KITP Colloquium
2-25-04

Quantum Algorithms

MITCTP group

Andrew Childs
Enrico Deotto
Edward Farhi
JG
Sam Gutmann
Andrew Landahl
James McBride

1) Complexity Classes
P, NP, QMA
2) Shor and Grover
3) Quantum Walk algorithms
4) Adiabatic algorithms

NOT

Building computers

Controlling and correcting errors

Simulation of physics

Entanglement

Communication (Alice and Bob)

(1)

The class (of decision problems)

NP

Standard model of classical Computer is Turing Machine

Input: bit string (code)

Output: YES or NO (or runs forever)

Poly time machine gives YES or NO after n^k steps.

(2)

Problem is in P if there is a poly time machine for it.

Example: 2-SAT

Is there a bit string $\{z_1 z_2 \cdots z_n\}$ SATisfying a set of constraints.

Each constraint (clause) involves 2 bits z_i, z_j and excludes 1 pair of values (00, 01, 10, 11) — frustration.

(3)

Code constraints as bit string.

Poly time machine gives YES if and only if constraints are satisfiable.

[Machine ACCEPTS the LANGUAGE L which consists of the codes for all satisfiable INSTANCES of the PROBLEM 2-SAT]

(4)

$L_{2\text{-SAT}} \in P$

Replace 2 by 3 : 3-SAT

No known poly time machine

i.e polynomial algorithm.

Instead (Cook-Levin theorem)

3-SAT is NP-complete.

[NP stands for nondeterministic polynomial]

(5)

Roughly, NP can be checked in poly time.

Language $L \in NP$ iff there is a machine, poly time, input all pairs of bit strings (x, y) $|y| < |x|^k$

and $x \in L$ if $\exists\, y$ with

$(x, y) \rightarrow$ YES

(6)

SAT $\in$ NP

M checks if y satisfies x

NP-complete:

Problem is NP-complete if it is in NP and every problem in NP can be reduced to it in polynomial time.

So a polytime algorithm for 3-SAT would solve all NP in polytime

(7)

[See Cook's note on P versus NP on Clay institute web-site]

QUANTUM analogue of TM is circuit model of quantum computer:

Set of gates, each operates on a few q-bits by a unitary transformation chosen from some standard set.

(8)

Analogue of NP is QMA (Kitaev)

x is a state $|x_1 x_2 \cdots x_n\rangle$ of n q-bits.

y is a state $|y\rangle$ of n^k q-bits.

M is a poly time quantum machine

(9)

If $x \in L$, $\exists\ |y\rangle$ such that

$M\{|x\rangle|y\rangle\} = 0$ with probability $> \frac{2}{3}$

If $x \notin L$, for any $|y\rangle$

$M\{|x\rangle|y\rangle\} = 0$ with probability $< \frac{1}{3}$

Kitaev found a QMA-complete problem:

(10)

Hamiltonian $H = H_1 + H_2 + \cdots + H_r$

Each H_i operates on 3 q-bits.

PROMISE that smallest eigenvalue is either < 0 or $> \frac{1}{n^k}$

Determine which.

(All numbers given by n bits)

(11)

Period determination

Used by Shor to factorize.

A predecessor (Simon)

$y = F(x)$ is a function from $(Z_2)^n$ to $(Z_2)^n$

i.e. x and y are n-bit strings

[Shor replaces $(Z_2)^n$ by Z_{2^n}]

F depends only on $x_{i_1} \cdots x_{i_m}$ and takes 2^m different values

(12)

Want to find $i_1 \ldots i_m$

[Special case of 'hidden coset' problem.

