Phase transition phenomena of statistical mechanical models of the integer factorization problem

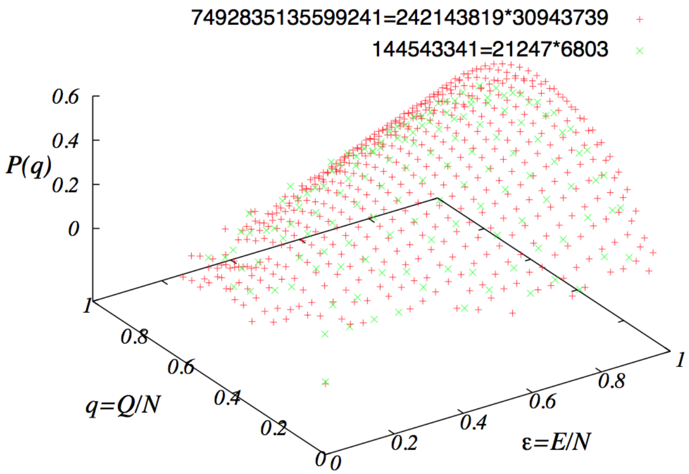
(submitted to JPSJ, now in review process)

Chihiro Nakajima
WPI-AIMR, Tohoku University

Masayuki Ohzeki
Graduate School of Information Sciences, Kyoto University

科研費
KAKENHI

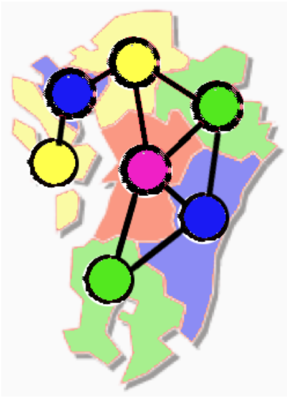
QUANTUM ANNEALING MACHINE LEARNING



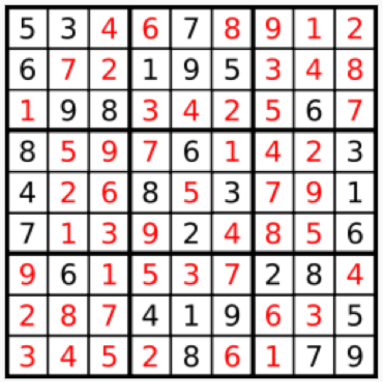
From spin glass to computational problem

Statistical physics of spin glass spreads to various computational problems.
-- optimization or constraint satisfaction including NP-hard or NP-complete problems.

Traveling salesman problem



Graph coloring



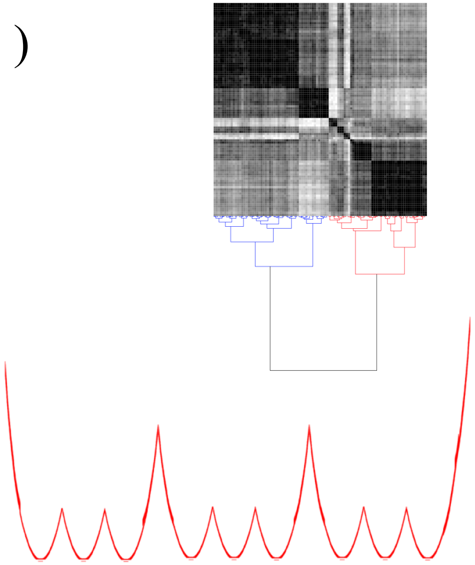
5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Number placing (sudoku)

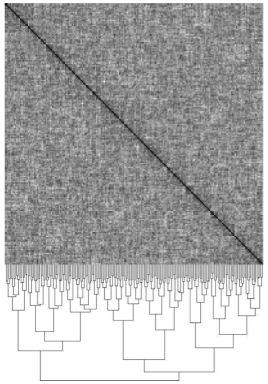
- Many algorithms from statistical mechanics, such as simulated annealing
- Recently taken over by quantum annealing.

Statistical mechanical study of (NP-complete/NP-Hard) CSPs

- 2-SAT and 3-SAT (*Different behavior for P and NP-complete problems*)
  R. Monasson *et. al.*, Nature (1999)
- Graph coloring
  L. Zdeborova, and F. Krzakala, Phys. Rev. Lett. (2007).
  F. Krzakala et. al., Proc. Nat. Acad. Sci. (2007).



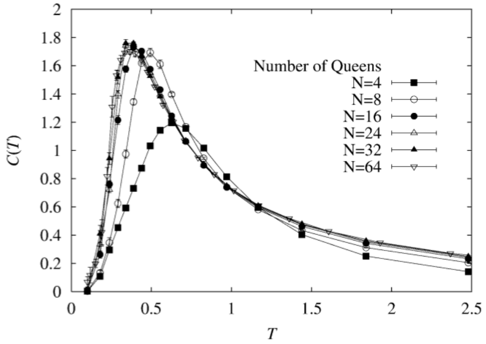
- vertex cover
  Hierarchical clustering of energy landscape
  A. K. Hartmann, and A. Mann, J.Phys.: Conference Series (2008).
  A. Mann, and A. K. Hartmann, Phys. Rev. E. (2010).
  RSB
  M. Weigt, and A. K. Hartmann, Phys. Rev. Lett., (2010)



- Number partitioning
  A. K. Hartmann, and A. Mann, J.Phys.: Conference Series (2008).
  S. Mertens, Phys. Rev. Lett. (1998).

Still unclear for glass transition (?)

- N-queen problem
  K. Hukushima, Comp. Phys. Commun. (2002).



Phase transition(s) of NP-complete problems

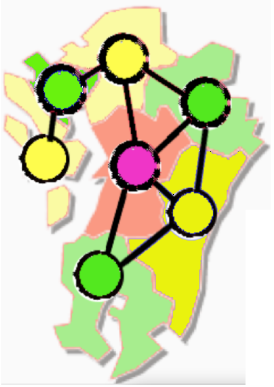
On the example of graph coloring

[Mézard, Parisi, Zecchina, Science (2002), Mulet, Pagnani, Weigt, Zeccina (2002)]

N : Number of vertices

M : Number of edges

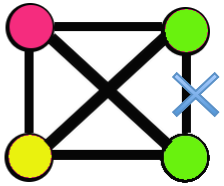
α : Mean connectivity



$N = 7$

$M = 9$

$\alpha \approx 1.286$



Random graph instances,
for example Erdos-Renyi graph.

$$P(J_{ij}) = \frac{\alpha}{N}\delta(J_{ij} - 1) + \left(1 - \frac{\alpha}{N}\right)\delta(J_{ij})$$

$$\alpha = \frac{M}{N} \approx O(N^0)$$

$$\sigma_i \in \{1, \cdots q\},$$

$$H(\{\sigma\} \mid J) = \sum_{(ij)} J_{ij}\delta_{\sigma_i \sigma_j}$$, 0/1 for satisfied/violated edges.

$$Z(J) = \sum_{\{\sigma\}} \exp\left(-\beta H(\{\sigma\} \mid J)\right) = \exp\left(-\beta F(J)\right)$$

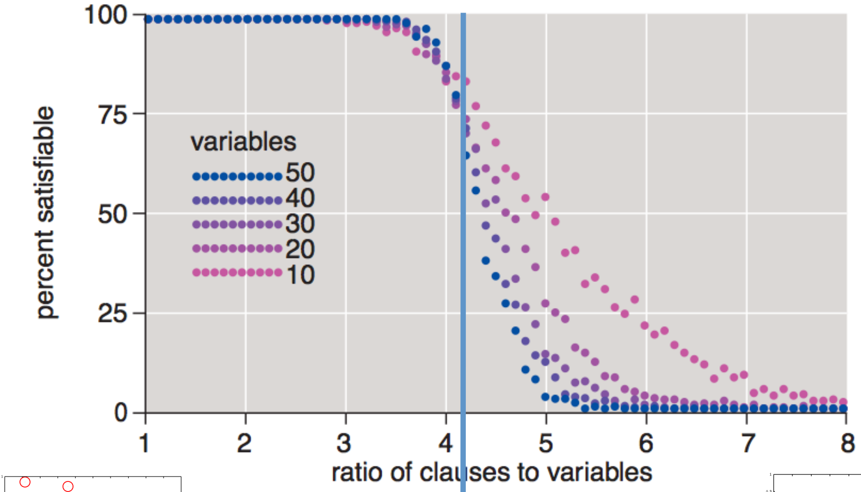
$$[F]_\alpha = \sum_{\{J\}} F(J)\delta(M/N - \alpha)$$, ensemble of thermodynamic quantities on random instances.

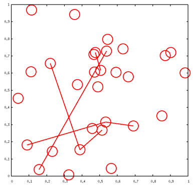
Averaging over random graph instances and taking $N \to \infty$ limit.

Phase transition(s) of NP-complete problems

Graphs from [Hayes, American Scientist **85**, (1997)], for 3-SAT.

