"Mind the gap"

Solving optimization problems with a quantum computer

A.P. Young

http://physics.ucsc.edu/~peter

UNIVERSITY OF CALIFORNIA SANTA CRUZ

Work supported by

SCIENCE TO SHAPE THE FUTURE OF THE ARMY · ARMY RESEARCH OFFICE · 1951

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

Google

NSF National Science Foundation WHERE DISCOVERIES BEGIN

Colloquium at Oldenburg University, October 29, 2012

Collaborators: I. Hen, E. Farhi, P. Shor, D. Gosset, A. Sandvik, V. Smelyanskiy, S. Knysh, M. Guidetti.

Synopsis: Mind the Gap

iStockphoto.com/cinoby

Exponential complexity of the quantum adiabatic algorithm for certain satisfiability problems

Itay Hen and A. P. Young
Phys. Rev. E **84**, 061152 (2011)
Published December 29, 2011

Quantum computers promise to accelerate some kinds of calculations in a remarkable manner. But as in present-day classical computing, hardware is only half the story: efficiency requires development of appropriate algorithms, such as the fast Fourier transform.

To apply a quantum computer to a broad class of problems, general-purpose algorithms are needed. One such method is the quantum adiabatic algorithm, in which the problem to be solved is coded into a Hamiltonian H. One prepares the quantum computer in the ground state of a reference Hamiltonian H_R and then has it evolve under a time-dependent Hamiltonian $H(t)$ that gradually switches from H_R to H. If the evolution is slow enough ("adiabatic") the system ends up in the ground state of H, which contains information about the desired solution.

In a paper in *Physical Review E*, Itay Hen and Peter Young of the University of California, Santa Cruz, show that "slow enough" may be very slow indeed. The reason is that the time required for adiabatic evolution depends inversely on the gap in energies between the ground and first excited states of $H(t)$. Using computer simulations, Hen and Young show that for three classes of logic problems, the scaling of the gap is such that the computational time can be expected to grow exponentially with the size of the problem. The authors suggest that it might be possible to optimize the evolution of $H(t)$ to avoid the bottleneck associated with a vanishing gap. – *Ron Dickman*

Synopsis: Mind the Gap

iStockphoto.com/cinoby

Exponential complexity of the quantum adiabatic algorithm for certain satisfiability problems

Itay Hen and A. P. Young
Phys. Rev. E **84**, 061152 (2011)
Published December 29, 2011

Quantum computers promise to accelerate some kinds of calculations in a remarkable manner. But as in present-day classical computing, hardware is only half the story: efficiency requires development of appropriate algorithms, such as the fast Fourier transform.

To apply a quantum computer to a broad class of problems, general-purpose algorithms are needed. One such method is the quantum adiabatic algorithm, in which the problem to be solved is coded into a Hamiltonian H. One prepares the quantum computer in the ground state of a reference Hamil me-dependent Hamiltonian $H(t)$ that gradually switches from H_R to H. If the evolution is slow enough ("adia tate of H, which contains information about the desired solution.

In a p Peter Young of the University of California, Santa Cruz, show that "slow enough" may be very slow indeed. The r c evolution depends inversely on the gap in energies between the ground and first excited states of $H(t)$. Using ow that for three classes of logic problems, the scaling of the gap is such that the computational time can be ex of the problem. The authors suggest that it might be possible to optimize the evolution of $H(t)$ to avoid the bottle *lon Dickman*

Synopsis: Mind the Gap

iStockphoto.com/cinoby

Exponential complexity of the quantum adiabatic algorithm for certain satisfiability problems

Itay Hen and A. P. Young

Ph

Pu

Quantum computers promise to accelerate some kin
only half the story: efficiency requires development c

To apply a quantum computer to a broad class of pro
algorithm, in which the problem to be solved is coded
Hamil me-d
("adia tate

In a p eter
The r c evo
Using ow th
be ex of th
bottle *on D*

d.
an
he

Plan

Plan

What is a quantum computer?

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **“optimization problems”**, of broad interest in science and engineering (including industry)?

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)
- The Quantum Monte Carlo Method (QMC)

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)
- The Quantum Monte Carlo Method (QMC)
- Results for satisfiability (SAT) problems and comparison with a classical algorithm (WALKSAT)

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)
- The Quantum Monte Carlo Method (QMC)
- Results for satisfiability (SAT) problems and comparison with a classical algorithm (WALKSAT)
- Results for a spin glass problem

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)
- The Quantum Monte Carlo Method (QMC)
- Results for satisfiability (SAT) problems and comparison with a classical algorithm (WALKSAT)
- Results for a spin glass problem
- Conclusions

Plan

What is a quantum computer?

What could an eventual quantum computer do better than a classical computer? (Shor and Grover)

Could a quantum computer be of **broader utility** by efficiently solving **"optimization problems"**, of broad interest in science and engineering (including industry)?

- The Quantum Adiabatic Algorithm (QAA)
- The Quantum Monte Carlo Method (QMC)
- Results for satisfiability (SAT) problems and comparison with a classical algorithm (WALKSAT)
- Results for a spin glass problem
- Conclusions

Note: the QAA is **inspired by physics** and QMC is a **technique from physics**

What is a quantum computer?

Classical computer: bit is 0 **or** 1

Quantum computer: qubit: linear superposition of 0 **and** 1.

N qubits: linear superposition of 2^N basis states

Actions on the quantum state act on all 2^N basis states

⇒ Quantum Parallelism

What is a quantum computer?

Classical computer: bit is 0 **or** 1

Quantum computer: qubit: linear superposition of 0 **and** 1.

N qubits: linear superposition of 2^N basis states

Actions on the quantum state act on all 2^N basis states

⇒ Quantum Parallelism

But: to get the result, need to make a measurement

⇒ Don't get 2^N results. Rather there are 2^N probabilities and one gets **one result** according to these probabilities.

What is a quantum computer?

Classical computer: bit is 0 **or** 1

Quantum computer: qubit: linear superposition of 0 **and** 1.

N qubits: linear superposition of 2^N basis states

Actions on the quantum state act on all 2^N basis states

⇒ Quantum Parallelism

But: to get the result, need to make a measurement

⇒ Don't get 2^N results. Rather there are 2^N probabilities and one gets **one result** according to these probabilities.

Seems that quantum mechanics is not useful for computing

Nonetheless, in some cases useful results can be obtained by doing clever processing **before** the measurement.

What is a quantum computer?

Classical computer: bit is 0 **or** 1

Quantum computer: qubit: linear superposition of 0 **and** 1.

N qubits: linear superposition of 2^N basis states

Actions on the quantum state act on all 2^N basis states

⇒ Quantum Parallelism

But: to get the result, need to make a measurement

⇒ Don't get 2^N results. Rather there are 2^N probabilities and one gets **one result** according to these probabilities.

Seems that quantum mechanics is not useful for computing

Nonetheless, in some cases useful results can be obtained by doing clever processing **before** the measurement.

The most famous is Shor's algorithm for factoring integers

Integer factoring

Integer factoring

Let N = p q, where p and q are prime. Let N have n bits.

How hard is it to factor N?

Classical, ~ $\exp(n^{1/3} (\log n)^{2/3})$ (exponential)

i.e **hard**. This is the basis of RSA encryption method

Quantum (Shor), ~ n^3 (polynomial)

Shor uses a "Quantum Fourier Transform"

Needs 3n qubits plus ???? for error correction.

Need coherence during the running of the algorithm.

n ~ 1000 would be useful

Integer factoring

Let N = p q, where p and q are prime. Let N have n bits.

How hard is it to factor N?

Classical, ~ $\exp(n^{1/3} (\log n)^{2/3})$ (exponential)

i.e **hard**. This is the basis of RSA encryption method

Quantum (Shor), ~ n^3 (polynomial)

Shor uses a "Quantum Fourier Transform"

Needs 3n qubits plus ???? for error correction.

Need coherence during the running of the algorithm.

n ~ 1000 would be useful

⇒ We are very far from having a useful quantum computer

Integer factoring

Let N = p q, where p and q are prime. Let N have n bits.

How hard is it to factor N?

Classical, ~ $\exp(n^{1/3} (\log n)^{2/3})$ (exponential)

i.e **hard**. This is the basis of RSA encryption method

Quantum (Shor), ~ n^3 (polynomial)

Shor uses a "Quantum Fourier Transform"

Needs 3n qubits plus ???? for error correction.

Need coherence during the running of the algorithm.

n ~ 1000 would be useful

⇒ We are very far from having a useful quantum computer

Still: interesting to investigate what could be done with a quantum computer if and when one will eventually be built.

RSA Encryption

Alice wants to send a message to Bob down a public channel.

Bob sends to Alice a "public key" **N**, a product of 2 large random primes p and q, i.e. N = p q, and an **encoding integer e** which has no factors in common with (p-1)(q-1) (e.g. N has 1024 bits)

Alice's message m is a binary string (m < N). She forms the encoded message m′ from

$m' = m^e \bmod N$ **N and e are the public key**

Alice sends m' to Bob down the public channel.

Bob knows his "private key" d, the **decoding integer**, which is determined by $d\,e = 1 \bmod (p-1)(q-1)$

which is easily found (generalized Euclid) if one knows p and q

Bob computes $(m')^d \bmod N$ which, is **Alice's message:**

$m = (m')^d \bmod N$ **N and d are the private key**

Optimization problems

Shor's algorithm (and Grover's, searching an unstructured data base of size N with ~√N operations rather than ~ N/2) is rather specialized.

Would a quantum computer also be useful for more general problems, such as optimization problems, i.e. minimizing a function of N variables with constraints?

Of interest in many fields in science and engineering.

Here we will take "Problem Hamiltonians" (i.e. the function to be minimized) which involve binary variables, 0 or 1, (or equivalently Ising spins $\sigma^z = \pm 1$).

How could we try to solve such optimization problems on a quantum computer?

An idea from physics ....

Quantum Adiabatic Algorithm

Proposed by Farhi et. al (2001) to solve hard optimization problems on a quantum computer.

$$\mathcal{H}(t) = [1 - s(t)]\mathcal{H}_D + s(t)\mathcal{H}_P$$

$\mathcal{H}_P$ is the problem Hamiltonian, depends on the σ_i^z

$\mathcal{H}_D$ is the driver Hamiltonian $= -h\sum \sigma_i^x$

$0 \le s(t) \le 1, \qquad s(0) = 0, \qquad s(\mathcal{T}) = 1$

$\mathcal{T}$ is the running time

The quantum computer simulates H(t).

System starts in ground state of driver Hamiltonian. If process is adiabatic (and $T \to 0$), it ends in g.s. of problem Hamiltonian, and problem is solved. Minimum $\mathcal{T}$ is the "complexity".

Quantum Adiabatic Algorithm

Proposed by Farhi et. al (2001) to solve hard optimization problems on a quantum computer.

$$\mathcal{H}(t) = [1 - s(t)]\mathcal{H}_D + s(t)\mathcal{H}_P$$

$\mathcal{H}_P$ is the problem Hamiltonian, depends on the σ_i^z

$\mathcal{H}_D$ is the driver Hamiltonian $= -h\sum \sigma_i^x$

$0 \le s(t) \le 1, \qquad s(0) = 0, \qquad s(\mathcal{T}) = 1$

$\mathcal{T}$ is the running time

The quantum computer simulates H(t).