Shor needs to find period

$f(0)\, f(1) \cdots f(r-1)$ all different,

then f repeats: r is a factor of N]

Function is available in the form of unitary transformation

$$|x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$$

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_x |x\rangle|f(x)\rangle$$

(13)

Measure second register

f depends only on $x_1 \ldots x_m$

Get $\frac{1}{2^{\frac{n-m}{2}}} \sum_{x_{m+1} \ldots x_n} |\hat{x}_1 \ldots \hat{x}_m\, x_{m+1} \ldots x_n\rangle$

for some random $\hat{x}_1 \ldots \hat{x}_m$.

Now do Hadamard transform on each bit $U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

First m bits, get $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$

Bits $m+1$ to n get $|0\rangle$

Measure $\{Z_j\}$, and repeat.

14

[Shor replaces Hadamard by Fourier transform.

Quantum FFT ($2^n \times 2^n$ matrix) takes n^2 steps instead of classical $n \times 2^n$]

$$\langle r|\mathcal{F}|s\rangle = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} rs}$$

$N = 2^n$ $\quad r, s = 0, 1, \ldots N-1$

15

GROVER: search for a marked state [bit structure irrelevant]

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

$f(w) = -1$, $f(x) = +1$ $\quad x \neq w$

[Oracle] $\quad U_w = 1 - 2|w\rangle\langle w|$

Find $V_1 V_2 \cdots V_k$ not depending on w such that

$$V_k U_w V_{k-1} U_w \cdots V_1 U_w |s\rangle = |w\rangle$$

(16)

Grover's solution is

$$|s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$V_1 = V_2 = \cdots = 1 - 2|s\rangle\langle s|$$

Calculate in 2 dimensional Hilbert space of $|s\rangle$, $|w\rangle$ $\left[\langle w|s\rangle = \frac{1}{\sqrt{N}}\right]$

VU is rotation by 2δ (and multiply by -1)

$$\sin\frac{\delta}{2} = \frac{1}{\sqrt{N}}$$

(17)

So takes $O(\sqrt{N})$ queries of oracle instead of classical $O(N)$.

Best possible (proved first)

[Compare to classical information theory proof that it takes N: replaces L_1 norm by L_2 norm]

(18)

QUANTUM WALKS

EF, SG qu-ph/9612026

EF, SG qu-ph/9706062

AMC, EF, SG qu-ph/0103020

AMC, ED, EF, SG qu-ph/0209131
Richard CLEVE, Daniel SPIELMAN

AMC, JG qu-ph/0306054

AMBAINIS, KEMPE, RIVOSH qu-ph/0402107

AMC, JG coming shortly

(19)

CLASSICAL random walk on graph

(continuous time)

Nodes $a, b, c \cdots$

Prob $K_{ab}\, dt$ 

$$\frac{d}{dt} P_a = \sum_{b \neq a} K_{ab} P_b - \left(\sum_{b \neq a} K_{ba}\right) P_a$$

$$= \sum_b K_{ab} P_b$$

$K_{ab} \geq 0 \quad a \neq b, \quad \sum_b K_{ba} = 0$

$$\Rightarrow \frac{d}{dt} \sum_a P_a = 0$$

20

On graph, $K_{ab} = \gamma$ if $ab \in G$

$K_{ab} = K_{ba}$; $K_{aa} = -\gamma d(a)$

G will have $d(a)$ small, K sparse

QUANTUM walk on G.

Hilbert space basis $|a\rangle$

Hamiltonian H

$\langle a|H|b\rangle = K_{ab}$ $a \neq b$

$\langle a|H|a\rangle = 0$

21

$K_{ab} = K_{ba}$ makes probability conserved.

$$i \frac{d}{dt} \langle a|\psi\rangle = \sum_{b \neq a} K_{ab} \langle b|\psi\rangle$$

$$P_a = |\langle a|\psi\rangle|^2$$

Time evolution very different

Example 1)

