

Quantum Computing – Power and Limitations

Martin Rötteler

NEC Laboratories America
Princeton, U.S.A.

CES/HPC Workshop
Lehigh University

October 6, 2009



NEC Laboratories
America
Relentless passion for innovation



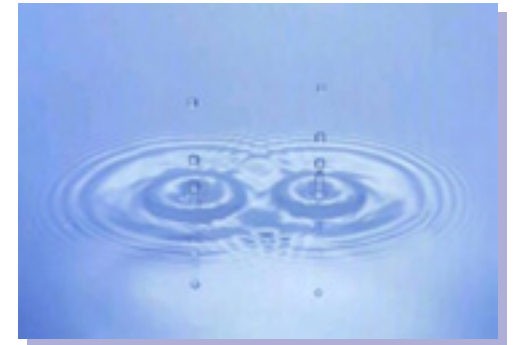
www.nec-labs.com

NEC Quantum Computing Research

Main goal: find quantum speedups!

■ Problem Definition

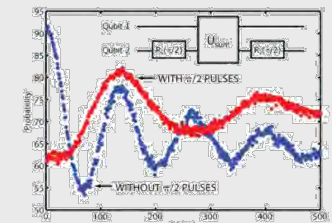
- Find problems of practical significance that a quantum computer can solve significantly faster than any classical computer. Ideally, we are looking for an **exponential** speedup.



■ Significance of Problem

- Quantum computers would make public key cryptography **insecure**, including RSA, DSA, elliptic curve cryptography, pairing based cryptography.
- Efficient **simulation** of quantum systems would be a major application for a quantum computer and a task for which any classical computer requires exponentially more time.

Quantum computer at NEC Tsukuba Lab:



Quantum Computer Technology

Nuclear magnetic resonance (12 qubits):



The qubits are nuclear spins of atoms such as C^{13} and H . Main players: U Waterloo, MIT, TU Munich.

Ion traps (7 qubits):










The qubits are the internal energy levels of several ions such as Ca^+ , Hg^+ , or Be^+ . Main players: NIST Boulder, U Maryland, U Innsbruck, MIT.

Superconductors (2 qubits):



The qubits are charge degree of freedom or magnetic flux of a Josephson Junction realized by superconductors. Main players: NEC Tsukuba, UCSB, Yale, U Delft.

Overview: Quantum Computer Technologies

Quantum system	Qubits	# Qubits	Scalable?
Liquid state NMR	magnetic moment	12 2005: 7	
Linear ion traps	energy levels of the ions	7 2005: 3	
Solid state NMR	magnetic moment	3 2005: 0	 / 
Josephson Junctions	Cooper pairs	2 2005: 2	
Quantum dots	electron spin	1 2005: 0	
Linear optics (KLM)	photon modes	0 2005: 0	

Example 1: Quantum Speedups

Problem: prime factorization of an n digit number

279978339112213278708294676387226016210 704467869554285375600099293261284001076 093456710529553608560618223519109513657 886371059544820065767750985805576135790 987349501441788631789462951872378692218 23983	=	353246193440277012127260497819846436867 119740019762502364930346877612125367942 3200058547956528088349	×	792586995447833303334708584148005968773 797585736421996073433034145576787281815 2135381409304740185467
--	---	--	---	--

Classical running time: $O(\exp(n^{\frac{1}{3}}(\log n)^{\frac{2}{3}}))$

Quantum running time: $O(n^2 \log n)$ [Shor 94]



Cryptography for internet commerce:

RSA

Digital signatures (RSA, elliptic curves)

Diffie-Hellman

Broken!



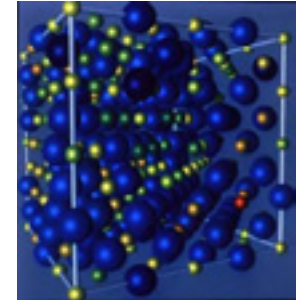
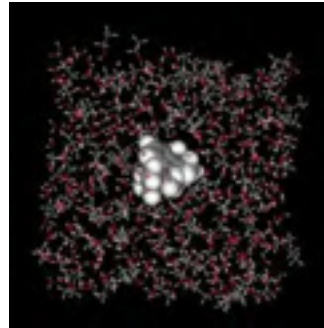
We study generalizations of this problem (“hidden subgroups”)



NEC Labs research made contributions to “post-quantum” crypto

Example 2: Simulation of Quantum Systems

- Why build a quantum computer if main application is of potential interest only to the NSA?
- “Killer application”: Simulation of quantum systems crucial to biology, chemistry, material science,



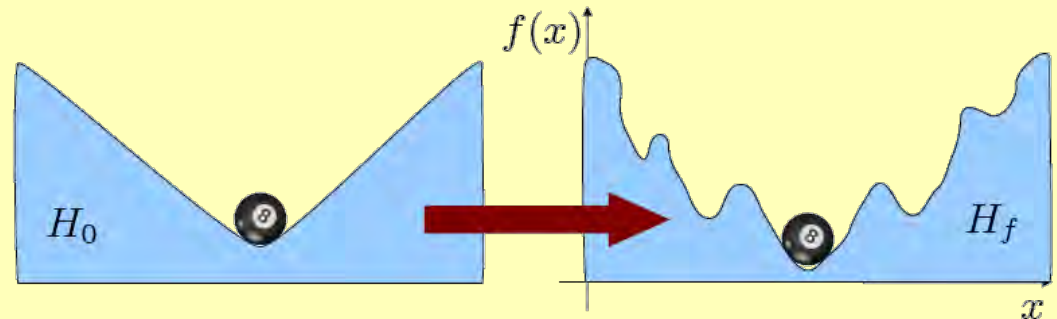
“How can we simulate quantum mechanics?...Can we do it with a new kind of computer...a quantum computer? It’s not a Turing machine but a machine of a different kind” Feynman, 1981

Example 3: Adiabatic Quantum Computing

Adiabatic paradigm:

