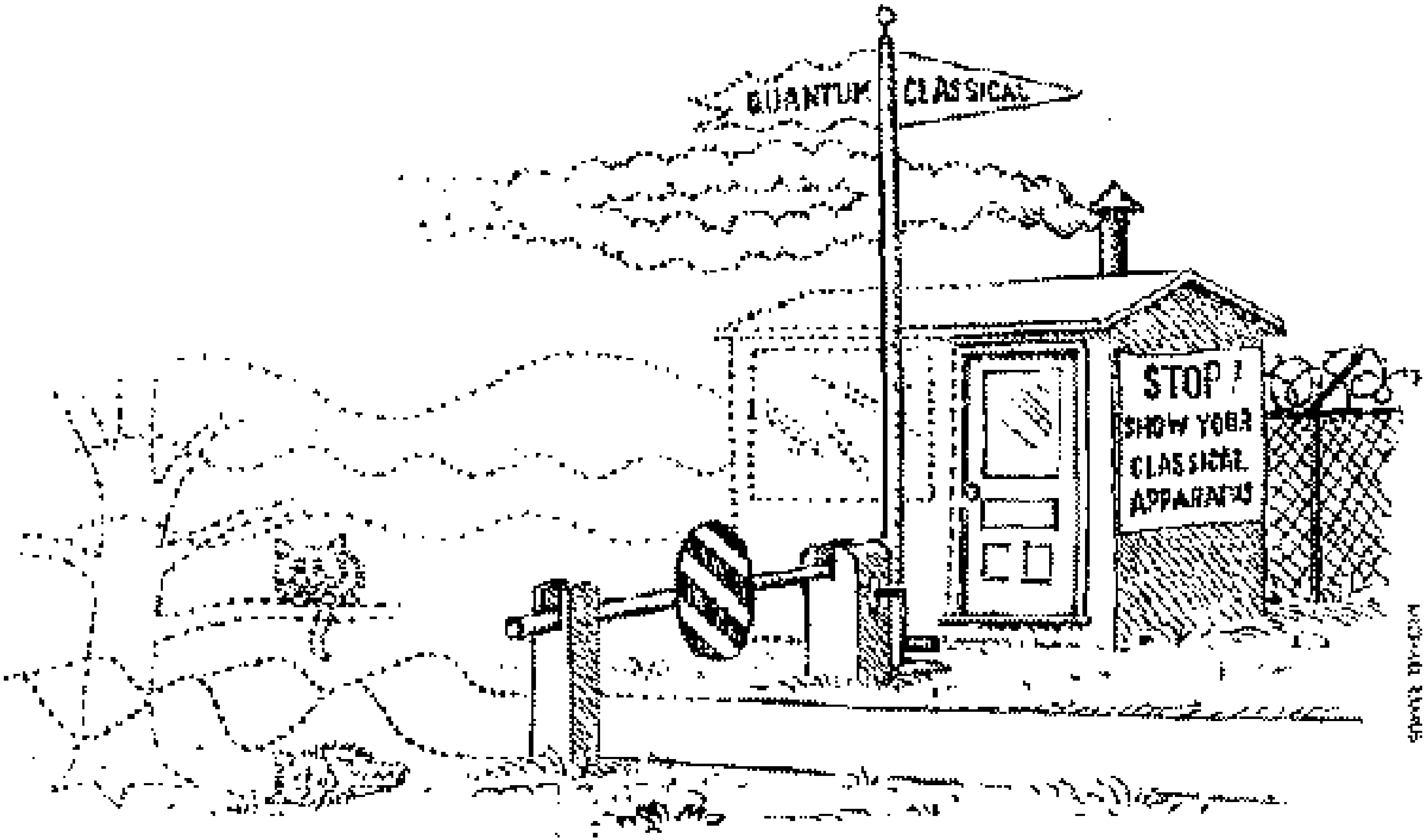
Quantum Computing



Information is Physical

information is always tied to a physical realization

fundamental limits:

speed-limit: c (relativity)

resetting a bit costs > $kT \ln 2$ (statistical mechanics)

Cbit

dynamical RAM represents bit by charge on capacitor:

b=1 – capacitor charged

b=0 – capacitor uncharged

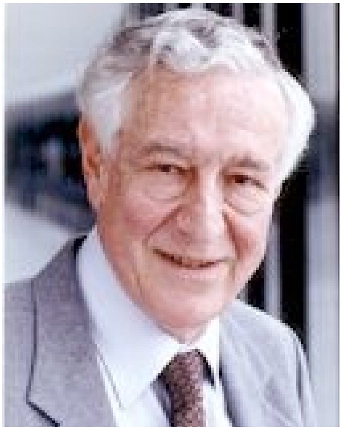
Qbit

alternative: **represent bit by spin-½**

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

superposition of (classical) bits

Rolf Landauer



Quantum Information

Qbits cannot be copied
(no-cloning theorem)

disadvantage:
information in Qbit not fully accessible
(uncertainty!)

advantage:
eavesdropping on a quantum channel detectable
$\Rightarrow$ quantum cryptography

No-Cloning Theorem

Wootters&Zurek Nature **299**, 802 (1982)

it is impossible to copy an *unknown* quantum state

proof by *reductio ad absurdum*

let U be unitary cloning operator: $U|\Psi\rangle|s\rangle = |\Psi\rangle|\Psi\rangle$ for *any* $|\Psi\rangle$

then $\langle s|\langle\Psi|U^\dagger \cdot U|\Phi\rangle|s\rangle \overset{\text{unitary}}{=} \underbrace{\langle s|s\rangle}_{=1}\langle\Psi|\Phi\rangle$

$\overset{\text{def}}{=} \langle\Psi|\langle\Psi| \cdot |\Phi\rangle|\Phi\rangle = \langle\Psi|\Phi\rangle^2$

thus $\langle\Psi|\Phi\rangle^2 \overset{!}{=} \langle\Psi|\Phi\rangle$; only possible if $\langle\Psi|\Phi\rangle = 0$ or 1

⇒ only orthogonal basis states can be cloned

(reversible copying of Cbits)

classical logics

Boolean operations

NOT gate

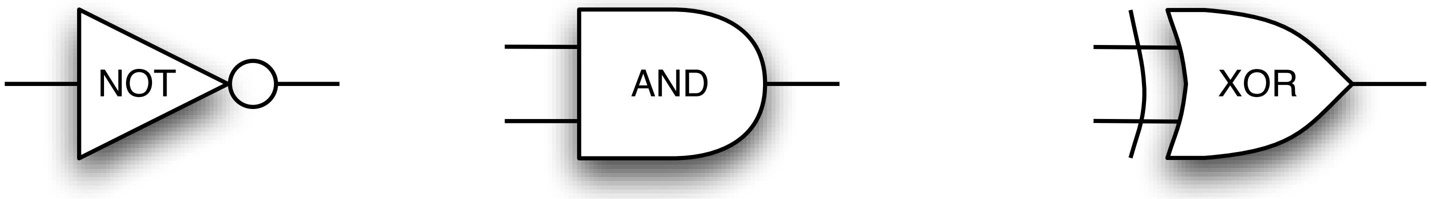
a	¬a
0	1
1	0

AND gate

a	b	$a \cdot b$
0	0	0
0	1	0
1	0	0
1	1	1

XOR gate

a	b	$a \oplus b$	a
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1



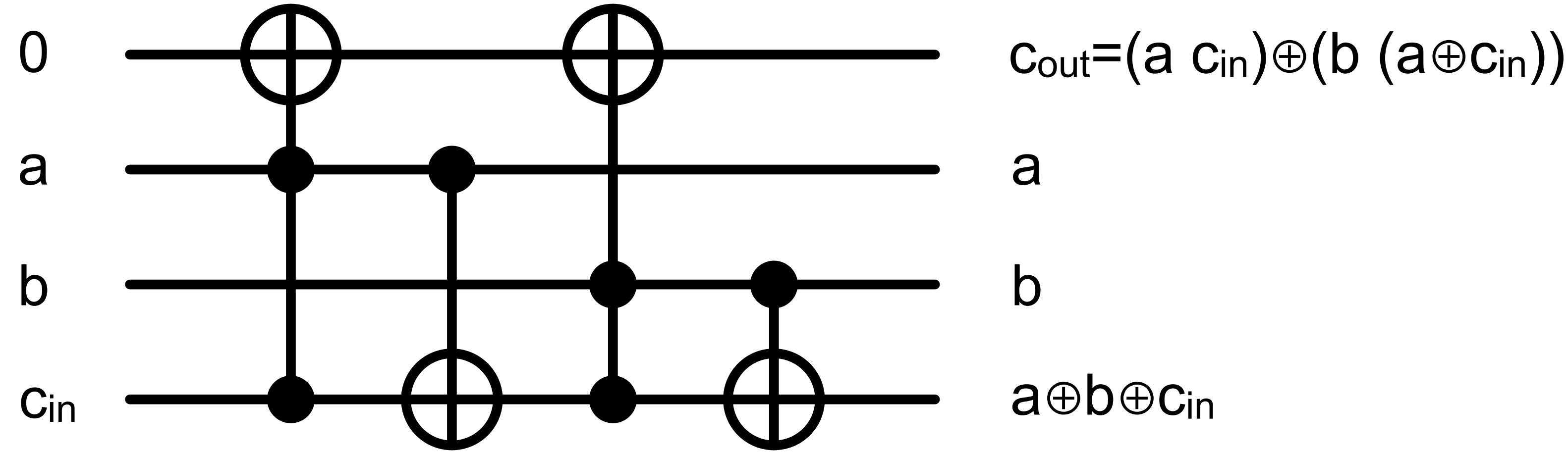
not reversible!