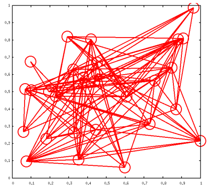
Fraction of satisfiable instances





$\left[\langle E\rangle_{T=0}\right]_{\alpha} = 0$

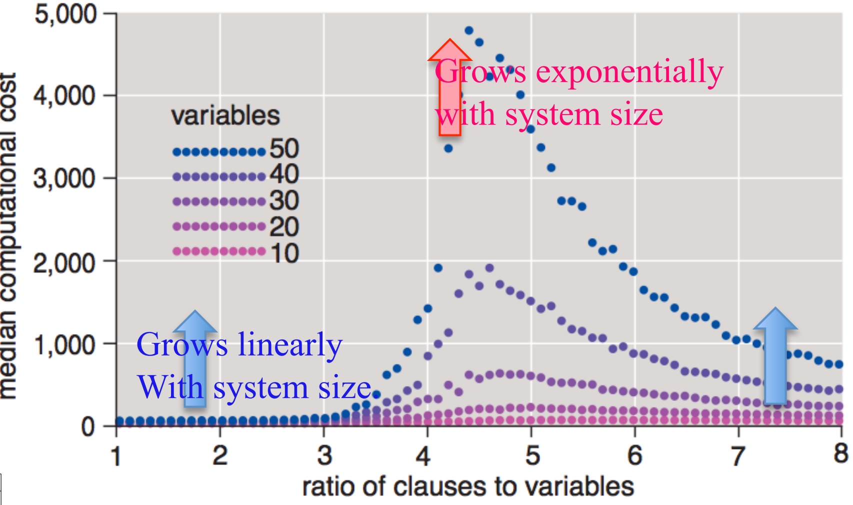
$\left[\langle E\rangle_{T=0}\right]_{\alpha} > 0$



Typically satisfiable.

Typically unsatisfiable.

Computational time by DPLL algorithm



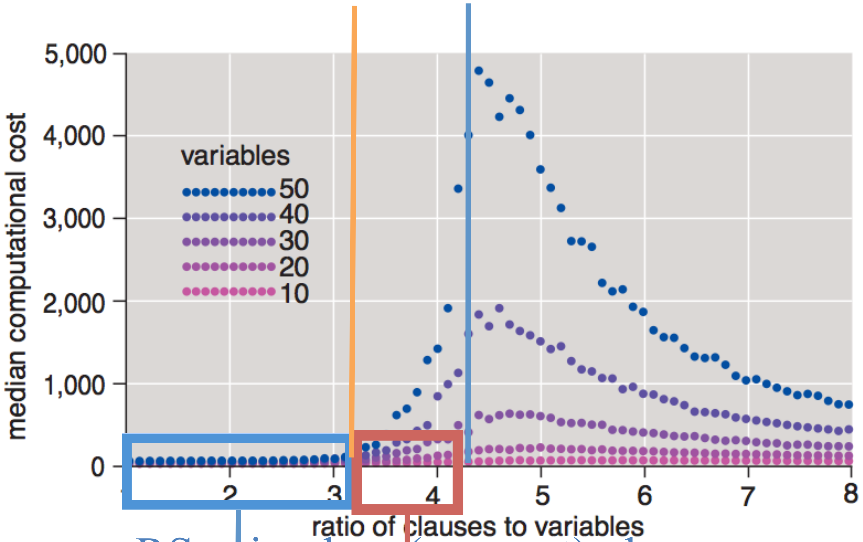
Grows exponentially with system size

Grows linearly With system size

Computational time seems to increase exponentially NEAR sat-unsat transition threshold (with graph coloring, called col-uncol transition).

Phase transition(s) of NP-complete problems

In fact there is another (or more) phase transition, which is described in terms of spin glass theory.

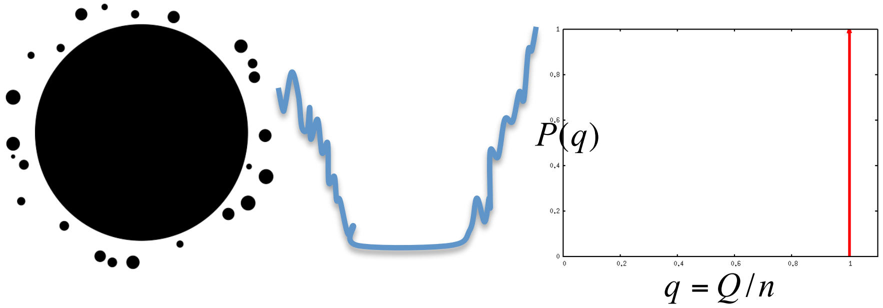


RS spin glass (easy sat) phase

1RSB spin glass (hard sat) phase

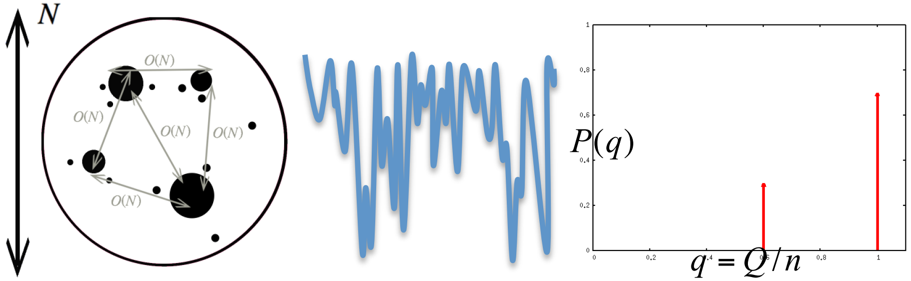
Replica symmetric phase (easy sat phase)

- Most of solutions are connected each other. (They can come/go with flipping a single spin)
- Overlap distribution has unimodal shape.
- Energy landscape has basin of solutions.



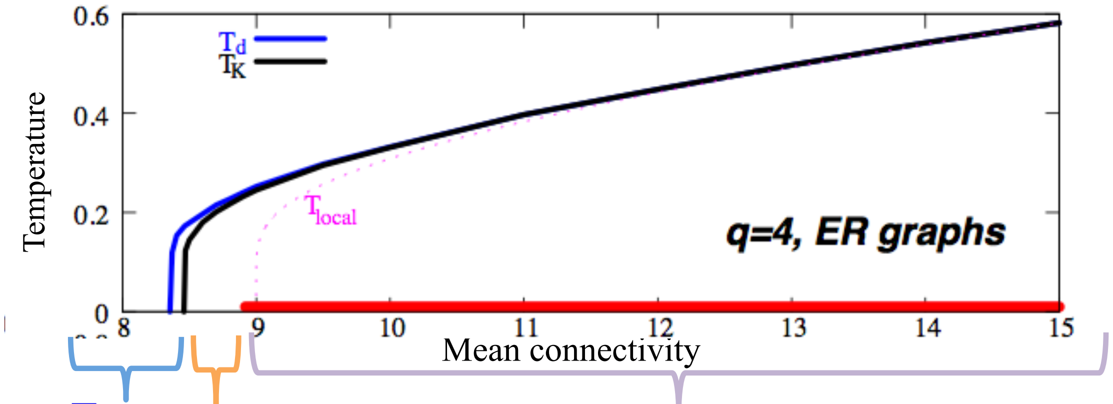
Replica symmetry breaking phase (hard sat phase)

- Clustered solutions are embedded sparsely.
- Overlap distribution has multimodal shape.
- Energy landscape is rugged.



In 1RSB phase, overlap distribution has multimodal character (even in thermodynamic limit), and computational time grows exponentially with the system size.

Hard/Easy transition extends to finite temperature regime



Easy Hard UNSAT (UNCOL)

Graphs from
[Zdeborova, Eur. Phys. Lett, (2008)]
for 4-coloring case.

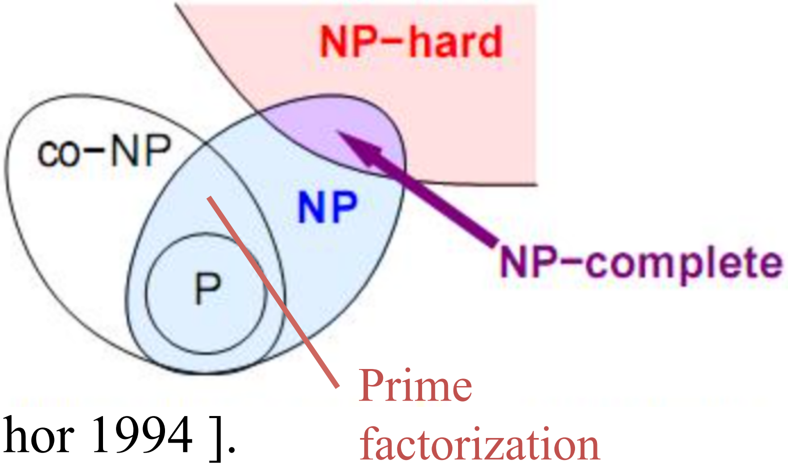
Fraction of success

The prime factorization is (hard but) not NP-complete

- For prime factorization, no polynomial time algorithm have been found, but it is in $\mathrm{NP} \cap \mathrm{co-NP}$.
  -- not thought to be NP complete.

