Quantum Computing for PLaypersons

William D Clinger

9 February 2011

- reversible operations on classical bits
- unitary operators on Hilbert spaces
- photon polarization
- quantum key distribution
- quantum computation

Reversible operations on 1 classical bit

- 1 (identity)
- X (NOT)

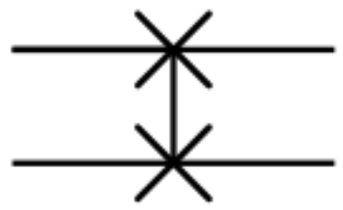
Reversible operations on 2 classical bits

x_0	x_1	y_0	y_1	
0	0	1	1	
0	1	1	0	
1	0	0	1	
1	1	0	0	X_0X_1

Reversible operations on 2 classical bits

x_0	x_1	y_0	y_1
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

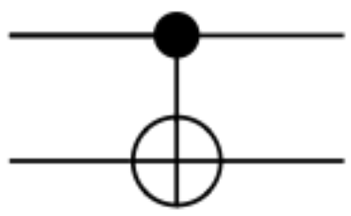
S_{01}



Reversible operations on 2 classical bits

x_0	x_1	y_0	y_1
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$cNOT_{01}$



$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|0\rangle_2 = |00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle$$

$$|1\rangle_2 = |01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle$$

$$|2\rangle_2 = |10\rangle = |1\rangle|0\rangle = |1\rangle \otimes |0\rangle$$

$$|3\rangle_2 = |11\rangle = |1\rangle|1\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \otimes \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \otimes \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} = \begin{bmatrix} x_0y_0z_0 \\ x_0y_0z_1 \\ x_0y_1z_0 \\ x_0y_1z_1 \\ x_1y_0z_0 \\ x_1y_0z_1 \\ x_1y_1z_0 \\ x_1y_1z_1 \end{bmatrix}$$

$$\mathrm{cNOT}_{01} = C_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$S_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_{ij} = C_{ij} C_{ji} C_{ij}$$

Unitary operators on a Hilbert space

$$|\psi\rangle = \alpha_0|0\rangle + \cdots + \alpha_{N-1}|N-1\rangle = \sum_x \alpha_x|x\rangle$$

$$|\phi\rangle = \beta_0|0\rangle + \cdots + \beta_{N-1}|N-1\rangle = \sum_x \beta_x|x\rangle$$

$$\langle\phi| = \beta_0^*\langle 0| + \cdots + \beta_{N-1}^*\langle N-1| = \sum_x \beta_x^*\langle x|$$

$$\langle\phi|\psi\rangle = \langle\phi||\psi\rangle = \sum_x \beta_x^*\alpha_x$$

Hadamard transform

$$\mathsf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \mathsf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$(\mathsf{H} \otimes \mathsf{H})(|0\rangle \otimes |0\rangle) = \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2)$$

The Born Rule

If the possible outcomes of a quantum measurement correspond to unit vectors $|0\rangle$ and $|1\rangle$, and the normalized quantum state is

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

then

$$P(|0\rangle) = |\alpha_0|^2$$
$$P(|1\rangle) = |\alpha_1|^2$$

Qbits are mutable objects!

If a Qbit's state is classical, then reading its state with respect to the classical basis will leave its state unchanged.

If a Qbit's state is a nontrivial mixture of basis vectors, however, then reading its state with respect to that basis will change its state.

Photon polarization

$$|\psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$|\psi_1\rangle = |0\rangle = \frac{1}{\sqrt{2}}(\mathrm{H}|0\rangle + \mathrm{H}|1\rangle)$$

$$|\psi_2\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\psi_3\rangle = |1\rangle$$

Quantum key distribution

Alice wants to generate a random secret key and send it to Bob.

Eve wants to eavesdrop.

Two insecure channels are available:

1 classical channel

1 quantum channel

BB84 algorithm

Alice generates 8n classical bits at random.

Alice encodes 4n of those bits as Qbits, using the other 4n bits to select the basis:

- vertical/horizontal
- Hadamard

Alice transmits those 4n Qbits to Bob.

For each of those 4n Qbits, Bob randomly chooses a decoding basis:

vertical/horizontal

Hadamard

Bob tells Alice the sequence of bases he used to decode the Qbits.

Alice tells Bob which Qbits he decoded incorrectly. Bob discards those bits.

After discarding the bits he decoded using the wrong basis, Bob has about 2n bits left.

Bob chooses half of those 2n bits at random, and tells Alice the values of those bits.