CLASSICAL $\frac{d}{dt}(P_a - P_b) = -2\gamma(P_a - P_b)$

$P_a \to \frac{1}{2}$, $P_b \to \frac{1}{2}$

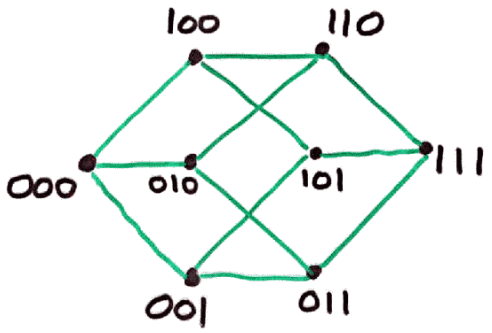
22

QUANTUM $(t=0,\ P_a=1)$

$$P_a = \cos^2 \gamma t\ ,\quad P_b = \sin^2 \gamma t$$

So after time $\frac{\pi}{2\gamma}$, $P_b = 1$

Example 2) Hypercube with $N=2^n$ nodes



23

n independent c-bits or q-bits

Start at $00\cdots0$ at $t=0$

CLASSICAL $P_{11\cdots1} = \left(\frac{1-e^{-2\gamma t}}{2}\right)^n \to \frac{1}{N}$

QUANTUM $P_{11\cdots1} = (\sin \gamma t)^{2n}$

$= 1$ at $t = \frac{\pi}{2\gamma}$

Another way of looking at this.

P or ψ depend only on

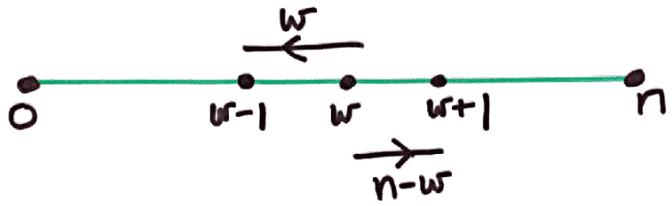
$$w = i_1 + i_2 + \cdots + i_n$$

(Hamming weight)

24

Reduce to walk on line

CLASSICAL



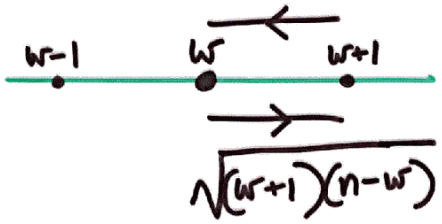
$$\frac{1}{\gamma}\frac{d}{dt}P(w) = (w+1)P(w+1) + (n-w+1)P(w-1) - nP(w)$$

$$P(w) \longrightarrow \binom{n}{w}\frac{1}{2^n}$$

Get stuck near $w = \frac{n}{2}$

25

QUANTUM



$$\frac{i}{\gamma}\frac{d}{dt}\psi(w) = \sqrt{(w+1)(n-w)}\,\psi(w+1) + \sqrt{w(n-w+1)}\,\psi(w-1)$$

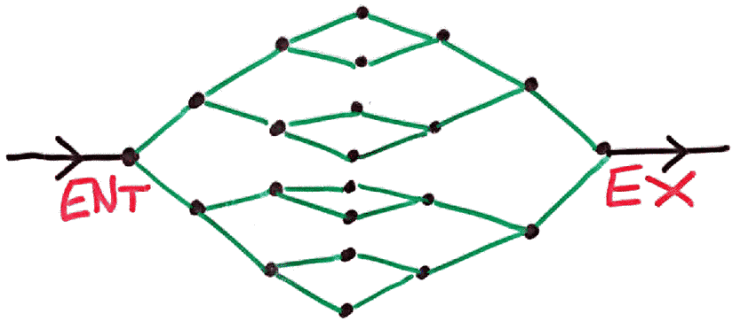
$$P(w) = |\psi(w)|^2 = \binom{n}{w}[\cos^2\gamma t]^{n-w}[\sin^2\gamma t]^w$$

$$\langle w \rangle = n\sin^2\gamma t$$

(26)

Example 3)

Back to back trees:



CLASSICAL walk drives to center

QUANTUM walk reduces to

(27)

Turn this into an ORACULAR problem.