- With the number sieve method, it is solved with quasi-exponential ($\exp(n^{\alpha})$) time in classical computation.
  -- sub-exponential algorithms are found.

- Polynomial time quantum algorithm is found [Shor 1994].



Question (Interest)

▪ *Does any phase transition or non-trivial behavior of thermodynamic quantity explains the complexity of factorization problems?*
-Can we apply the landscape or phase transition picture to the factorization problems, 'beyond' the NP-complete problem ?

Testing the Prime factorization

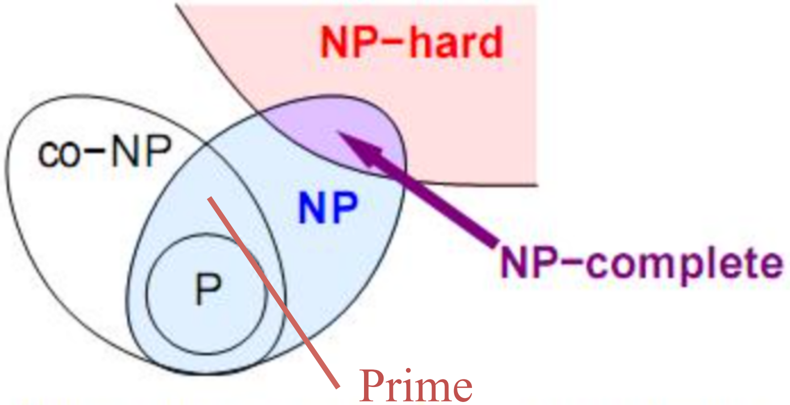
To tackle the relation among phase transition phenomena or landscape and the computational hardness,
exploring beyond NP-complete problems may be worth.

Testing the Prime factorization is …
in the context of classical picture,
it can be to test the applicability/extensibility of the replica-theoretic picture.

in the context of quantum annealing picture,
it may be worth exploring a case of scaling of minimal energy gap
with HARD BUT NOT NP-complete case.

The prime factorization is (hard but) not NP-complete

- For prime factorization, no polynomial time algorithm have been found, but it is in $\mathrm{NP} \cap \mathrm{co} - \mathrm{NP}$.
  -- not thought to be NP complete.
- With the number sieve method, it is solved with quasi-exponential ($\exp\left(n^{\alpha}\right)$) time in classical computation.
  -- sub-exponential algorithms are found.
- Polynomial time quantum algorithm is found [Shor 1994].



Prime factorization

Question (Interest)

- *Does any phase transition or non-trivial behavior of thermodynamic quantity explains the complexity of factorization problems?*
  -Can we apply the landscape or phase transition picture to the factorization problems, ‘beyond’ the NP-complete problem ?

Formulation of the problem

- The situation of dividing$N = p_1 \times \cdots p_l \times \cdots p_m$ with a trial divisor d.
  Such that$2^{n-1} < \sqrt{N} < 2^n$ and $d \in \{2, \cdots, 2^n\}$.

- Binary (spin) variable representation of d ;

$$d(\{s_i\}) = 2 + \sum_{i=0}^{n-1} s_i 2^i, \;\; s_i \in \{0,1\}$$

- Cost function H which is extensive with n ,
  for sound property of thermodynamic function or phase transition ;

-- $H(d) = 0$ if and only if d is a correct divisor of N, otherwise $H(d) > 0$.

-- $$\langle H \rangle_\beta = \frac{\sum_{\{s_i\}} H(\{s_i\}) \exp(-\beta H(\{s_i\}))}{\sum_{\{s_i\}} \exp(-\beta H(\{s_i\}))} \approx n$$

$$\sigma_j \in \{0,1\}$$

$$H(d) = \lceil \log_2(1 + \mathrm{mod}(N,d)) \rceil$$

-- Maximum digit based model

$$H(d) = \sum_{j=0}^{n-1} \sigma_j, \;\; \mathrm{mod}(N,d) = \sum_{j=0}^{n-1} \sigma_j 2^j$$

-- Summation based model

Formulation of the problem

For sufficiently large m, it has exponential numbers of ground states, like spin glass models.

For $N = p_1 \times \cdots p_l \times \cdots p_m$, this model has ground states

$$d_{sol} \in \left\{ \begin{matrix} p_1, \cdots, p_m, \\ p_1 p_2, \cdots, p_{m-1} p_m, \cdots, \\ p_1 p_2 p_3, \cdots, \\ p_1 \cdots p_{m-1}, \cdots, p_2 \cdots p_m \end{matrix} \right\}.$$

Totally $2^m - 2$ ground states, 1 and N itself are excluded.
-- exponential number of system size.

Here we treat the case with $N = p_1 p_2$.

Quantities of interest

Hamming distance from correct solution
(Overlap function with ground state)

$$\hat{Q}(\{s_i\}) = \sum_{i=0}^{n-1} \frac{1 - (2s_i - 1)(2s_i^* - 1)}{2}$$

Density of states on hamming distance Q and energy E ;

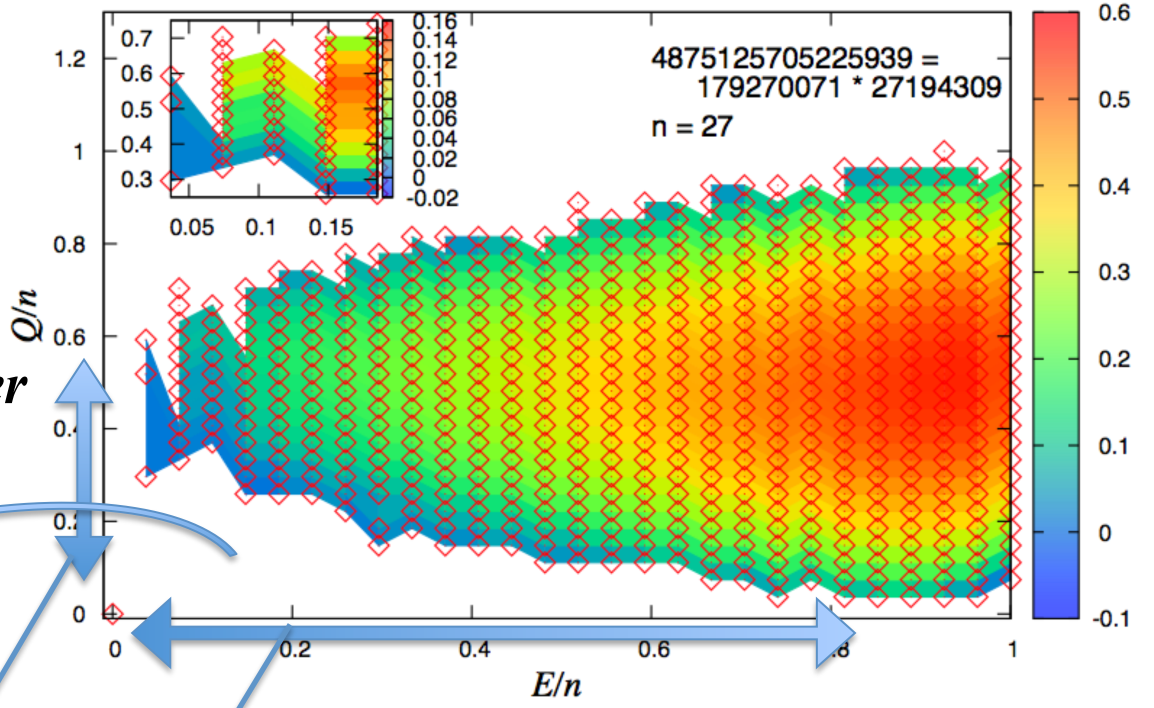
$$W(E, Q) = \sum_{\{s_i\}} \delta\left(\hat{Q}(\{s_i\}) - Q\right) \delta\left(H(\{s_i\}) - E\right) = \exp\left(S(E, Q)\right)$$

Behavior of the model : Isolated solution

$H(d) = \lceil \log_2(1 + \mathrm{mod}(N, d)) \rceil$: Maximum digit model

- ***The ground state is isolated in configuration space.***
- ***Both the distance from other low energy states and the height of energy barrier are proportional to system size.***

Support of $W(E,Q)$



There is region with no support
$(W(E,Q) = 0)$
around ground state.

Energy barrier with depth
$\Delta E = O(n) \quad (\approx 0.8n)$.