If Alice confirms those n bits, then the other n bits will be the secret key that Alice and Bob share.

It is extremely unlikely that Eve overheard more than a few of those n bits. Why?

If Eve decoded any of the quantum bits, then she had to guess which basis to use:

vertical/horizontal

Hadamard

If Eve guesses wrong, she changes the state of the Qbit. Half of those altered Qbits would be received incorrectly by Bob.

No-cloning theorem

Suppose

$$\forall\psi \quad \mathsf{U}(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

Then

$$\begin{aligned}\mathsf{U}(\alpha|\psi\rangle + \beta|\phi\rangle)|0\rangle &= (\alpha|\psi\rangle + \beta|\phi\rangle)(\alpha|\psi\rangle + \beta|\phi\rangle) \\ &= \alpha^2|\psi\rangle|\psi\rangle + \beta^2|\phi\rangle|\phi\rangle \\ &\quad + \alpha\beta|\psi\rangle|\phi\rangle + \alpha\beta|\phi\rangle|\psi\rangle\end{aligned}$$

but

$$\begin{aligned}\mathsf{U}(\alpha|\psi\rangle + \beta|\phi\rangle)|0\rangle &= \alpha\mathsf{U}|\psi\rangle|0\rangle + \beta\mathsf{U}|\phi\rangle|0\rangle \\ &= \alpha|\psi\rangle|\psi\rangle + \beta|\phi\rangle|\phi\rangle\end{aligned}$$

$$f : 2^n \to 2^m$$

$$\mathsf{U}_f(|x\rangle_n|y\rangle_m) = |x\rangle_n|y \oplus f(x)\rangle_m$$

$$\mathsf{U}_f(|x\rangle_n|0\rangle_m) = |x\rangle_n|f(x)\rangle_m$$

$$\begin{aligned}
\mathsf{U}_f(\mathsf{U}_f(|x\rangle|y\rangle)) &= \mathsf{U}_f(|x\rangle|y \oplus f(x)\rangle) \\
&= |x\rangle|y \oplus f(x) \oplus f(x)\rangle \\
&= |x\rangle|y\rangle
\end{aligned}$$

Quantum parallelism

$$x = (\mathsf{H} \otimes \cdots \otimes \mathsf{H})(|0\rangle \otimes \cdots \otimes |0\rangle)$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n$$

$$\mathsf{U}_f(|x\rangle_n|0\rangle_m) = |x\rangle_n|f(x)\rangle_m$$

$$f(x) = \begin{cases} 0 & \text{if } x \neq a \\ 1 & \text{if } x = a \end{cases}$$

$$\mathsf{U}_f(|x\rangle_n|y\rangle_1) = |x\rangle_n|y \oplus f(x)\rangle_1$$

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

$$\mathsf{U}_f(|x\rangle \otimes \mathsf{H}|1\rangle) = (-1)^{f(x)}(|x\rangle \otimes \mathsf{H}|1\rangle)$$

$$\mathsf{V}|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq a \\ -|a\rangle & \text{if } x = a \end{cases}$$