System starts in ground state of driver Hamiltonian. If process is adiabatic (and $T \to 0$), it ends in g.s. of problem Hamiltonian, and problem is solved. Minimum $\mathcal{T}$ is the "complexity".

Quantum Adiabatic Algorithm

Proposed by Farhi et. al (2001) to solve hard optimization problems on a quantum computer.

$$\mathcal{H}(t) = [1 - s(t)]\mathcal{H}_D + s(t)\mathcal{H}_P$$

$\mathcal{H}_P$ is the problem Hamiltonian, depends on the σ_i^z

$\mathcal{H}_D$ is the driver Hamiltonian $= -h\sum \sigma_i^x$

$0 \le s(t) \le 1, \qquad s(0) = 0, \qquad s(\mathcal{T}) = 1$

$\mathcal{T}$ is the running time

The quantum computer simulates H(t).

System starts in ground state of driver Hamiltonian. If process is adiabatic (and T → 0), it ends in g.s. of problem Hamiltonian, and problem is solved. Minimum $\mathcal{T}$ is the "complexity".

Is $\mathcal{T}$ exponential or polynomial in the problem size N?

Early Numerics

Early numerics, Farhi et al. for very small sizes $N \leq 20$, on a particular problem found the time varied only as N^2 , i.e. polynomial!

But possible “crossover” to exponential at larger sizes?

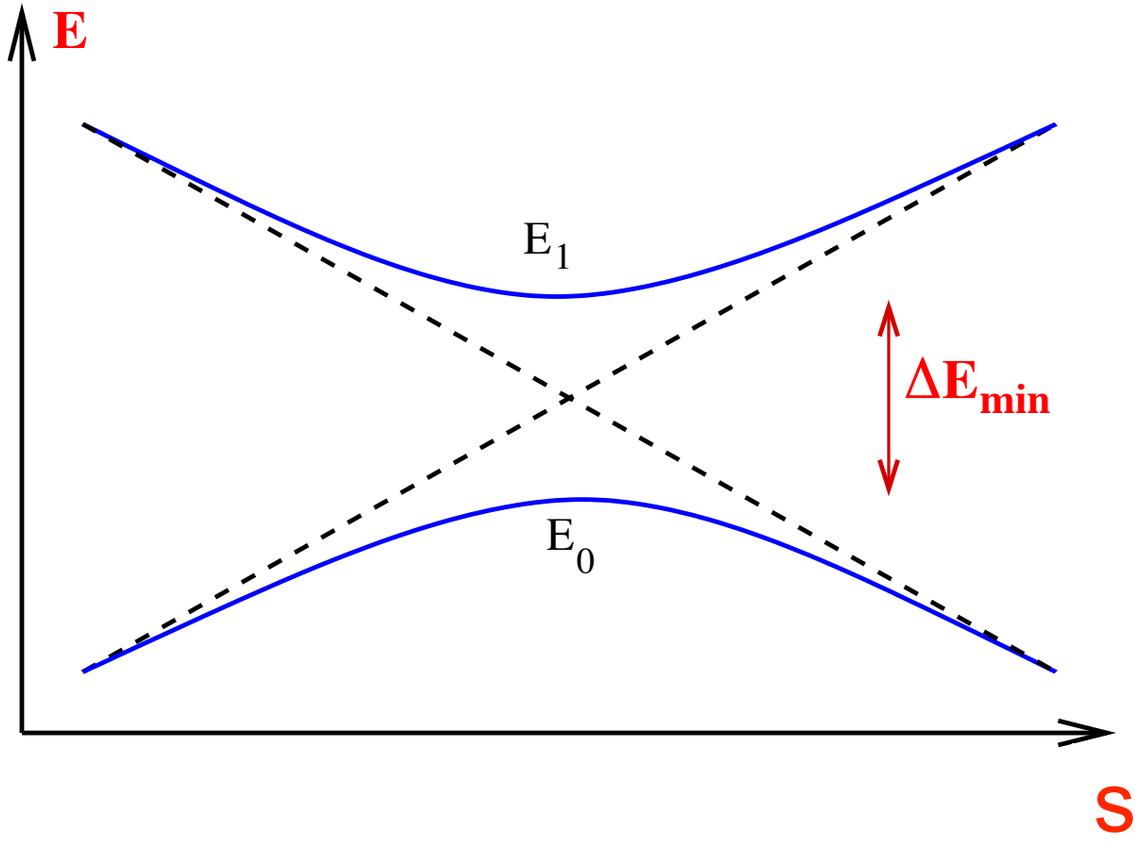
To explore large sizes, need techniques from statistical physics, Quantum Monte Carlo.