- System Hamiltonian:

$$H = (1-t) H_0 + t H_f$$

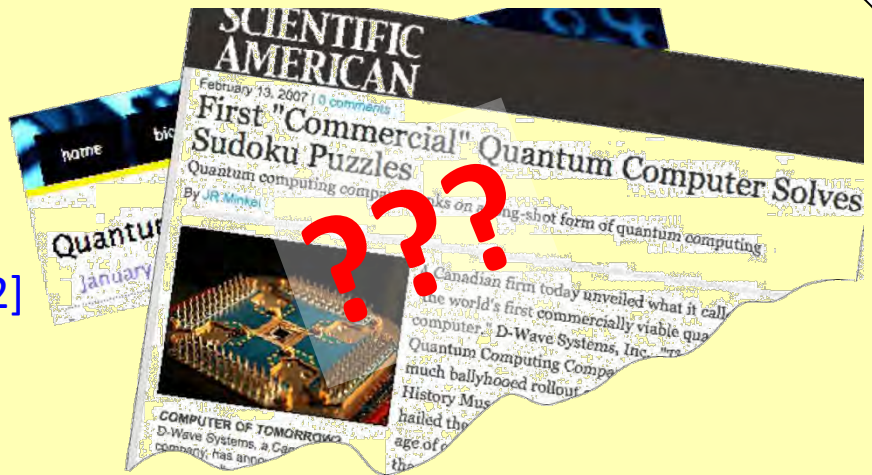


- Ground state of H_0 easily accessible
- Ground state of H_f encodes the solution to a problem

(This model is computationally equivalent to the “standard” model of quantum computing.)

NEC Labs result:

- Random instances of the NP complete Exact Cover problem cannot be solved by the standard adiabatic algorithm
[\[Altshuler, Krovi, Roland, arXiv:0908.2782\]](#)
- Methods used: Perturbation Theory, Anderson localization



Quantum Algorithm Pioneers

Peter Shor (1994):



He found quantum algorithms that allow to factorize integers and to compute discrete logarithms in polynomial time.

Lov Grover (1996):



He found a quantum algorithm which can search an element in a list of length N in $N^{1/2}$ steps.

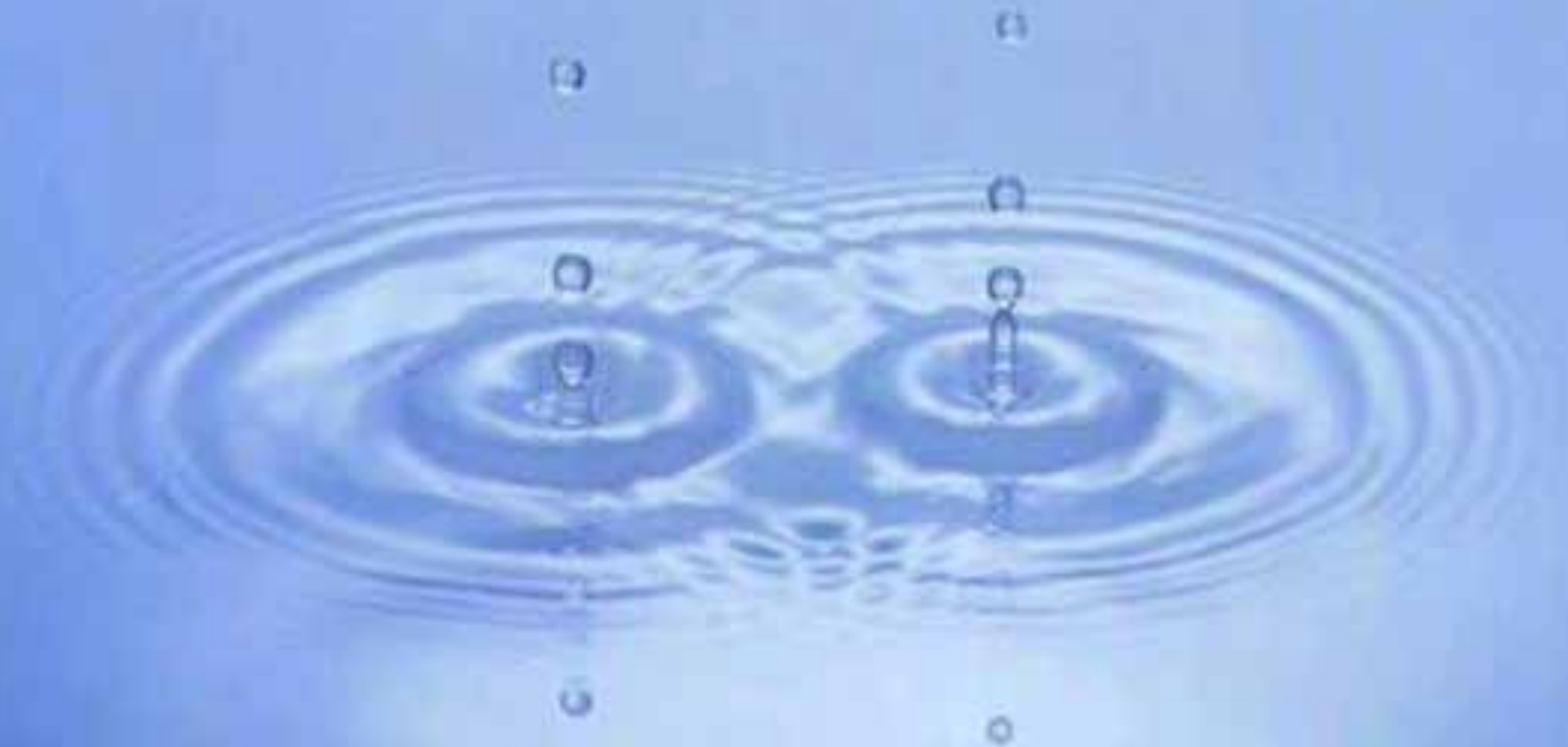
Some Developments in Quantum Algorithms

- Factoring, Discrete log [Shor 94]
- Unstructured search [Grover 96]
- Abelian hidden subgroup problems [Shor 94, Kitaev 95]
- Some non-abelian HSPs [Roetteler, Beth 98]
- Solving Pell's equation [Hallgren 02]
- Some hidden shift problems [van Dam, Hallgren, Ip 03]
- Graph traversal [CCDFGS 03]
- Spatial search [AA 03, CG 03/04, AKR 04]
- Element distinctness [Ambainis 03]
- Various graph problems [DHMM 04, MSS 03,...]
- Testing matrix multiplication [Buhrman, Spalek 04]
- HSP in Heisenberg groups [Roetteler, Sen 04, BCvD 05]
- Eigenvalue problems [Papageorgiou, Woźniakowski 05]
- Matching and network flows [Ambainis, Spalek 06]
- Approximate evaluation of the Jones polynomial [AJL 06]
- Limitations of coset states for GI [Hallgren, Roetteler, Sen 06]
- Evaluating NAND trees [FGG 07, ACRSZ 07]
- Hidden polynomial problems [CSV 07, DDW 07]
- Random bases for HSP [Radhakrishnan, Roetteler, Sen 07]
- ...