reversible: cNOT

reversible logics

e.g. controled NOT and Toffoli gates

example:
full adder



reversible gate defines operation on basis states
naturally extends to unitary operators

quantum gates without classical analogon:
e.g. Hadamard gate (creates superpositions)

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

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

quantum parallelism

$$U_H|0\rangle U_H|0\rangle \ldots U_H|0\rangle = U_H^{\otimes n}|00\ldots 0\rangle = \sum_x |\mathbf{x}\rangle$$

superposition of all 2^n basis states

implement classical function f(x) as unitary operator:

$$U_f|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|\mathbf{y} \oplus f(\mathbf{x})\rangle$$

then $$U_f U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_x |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_x \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}_{x \text{ and } f(x) \text{ entangled!}}$$

simultaneous evaluation of 2^n function values!

problem: only one (random!) *f(x)* can be measured

The Art of Quantum Computing:
use interference to extract relevant information

dimension of Hilbert space

n-Qbit Hilbert space dimension

n	2^n		
10	1,024	kb	kilo
20	1,048,576	Mb	Mega
30	1,073,741,824	Gb	Giga
40	1,099,511,627,776	Tb	Tera
50	1,125,899,906,842,620	Pb	Peta
60	1,152,921,504,606,850,000	Eb	Exa
70	1,180,591,620,717,410,000,000	Zb	Zetta
80	1,208,925,819,614,630,000,000,000	Yb	Yotta

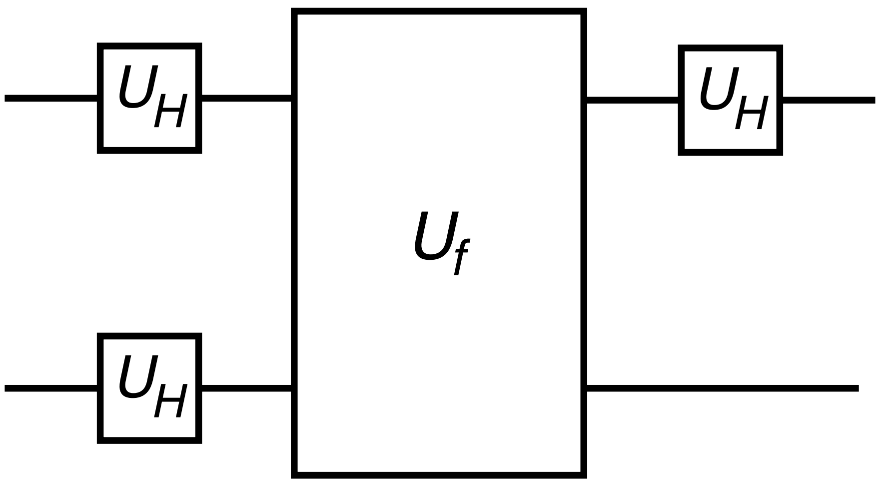
Deutsch algorithm

Proc. Roy. Soc. London, Ser. A **400**, 97 (1985)

given f: {0,1} → {0,1}   is f(0)=f(1) or not?

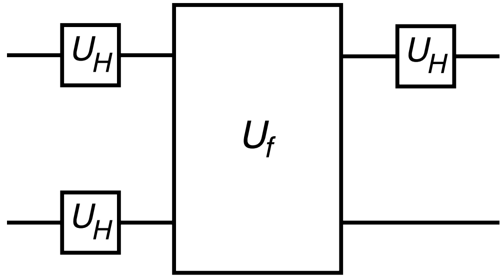
classical computing: need two calls to f

quantum computing: single call to f sufficient



Deutsch algorithm

Proc. Roy. Soc. London, Ser. A **400**, 97 (1985)



prepare superposition

$$U_H|0\rangle\, U_H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}\Big(|0\rangle|0\rangle \quad -|0\rangle|1\rangle \quad +|1\rangle|0\rangle \quad -|1\rangle|1\rangle \Big)$$

evaluate f (using $0 \oplus a = a$ and $1 \oplus a = \overline{a}$)

$$\xrightarrow{U_f} \frac{1}{2}\Big(|0\rangle|0\oplus f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle\Big)$$

$$= \frac{1}{2}\Big(|0\rangle|f(0)\rangle \quad -|0\rangle|\overline{f(0)}\rangle \quad +|1\rangle|f(1)\rangle \quad -|1\rangle|\overline{f(1)}\rangle \Big)$$

$$= \frac{1}{2}\Big(\; |0\rangle\,[|f(0)\rangle - |\overline{f(0)}\rangle] \quad + \; |1\rangle\,[|f(1)\rangle - |\overline{f(1)}\rangle] \Big)$$

interference step

$$= \begin{cases} \frac{1}{2}(|0\rangle + |1\rangle)\,[|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \frac{1}{\sqrt{2}}|0\rangle\,[|f(0)\rangle - |\overline{f(0)}\rangle] & \text{if } = \\ \frac{1}{2}(|0\rangle - |1\rangle)\,[|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \frac{1}{\sqrt{2}}|1\rangle\,[|f(0)\rangle - |\overline{f(0)}\rangle] & \text{if } \neq \end{cases}$$

Quantum Computing

notion of computability unchanged
quantum systems can be simulated on a classical computer

computational complexity reduced:
quantum computers can be much faster than classical ones

problem	classical algorithm	quantum algorithm
factoring N	number field sieve $O(e^{(\log N)^{1/3} (\log \log N)^{2/3}})$	Shor algorithm: $O(\log^3 N)$
unstructured search in N items	brute force: O(N)	Grover algorithm: $O(\sqrt{N})$