$$\mathsf{V}|\psi\rangle = |\psi\rangle - 2|a\rangle\langle a|\psi\rangle$$

$$\mathsf{V} = 1 - 2|a\rangle\langle a|$$

$$\phi = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n$$

$$\mathrm{W}|\psi\rangle = 2|\phi\rangle\langle\phi|\psi\rangle - |\psi\rangle$$

$$\mathrm{W} = 2|\phi\rangle\langle\phi| - 1$$

$$\mathsf{V}|a\rangle = -|a\rangle$$

$$\mathsf{V}|\phi\rangle = |\phi\rangle - \frac{2}{2^{n/2}}|a\rangle$$

$$\mathsf{W}|a\rangle = \frac{2}{2^{n/2}}|\phi\rangle - |a\rangle$$

$$\mathsf{W}|\phi\rangle = |\phi\rangle$$

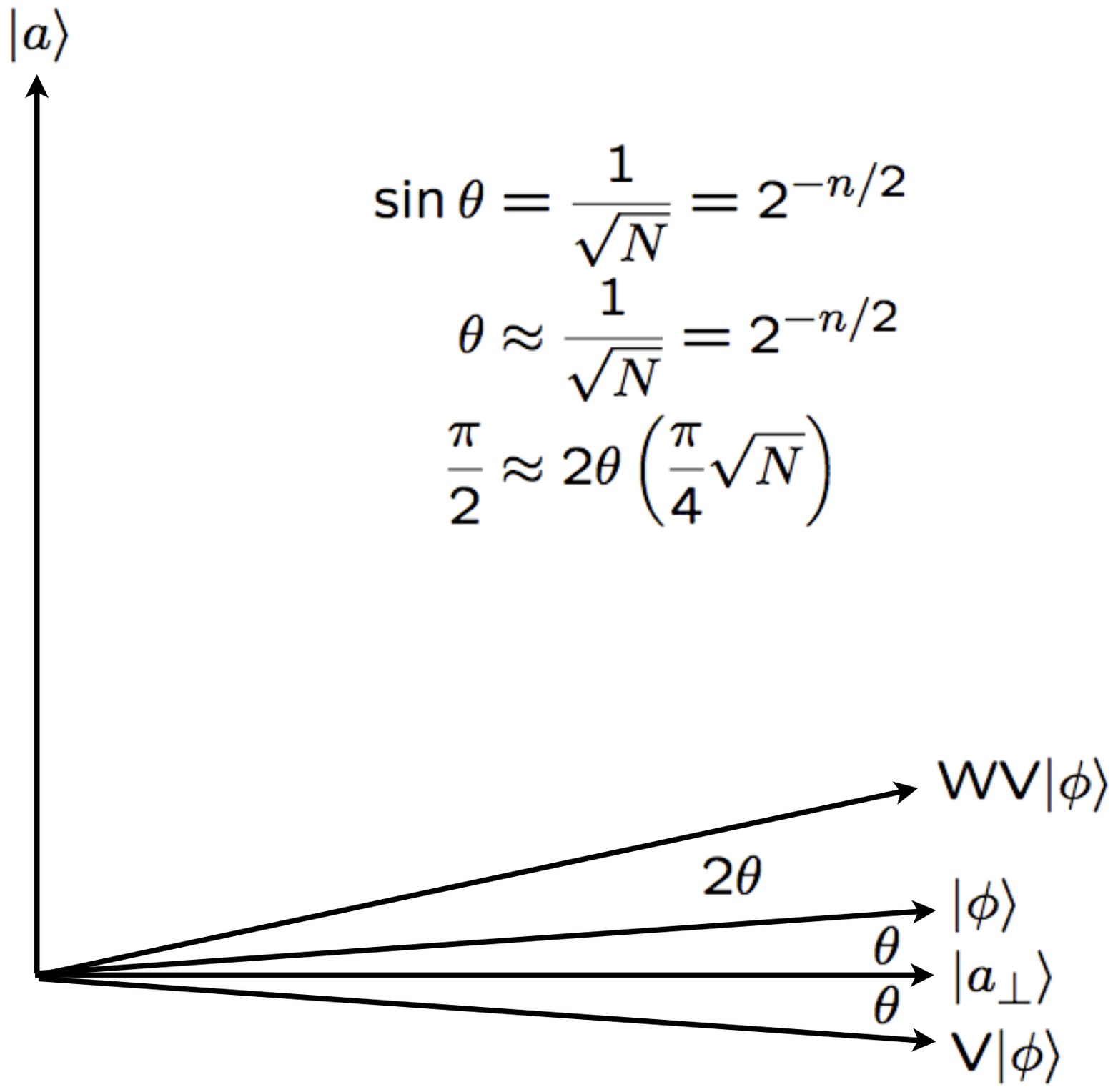
$$\langle a|\phi\rangle = \frac{1}{2^{n/2}} = \frac{1}{\sqrt{N}}$$

$$= \cos\gamma = \sin\theta$$

$$\sin\theta = \frac{1}{\sqrt{N}} = 2^{-n/2}$$

$$\theta \approx \frac{1}{\sqrt{N}} = 2^{-n/2}$$

$$\frac{\pi}{2} \approx 2\theta\left(\frac{\pi}{4}\sqrt{N}\right)$$



Grover's algorithm

1. Let

$$j = \left\lfloor \frac{\pi}{4} 2^{n/2} \right\rfloor = \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor$$

2. Compute $|\psi\rangle = (\mathsf{WV})^j |\phi\rangle$.

3. Reading $|\psi\rangle$ probably yields $|a\rangle$.

Quadratic speedup

Grover's algorithm takes $O(\sqrt{N})$ time.

Classical algorithms take $O(N)$ time.

Exponential speedup?