(bold = exponential speedup)

Power of Quantum Computing

The Power of Quantum Computing



The Fast Fourier Transform (FFT)

Definition: $\text{DFT}_N = \frac{1}{\sqrt{N}} \left[\omega_N^{k \cdot \ell} \right]_{k, \ell=0 \dots N-1}$, $\omega_N = e^{2\pi i/N}$

Cooley-Tukey FFT:

$$\text{DFT}_4 = \Pi_{rev} \cdot (\mathbf{1}_2 \otimes \text{DFT}_2) \cdot \text{diag}(1, 1, 1, i) \cdot (\text{DFT}_2 \otimes \mathbf{1}_2)$$

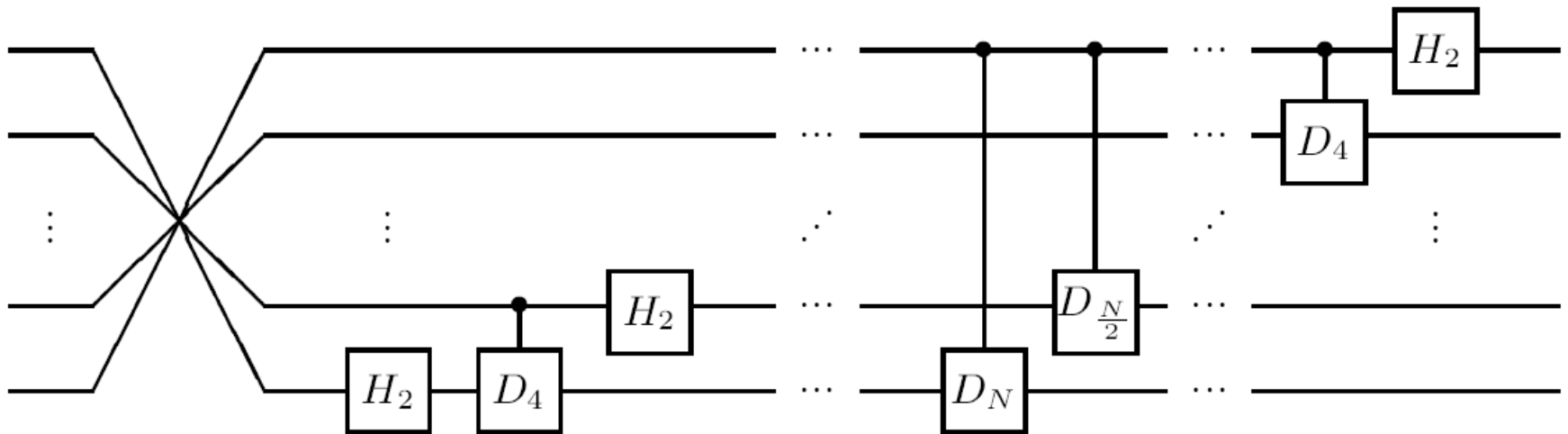
$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & & \\ & 1 & 1 & \\ & & 1 & -1 \\ & & & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & i \end{bmatrix} \cdot \begin{bmatrix} 1 & & 1 & \\ & 1 & & 1 \\ & & -1 & \\ & & & -1 \end{bmatrix}$$

Theorem: Multiplication with DFT_N can be performed classically in $O(N \log N)$ elementary operations.

We can do much better on a quantum computer!

Quantum Fast Fourier Transform

Quantum circuit for DFT_N



Cost:

Classical Computer

$$T(N) = 2T(N/2) + O(N)$$

$$T(N) = O(N \log N)$$

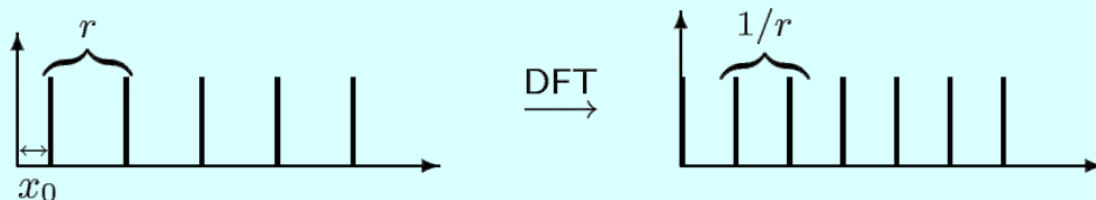
Quantum Computer

$$T(N) = T(N/2) + O(\log N)$$

$$T(N) = O(\log^2 N)$$

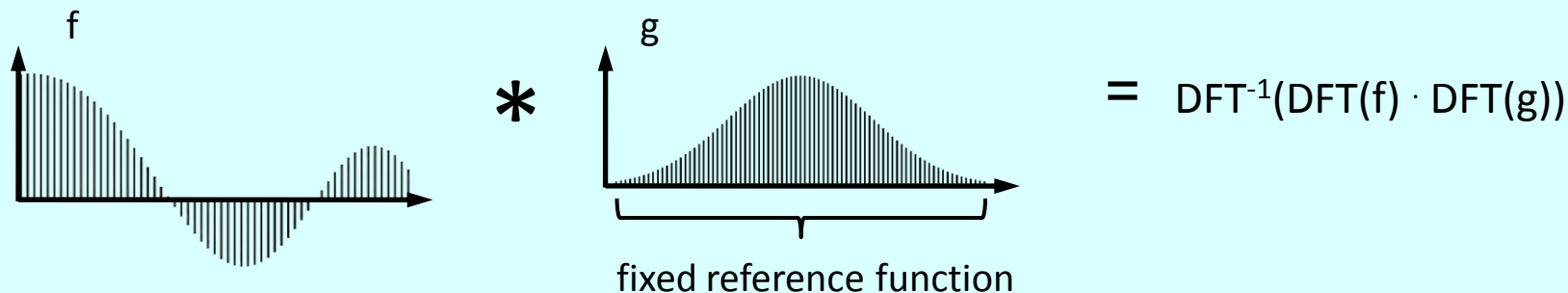
Applying the Quantum Fourier Transform

Shift invariance of the power spectrum:



How is this used? “Forget” information about coset. Used in factoring/order finding, dlog, [Shor’94], HSP [Kitaev’95], Pell’s equation [Hallgren’02], hidden radius problem [Childs, Schulman, Vazirani’07], ...