Shor algorithm

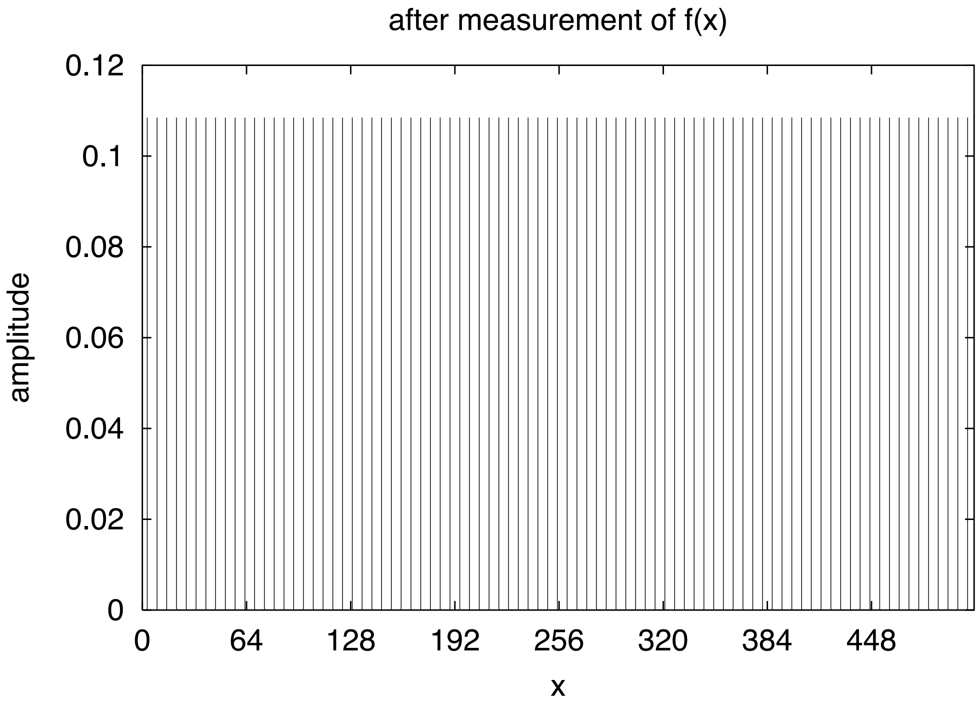
factorize M

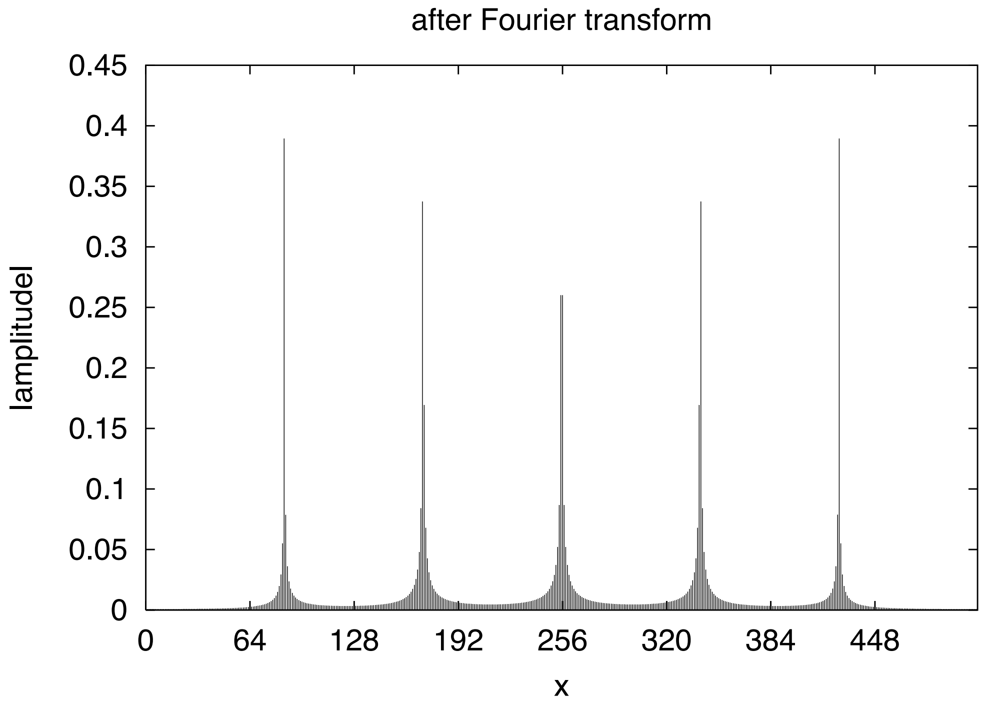
pick $a > 1$ with $\gcd(M, a)=1$ (otherwise factor found already)

calculate $f(x)=a^x \bmod M$

find period $f(x+r) = f(x)$ (quantum Fourier transform)

then $\gcd(a^{r/2} \pm 1, M)$ gives factor of M





probabilistic result for r, but easy to check if correct!

factoring with bc

```
#!/usr/bin/env bc -q
define gcd(a,b) {
  auto r;
  while(a%b > 0) { r=a%b; a=b; b=r; }
  return(b);
}
define fact(m,a) { /* find factor of m with aux a>1 */
  auto e,x,r,p;
  if (a<=1) a=2;   /* otherwise error */
  e=gcd(m,a); if (e>1) return(e);
  /* find period of f(x)=a^x mod m; note that f(0)=1 */
  for (x=1; a^x % m != 1; x++) r=x
  p=a^(r/2)
  e=gcd(m,p+1); if (e>1) return(e);
  e=gcd(m,p-1); if (e>1) return(e);
}

fact(21,5)
3
fact(21,250)
3
```

Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

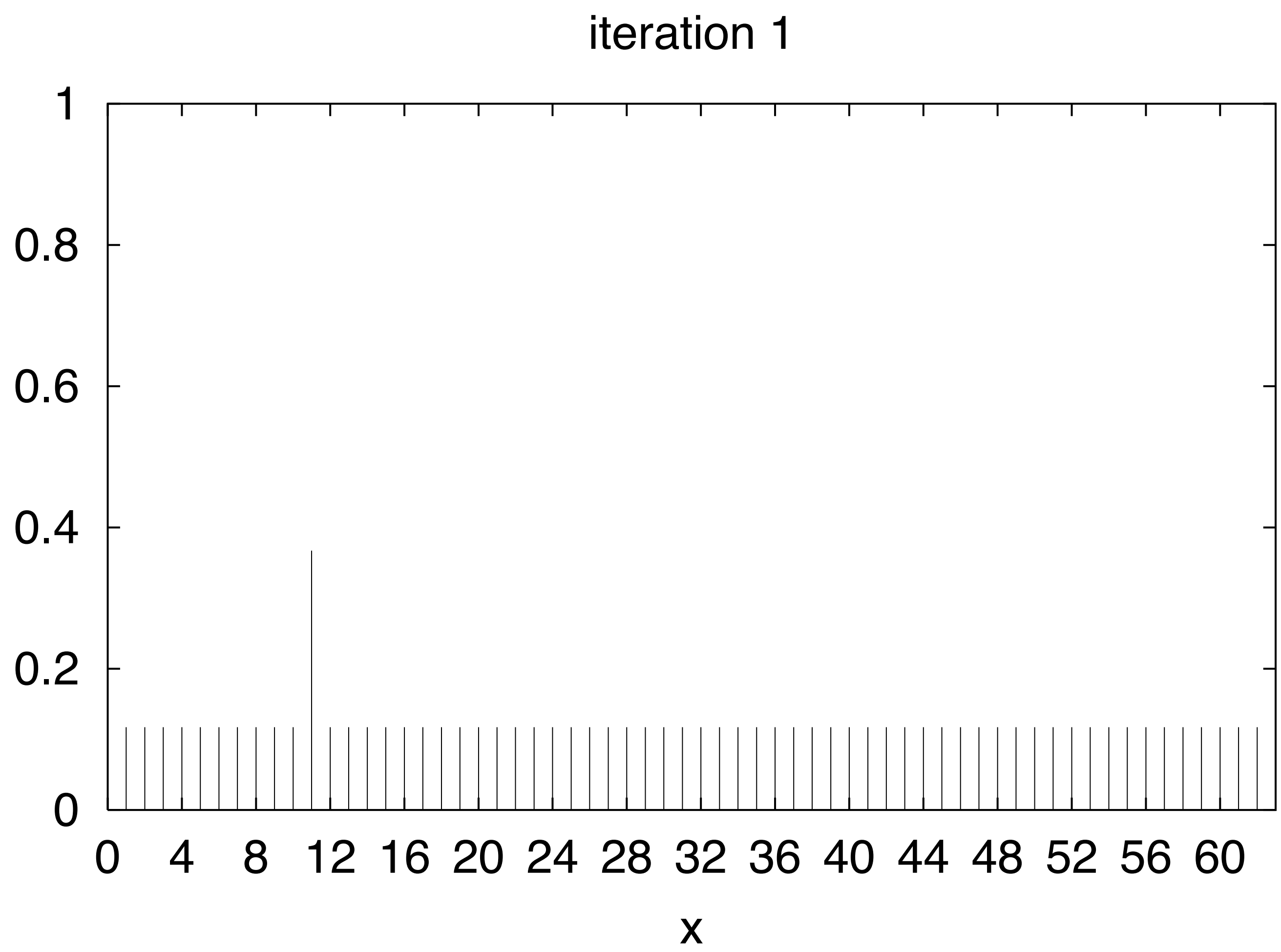
$$U_p \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle = \frac{1}{\sqrt{2^n}} \sum |0, p(x)\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x \neq x_p} |x, 0\rangle + |x_p, 1\rangle \right)$$

Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

iterative amplitude amplification

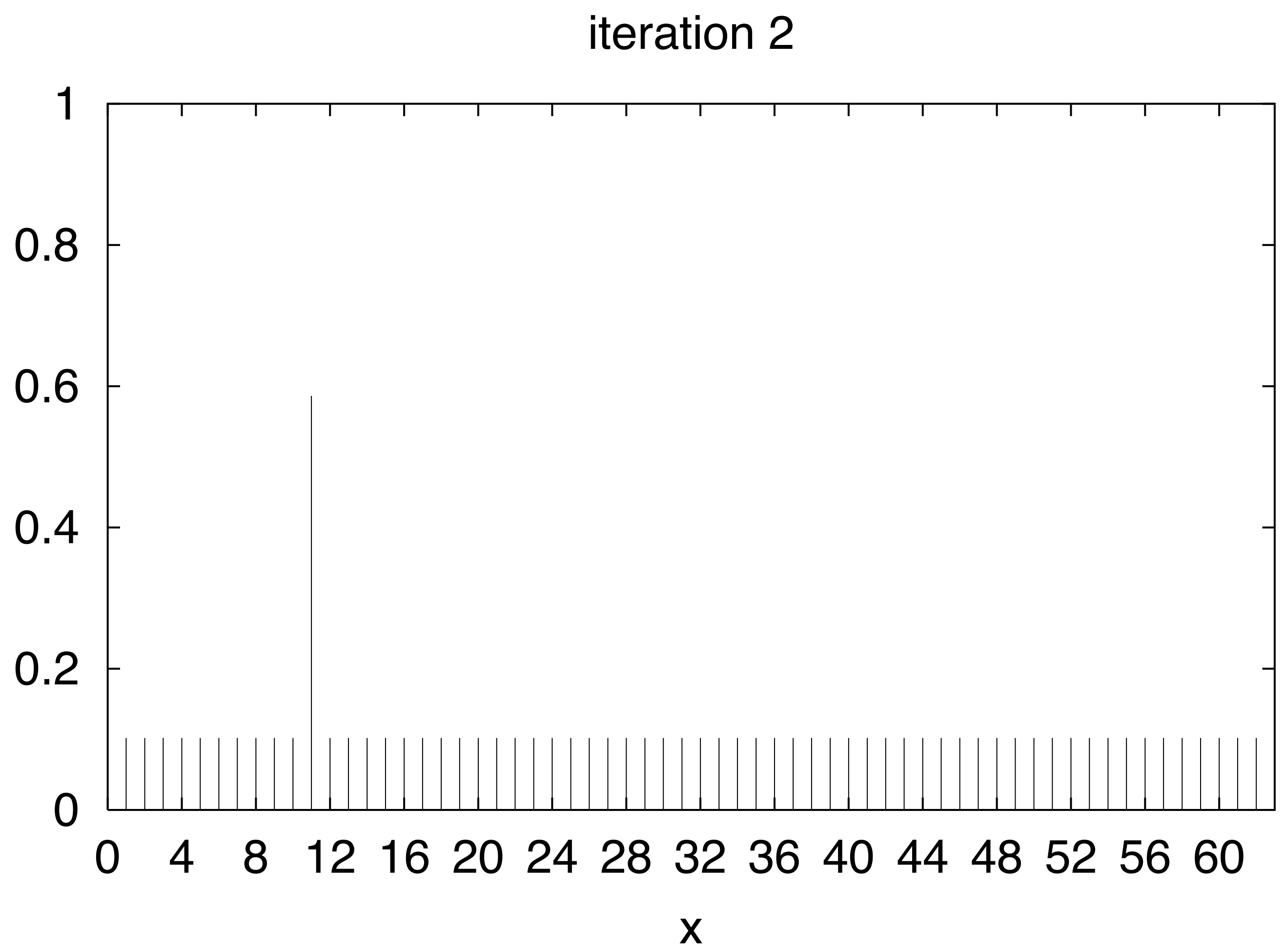


Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

iterative amplitude amplification

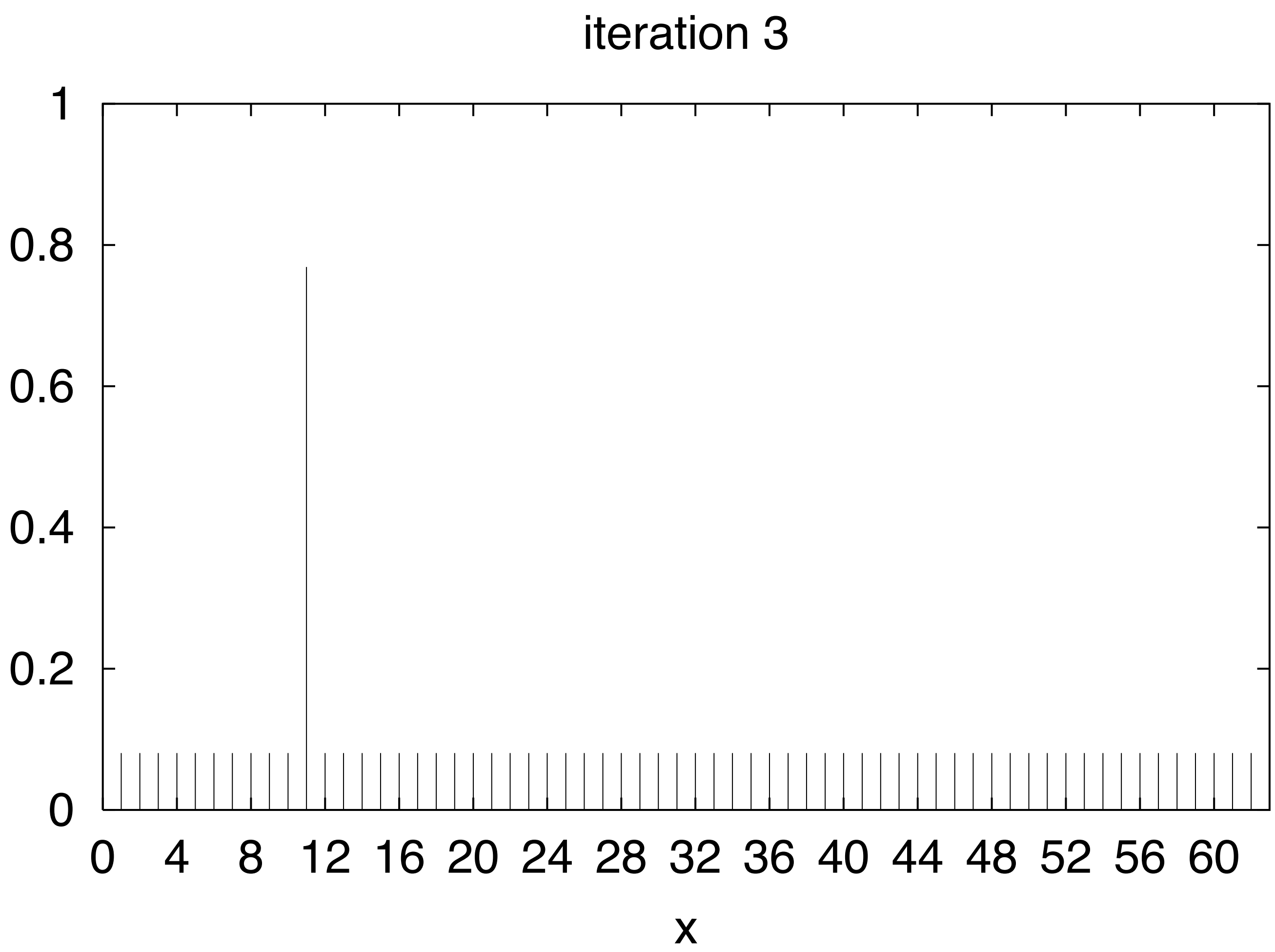


Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

iterative amplitude amplification

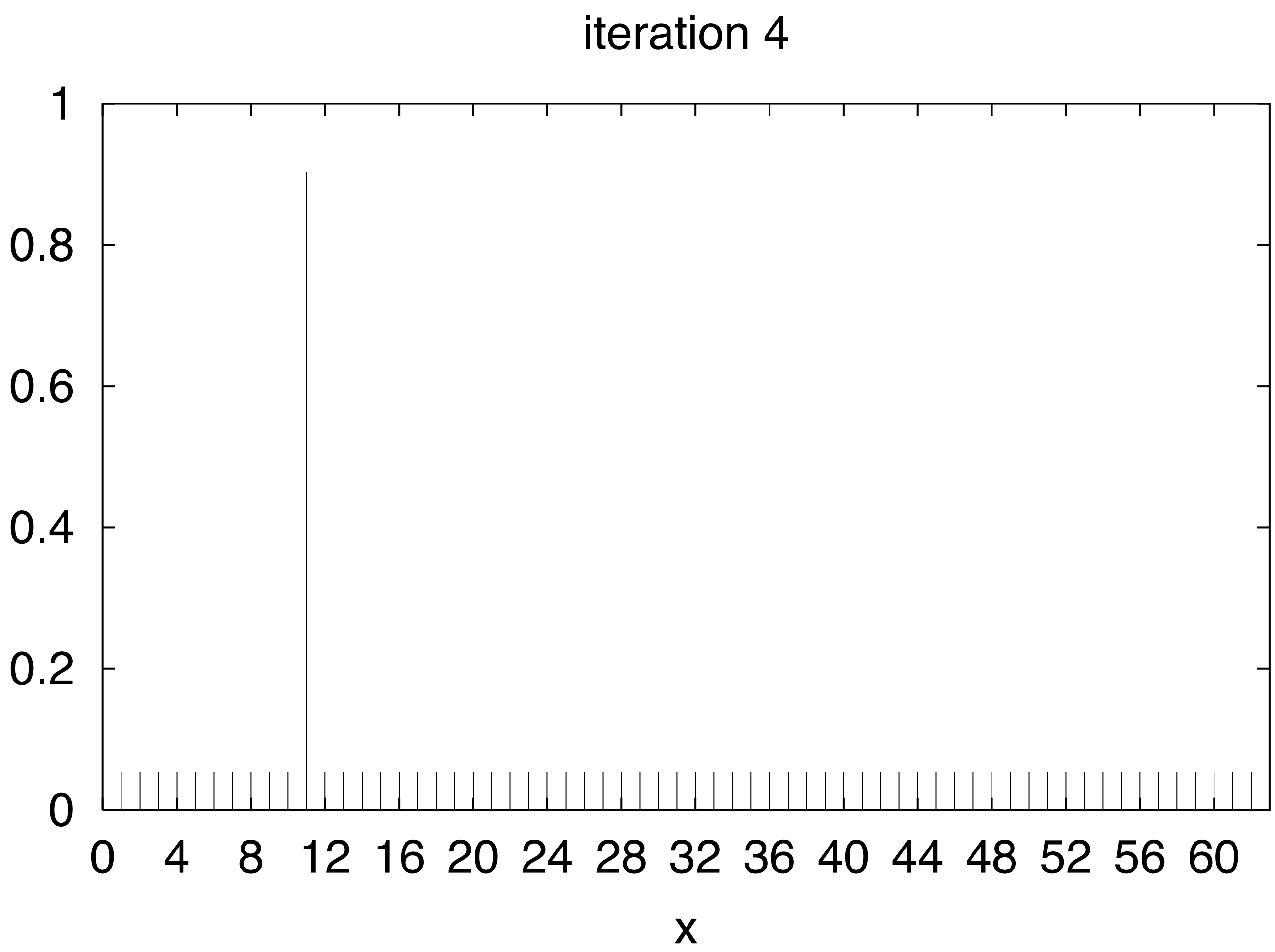


Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find x with f(x)=1

iterative amplitude amplification

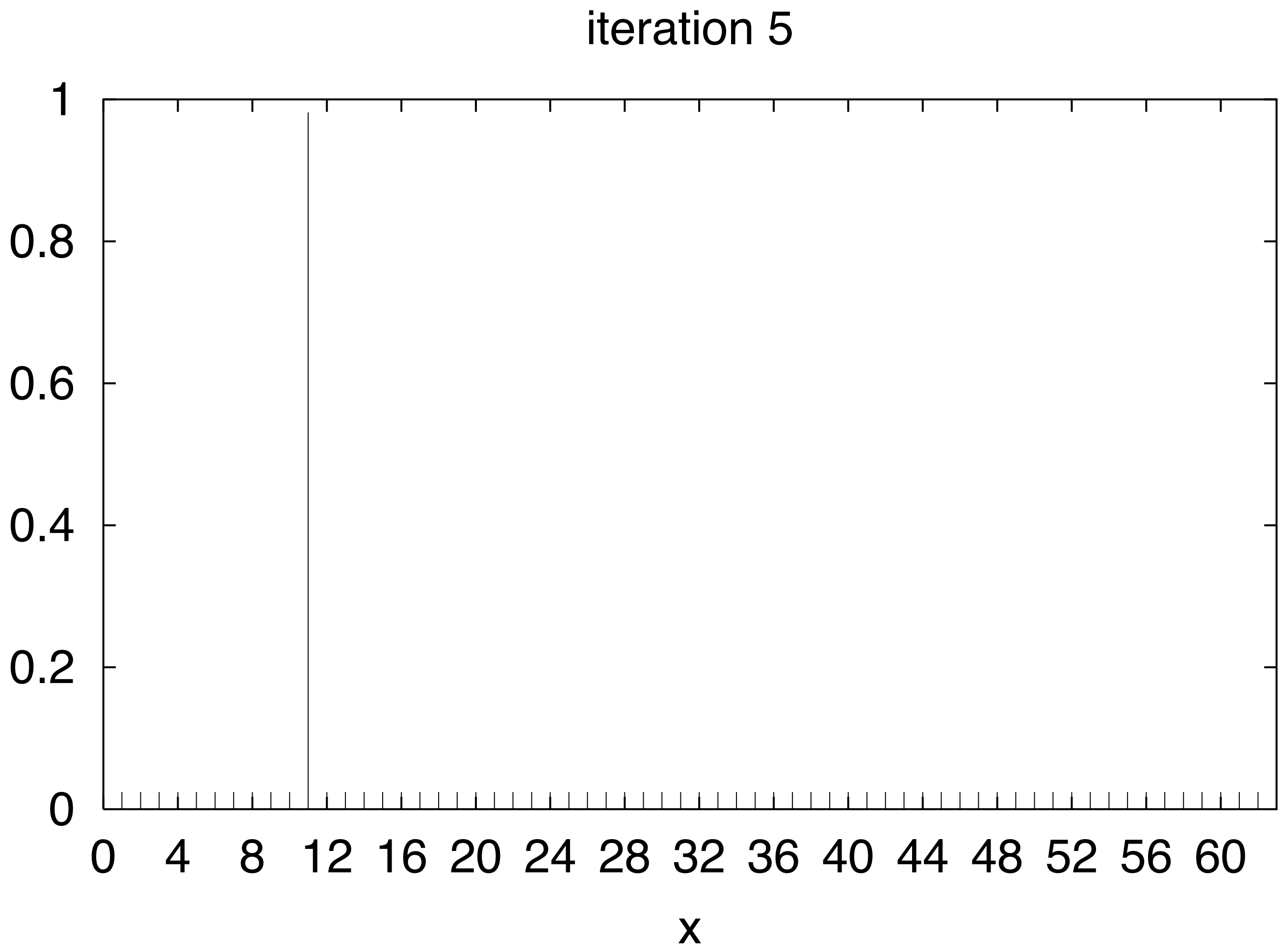