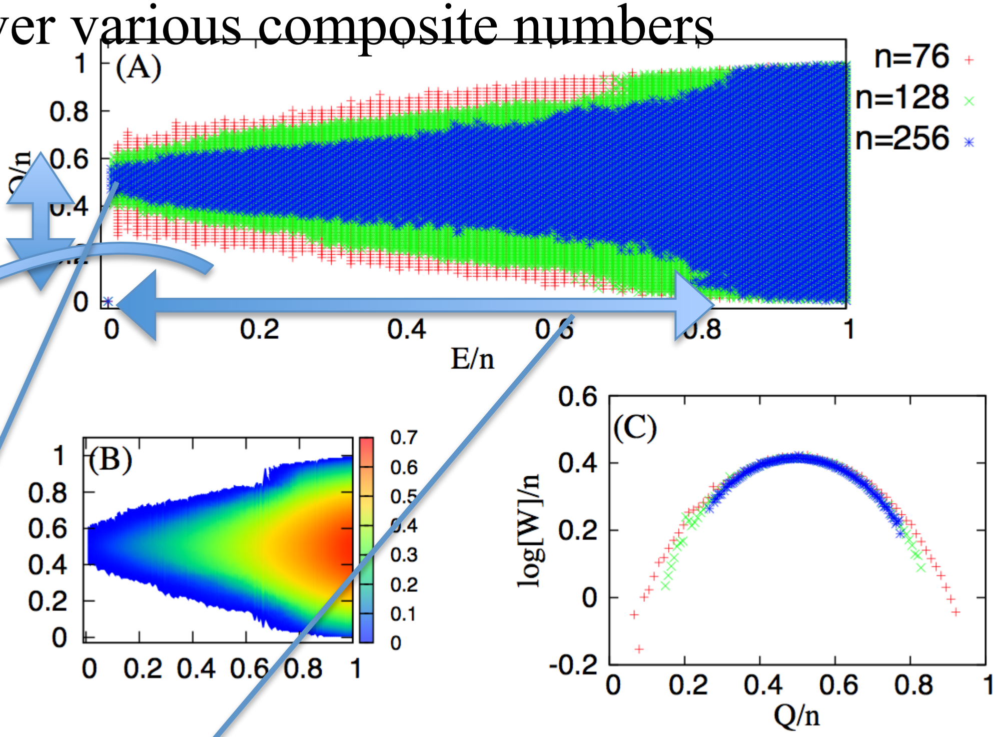
Largely distant $\Delta Q = O(n) \quad (\approx 0.5n)$
between low energy excited states and ground state.

Behavior of the model : Isolated solution

$H(d) = \lceil \log_2 (1 + \mathrm{mod}(N, d)) \rceil$: Maximum digit model

Up to n=256 (N=2^512), averaged over various composite numbers

- ***The ground state is isolated in configuration space.***
- ***Both the distance from other low energy states and the height of energy barrier are proportional to system size.***



There is region with no support ($W(E,Q) = 0$) around ground state.

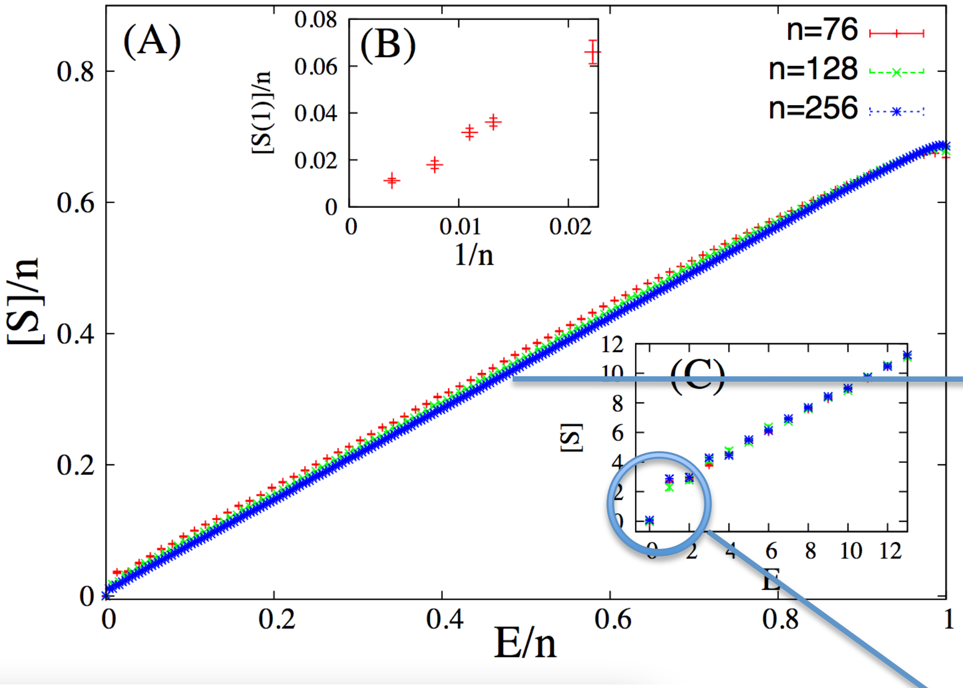
Energy barrier with depth $\Delta E = O(n) \quad (\approx 0.8n)$.

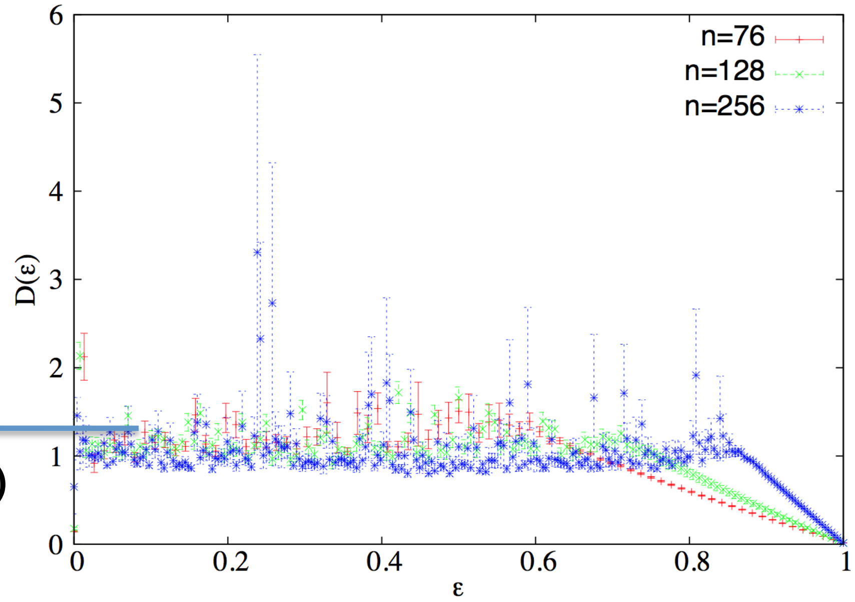
Largely distant $\Delta Q = O(n) \quad (\approx 0.5n)$ **between low energy excited states and ground state.**

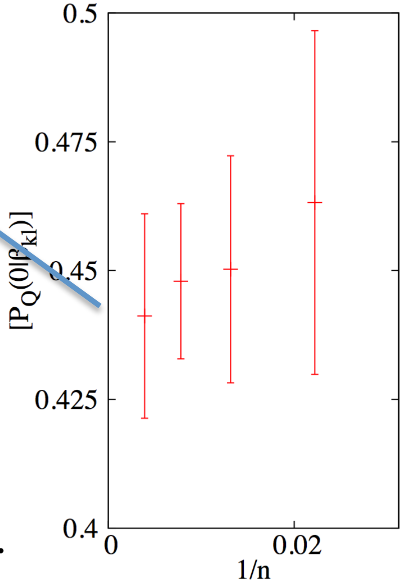
Shape of density of states and phase transition

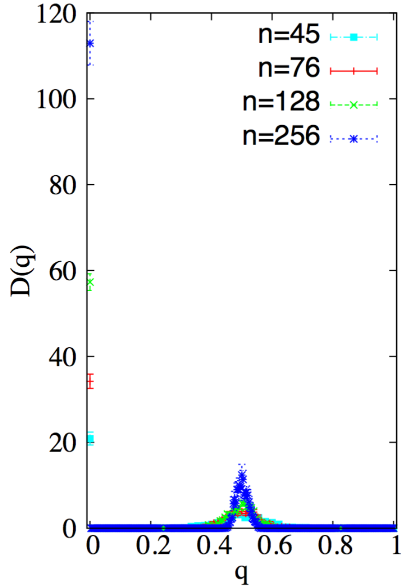
Microcanonical entropy $\frac{1}{n}[S(E)] = \frac{1}{n}[\log W(E)]$

$$H(d) = \lceil \log_2(1+\mathrm{mod}(N,d)) \rceil$$









(1) Slope : Broad region with $\frac{d^2S(E)}{dE^2} = 0$.