Convolution property:



How is this used? “Correlate” two functions. Used in hidden shift problem [van Dam, Hallgren, Ip ’03] for shifted Legendre symbol. Works for functions g with special properties only.

Other uses...: Phase estimation. And in a suitable sense, DFTs are even universal for QC [Aharonov, Jones, Landau ’06]

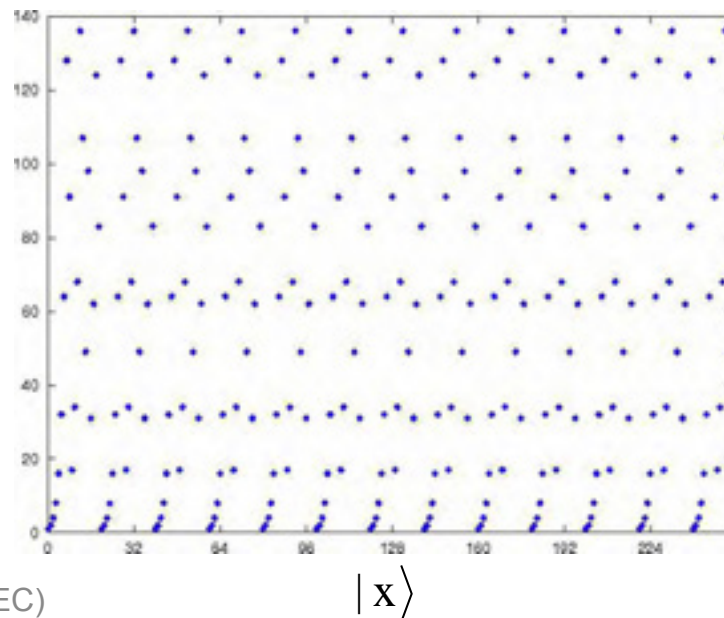
Factoring and Period Finding

- **Modular exponentiation:** Let N be an integer and let a be in Z_N . Modular exponentiation is the map $f(x) := a^x \bmod N$.
- **Facts:**
 - The map f can be implemented reversibly in $O(\text{poly}(\log N))$ operations.
 - The function $f(x) := a^x \bmod N$ is periodic with period r equal to the order of a modulo N , i. e., $f(x) = f(x + r)$ for all x .
 - The problem of factoring N can be reduced to period finding for modular exponentiation f (for random a).

- **Example:** graph of the function

$$f(x) = 2^x \bmod 165:$$

$$|y = f(x)\rangle$$



Quantum Period Finding

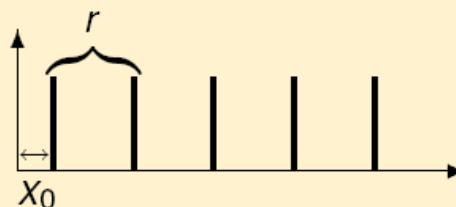
Computing the modular exponentiation

Let $f(x) = a^x \bmod N$ be modular exponentiation, let $M \gg N$, and compute:

$$|0\rangle |0\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{x \in \mathbb{Z}_M} |x\rangle |0\rangle \xrightarrow{f} \frac{1}{\sqrt{M}} \sum_{x \in \mathbb{Z}_M} |x\rangle |f(x)\rangle.$$

Collapsing this state

Now, measuring the second register will yield a random $s \in \mathbb{Z}_N$ in the image of f . The state collapses to (suppose that $r|M$)

$$\frac{1}{\sqrt{M/r}} \sum_{k=0}^{M/r-1} |x_0 + k \cdot r\rangle$$


This is an example of a coset state!

Period Finding and the Fourier Transform

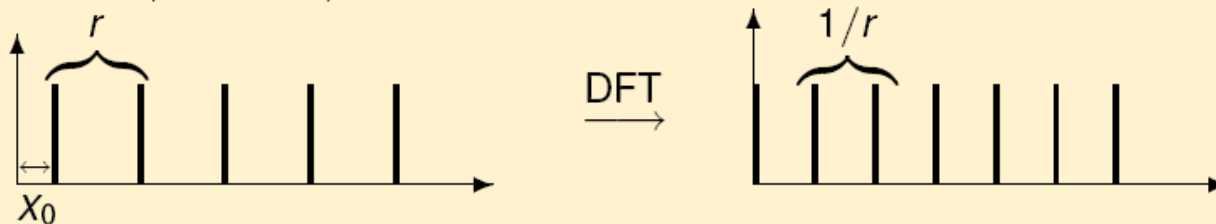
Coset state for the cyclic group

Let $G = \mathbb{Z}_M$, $x_0 \in G$, $H = \langle r \rangle$, where r is the order of a . Then:

$$|x_0 + H\rangle = \frac{1}{\sqrt{M/r}} \sum_{k=0}^{M/r-1} |x_0 + k \cdot r\rangle$$

Period finding (Shor'94)

Coset state $|x_0 + H\rangle$ and its Fourier transform:



Coset states in the abelian case

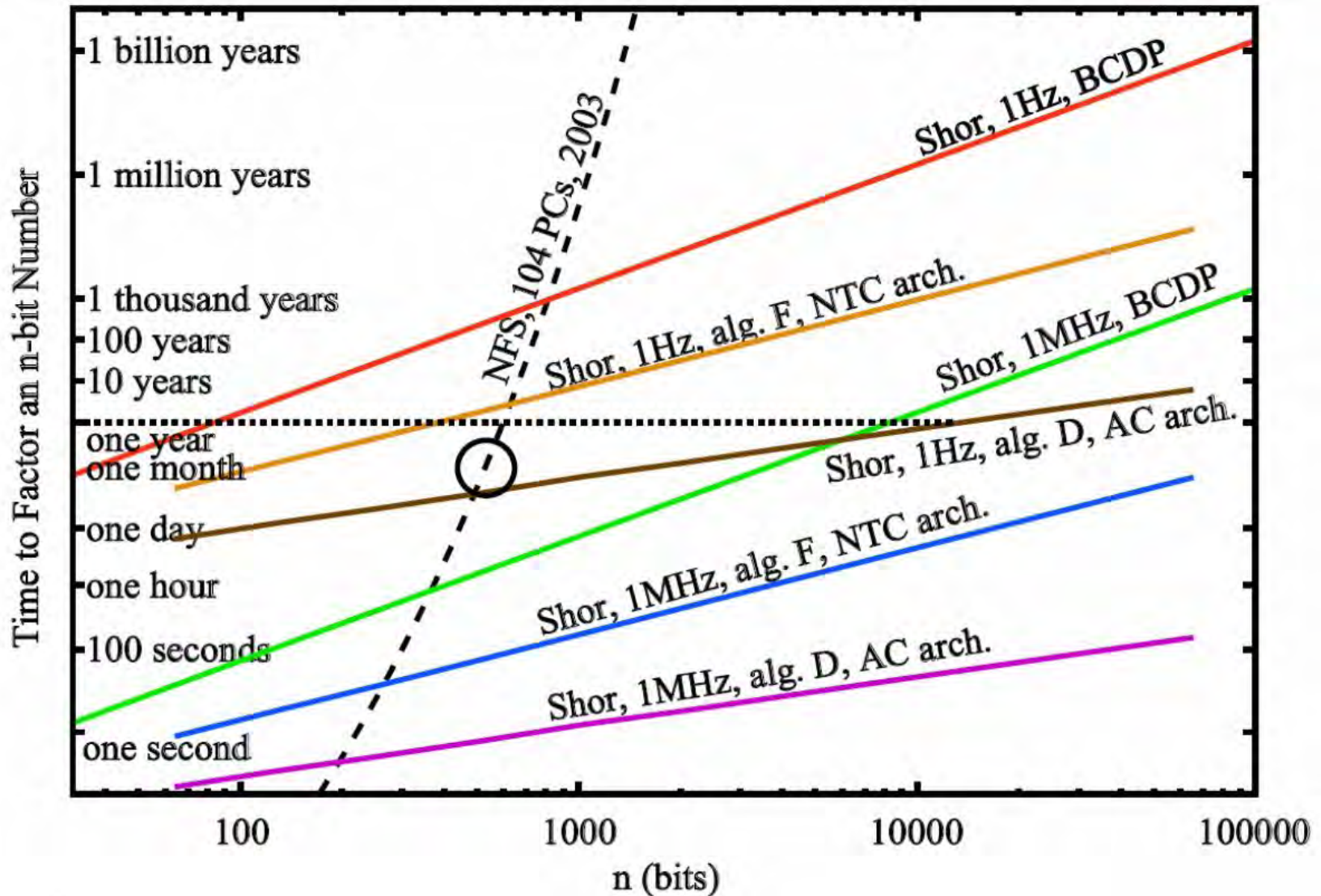
We can compute H efficiently from coset states!

Resource Requirements for Factoring

- **Number of qubits:** for n bit number, about $5n$ qubits are required (w/o error correction). With simple quantum error correction scheme (2 levels concatenation of a $[[7,1,3]]$ QECC), this becomes about $250n$.
- **Number of operations:**
 - **Modular exponentiation:** for an n bit number, using a simple implementation, $400 n^3$ ops are required (this can be improved to $n^2 \log n \log \log n$).
 - **Quantum Fourier transform:** for n bit number, about $15 n \log n$ ops.
- **Example ballpark figures:**

Task	#qubits	#operations
Factor 128 bit number	650 32500 (w/qecc)	8.4×10^8
Factor 1024 bit number	5200 260000 (w/qecc)	4.3×10^{11}
Search list of 2^{100} items	100 5000 (w/qecc)	10^{15}

The Need for Quantum Speed



The Hidden Shift Problem

Problem definition

- Given:** Finite group G , finite set R , maps $f, g : G \rightarrow R$
Promise: There is $s \in G$ such that $g(x) = f(x + s)$ for all x
Task: Find s .

Examples

- If f is a delta function, then finding s is the same as searching a list of 2^n items. This needs $\Theta(\sqrt{2^n})$ operations.
- There are functions f, g which lead to a better speedup, e. g., the Legendre symbol [van Dam, Hallgren, Ip'02]

$$f(x) = \left(\frac{x}{p}\right) = \begin{cases} 1 & : x \text{ is a square in } \mathbb{F}_p^\times, \\ -1 & : x \text{ is a nonsquare in } \mathbb{F}_p^\times, \\ 0 & : \text{if } x = 0. \end{cases}$$

- For Legendre symbol, s can be found efficiently by a quantum computer. However, no separation known.

Hidden Shifts: Correlation Method

Input: Let f and g be Boolean functions such that $g(x) = f(x + s)$. Assume $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$, respectively $|x\rangle \mapsto (-1)^{g(x)} |x\rangle$, are given.

Quantum algorithm:

- 1.) Initialize quantum register: $|0\rangle$
- 2.) Equal distribution on register: $\sum_{x \in \mathbb{Z}_2^n} |x\rangle$
- 3.) Compute g in superposition: $\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x)} |x\rangle$
- 4.) Compute DFT of this state: $\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
- 5.) “Uncompute $\hat{F}(w)$ ”:
 $\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} |w\rangle$
- 6.) Compute DFT of this state: $|s\rangle$
- 7.) Measure register: obtain s

Problem: how to “uncompute” if spectrum not flat?

