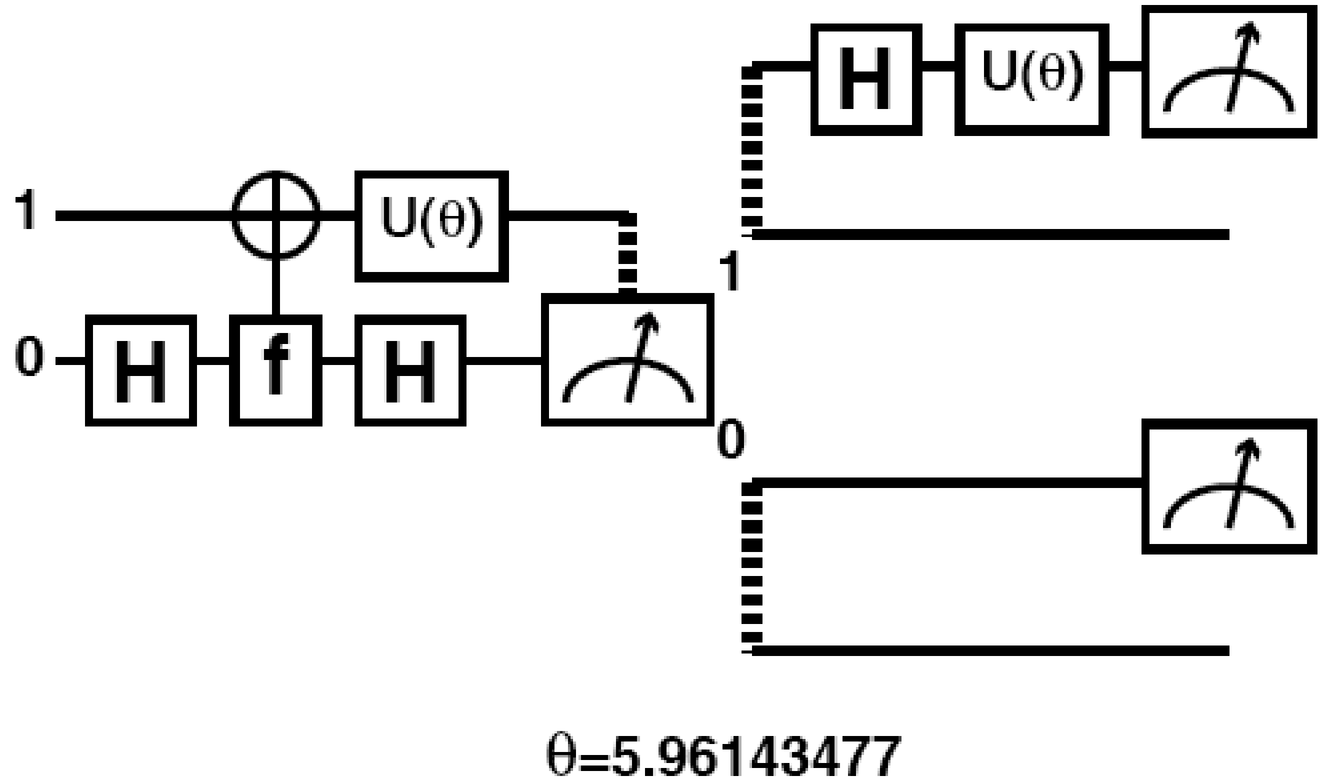
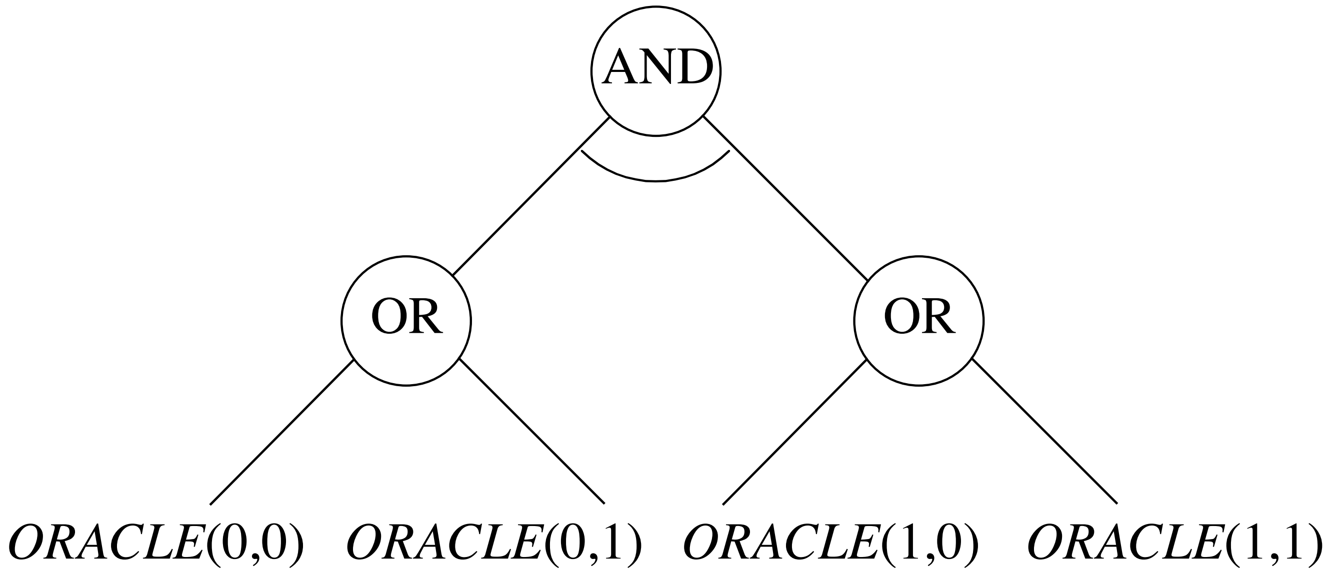