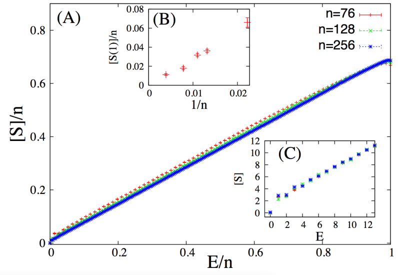
→ Peculiar phase transition

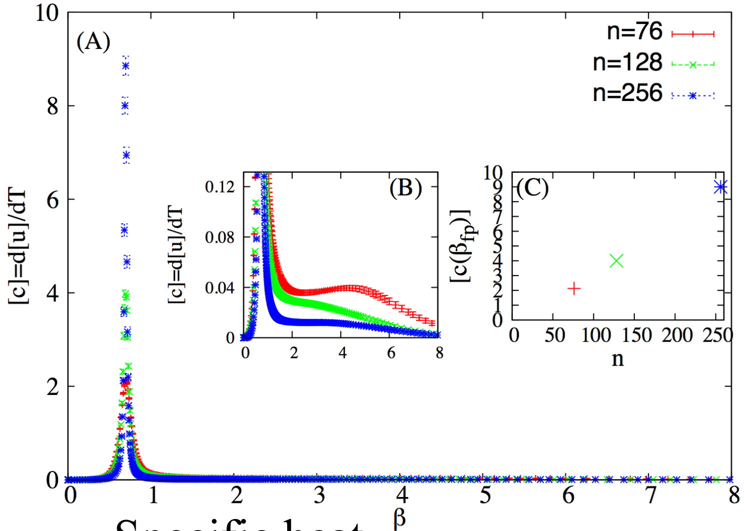
(2) Kink : Value of $\frac{dS(E)}{dE}$ is discontinuously different at E=1.

→ Dip in the specific heat.

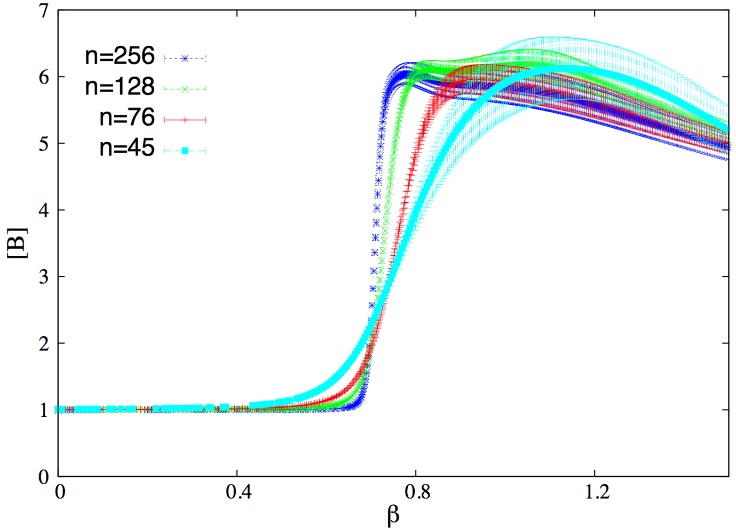
Internal energy depends very weakly on the temperature.

(1) : Peculiar first order transition(1/3)





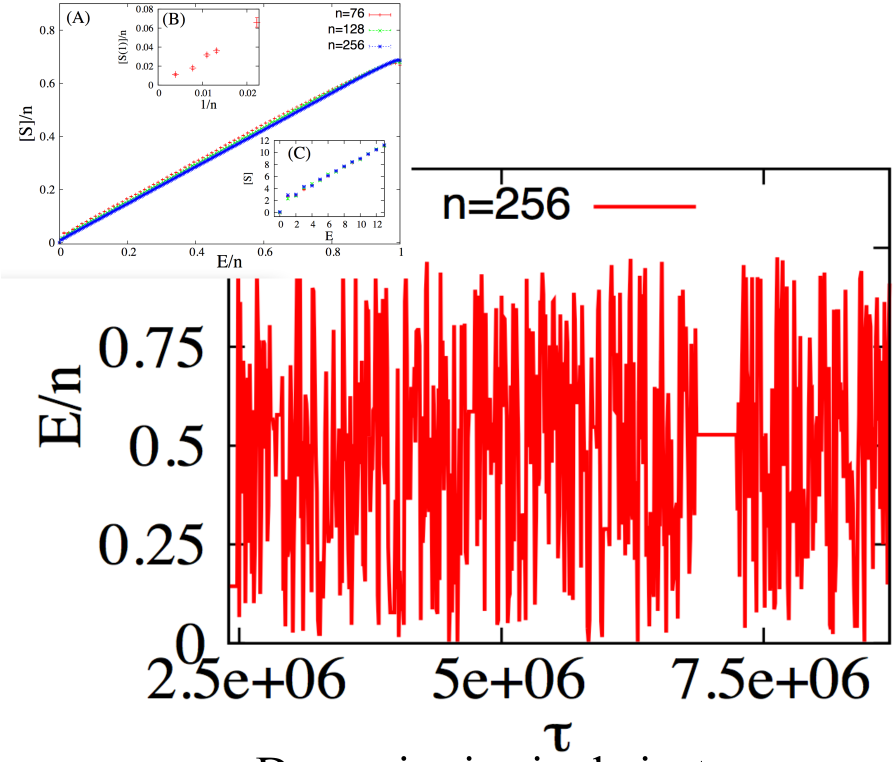
Specific heat
approaches to delta peak.



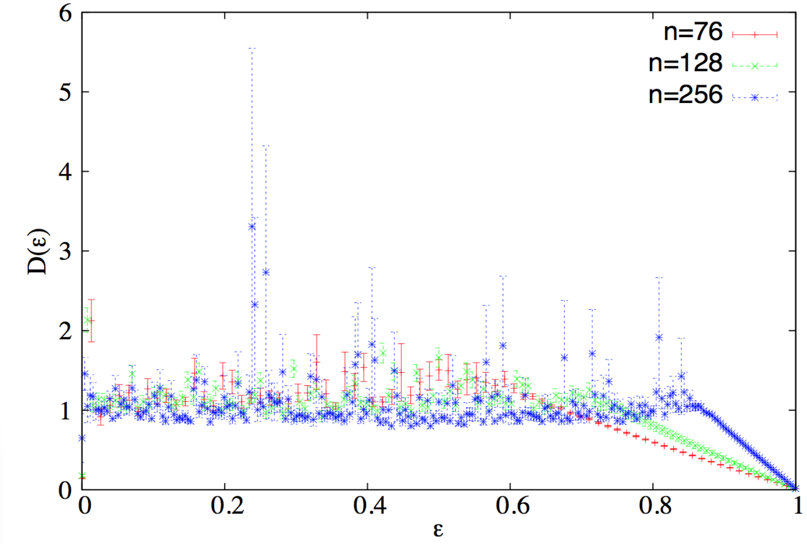
Binder ratio of energy converges to $\left[\frac{\langle E^4\rangle}{\langle E^2\rangle^2}\right] > 1$.
(Indicates the jump of the internal energy.)

These features are shared with the first order phase transition.

(1) : Peculiar first order transition (2/3)



Dynamics in single instance is different for that in bistable potential, it moves SMOOTHLY.

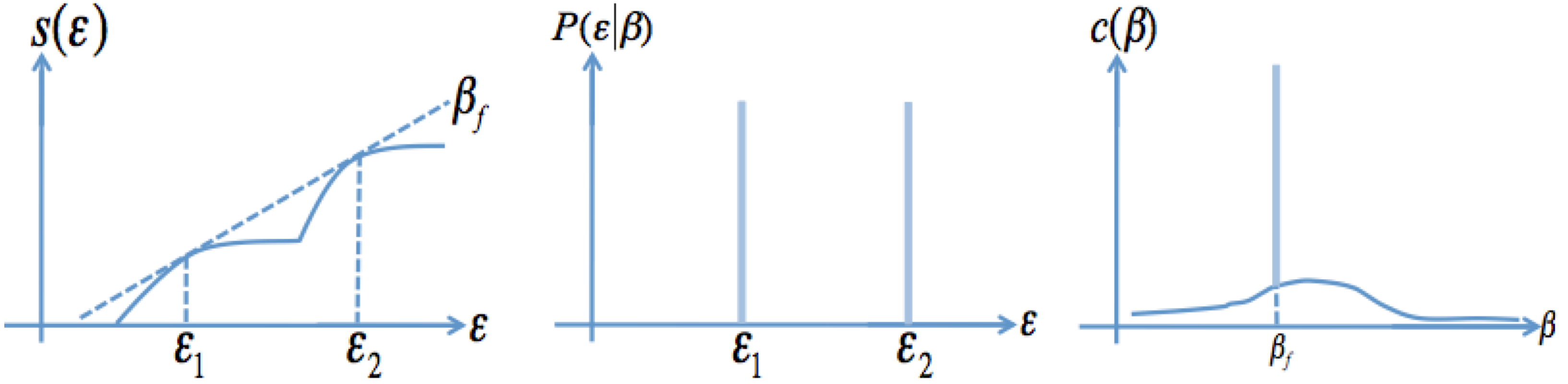


Energy distribution function has a FLAT region at the transition temperature. $\frac{d^2S(E)}{dE^2}\sim 0$