Quantum Phase Transition

Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small

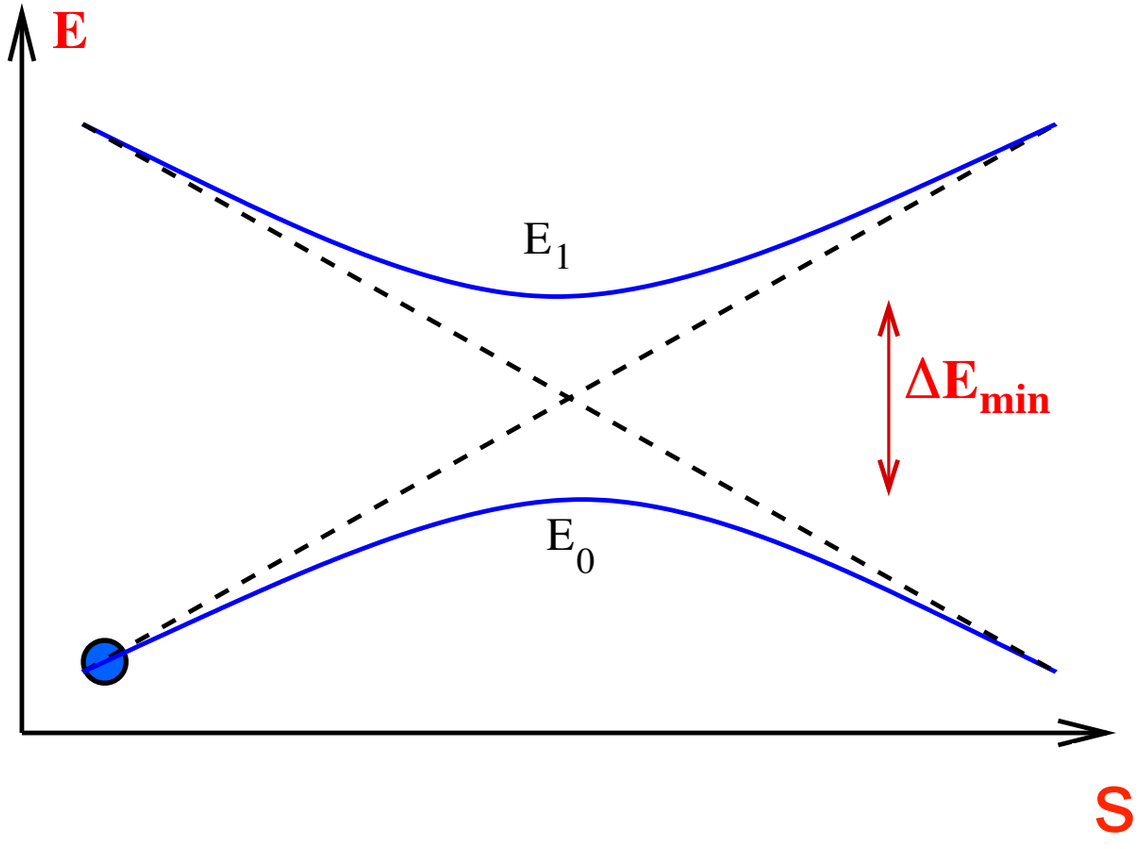
Quantum Phase Transition

Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small



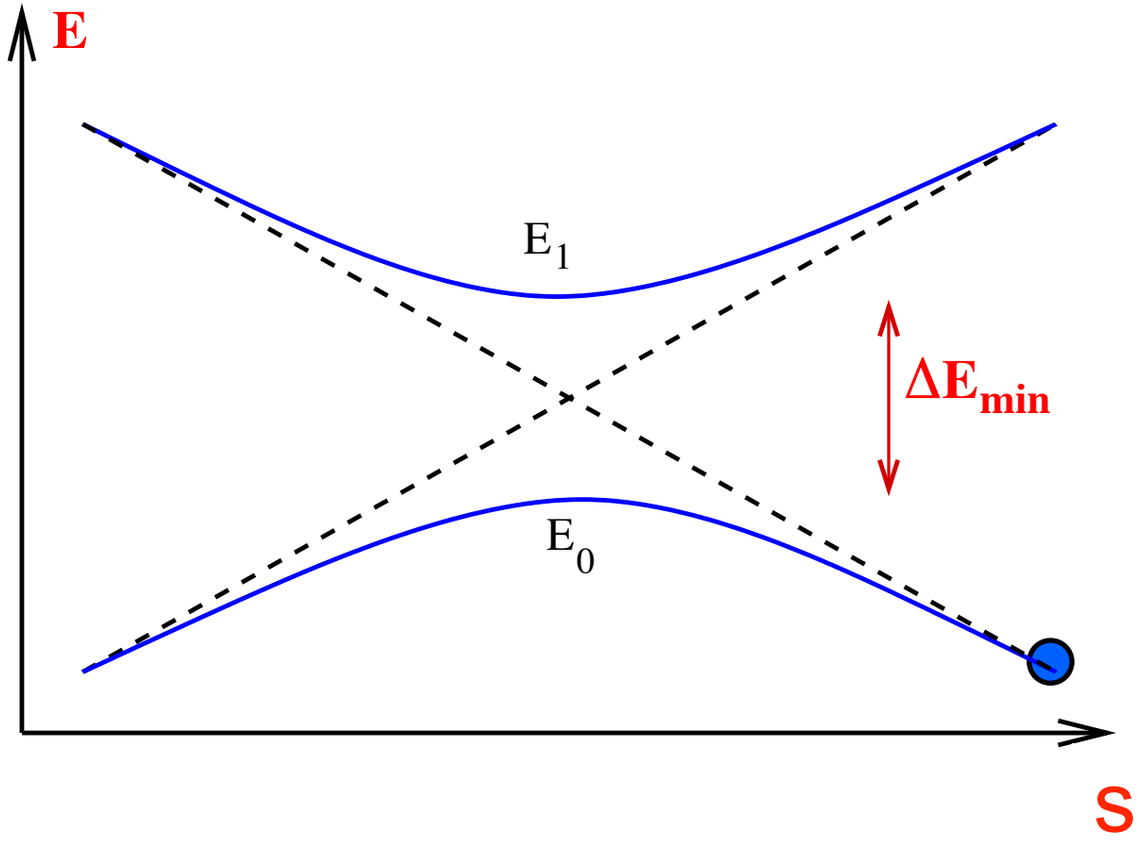
Quantum Phase Transition

Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small



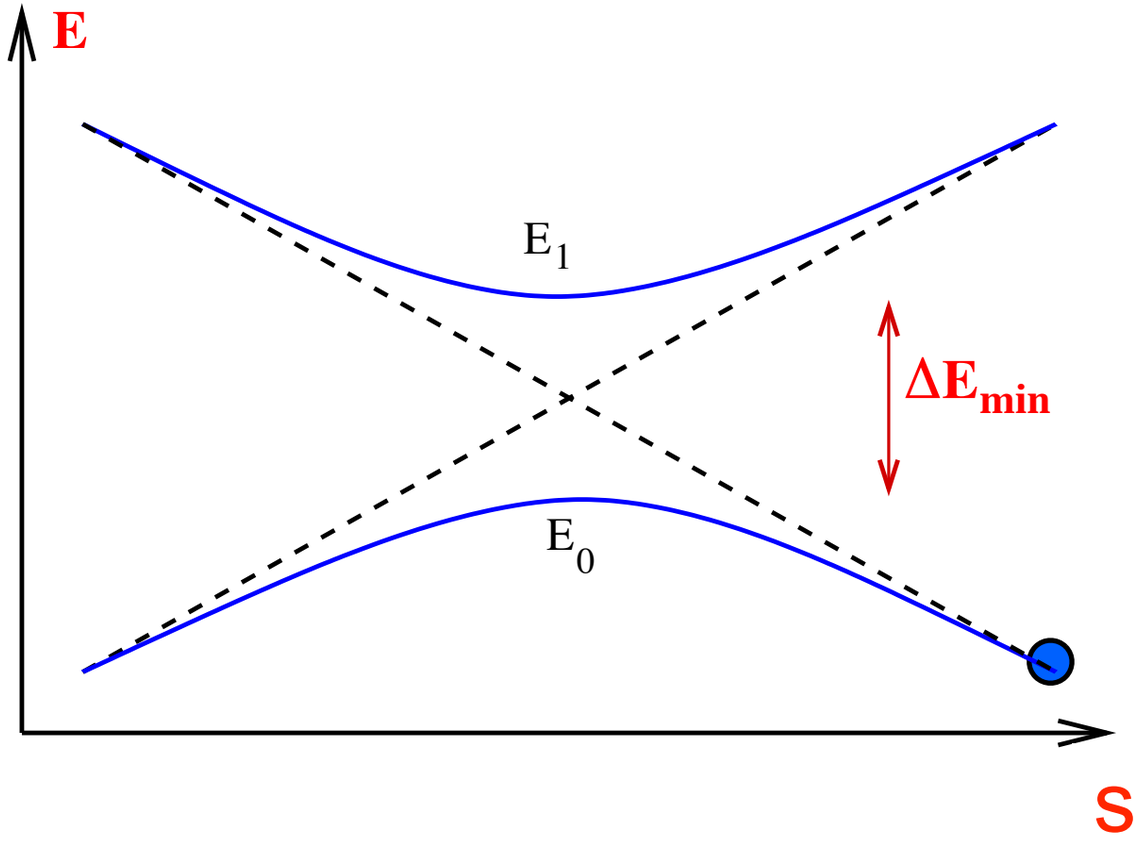
Quantum Phase Transition

Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small



Quantum Phase Transition

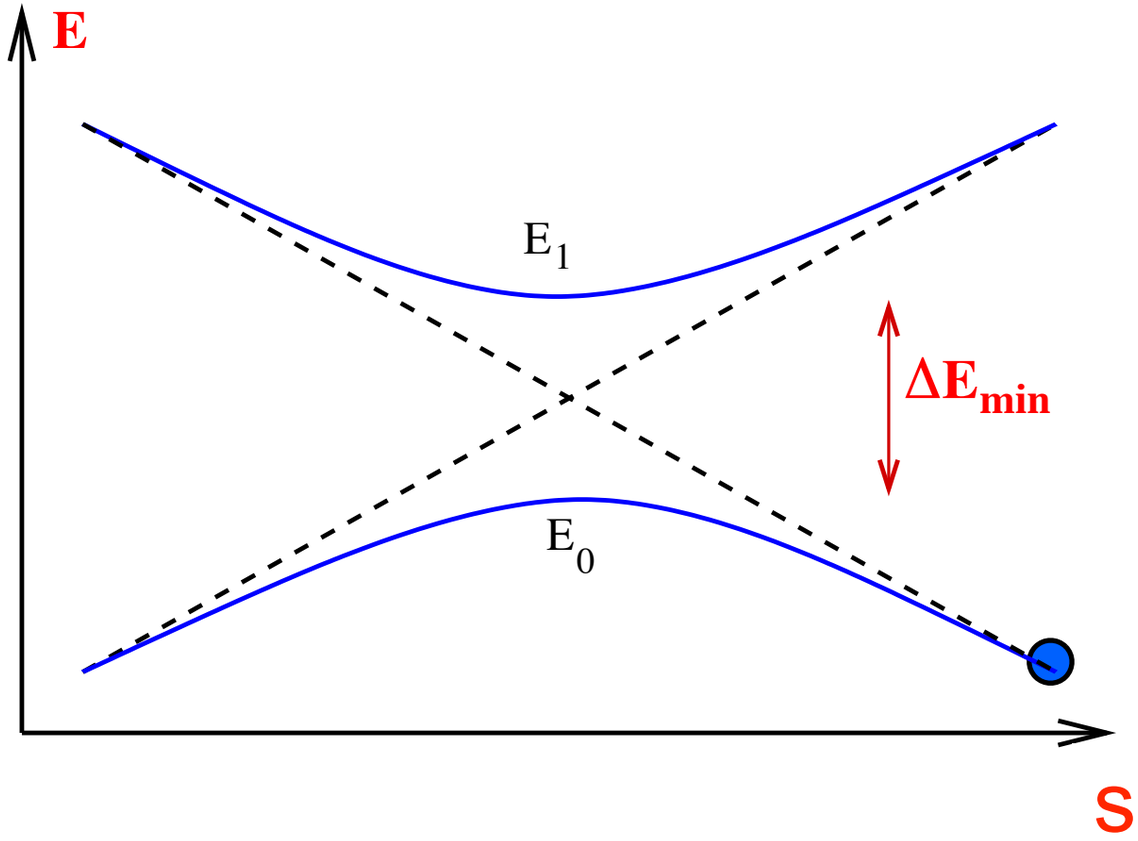
Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small



Landau Zener Theory:
To stay in the ground state the time needed is proportional to ΔE_{min}^{-2}

Quantum Phase Transition

Bottleneck is likely to be a quantum phase transition (QPT) where the gap to the first excited state is very small



Landau Zener Theory:
To stay in the ground state the time needed is proportional to ΔE_{min}^{-2}

Using QMC, we compute ΔE for different s: → ΔE_{min}

Quantum Monte Carlo

We do a sampling of the 2^N states (so statistical errors). Use analogy between time evolution operator in quantum mechanics, exp(-i t H), and the Boltzmann operator in **equilibrium** statmech, exp(-β H).

Study **equilibrium** properties of a quantum system by simulating a **classical model with an extra dimension**, imaginary time, τ, where $0 \leq \tau < 1/T.$

Not perfect, but the only numerical method available for large N.

We use the "stochastic series expansion" method for Quantum Monte Carlo simulations which was pioneered by Anders Sandvik.

$$Z \equiv \mathrm{Tr} e^{-\beta \mathcal{H}} = \sum_{n=0}^{\infty} \frac{\mathrm{Tr}\left(-\beta \mathcal{H}\right)^n}{n!}$$

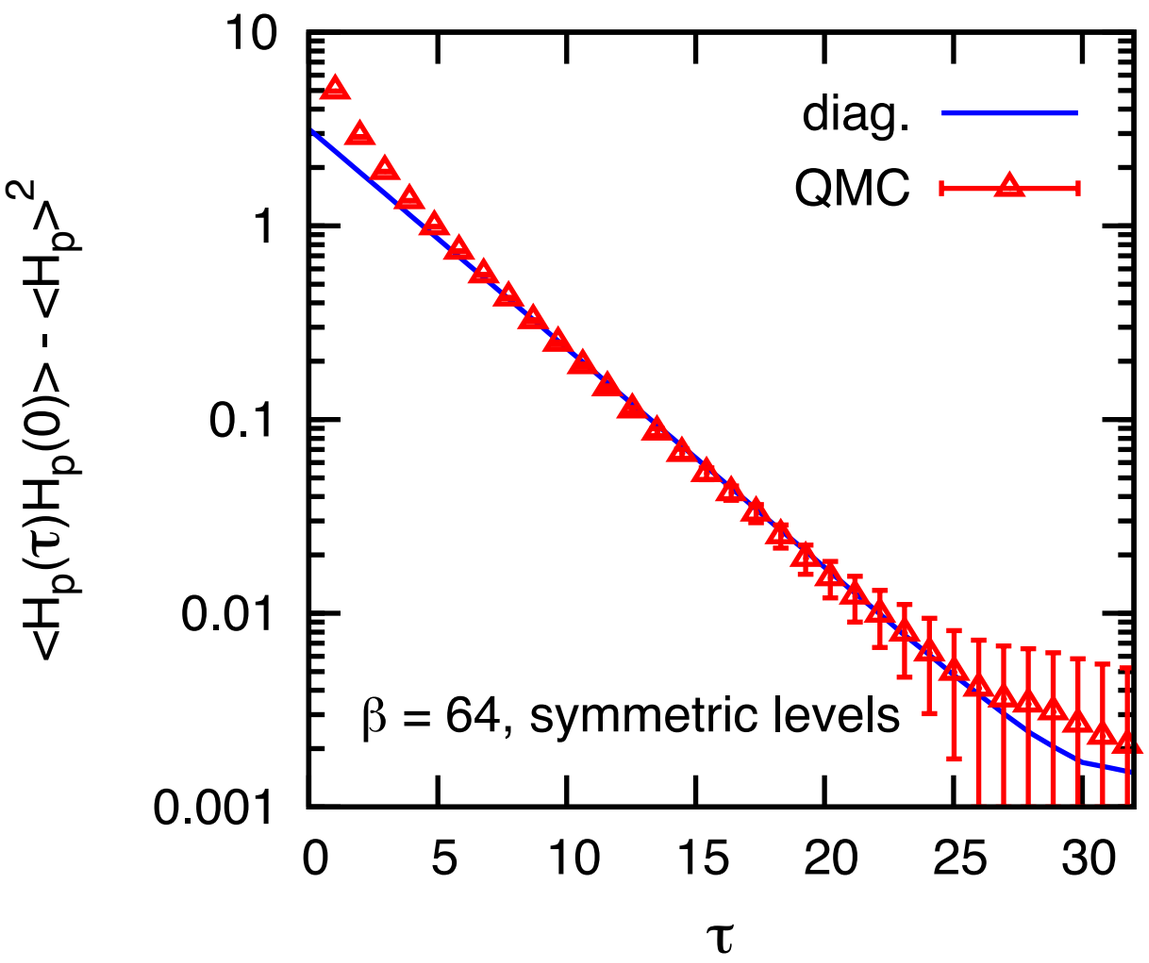
Stochastically sum the terms in the series.