Figure 8.9. A gate array diagram for an evolved solution to the OR oracle problem. The gate marked "f" is the oracle. The two sub-diagrams on the right represent the two possible execution paths following the intermediate measurement. In the bottom sub-diagram the result of the intermediate measurement is 0 and the result of the overall computation is read immediately from the other qubit. In the top sub-diagram the result of the intermediate measurement is 1 and additional gates are applied to the other qubit prior to the final measurement.

2-bit AND/OR Problem

- Determine whether the behavior of a black-box quantum oracle satisfies the AND/OR property using only one call to the oracle, with a probability of error no worse than 0.2874.
- Result produced by genetic programming with PushGP.



(Diagram on next slide)

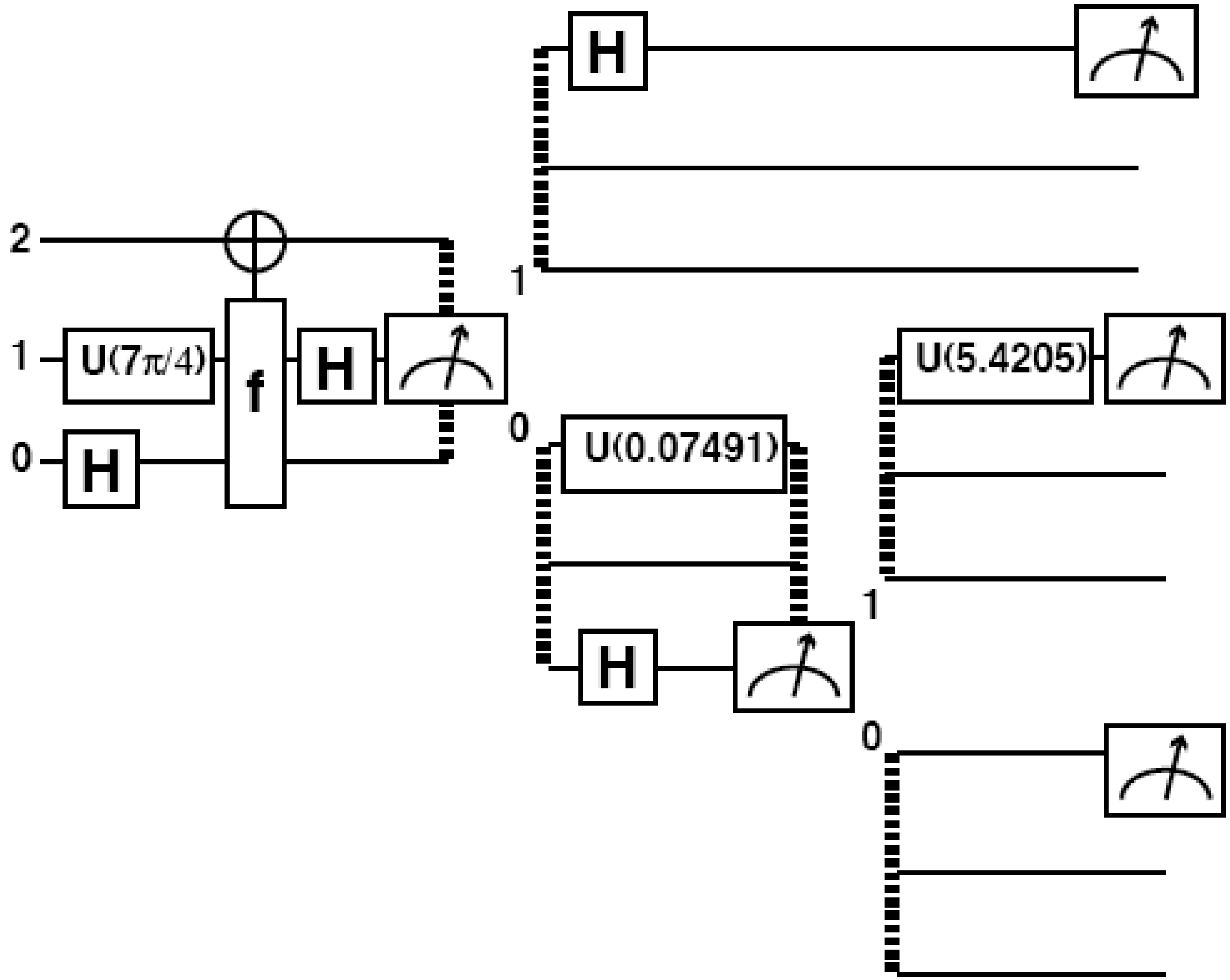
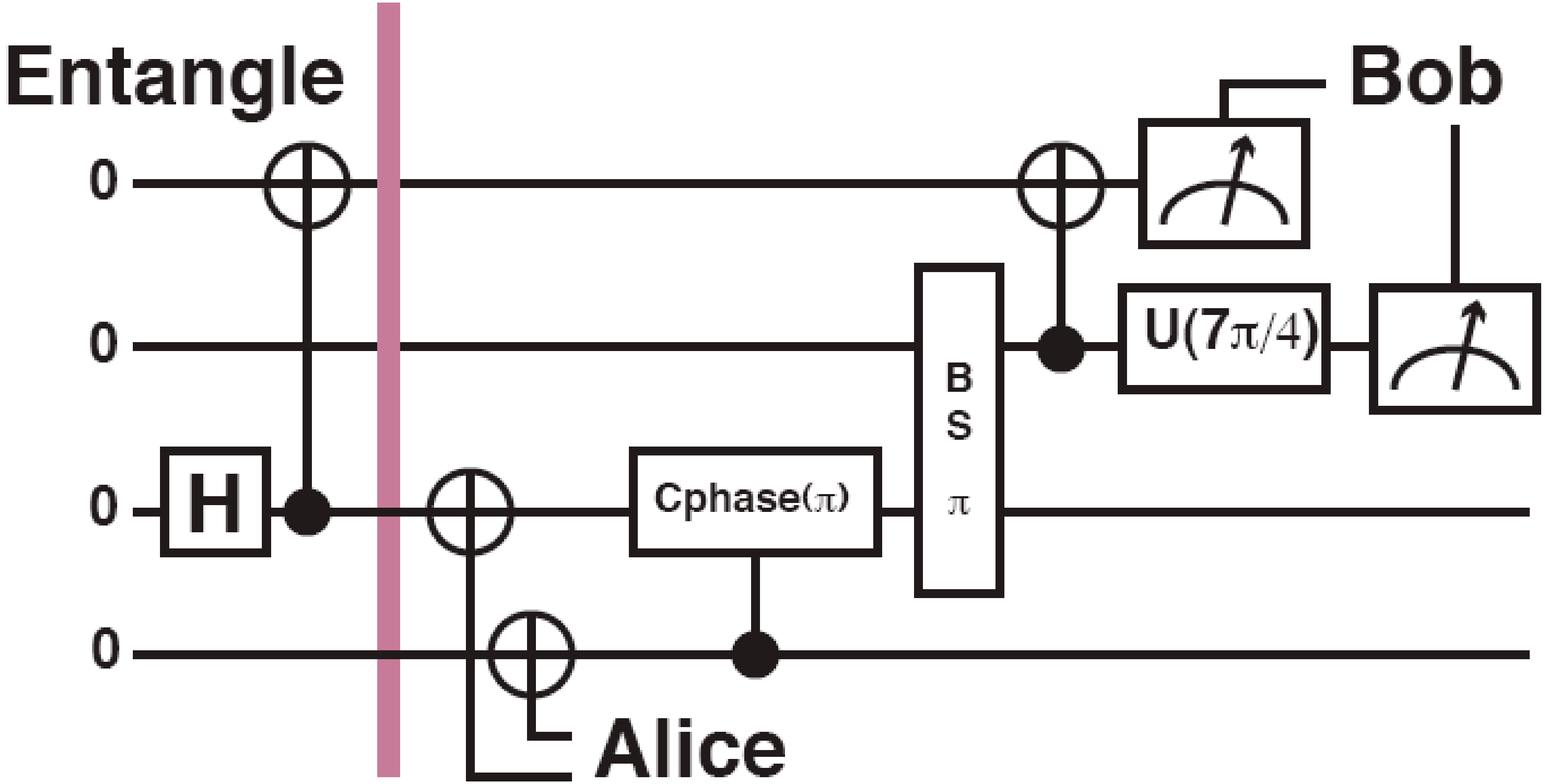


Figure 8.11. A gate array diagram for an evolved solution to the AND/OR oracle problem. The gate marked "f" is the oracle. The sub-diagrams on the right represent the possible execution paths following the intermediate measurements.

Dense Coding



- Two c-bits through BS(π) with zero error.
- Discovered by GP.

Conclusions

- Possibilities count.
- Evolution may help us to figure out *how* they count, and how to exploit these effects for practical applications.