Grover algorithm

reverse lookup

given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

iterative amplitude amplification

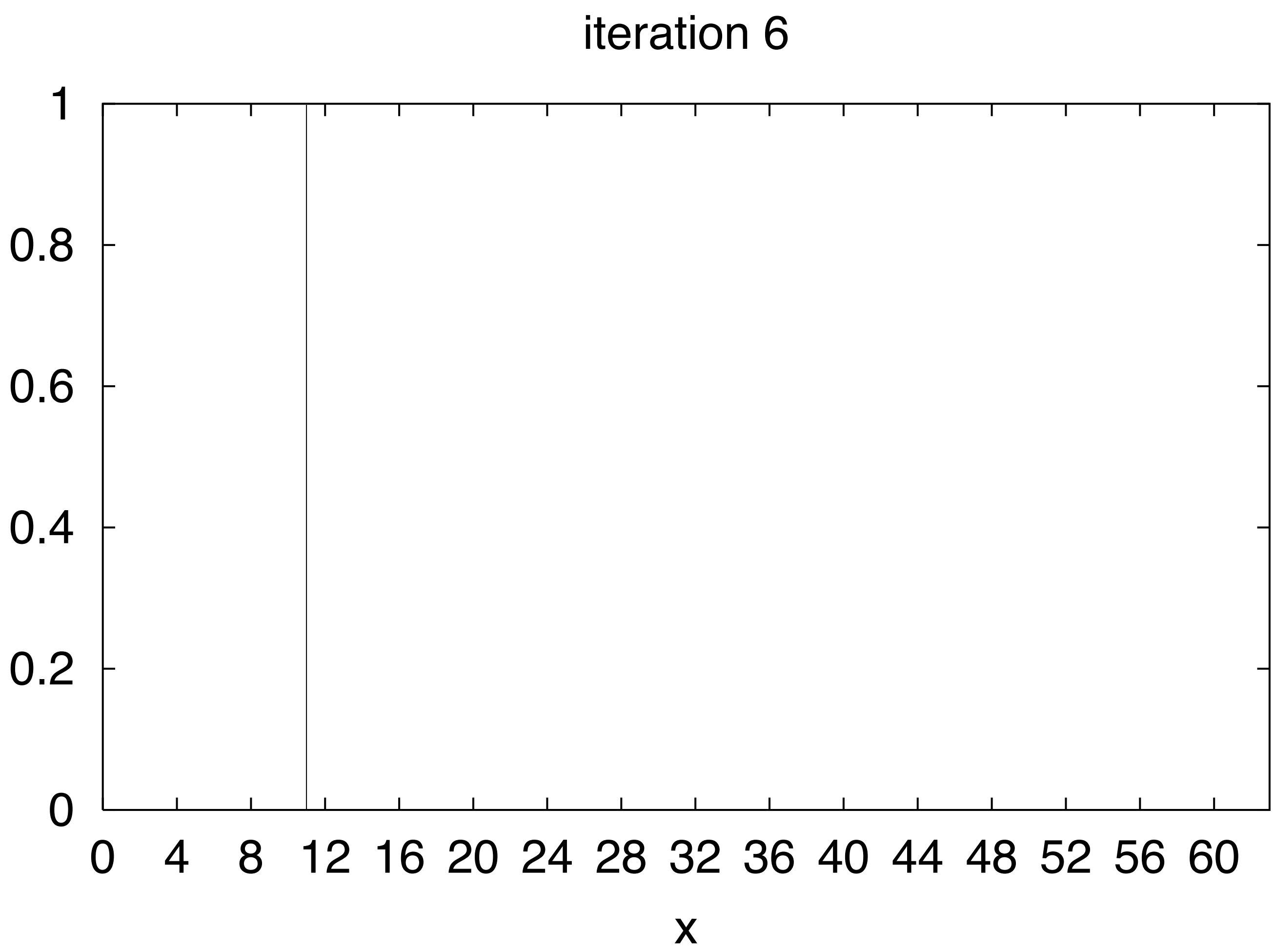


Grover algorithm

reverse lookup

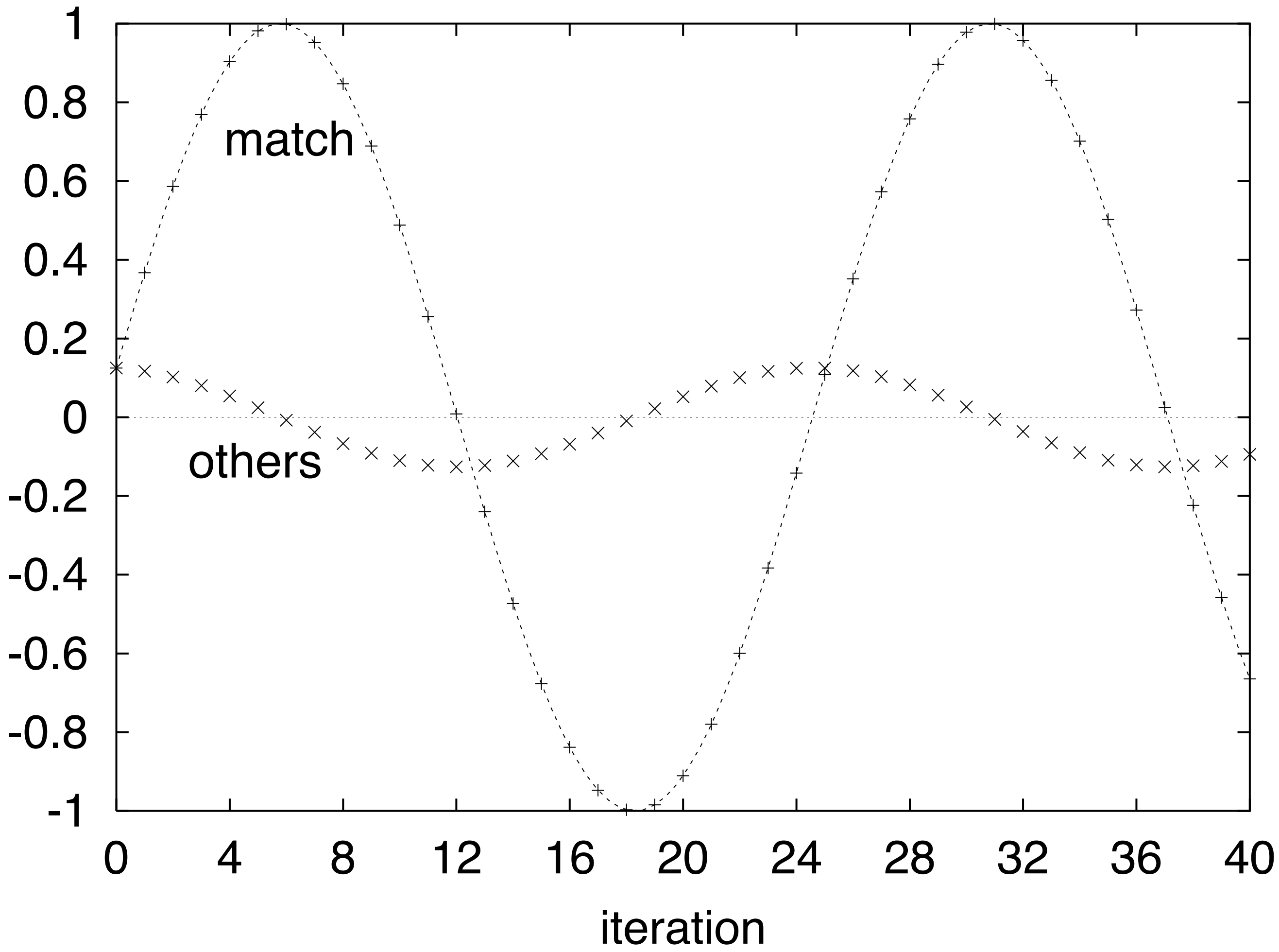
given f:{0,1,…,2^n-1} → {0,1} find *x* with f(*x*)=1

iterative amplitude amplification



Grover algorithm

amplitude for single match: $\sin((2n+1)\arcsin(N^{-½}))$



Qbits analog or digital?

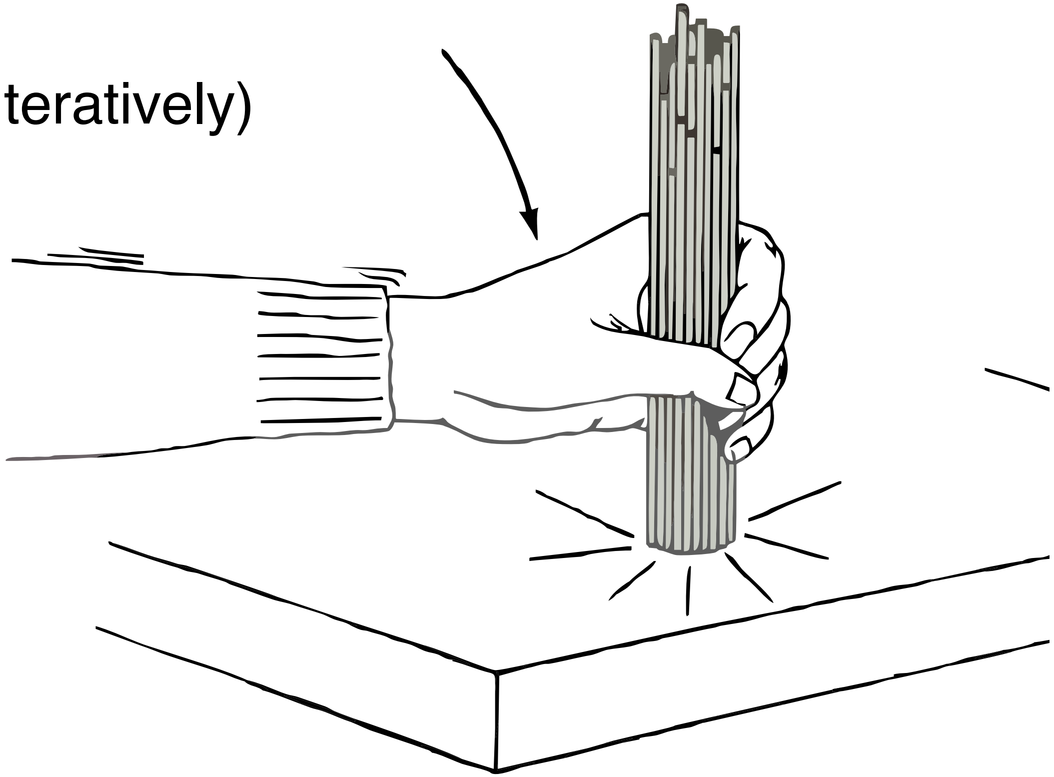
$$|b\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C} \text{ — Qbit analog!?}$$

but: α, β not accessible — measurement returns only 0 or 1

spaghetti computer

A.K. Dewdney, Scientific American **250**, 19-26 (June 1984)

- cut (uncooked!) spaghetti to length of numbers
- tap them on table
- pick tallest spaghetti (iteratively)
- gives sorted numbers



O(N) — faster than QuickSort O(N log(N))

Qbits analog or digital?

$|b\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}$ — Qbit analog!?

but: α, β not accessible — measurement returns only 0 or 1

error correction possible — digital!