Examples of results with the SSE code

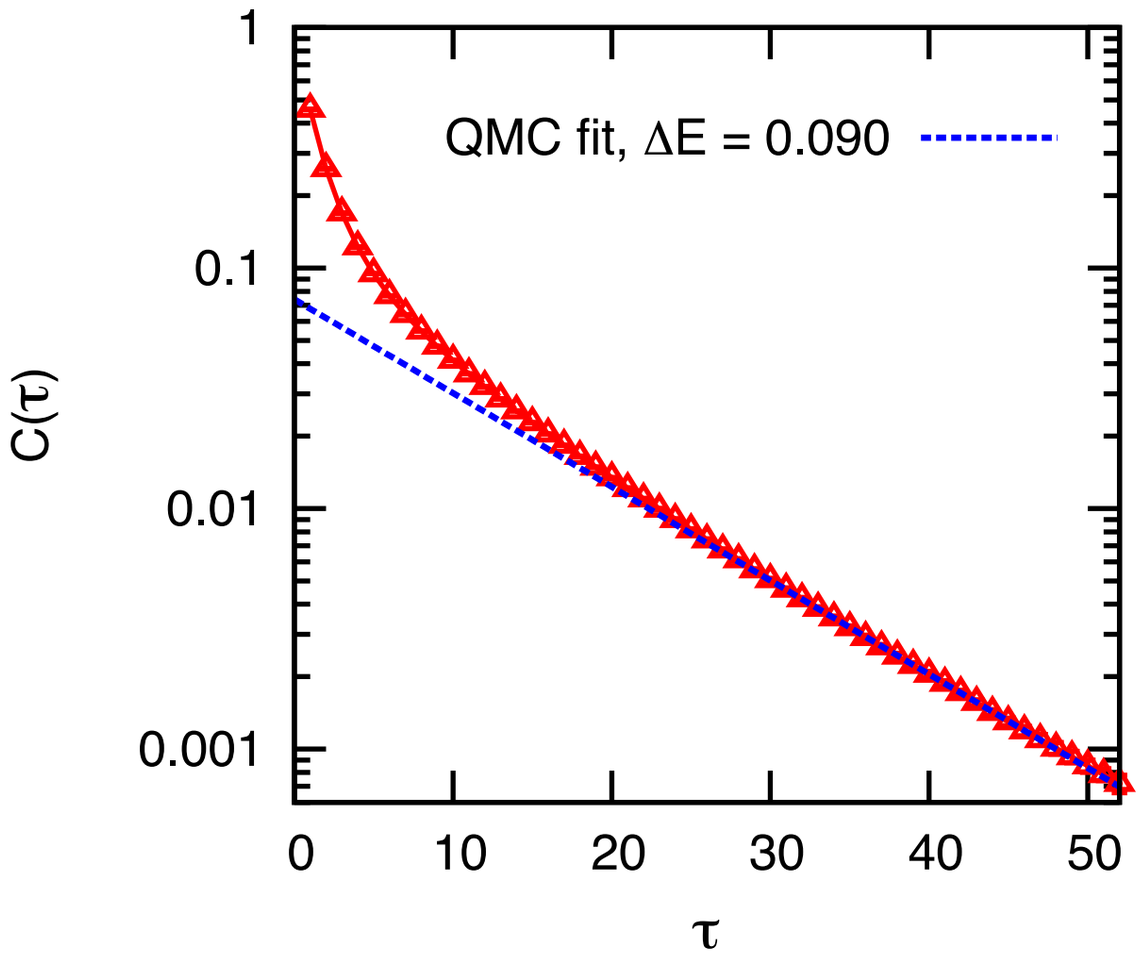
Time dependent correlation functions decay with τ as a sum of exponentials

$$\langle A(\tau)A(0)\rangle - \langle A\rangle^2 = \sum_{n\neq 0} |\langle 0|A|n\rangle|^2 \exp[-(E_n - E_0)\tau]$$

For large τ only first excited state contributes, → pure exponential decay

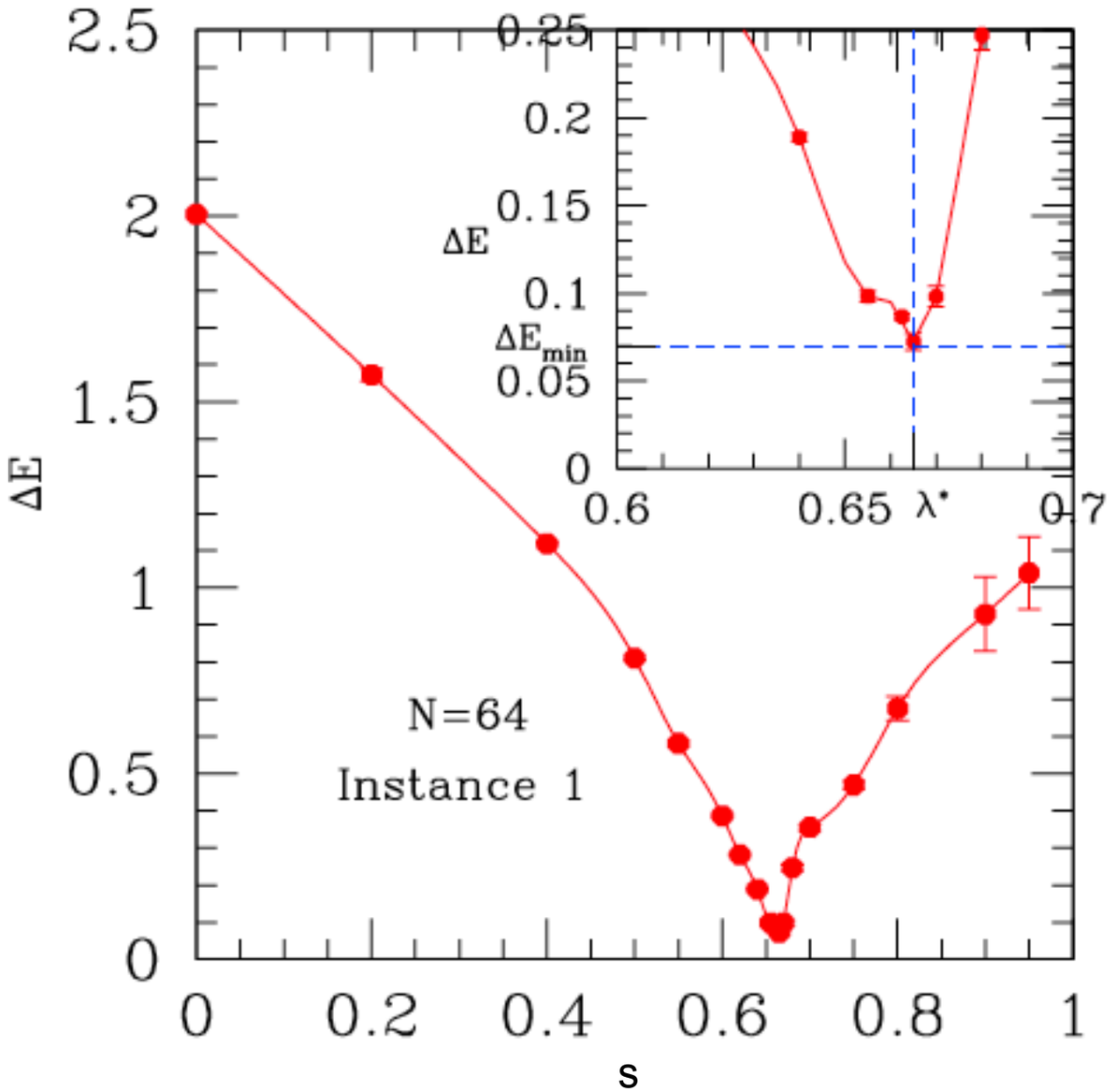


Small size, N= 24, excellent agreement with diagonalization.



Large size, N = 128, good quality data, slope of straight line → gap.

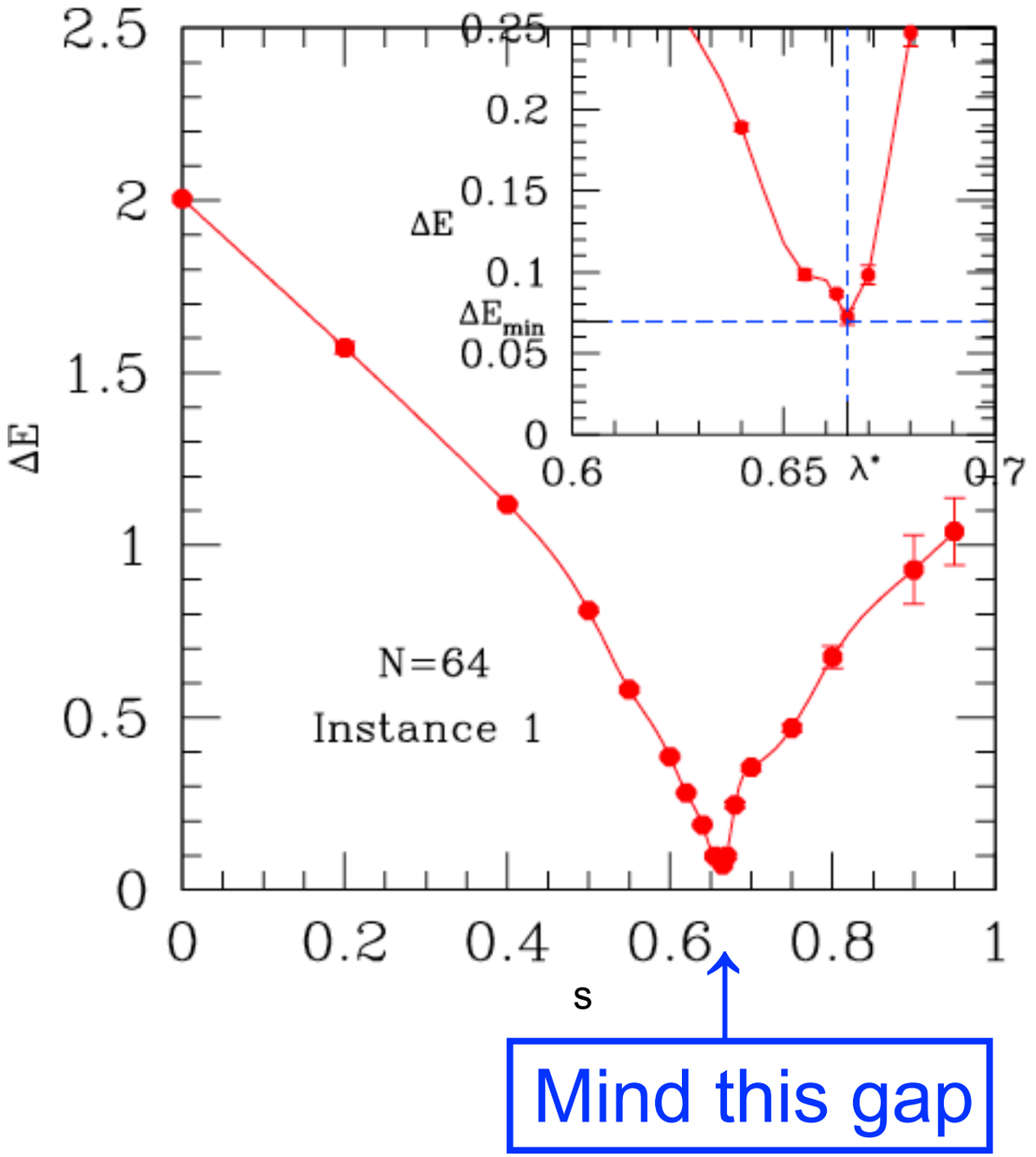
Dependence of gap on s



Results for the dependence of the gap to the first excited state, ΔE, with s, for one instance of 1-in-3 SAT with N = 64.