Black box: INPUT – name of node

OUTPUT – names of neighbors

Names chosen from big set

Problem: Given name of ENTrance, find name of EXit

Complexity: Number of queries

28

CLASSICAL random walk
takes N queries —
get stuck in middle.

QUANTUM walk Hamiltonian
evolution can be implemented
using quantum oracle.

[We think in continuous time
using H
Can translate into circuit model
to implement e^{-iHt}]

29

Propagator on discrete line is

$$\langle n|e^{-iHt}|m\rangle = J_{|n-m|}(t)$$

$$J_n(n) \sim n^{-\frac{1}{3}}$$

Line with ends introduces reflections

Run for time n and repeat
n times will give high
probability of finding exit.

30

BUT a little ingenuity makes classical walk work.

Do not reset node — reach center in n moves.

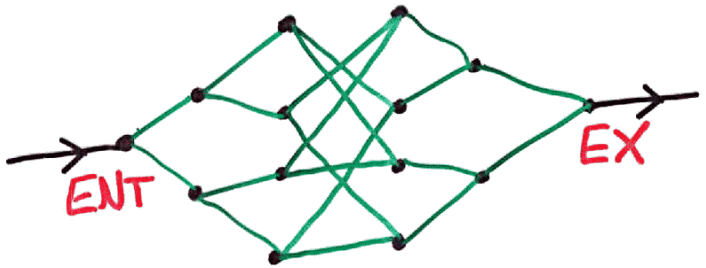
Check degree to see if you are at center.

If back at center after $2k$ moves you turned round after k.

31

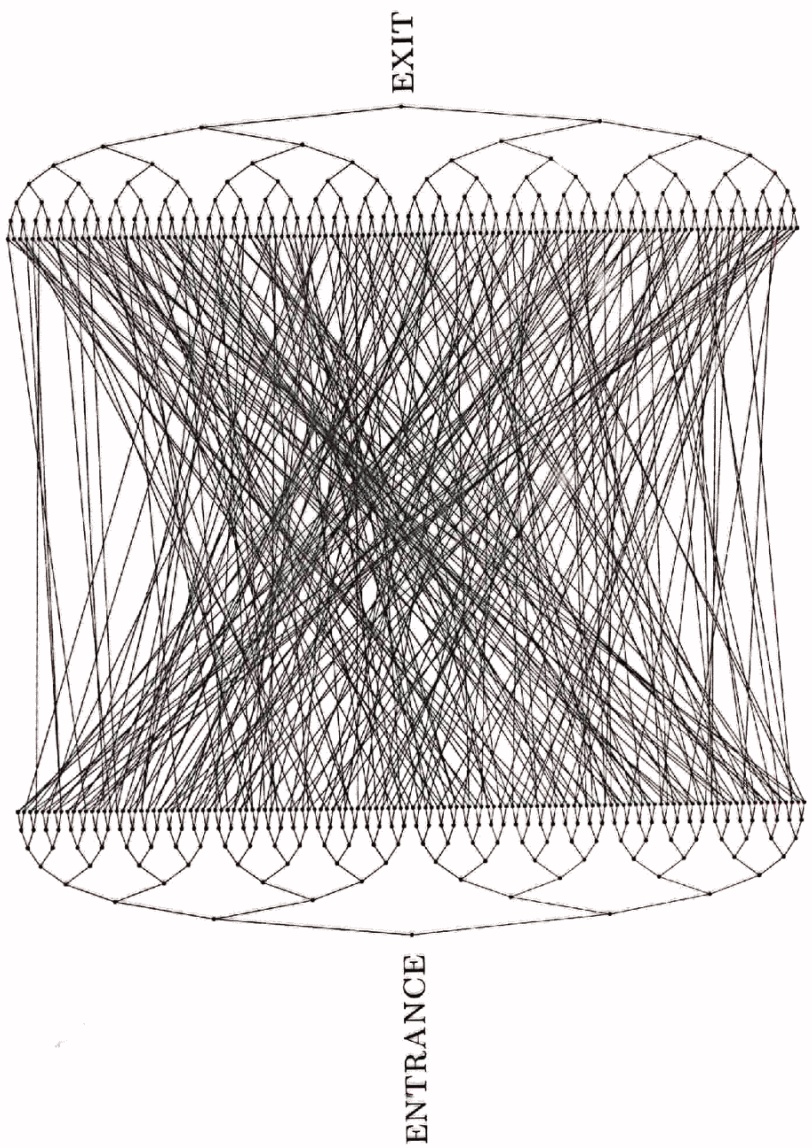
Find modification:

Randomize connections at center



Every node has degree 3 except entrance and exit.

In center have a random cycle alternating left and right



32

Now Spielman proved that

"any classical algorithm that makes at most $2^{n/6}$ queries finds exit with probability at most $4 \times 2^{-\frac{n}{6}}$,

33

But quantum walk in sector of Hilbert space where ψ is same for all nodes in a column still reduces to

Defect in center just gives extra reflexions

Find for $t = 2n$, (2^n nodes in center)

$$|\langle exit|e^{-iHt}|entrance\rangle|^2 \sim n^{-2/3}$$

34

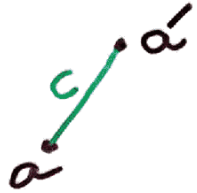
Implementation:

Color edges of graph so that no 2 edges at a node have same color. (Only a few colors)

CLASSICAL oracle

Input: name of node a, color c

Output: $U_c(a) = a'$



$$U_c[U_c(a)] = a$$

35

QUANTUM oracle:

Unitary transformations U_c

$$U_c|a, b\rangle = |a, b \oplus f_c(a)\rangle$$

a, b are bit-strings

$\oplus$ means bit-wise + mod 2

In circuit model of quantum computer, can simulate evolution by H,

$$H|a, 0\rangle = \sum_c |f_c(a), 0\rangle$$

36

SEARCH ON A GRAPH

Problem is to find a marked node w (like Grover),

using a walk on a d-dimensional toroidal lattice with N nodes

$$H = -\gamma L - |w\rangle\langle w|$$

L is the Laplacian

$$L|x\rangle = \sum_e |x+e\rangle - 2d|x\rangle$$

37

Start in state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

and evolve for time t.

$\gamma = 0$ Ground state is $|w\rangle$

$\gamma \to \infty$ Ground state is $|s\rangle$

? 'Phase transition' value of γ

with 2 eigenstates of H

Linear combinations of $|s\rangle, |w\rangle$

and $\Delta E \sim N^{-\frac{1}{2}}$

38

Example:

$$H = 1 - |s\rangle\langle s| - |w\rangle\langle w|$$

[$1 - |s\rangle\langle s| = -\frac{1}{N} L$ where L is Laplacian of complete graph i.e. every pair of nodes connected]

$\langle w|s\rangle = N^{-\frac{1}{2}}$ so

$|s\rangle \pm |w\rangle$ are eigenstates of H with $E = \mp N^{-\frac{1}{2}}$

and $|s\rangle$ evolves into $|w\rangle$ after $t = \frac{\pi}{2} N^{1/2}$

(39)

This is continuous time analogue of Grover.

Can't do better than $N^{1/2}$.