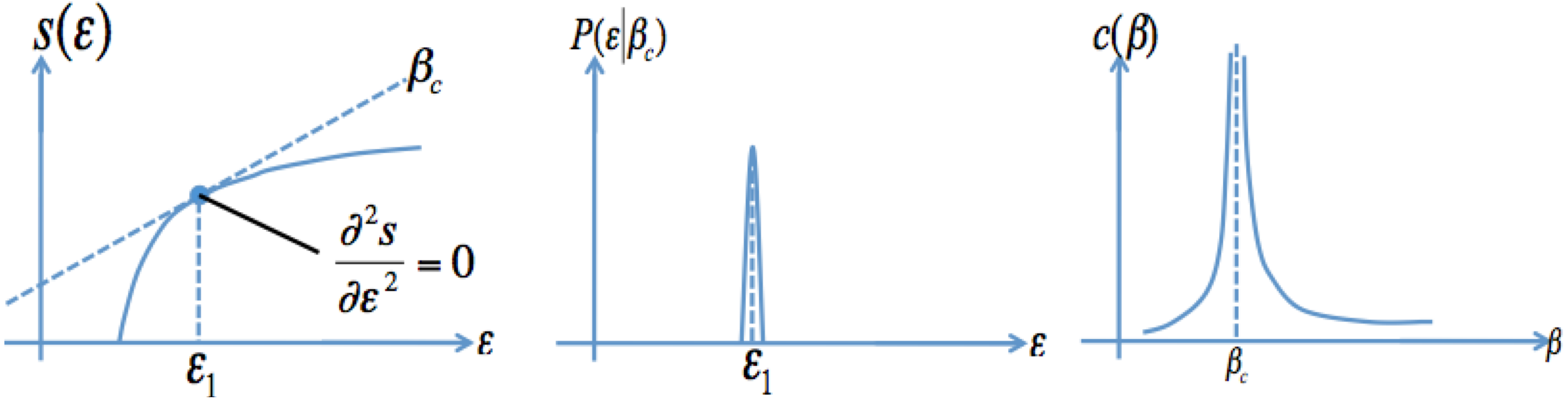
- The distance between low and high energy region is BRIDGED, NOT BISTABLE. This is NOT likely to the ordinary phase transition.
- It has a region with $\frac{d^2S(E)}{dE^2}=0$. This feature is in some sense common with the SECOND order phase transition (however, the region is much broader here).

Phase transition behavior

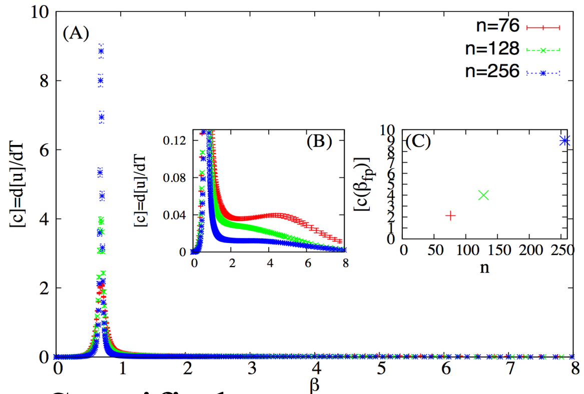
In the case of an ordinary first order phase transition



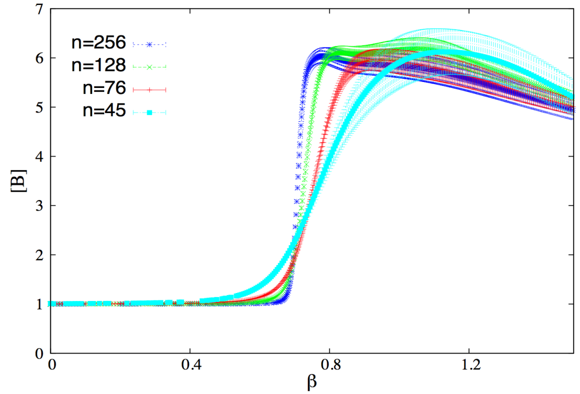
In the case of an ordinary second order phase transition (with critical exponent α > 0)



(1) : Peculiar first order transition (3/3)

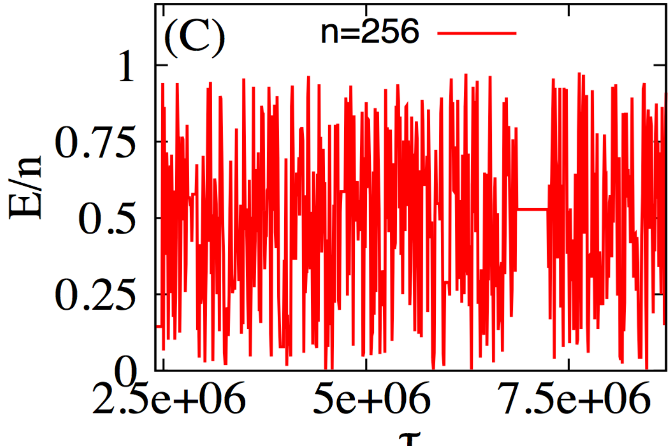


Specific heat approaches to delta peak.

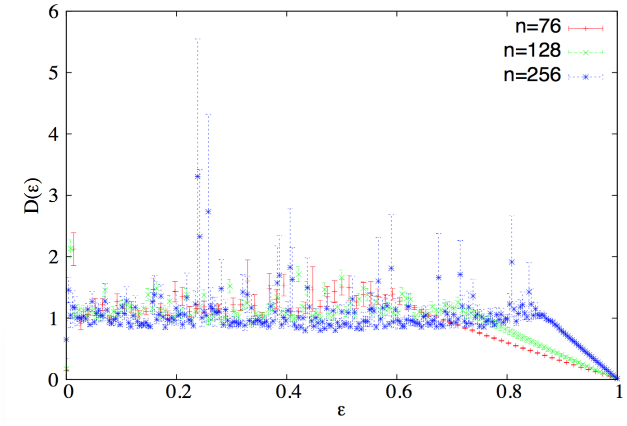


Likely to first order Transition.

Binder ratio of energy converges to $\left[\frac{\langle E^4\rangle}{\langle E^2\rangle^2}\right] > 1$.



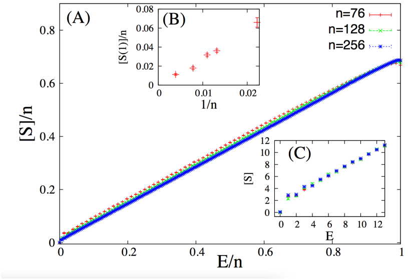
Dynamics is different for that in bistable potential, it moves smoothly.



Not likely to first order (rather likely to second order) Transition.

Energy distribution function has a flat region at the transition temperature.

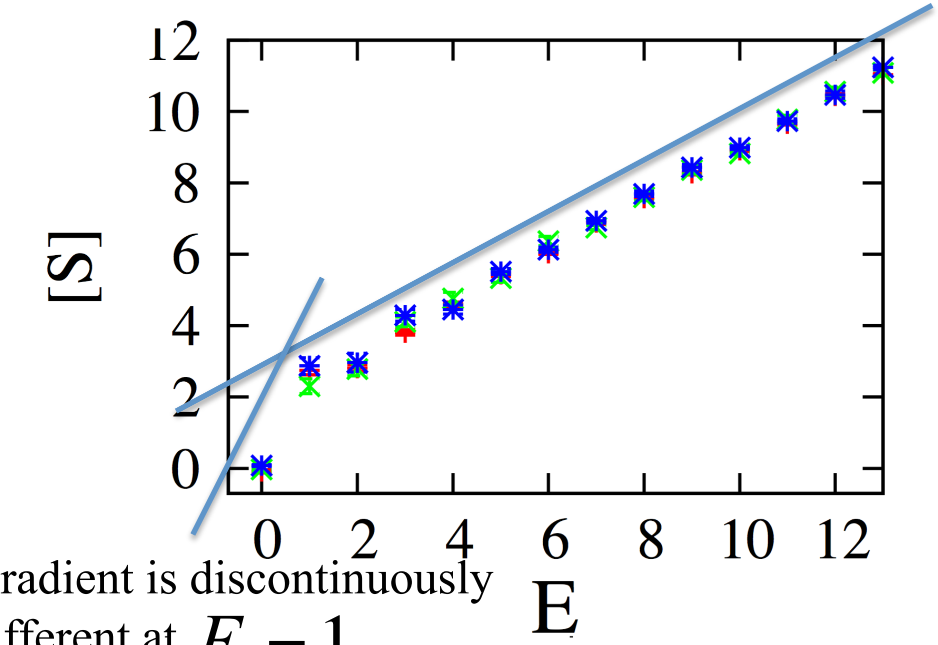
$$\frac{d^2S(E)}{dE^2} \approx 0$$



It has both features of first and second order phase transition.