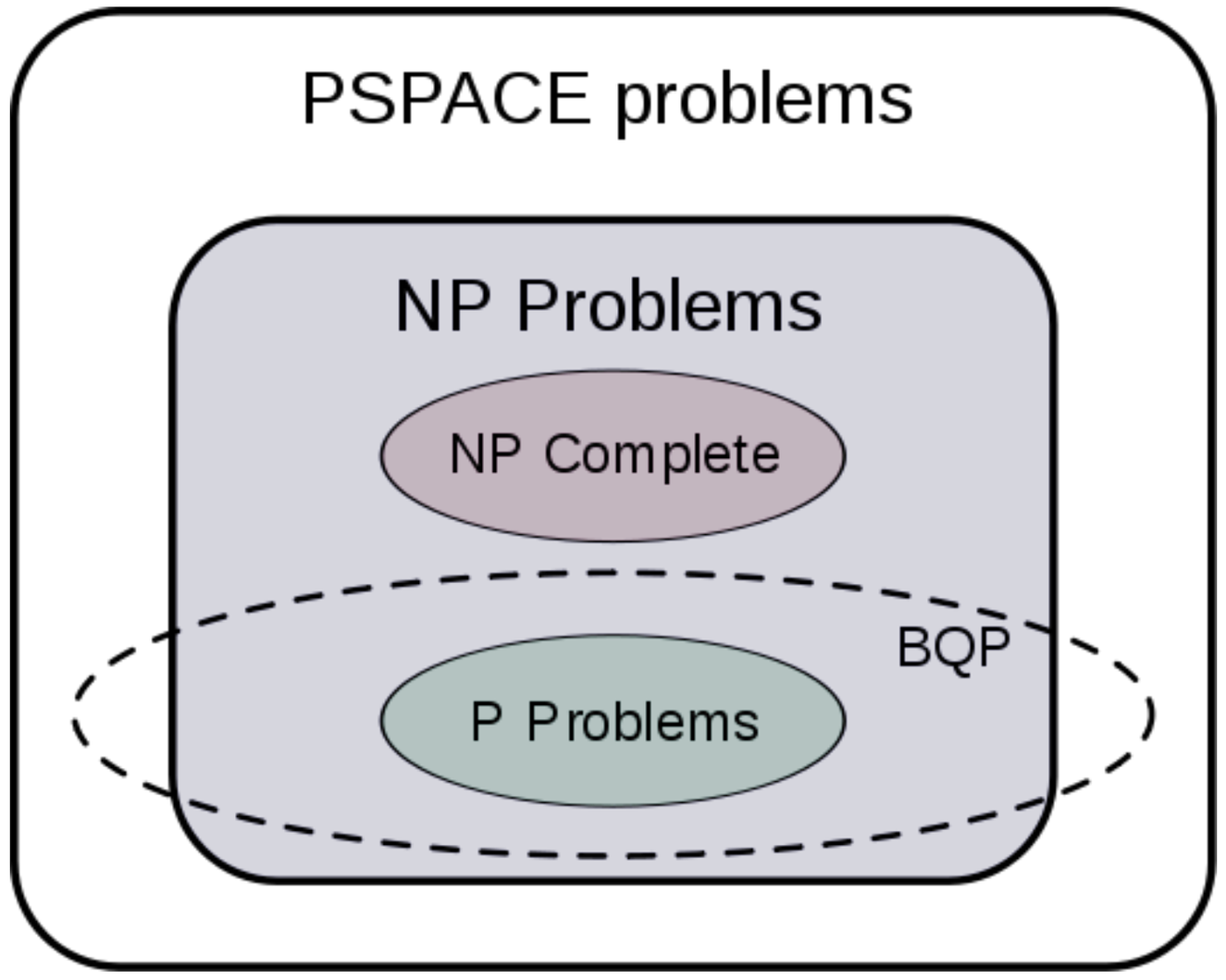
Period-finding is in BQP (Shor's algorithm).

So prime factorization is in BQP.

So RSA cipher-breaking is in BQP.

Classically, factorization is $O(1+\varepsilon)^b$ and is NP but is not believed to be NP-complete or P.

Computational complexity



Programming languages

QCL (Ömer, 1998)

QFC, QPL, cQPL (Selinger, 2004)

QML (Altenkirch, Grattage, 2005)

Quantum λ-calculus (van Tonder, 2004)

Challenges

Build quantum computers.

Design quantum circuits.

Invent quantum algorithms.

Resolve computational complexity classes.

References

N David Mermin. *Quantum Computer Science: An Introduction.* Cambridge University Press, 2007.