On d-dimensional lattice, eigenvalues are solutions of

$$F(E) = 1$$

$$F(E) \equiv \frac{1}{N} \sum_k \frac{1}{\gamma \mathcal{E}(k) - E}$$

$$\mathcal{E}(k) = 2 \sum_{i=1}^{d} (1 - \cos k_i)$$

$$k_i = 2\pi m_i N^{-\frac{1}{d}}, \quad m_i = 0, 1, \cdots N^{\frac{1}{d}} - 1$$

(40)

Lowest values of $\mathcal{E}(k)$ are

$$0, \quad (2\pi)^2 N^{-2/d}$$

What happens depends on infrared behavior of sums

$$S_{j,d} = \frac{1}{N} \sum_{k \neq 0} \frac{1}{[\mathcal{E}(k)]^j}$$

$d > 2j$ $\quad S_{j,d} = \frac{1}{(2\pi)^d} \int_{-\pi}^{\pi} \frac{d^d k}{\mathcal{E}(k)^j}$

$d < 2j$ $\quad S_{j,d} = N^{\frac{2j}{d}-1} \frac{1}{(2\pi)^{2j}} \sum \frac{1}{(m^2)^j}$

(41)

$d=2j$, $S_{j,d} = \frac{\ln N}{(4\pi)^j j!} + O(1)$

Find a critical value of $\gamma = \gamma_c$

$= S_{1,d}$ which is

$O(1)$ in $d \geq 3$, $O(\log N)$ in $d=2$

$\gamma > \gamma_c$ $|s\rangle$ is ground state

$\gamma < \gamma_c$ $|s\rangle$ is first excited state

so unless γ is fine-tuned

close to γ_c state stays near $|s\rangle$

(42)

Find that critical dimension is

$d = 4$

In $d > 4$, 2 eigenvalues

$E = \pm c N^{-\frac{1}{2}}$ $\left(N^{-\frac{1}{2}} \ll N^{-\frac{2}{d}}\right)$

and $|\langle w| e^{-iHt} |s\rangle|^2$ is $O(1)$

for $t = \frac{\pi}{2c} N^{1/2}$

In $d=4$ $|\langle w| e^{-iHt} |s\rangle|^2$ is $O\left(\frac{1}{\log N}\right)$

for $t = a(N \log N)^{1/2}$

In $d<4$, no success

(43)

Aaronson and Ambainis (qu-ph/0303041) give a recursive algorithm for $d \geq 2$.

Can lower critical dimension to 2 by using Dirac walk.

$$H = H_D - [|w\rangle\langle w| \otimes \beta]$$

$$H_D = a \sum_{i=1}^{d} \alpha_i \sin k_i + b\beta \sum_{i=1}^{d} (1 - \cos k_i)$$

(44)

This is a walk:

e^{ik_i} sends x_i to $x_i + 1$

[$|k_i| < \pi$ because x_i integer

$\Delta k_i = 2\pi N^{-1/d}$ because $x_i + N \equiv x_i$]

Ambainis et al find discrete time version of same algorithm — they have to use a 'coin' to get a quantum walk.

(45)

ADIABATIC ALGORITHMS

EF, JG, SG and Michael SIPSER quant-ph/0001106

et al quant-ph/0104129

Turn SAT problems into finding ground state of H by defining

H = cost.

(45)

Exact cover 3 : $Z_i + Z_j + Z_k = 1$

i.e only 100, 010, 001 satisfy

These are NP complete problems.

Need to generate ensembles of hard instances.

e.g. add clauses until there is a unique satisfying assignment.

(47)

Set of n spins $\vec{\sigma}_i$, $\sigma_i^z = 1 - 2z_i$

Problem is to put system in ground state of

$$H_P = \sum_C h_C(\sigma_i^z \sigma_j^z \cdots)$$

where h_C takes values 0 or 1

Method is to turn off a transverse magnetic field.

(48)

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \frac{t}{T} H_P$$

$$H(0) = H_B = \sum_C \sum_{i \in C} (1 - \sigma_i^x)$$

$$H(T) = H_P$$

Start in ground state of H_B

i.e $|\psi(0)\rangle = \prod_i |\sigma_i^x = 1\rangle$

$$= \frac{1}{2^{n/2}} \sum_{\{z_i\}} |z_1 \cdots z_n\rangle$$

Evolve: $i \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle$

(49)

If T is big enough, $|\psi(T)\rangle$ will be close to a ground state of H_P.