The gap has a minimum for s about 0.66 which is the bottleneck for the QAA.

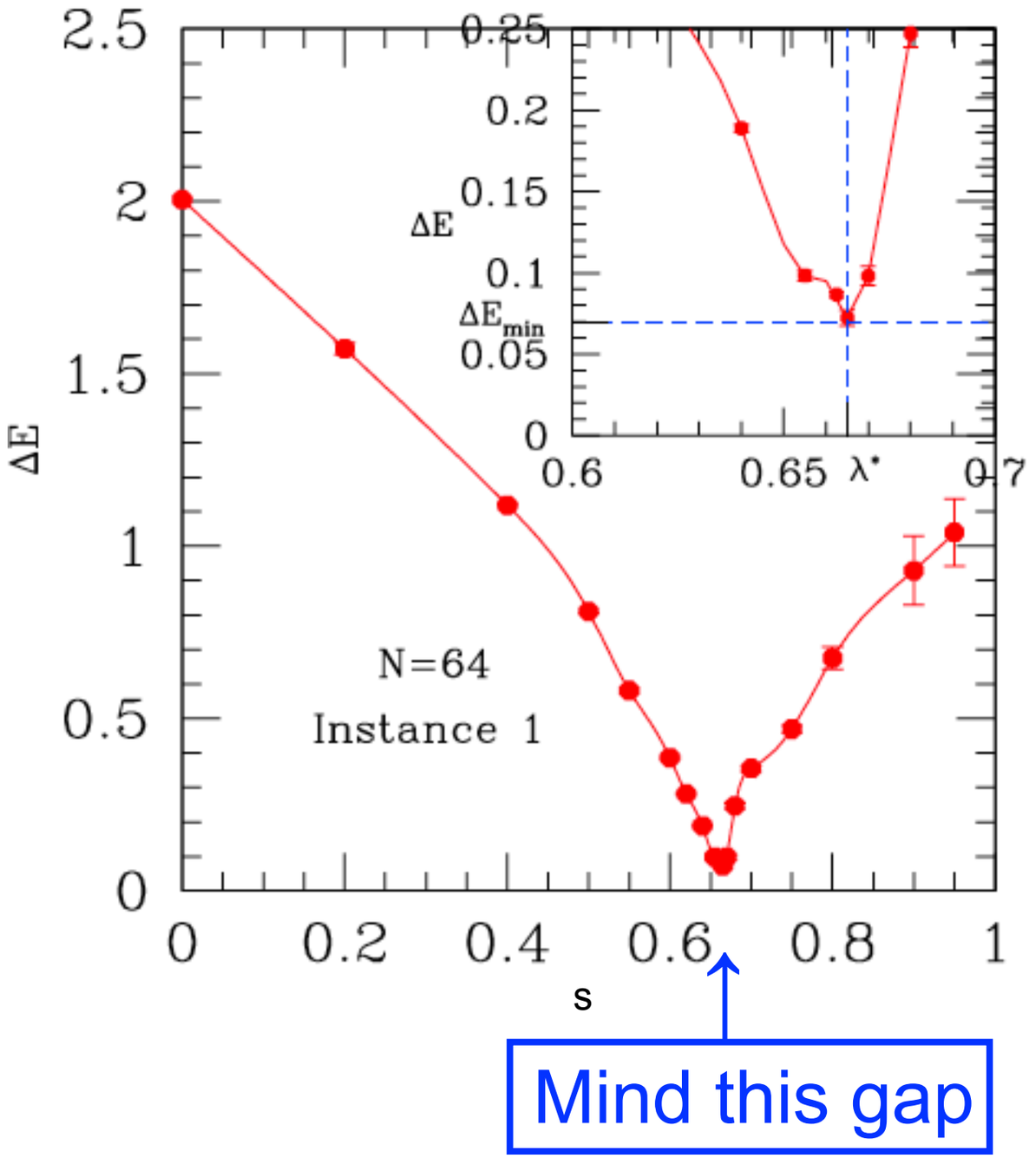
Dependence of gap on s



Results for the dependence of the gap to the first excited state, ΔE, with s, for one instance of 1-in-3 SAT with N = 64.

The gap has a minimum for s about 0.66 which is the bottleneck for the QAA.

Dependence of gap on s



Results for the dependence of the gap to the first excited state, ΔE, with s, for one instance of 1-in-3 SAT with N = 64.

The gap has a minimum for s about 0.66 which is the bottleneck for the QAA.

We compute the minimum gap for many (50) instances for each size N and look how the median minimum gap varies with size.

Satisfiability Problems I

In satisfiability problems (SAT) we ask whether there is an assignment of N bits which satisfies all of M logical conditions ("clauses"). We assign an energy to each clause such that it is zero if the clause is satisfied and a positive value if not satisfied.

i.e. We need to determine if the ground state energy is 0.

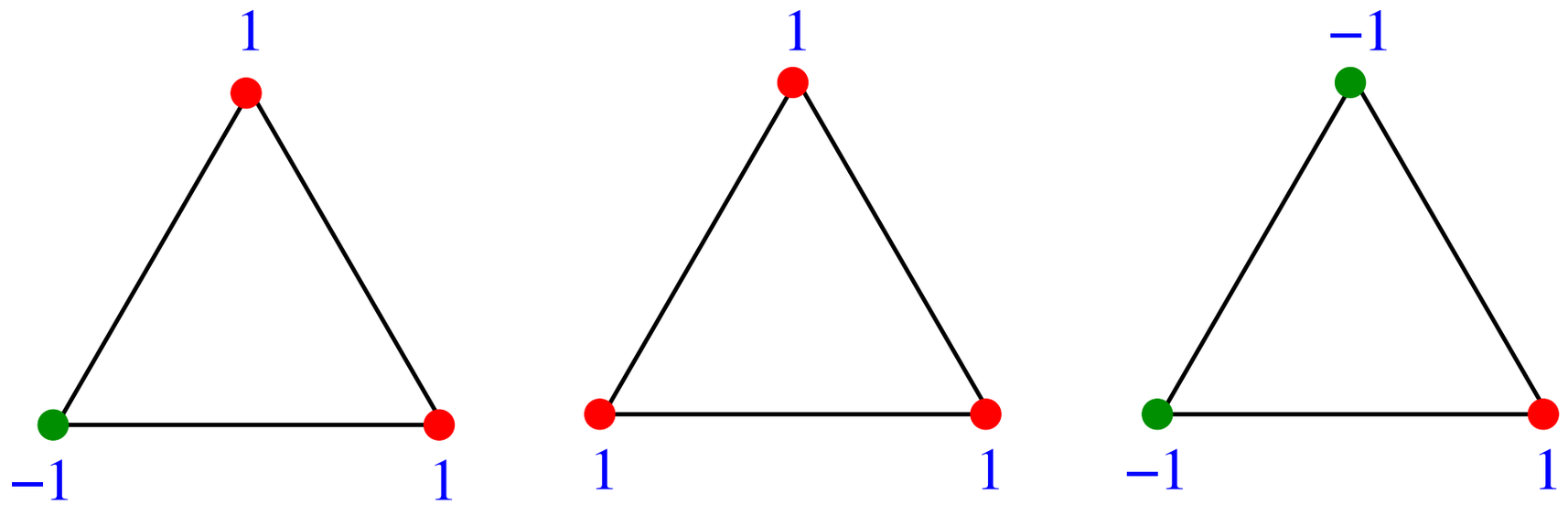
We take the ratio of M/N to be at the satisfiability threshold, and study instances with a "unique satisfying assignment" (USA).
(so gap to 1st excited state has a minimum whose value indicates the complexity.)

These SAT problems are "NP-complete", a category of hard problems for which the time is exponential with classical algorithms, at least in the worst case.

Satisfiability Problems II

- "Locked" 1-in-3 SAT

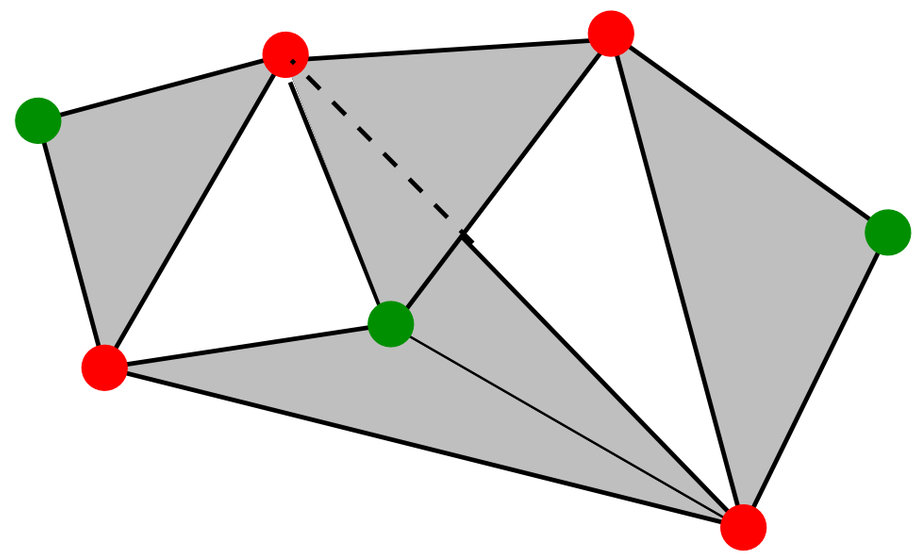
  The clause is formed from 3 bits picked at random. The clause is satisfied (has energy 0) if one is 1 and the other two are 0 (in terms of spins one is -1 (green) and the other two are +1 (red)). Otherwise it is not satisfied (the energy is 1).



Example of a satisfying assignment with N=7, M = 5.