(2) ‘Kink’ in energy density of states

When the governance changes between low but positive energy states and the true ground state,

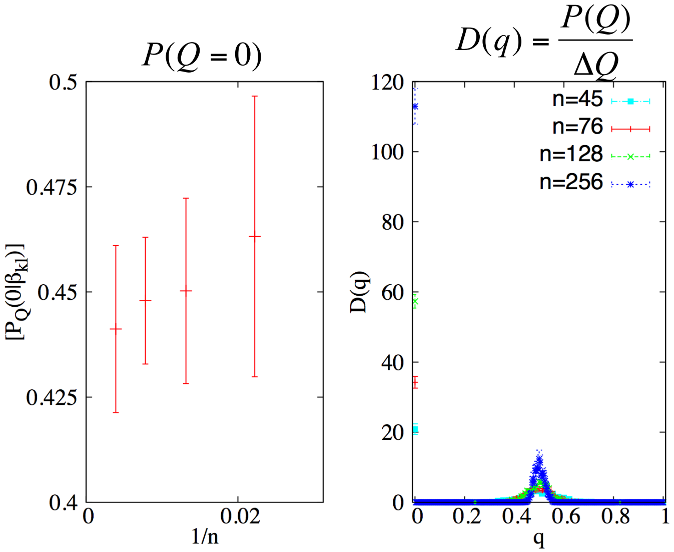


Gradient is discontinuously different at $E=1$.

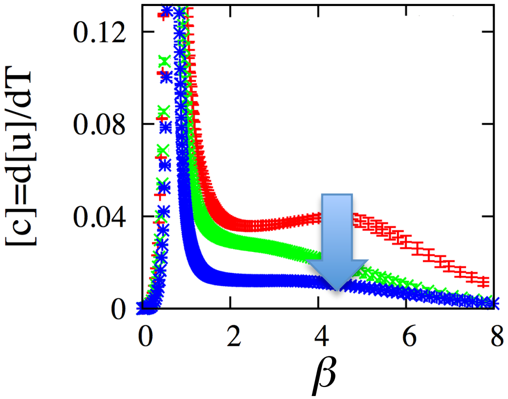
(Not normalized by the system size.)

The gradient $\frac{dS(E)}{dE}$ seems to be constant.

Internal energy depends very weakly on the temperature.



Distribution of normalized overlap at fixed temperature

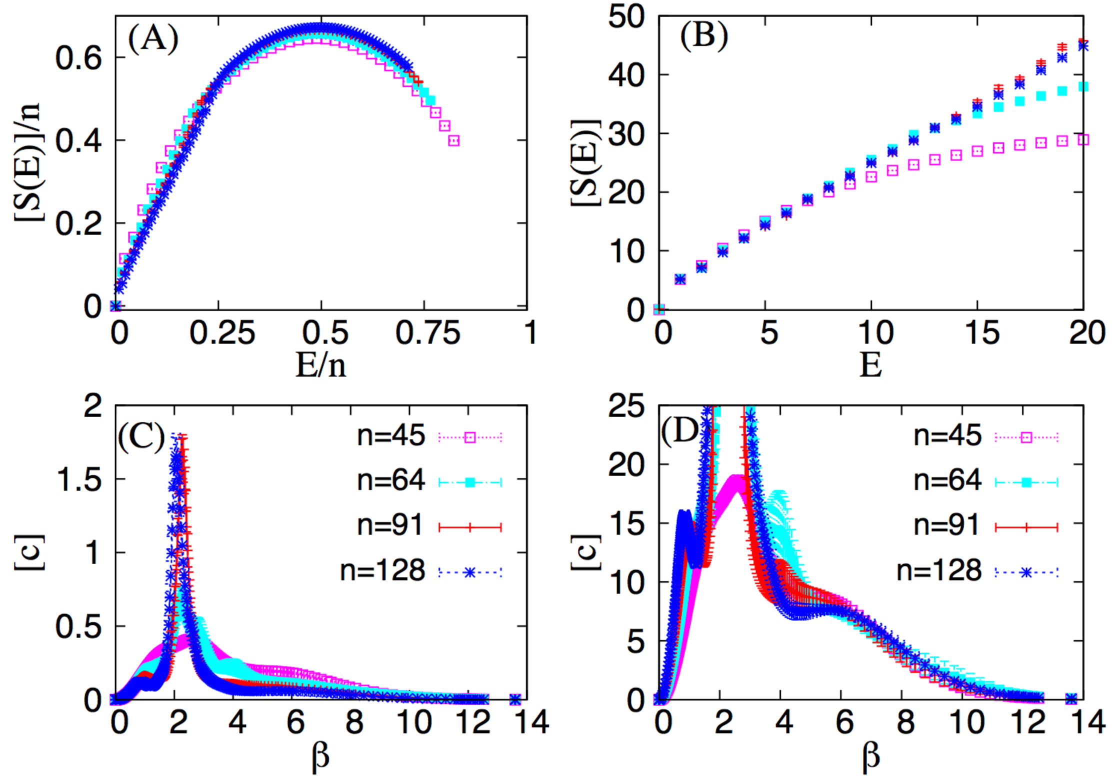


This is NOT a phase transition (dip of [c] disppears in thermodynamic limit).

But it is CHARACTERIZED by temperature.

Commonly exhibited in summation-based model

$$H(d)=\sum_{j=0}^{n-1}\sigma_j,\ \ \mathrm{mod}(N,d)=\sum_{j=0}^{n-1}\sigma_j 2^j$$: Summation-based model



‘Slope’ and ‘kink’ also appear in the profile of energy density of state of summation-based model.

Testing the Prime factorization

To tackle the relation among phase transition phenomena or landscape and the computational hardness,
exploring beyond NP-complete problems may be worth.

Testing the Prime factorization is …
in the context of classical picture,
it can be to test the applicability/extensibility of the replica-theoretic picture.

in the context of quantum annealing picture,
it may be worth exploring a case of scaling of minimal energy gap
with HARD BUT NOT NP-complete case.

As classical counterpart of quantum annealing ?

Scaling of minimal energy gap in quantum annealing

$$\tau \propto (\Delta E)^{-2}$$

$$\Delta E = E_1 - E_0 \propto \begin{cases} \exp(-\alpha n) \\ n^{-\gamma} \end{cases}$$

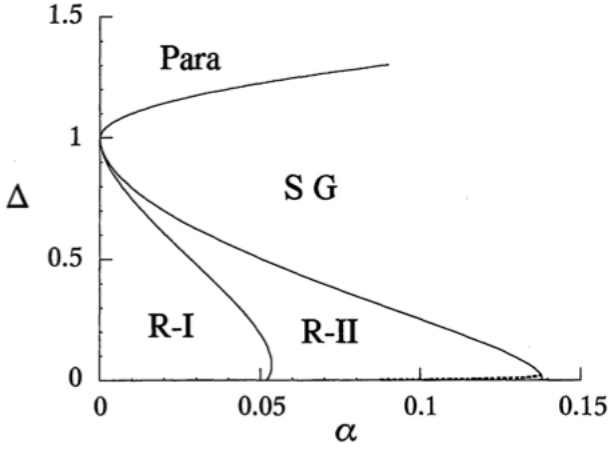
Then,,,

how is the peculiar phase transition of the factorization model ?

-- In the sense that it seems to occupy the intermediate position.

Is the transition represents an intermediate position of the factorization IN COMPLEXITY CLASS ?

Example of coincidence between quantum and classical phase diagram



[Nishimori and Nonomura, J. Phys. Soc. Jpn (1996)]

Quantum Hopfield model.
The ground state quantum phase diagram is quite similar to that of classical thermal version.

The overlap between the ground state and the low energy *eigen* state, $\langle \psi_{GS} | \psi_{FE} \rangle$ matters.

Summary

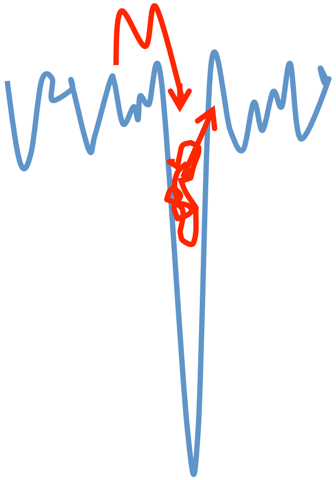
We analyzed the statistical mechanical model of integer factorization problem, focusing on its phase transition phenomena.

- We find that the ground state is completely isolated from other low energy states with $O(n)$ distant or height barrier.
- The peculiar shapes are found in the density of states, in addition they lead phase transition-like behavior;
  - -- Slope → Peculiar phase transition which has both feature of first and second order.
  - -- Kink → Dominant region in phase space drastically changes at second characteristic temperature.

- Is the potential energy landscape rather simple comparing to those of NP-complete problems?
  - -- If it is, that seems to have rich implication to the fact that the integer factorization problem is computationally hard problem but considered to be not enough to comparable to the NP-complete problems.

- We plan to pursue the behavior of this problem with quantum annealing.

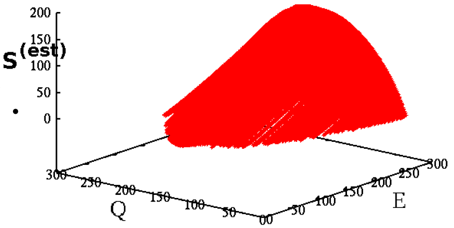
To avoid difficulty
with golf-course landscape, …



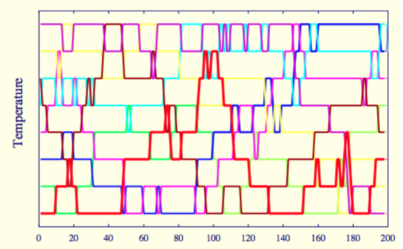
There is an extensive gap between the ground state and its vicinities.
The replica exchange Monte Carlo does not work efficiently in such case.