[No level crossings by Perron-Frobenius theorem:

Real symmetric matrix with

$H_{rs} > 0 \quad r \neq s$

Highest eigenvalue is non-degenerate and eigenvector is $\{x_r\}$, $x_r > 0$

Apply to $\{c1 - H(t)\}^n$]

(50)

T is controlled by minimum energy gap $(E_1 - E_0)$ of

$H(s) = (1-s)H_B + s H_P$

$[T \sim 1/(\text{gap})^2]$

Algorithm succeeds if 'gap' is polynomial in $\frac{1}{n}$

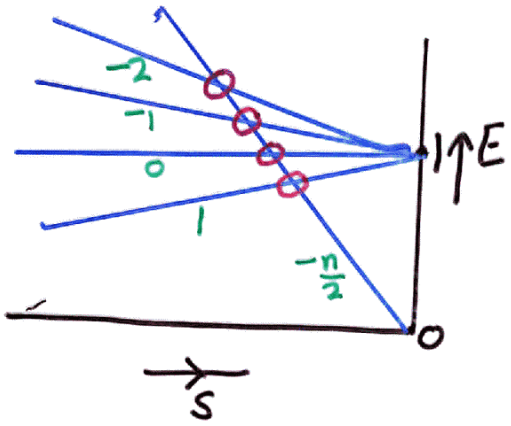
Example of failure is

$H_P = 1 - |\{z\}=0\rangle\langle\{z\}=0|$

Same as Grover.

Gap $= 2 \cdot 2^{-n/2}$

(51)



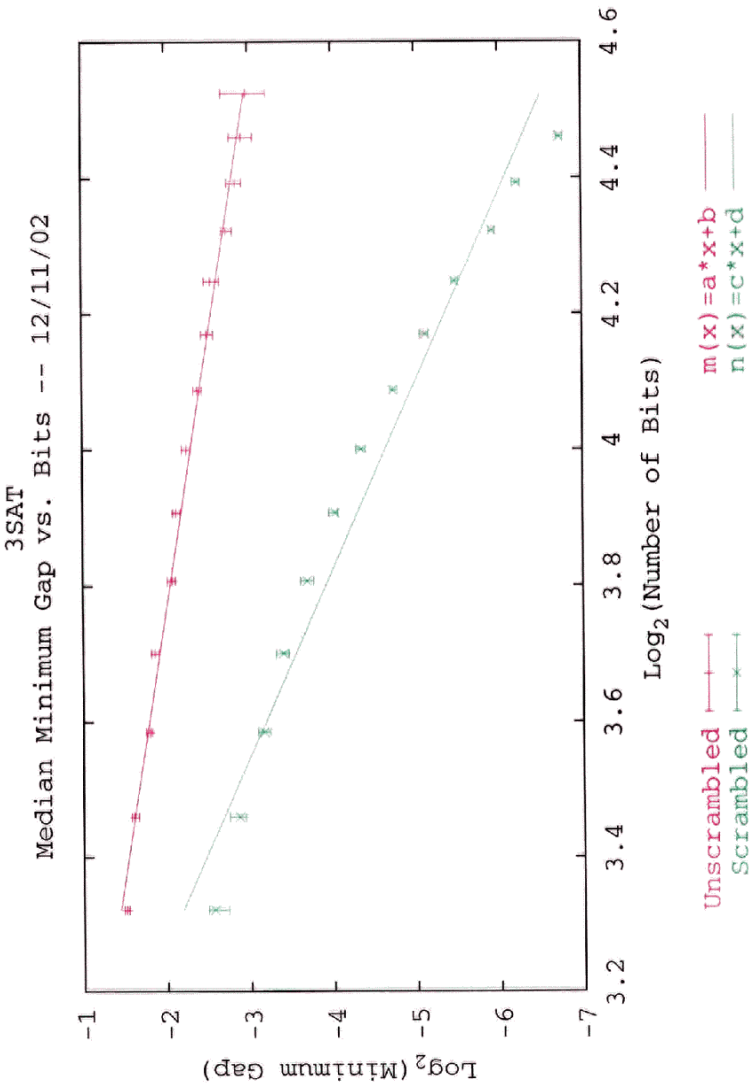
○ marks 'avoided crossings'