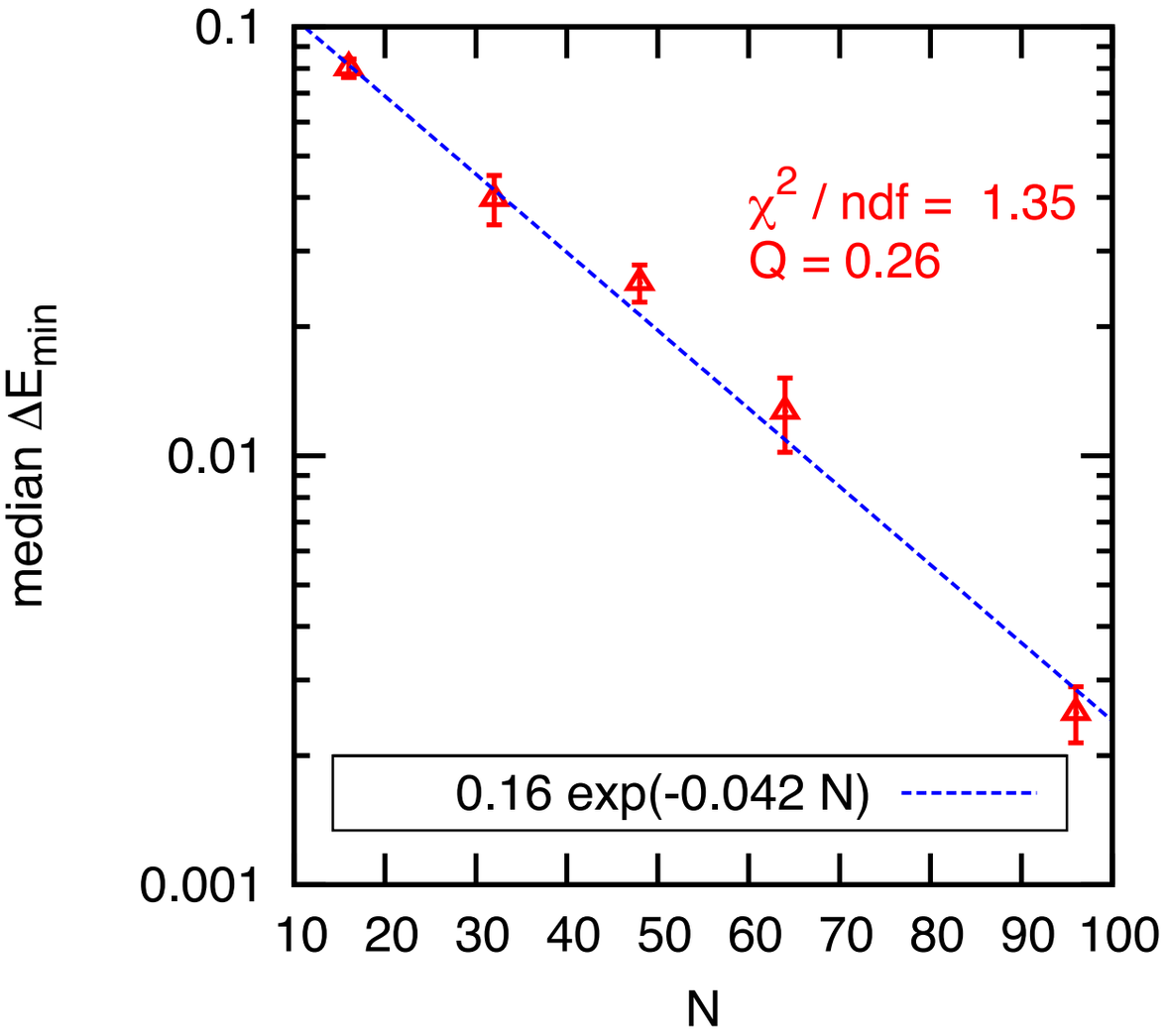
(V. Choi)

$$\mathcal{H}_P = \sum_{\text{clauses}} \left(\frac{\sigma_1^z + \sigma_2^z + \sigma_3^z - 1}{2} \right)^2$$

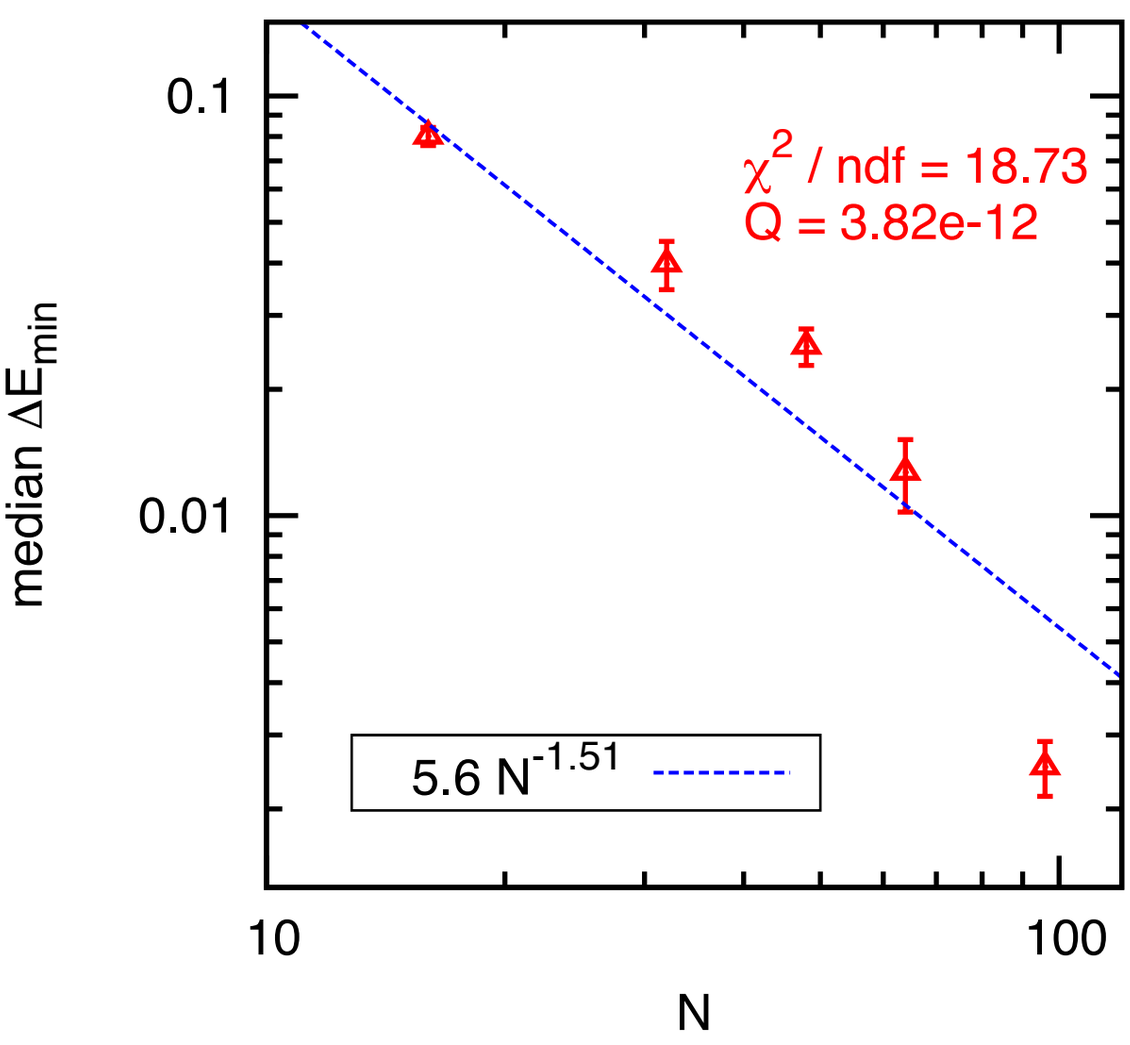


Locked 1-in-3

Plots of the median minimum gap (average over 50 instances)



Exponential fit



Power law fit

Clearly the behavior of the minimum gap is exponential

Comparison with a classical algorithm, WalkSAT: I

WalkSAT is a classical, heuristic, local search algorithm. It is a reasonable classical algorithm to compare with QAA.

We have compared the running time of the QAA for the three SAT problems studied with that of WalkSAT.

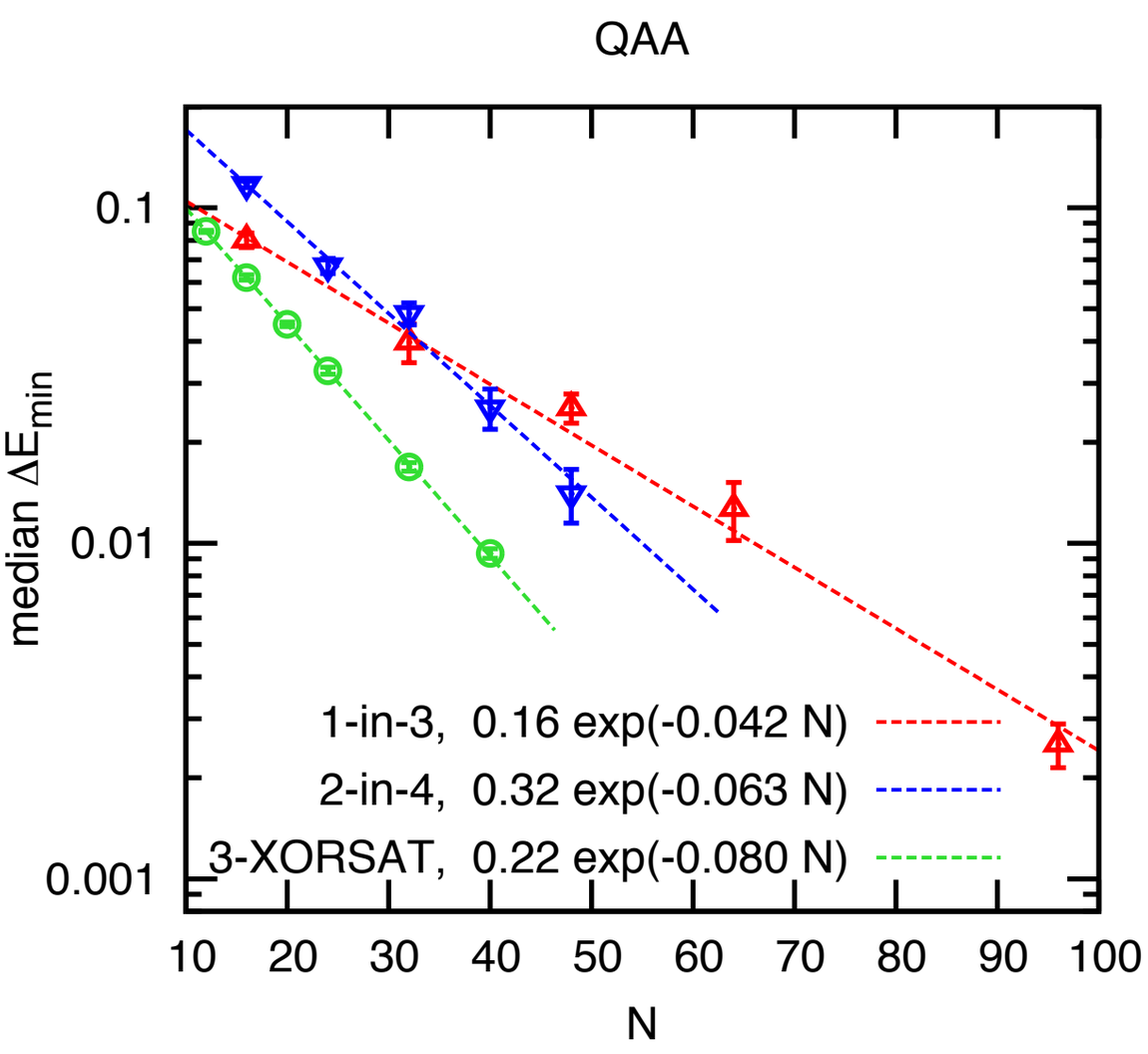
For QAA, Landau-Zener theory states that the time is proportional to $1/(\Delta E_{min})^2$ (neglecting N dependence of matrix elements).