Boolean Functions

The Hadamard transform

Let $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ be Boolean function. We associate with f the real valued function $F(x) = (-1)^{f(x)}$. Its Fourier transform is

$$\hat{F}(w) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} (-1)^{wx + f(x)}.$$

- **Boolean Fourier analysis has many applications**
 - Learning of DNF under uniform distribution
 - Characterization of juntas, AC^0 circuits
 - PCPs, etc.
- **Finite dimensional analogue of white Gaussian noise?**
 - Functions with many non-zero Fourier coefficients
 - Interesting from cryptographic point of view

Highly Non-Linear Functions

Bent functions

- A Boolean function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ is called *bent* [Rothaus76] if the Fourier coefficients satisfy $|\widehat{F}(w)| = 2^{-n/2}$ for all $w \in \mathbb{Z}_2^n$. Such functions are studied in cryptography.
- Necessary for existence is that n is even [Dillon75].
- If f is bent, then we obtain another bent function f^* via

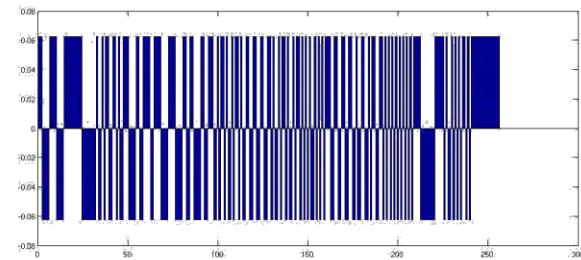
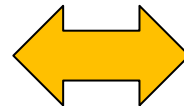
$$(-1)^{f^*(w)} := 2^{n/2} \widehat{F}(w).$$

By taking the dual twice we obtain f back: $(f^*)^* = f$.

Example: (here f is so-called Majorana-McFarland function)



f

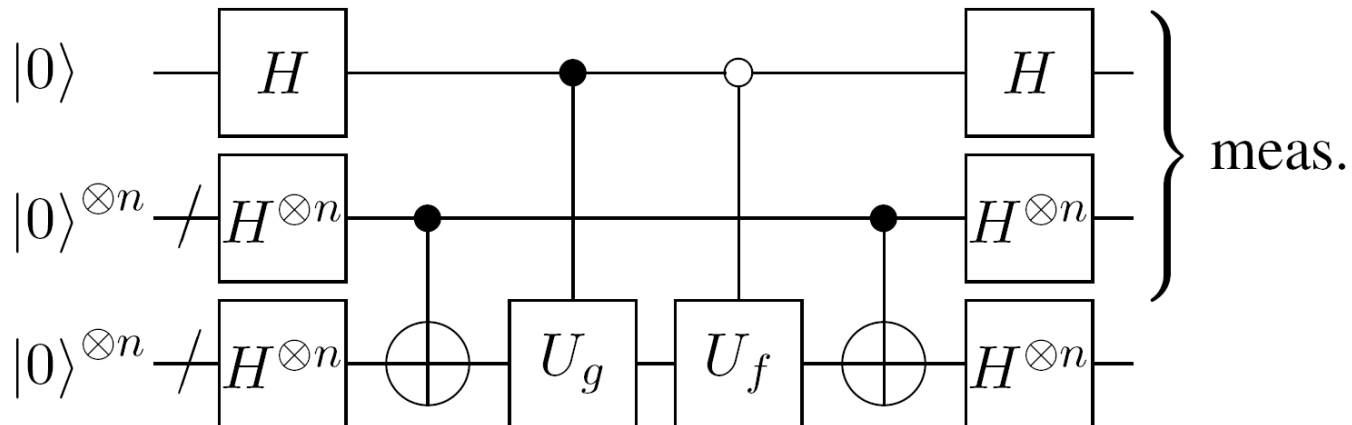


f^*

Finding Hidden Shifts: Method 2

Alternative: use reduction to abelian HSP

- In general for f, g injective, hidden shift can be reduced to a HSP.
- Not applicable here directly, since f, g are not injective. But reduction is possible using quantum functions $F : x \mapsto \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(x+y)} |y\rangle$
- Resulting quantum circuit:

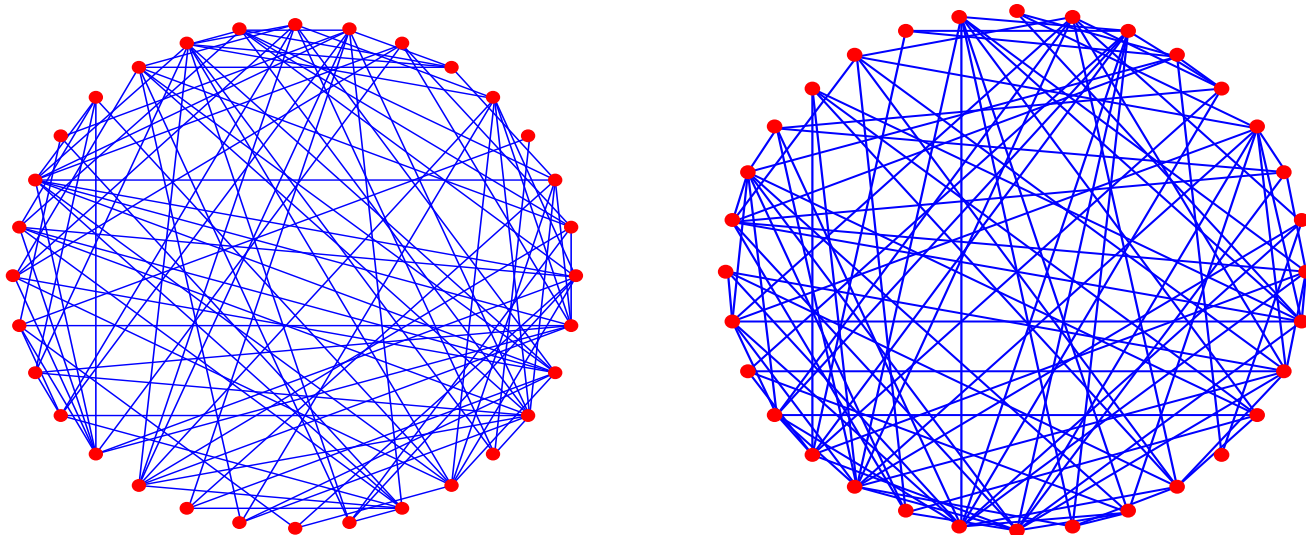


- This can be used to show an exponential separation in query complexity to find the hidden shift s , provided f and g are given as oracles. [R., SODA'10]