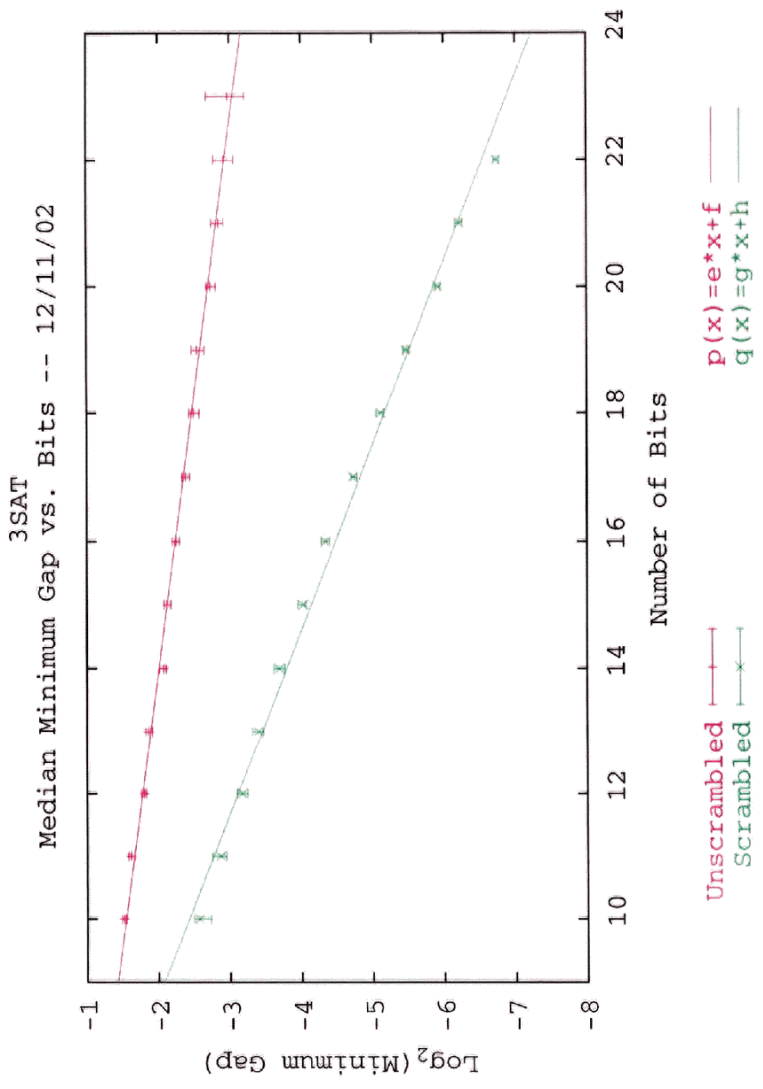
(52)

Extreme hostile position

Whenever adiabatic method works, so does Quantum MonteCarlo (a classical algorithm)

Not true, but we cannot make convincing positive assertions for interesting cases.


3SAT
Median Minimum Gap vs. Bits -- 12/11/02
Log2(Minimum Gap)
Log2(Number of Bits)
Unscrambled
Scrambled
m(x)=a*x+b
n(x)=c*x+d


3SAT
Median Minimum Gap vs. Bits -- 12/11/02
Log2(Minimum Gap)
Number of Bits
Unscrambled
Scrambled
p(x)=e*x+f
q(x)=g*x+h