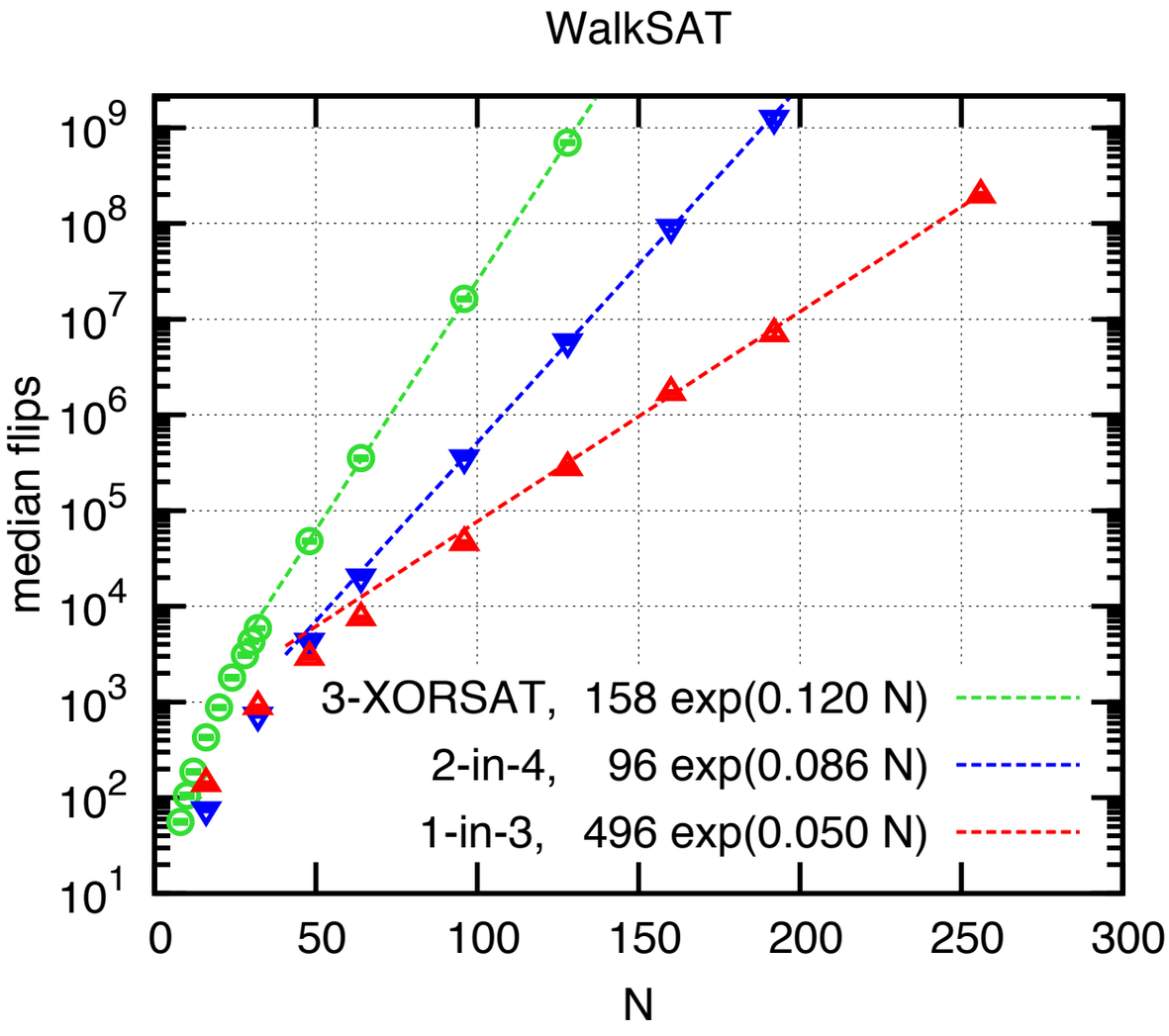
For WalkSAT the running time is proportional to number of "bit flips".

We write the running time as proportional to $\exp(\mu N)$.

We will compare the values of μ among the different models and between QAA and WalkSAT.

Comparison with a classical algorithm, WalkSAT: II





Exponential behavior for both QAA and WalkSAT

The trend is the same in both QAA and WalkSAT.
3-XORSAT is the hardest, and locked 1-in-3 SAT the easiest.

Comparison with a classical algorithm, WalkSAT: III

Model	QAA	WalkSAT	Ratio
1-in-3	0.084(3)	0.0505(5)	1.66
2-in-4	0.126(7)	0.0858(8)	1.47
3-XORSAT	0.159(2)	0.1198(4)	1.32

Exponential complexity in both cases. QAA not better than WalkSAT.

Values of μ (where time ~ exp[μ N]).

These results used the **simplest implementation** of the QAA **for instances with a USA**.

A “spin glass” on a random graph:

For simplicity we put the spins a regular random graph, each site having exactly three neighbor (3-regular). Spins prefer to be antiparallel, an antiferromagnet (but see next slide)

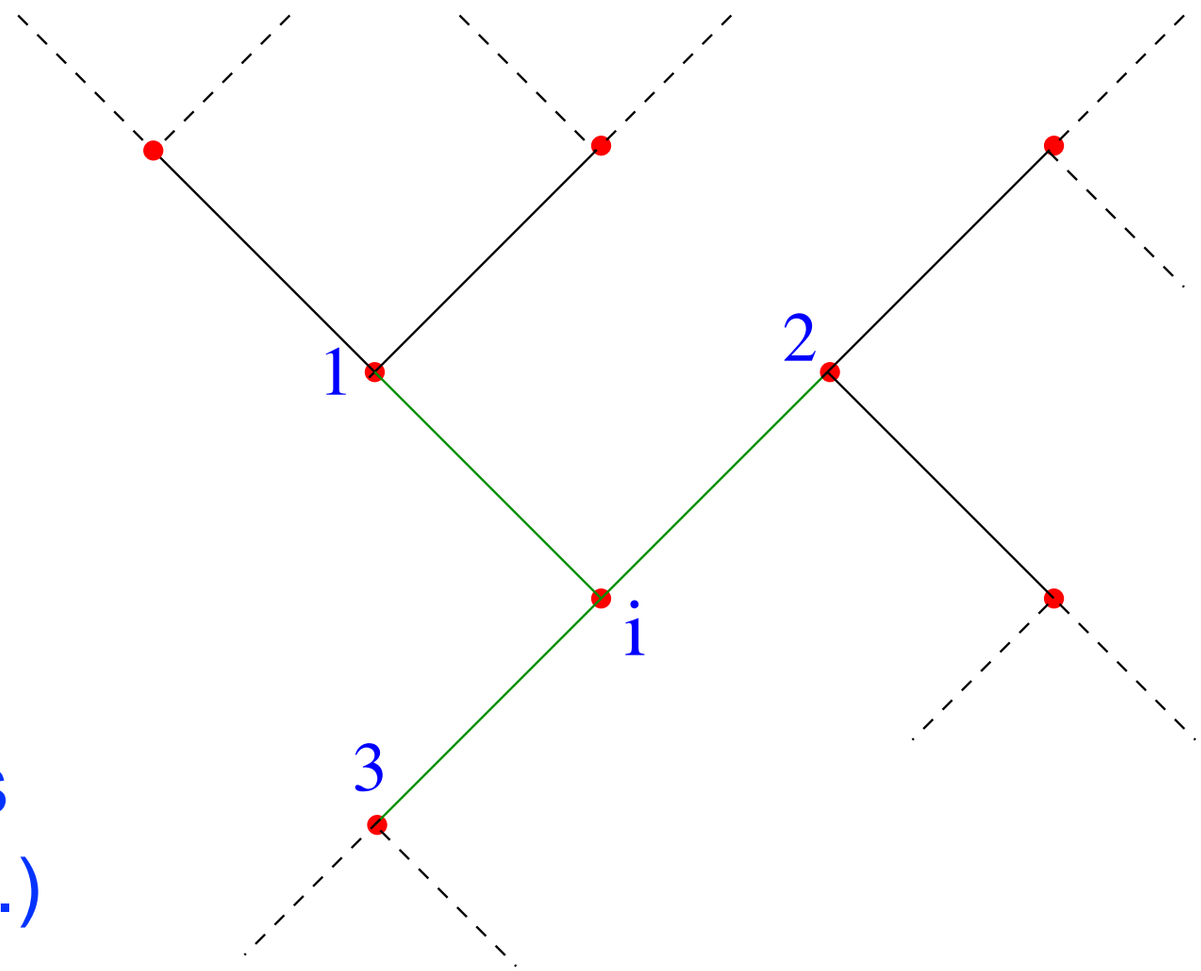
The problem Hamiltonian is

$$\mathcal{H}_P = \frac{1}{2}\sum_{\langle i,j\rangle}\left(1+\sigma_i^z\sigma_j^z\right)$$

Note the symmetry under

$$\sigma_i^z \rightarrow -\sigma_i^z,\ \forall i$$

“Replica” theory indicates that these 2-SAT-like problems are **different** from K-SAT problems for K > 2. (Hence we study it here.)



Note: there are large loops

Spin Glass on a random graph: II

Cannot form an “up-down” antiferromagnet because of loops of odd length. In fact, it is a “spin glass”, a system with disorder and “frustration”.

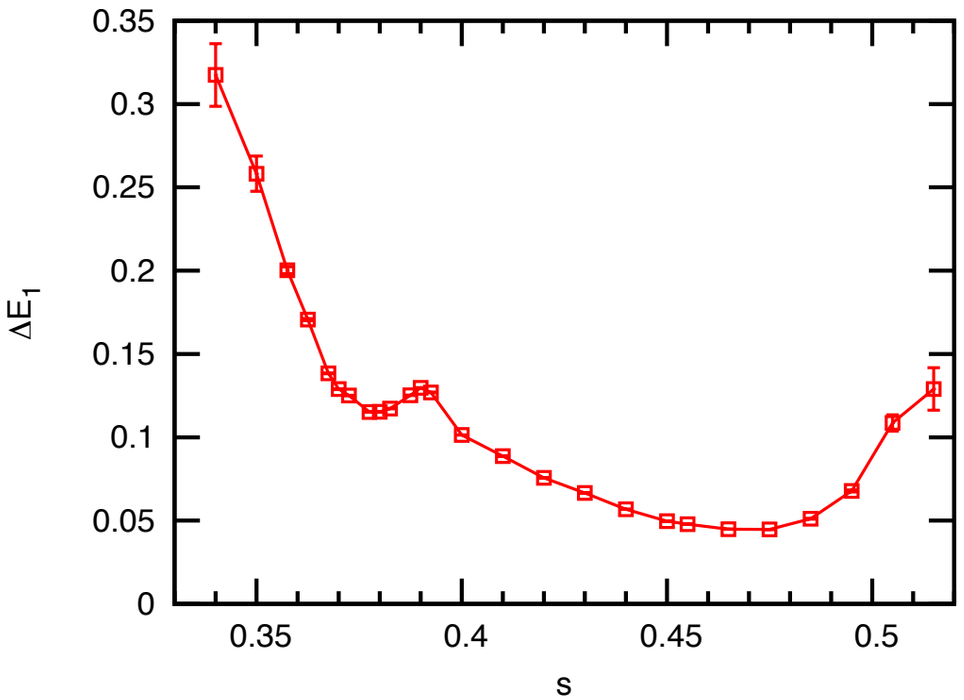
Adding the driver Hamiltonian there is a quantum phase transition at $s = s^*$ above which the symmetry is spontaneously broken.