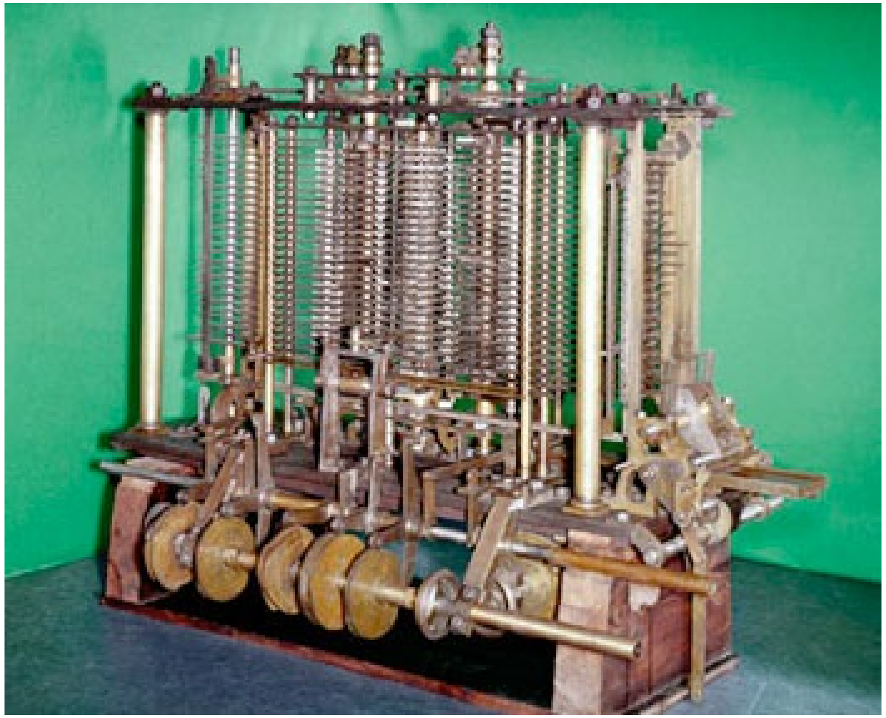
idea: bit errors can be described by Pauli matrices:
(discrete errors)

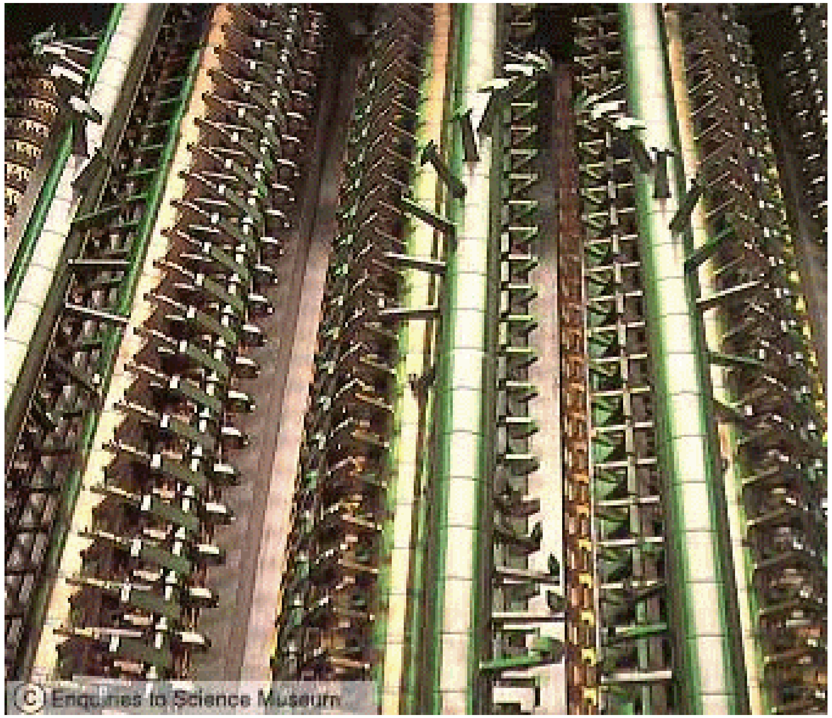
$\mathbf{I}$	—	no error	σ_x	—	bit-flip
σ_z	—	phase-flip	σ_y	—	bit-&phase-flip

project on one of the four error states and correct

inappropriate hardware

mechanical computers



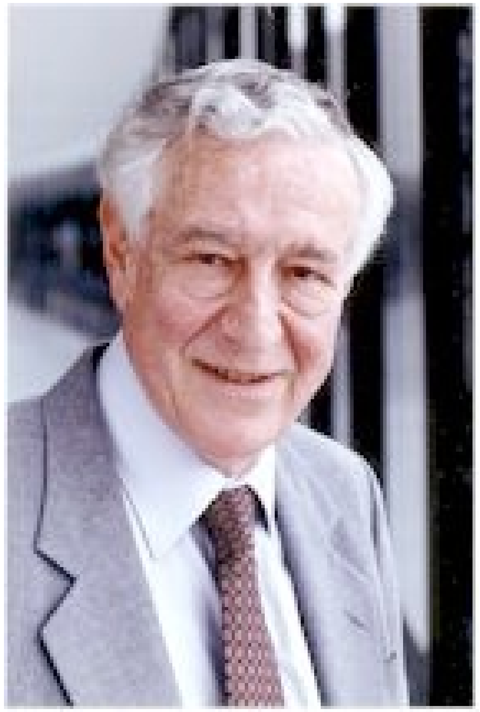


Charles Babbage: Analytical Engine (1834)

Landauer's Disclaimer

Nature **400**, 720 (1999)

This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work.