To avoid the difficulty,
Multi-histogram reweighting and replica exchange are combined.

1. Once the energy E and the Hamming distance Q is computed.
2. The transition (of microscopic state) is accepted with the difference of the potential $V(E,Q)$. $\gamma \in \{\gamma_1,\cdots,\gamma_R\}$
   (The canonical distribution with $P(E,Q|\gamma)=\frac{1}{Z}\exp[-\gamma V(E,Q)]$ is realized.)
3. Density of states $W(E,Q)$ is estimated from $P(E,Q|\gamma)$ with various γ .



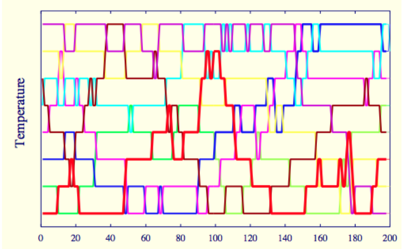
4. The histogram and potential are improved by iteration.



$P^{(n-1)}(E,Q) \propto \exp\left(-\gamma V^{(n-1)}(E,Q)\right)$

$$W_k=\frac{\sum_{j=1}^{R} h_k^{(j)}}{\sum_{j=1}^{R}\left\{\frac{\omega_k^{(j)}}{z_j}\left(\sum_{i=1}^{E} h_i^{(j)}\right)\right\}}$$

$V^{(n)}(E,Q)=-\log W^{(n-1)}(E,Q)$



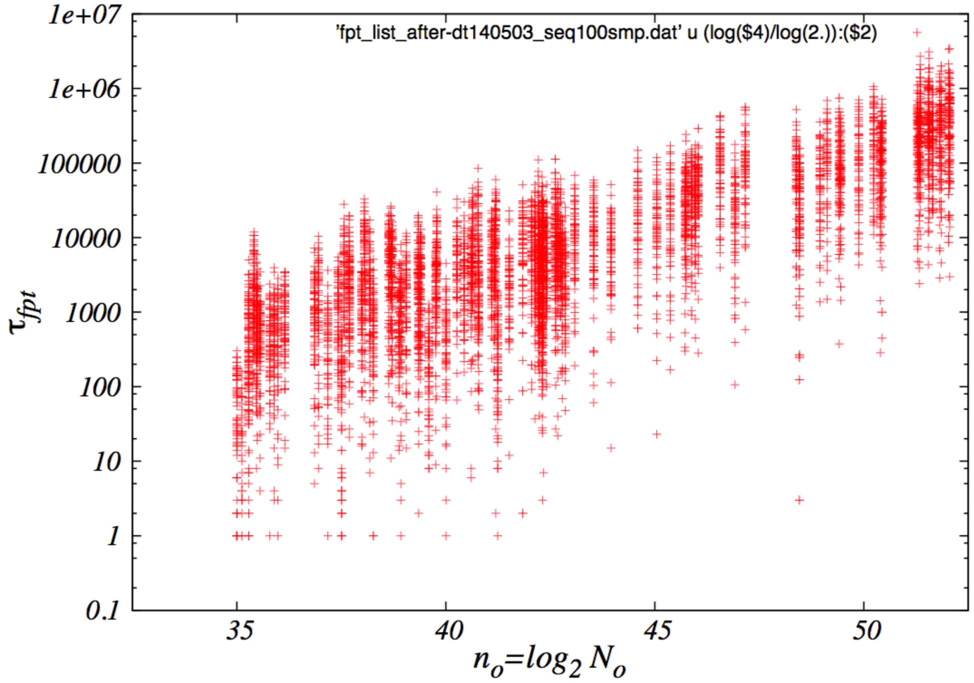
$P^{(n)}(E,Q) \propto \exp\left(-\gamma V^{(n)}(E,Q)\right)$

$$W_k=\frac{\sum_{j=1}^{R} h_k^{(j)}}{\sum_{j=1}^{R}\left\{\frac{\omega_k^{(j)}}{z_j}\left(\sum_{i=1}^{E} h_i^{(j)}\right)\right\}}$$

$V^{(n+1)}(E,Q)=-\log W^{(n)}(E,Q)$

Behavior of first passage time

First passage time (for summation based model)

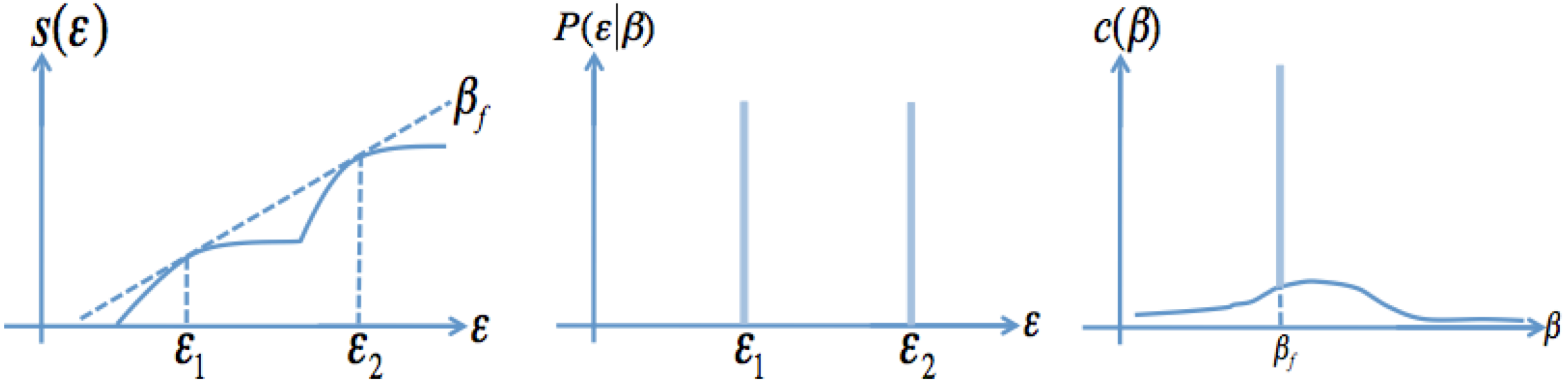


Replica exchange Monte Carlo simulation
of the summation based model.

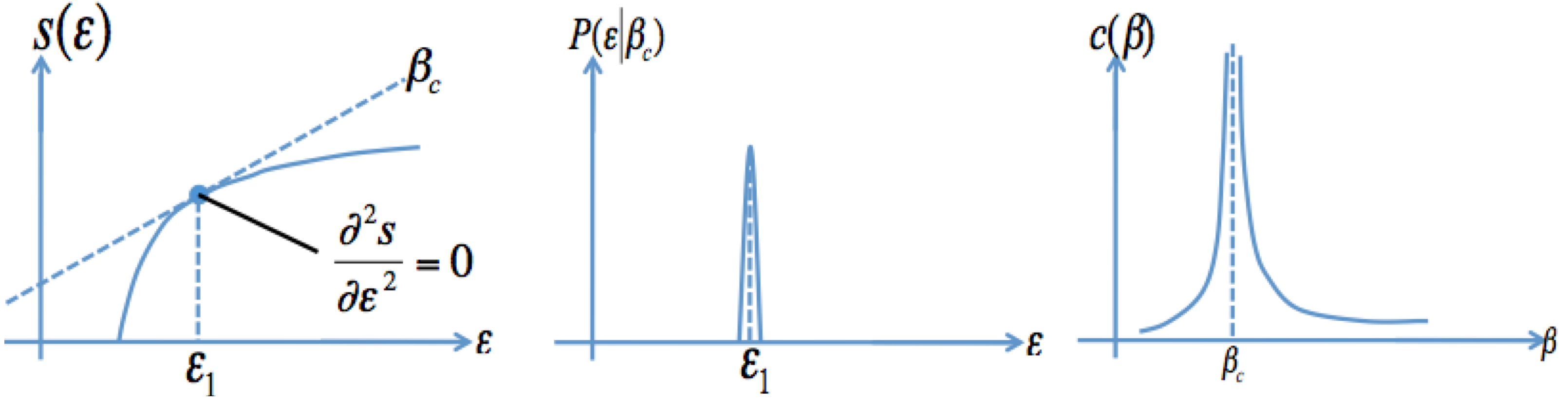
Seems to grow exponentially with its system size n .

Phase transition behavior

In the case of an ordinary first order phase transition



In the case of an ordinary second order phase transition (with critical exponent α>0)


$s(\varepsilon)$
β_c
$\frac{\partial^2 s}{\partial \varepsilon^2} = 0$
ε_1
ε
$P(\varepsilon|\beta_c)$
ε_1
ε
$c(\beta)$
β_c
β