Limitations of Quantum Computing

The Graph Isomorphism Problem

Problem: decide whether two given graphs are isomorphic or not



- No polynomial time algorithm classical algorithm known
- Run-time of best classical algorithm is $2^{\sqrt{O(n \log n)}}$
- Probably not NP-complete (otherwise polynomial hierarchy collapses)
- Factoring sits in related class $NP \cap coNP$

The Hidden Subgroup Problem

Definition of the problem

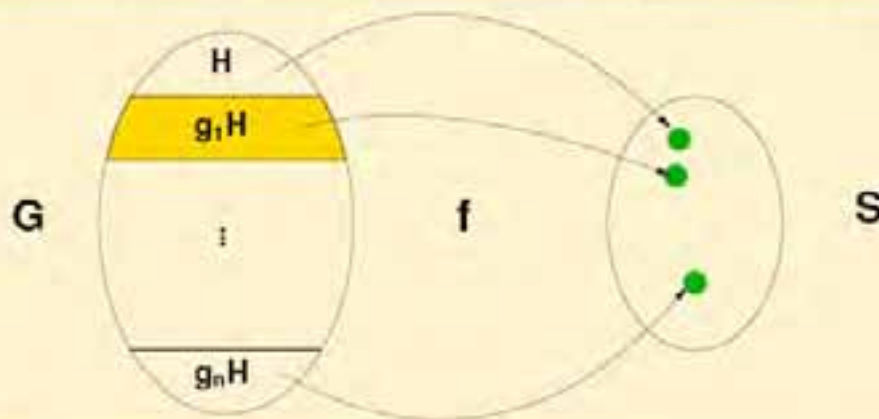
Given: Group G , set S , map $f : G \rightarrow S$ given as black box

Promise: There exists subgroup $H \leq G$ with

- f constant on each coset of H
- $g_1 H \neq g_2 H$ implies $f(g_1) \neq f(g_2)$

Problem: Find generators for H (input size: $\log |G|$)

Visualization of the cosets of H in G



Caveat

Difficulty of HSP depends crucially on the structure of the group G .

Hidden Subgroup Problems: Examples

Example: Shor's algorithm for integer factorization:

Goal is to factor n -bit integer N .

efficient q.alg.

- Group is $G = \mathbb{Z}$ (integers).
- For random a with $\gcd(a, N) = 1$, define $f(x) := a^x \bmod N$.
- Then $H = \{rx : x \in \mathbb{Z}\}$, where r is the order of a modulo N .
- Finding r allows to factor N in time $O(n^2 \log n \log \log n)$.

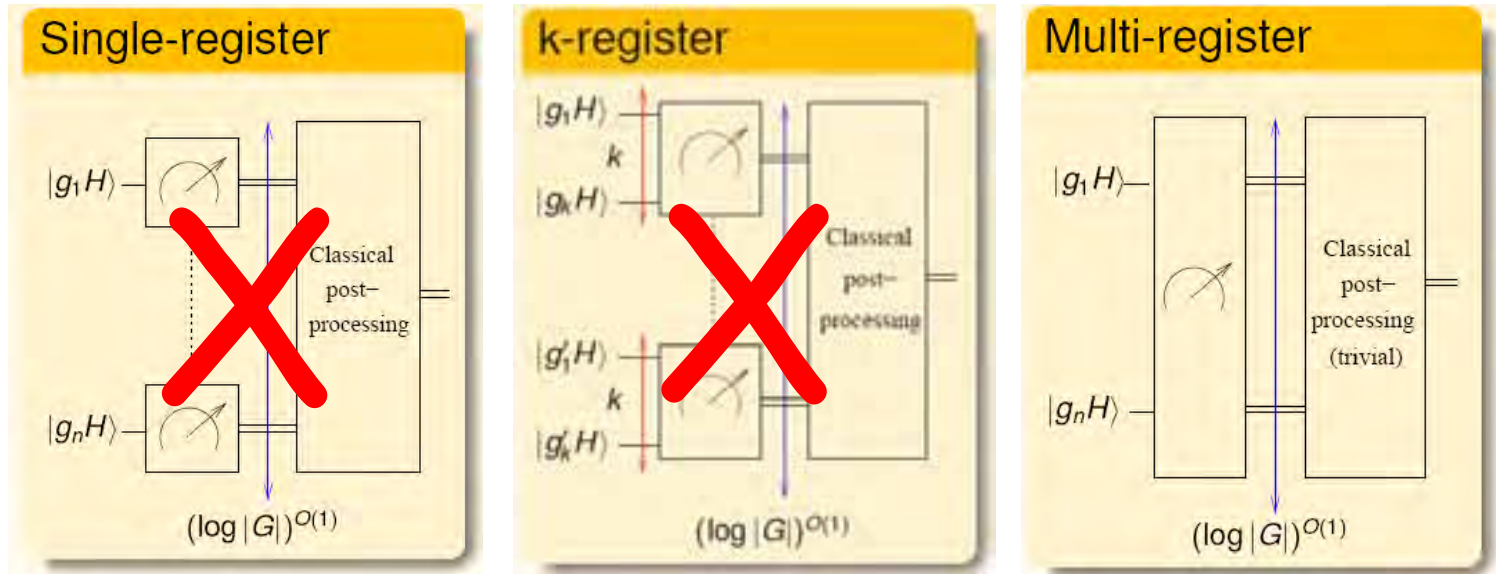
Other reductions to HSP problems:

- Discrete log [Shor'94]: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$
 - Pell's equation [Hallgren'02]: $G = \mathbb{R}$
 - Some lattice problems [Regev'02]: $G = D_n$
 - Graph isomorphism: $G = S_{2n}$
- efficient q.alg.**
- reduction only**

HSP captures most algorithms which give exponential speedup!