Did “cavity” calculations (Gosset, Zamponi), semi-analytical approach in which the thermodynamic limit has been taken, but needs approximations in the spin glass phase for $s > s^*$. These calculations find $s^* \cong 0.36$

Also investigated the problem by QMC near s^* ($s \leq 0.5$).

(Just considered instances with a “unique satisfying assignment”, apart from the degenerate state related by flipping all the spins. These are exponentially rare.)

Spin glass on a random graph : III (Gap)



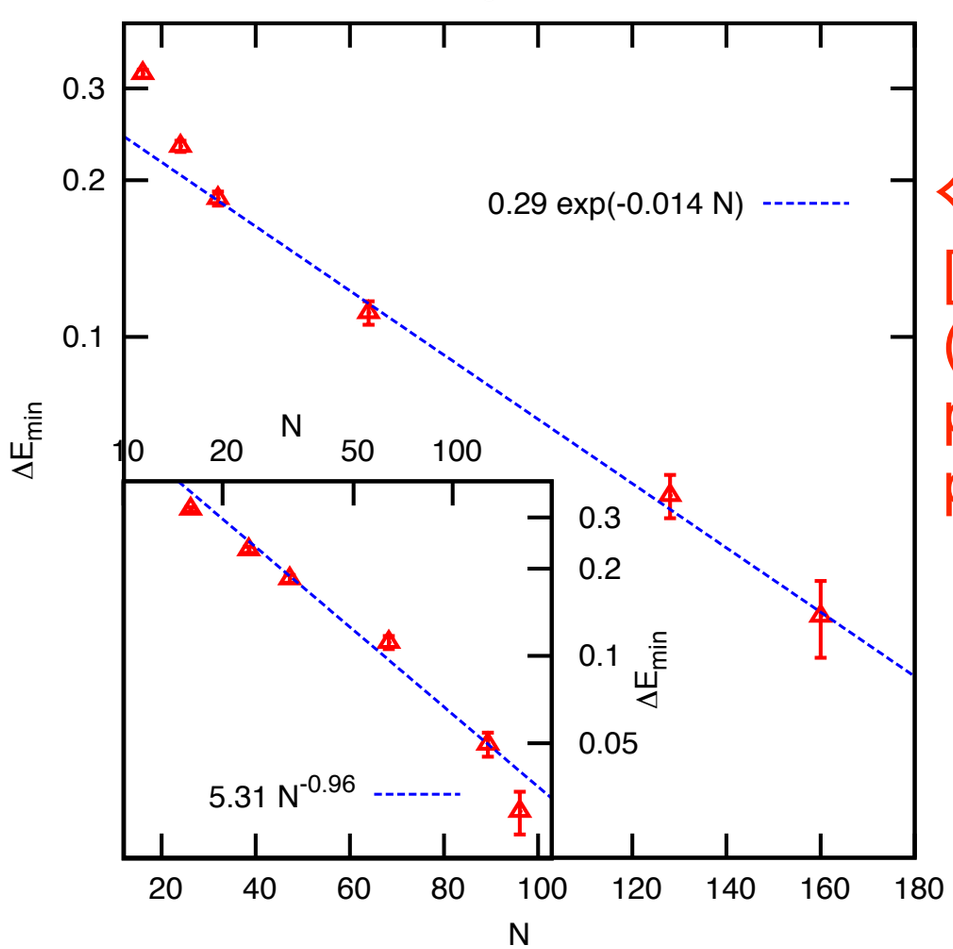
⇐ Figure shows an example for N = 128.

For larger sizes, a fraction of instances have **two minima**, one fairly close to s^* ($\simeq 0.36$) and other at larger s in the spin glass phase.

Hence did 2 analyses

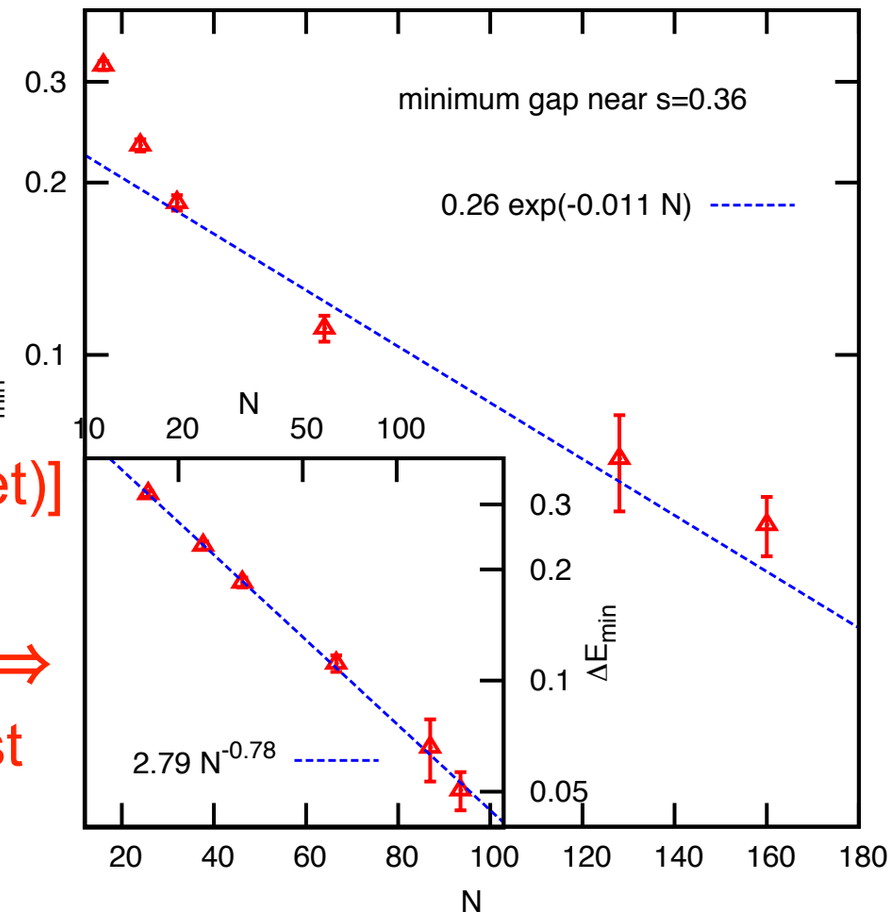
(i) Global minimum in range (up to s=0.5)

(ii) If two minima, just take the local minimum near s^*.



⇐Global
[exponential (main figure) preferred over power-law (inset)]

Local⇒
[power-law best (inset)]

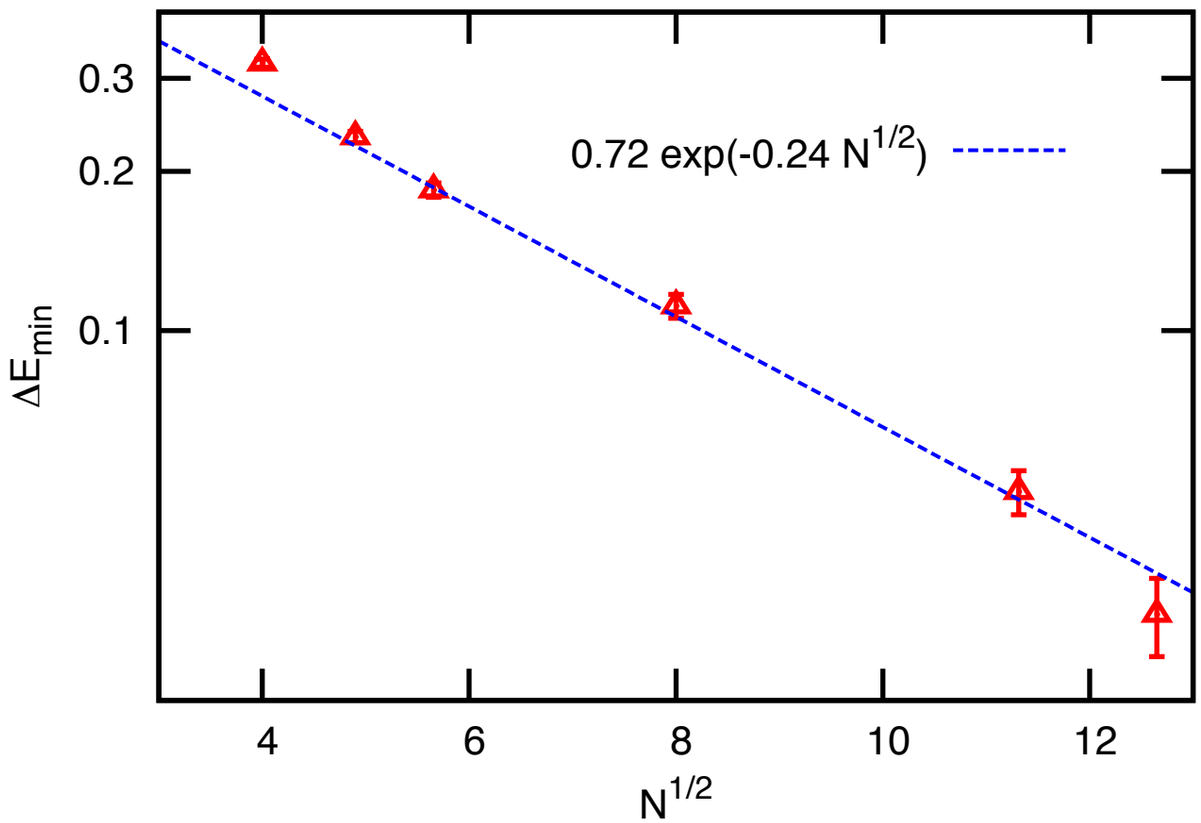


Spin Glass: IV (Summary)

For this spin glass the QAA **succeeds at** the quantum critical point (polynomial gap).

However, it appears **not to succeed at larger values of s** in the spin glass phase (exponential fit preferred over power-law for large sizes). But:

- This depends crucially on the last point (N = 160)
- A stretched exponential $\exp(-c\, N^x)$ $(x < 1)$ also works pretty well, e.g. $x = 1/2$ (figure). If this is the correct answer we would say that the QAA **does** succeed.



Conclusions

Conclusions

- Simple application of QAA seems to fail:

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems
  - In the spin glass phase, beyond the transition, in the spin glass model

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems
  - In the spin glass phase, beyond the transition, in the spin glass model
- What about other models?

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems
  - In the spin glass phase, beyond the transition, in the spin glass model
- What about other models?
- Perhaps the QAA could be useful to get an approximate ground state. (For some problems, even this is difficult).

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems
  - In the spin glass phase, beyond the transition, in the spin glass model
- What about other models?
- Perhaps the QAA could be useful to get an approximate ground state. (For some problems, even this is difficult).
- I have just described the simplest implementation of the QAA. Perhaps if one could find clever paths in Hamiltonian space one could do better. A subject for future research.

Conclusions

- Simple application of QAA seems to fail:
  - At the (first order transition) for SAT problems
  - In the spin glass phase, beyond the transition, in the spin glass model
- What about other models?
- Perhaps the QAA could be useful to get an approximate ground state. (For some problems, even this is difficult).
- I have just described the simplest implementation of the QAA. Perhaps if one could find clever paths in Hamiltonian space one could do better. A subject for future research.

Danke schön