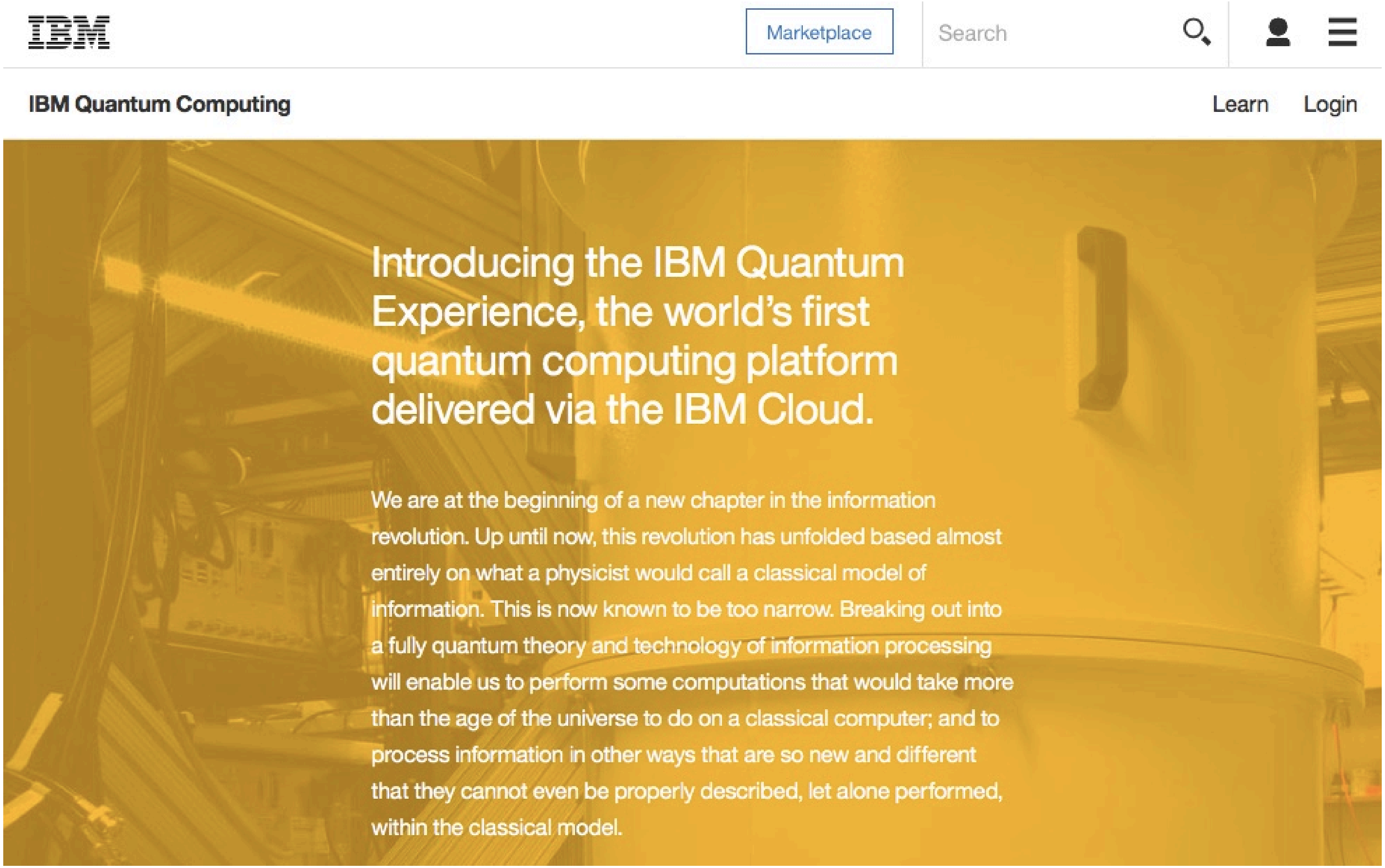


Quantum Cryptography

MagiQ: www.magiqtech.com
id quantique: www.idquantique.com

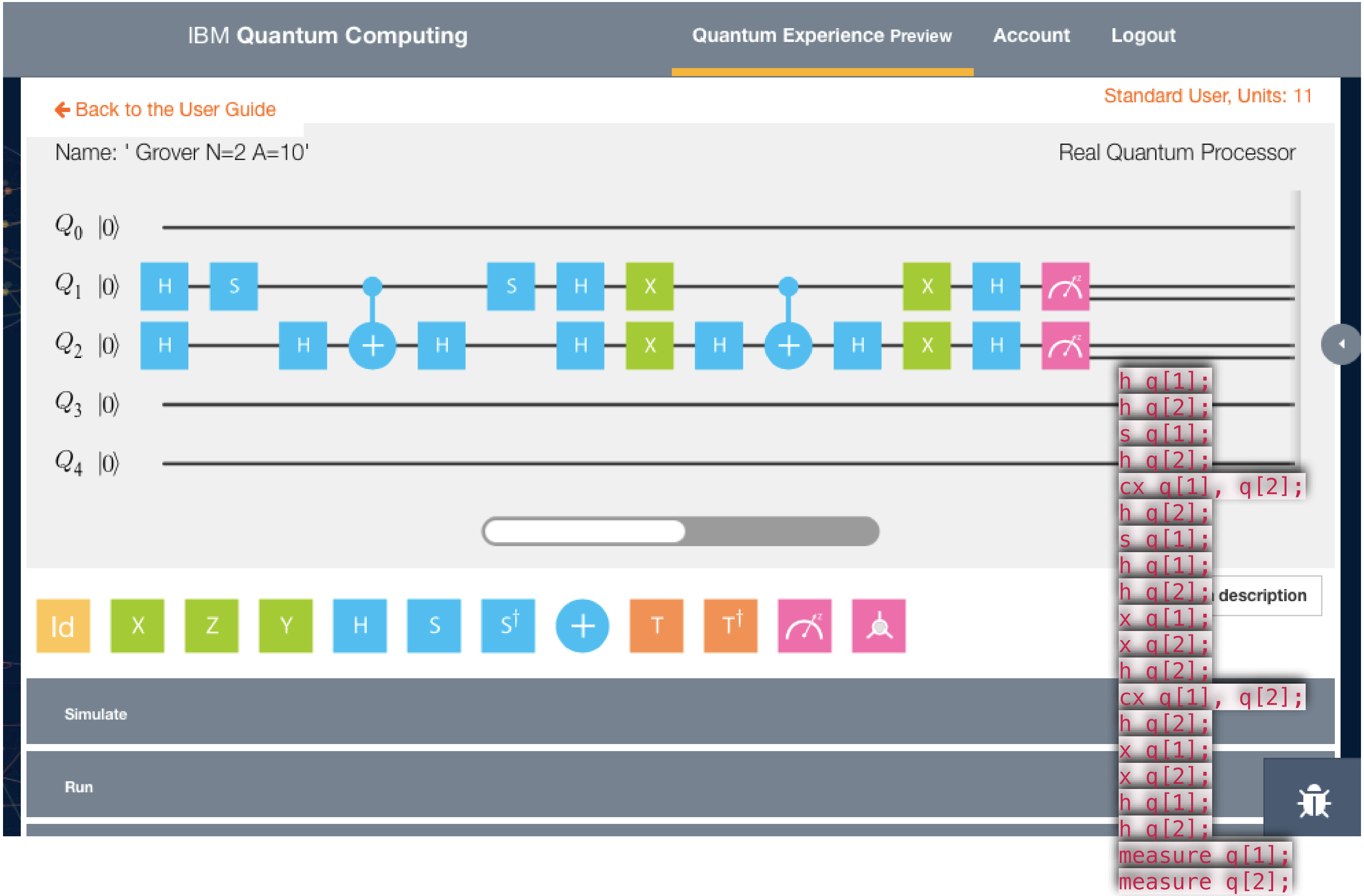
Figure 3: id Quantique's system exchanged keys over 67 km of standard optical fiber.

IBM Quantum Experience

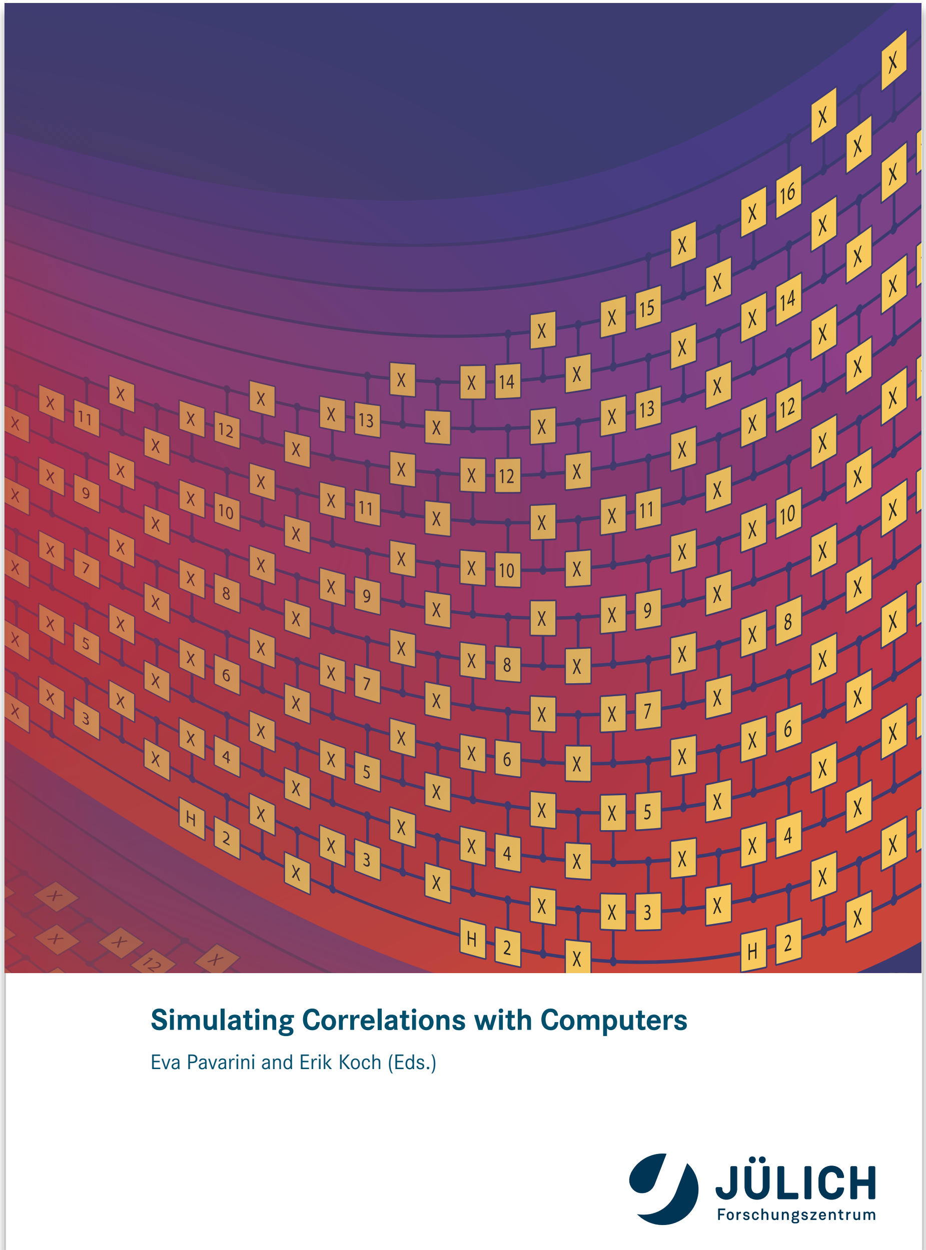


https://quantum-computing.ibm.com

IBM Quantum Experience



Simulating Materials



www.cond-mat.de/events/correl21

1. Erik Koch
   Second Quantization and Jordan-Wigner Representations
2. Klaus Doll
   Fundamentals of Quantum Chemistry
3. Kieron Burke
   Lies My Teacher Told Me About Density Functional Theory: See
4. Pina Romaniello
   Hubbard Dimer in GW and Beyond
5. Eva Pavarini
   Dynamical Mean-Field Theory for Materials
6. Robert Eder
   Green Functions and Self-Energy Functionals
7. Václav Janiš
   Green Functions in the Renormalized Many-Body Perturbation
8. Gianluca Stefanucci
   An Essential Introduction to NEGF Methods for Real-Time Simu
9. Christian Schilling
   Orbital Entanglement and Correlation
10. Walter Hofstetter
    Analog Quantum Simulations of the Hubbard Model
11. Kristel Michielsen
    Programming Quantum Computers
12. Libor Veis
    Quantum Chemistry on Quantum Computers
13. David DiVincenzo
    Quantum Computing — Quo Vadis?

quantum computing

- can only solve what classical computers can (*simulatable*) but possibly much faster (*quantum parallelism*)
- Qbits look analog but only *digital* information accessible
- results usually *probabilistic* — best for satisfiability problems
- no *reliable* hardware available yet
- noise, number of Qbits and connectivity matter

Confused?

Möglicherweise ist es, nebenbei gesagt, für die Kopenhagener Interpretation der Quantenmechanik wichtig, dass ihre Sprache in einem gewissen Grad unbestimmt ist, und ich bezweifle, dass sie durch den Versuch, diese Unbestimmtheit zu vermeiden, klarer werden kann. (W. Heisenberg)