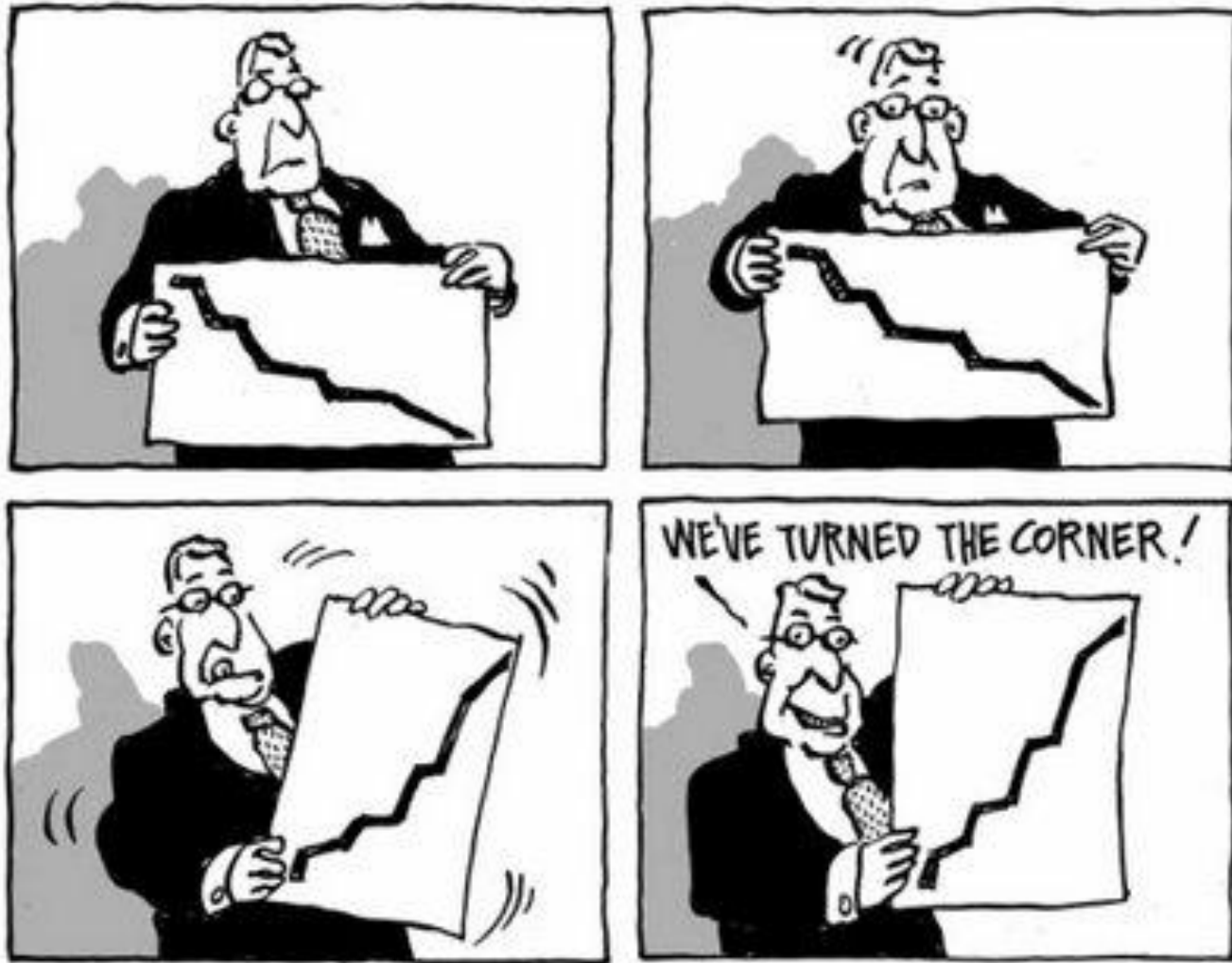
Limitations on Graph Isomorphism

- From single-register to multi-register quantum algorithms



- Result [Hallgren, Moore, R., Russell, Sen, STOC'06]:**
For graph isomorphism, the measurement has to be a joint measurement of $\Theta(n \log n)$ registers.
- Uses Fourier analysis over non-abelian groups, simple properties of geometry of Hilbert space, and the probabilistic method.

How to make use of this negative result?



Turning Lemons Into Lemonade

- **Goal:** Quantum resistant cryptography:
 - Create a cryptosystem that can be implemented efficiently on current (classical) computers.
 - Provide credible evidence that the cryptosystem will not be broken by quantum computers.
- **Good news:** Take random permutation π on n-bit strings and define one-way function on input x to be $\pi^{-1}(x)$. Then lower bound result by [\[Bennett, Bernstein, Brassard, Vazirani '93\]](#) implies that any quantum algorithm needs $2^{O(n)}$ queries.
- **Not so good news:** Not known how to do this efficiently.
- **Idea:** Come up with an efficient classical map such that inverting it implies an algorithm for graph isomorphism.



Turning Lemons Into Lemonade (cont'd)

- **Quantum resistant 1-way function** [Moore,Russell,Vazirani '07]
 - Fix m random vectors $V = \{v_1, \dots, v_m\}$ in $GF(p)^n$
 - The secret information to be mapped is an $n \times n$ matrix M .
 - Output the unordered set $\{M v_1, \dots, M v_m\}$.
 - Choose $m = n + O(\log^2 n)$. Hence, map n^2 bits to nm bits.
- **Properties of this function:**
 - Efficiently computable: map is matrix multiplication.
 - Reconstructing M is at least as hard as graph isomorphism due to [Petrank, Roth '97]. This holds true even for a polynomial fraction of whole space.
 - Construction closely related to McEliece cryptosystem.
 - For V and M uniform at random this corresponds to a HSP that is hard in the sense of [Hallgren, Moore, Roetteler, Russell, Sen, STOC'06].

“Post-Quantum” Cryptography?

- If a scalable quantum computer exists:
 - RSA is broken [Shor'94].
 - Elliptic curve systems are broken [folklore].
 - Buchmann-Williams system is broken [Hallgren'02].
- Cryptosystems that possibly are still secure:
 - McEliece public key system, HFE, etc.
 - Regev's lattice based public key system.
- Quantum-resilient classical cryptography:
 - One-way function secure against quantum attacks was introduced in [Moore, Russell, Vazirani '07].
 - Relies on limitations for quantum algorithms for the graph isomorphism problem [Hallgren et al '06].
- Quantum cryptography:
 - Uses quantum mechanics to generate a secret key.

Conclusions

- **Motivation**
 - Quantum computing
 - Quantum algorithms and the Fourier transform
- **Power of quantum computing**
 - Period finding and hidden subgroup problem
 - Correlations and hidden shift problem
- **Limitations of quantum computing**
 - Multi-register algorithms and tensor products
 - The trouble with graph isomorphism

- **Acknowledgment of support:**

