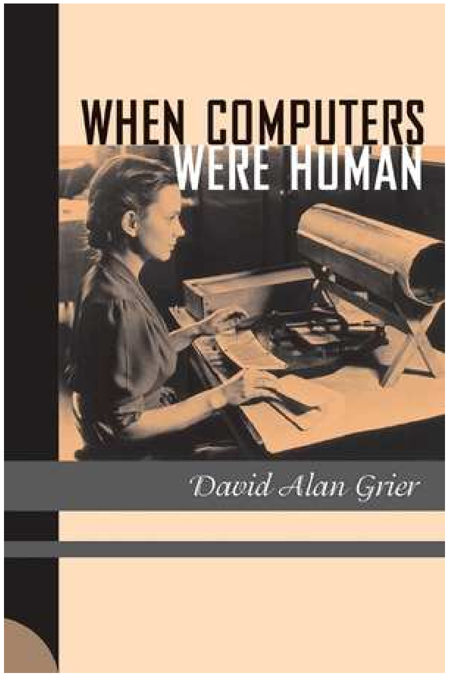
Computational Complexity

Am Introduction for Physicists

Stephan Mertens

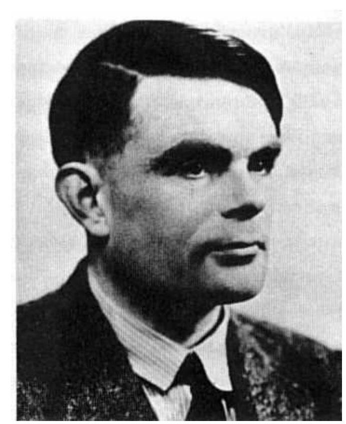
Precomputer Era



Computability

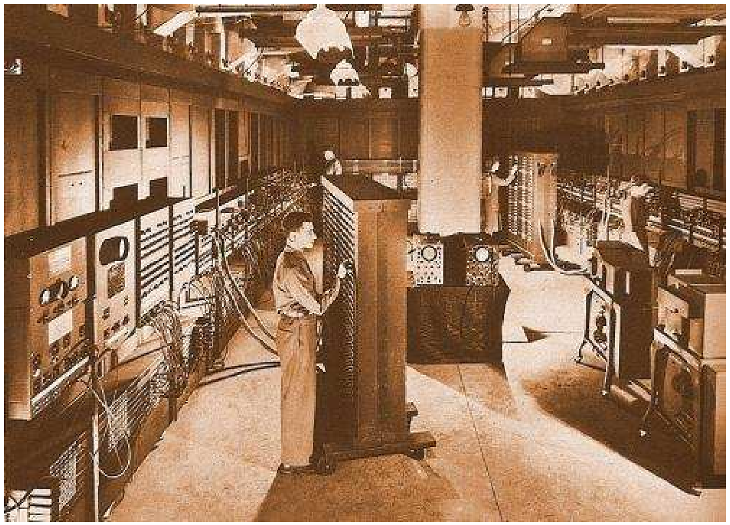
David Hilbert (1862-1943)

Kurt Gödel (1906-1978)



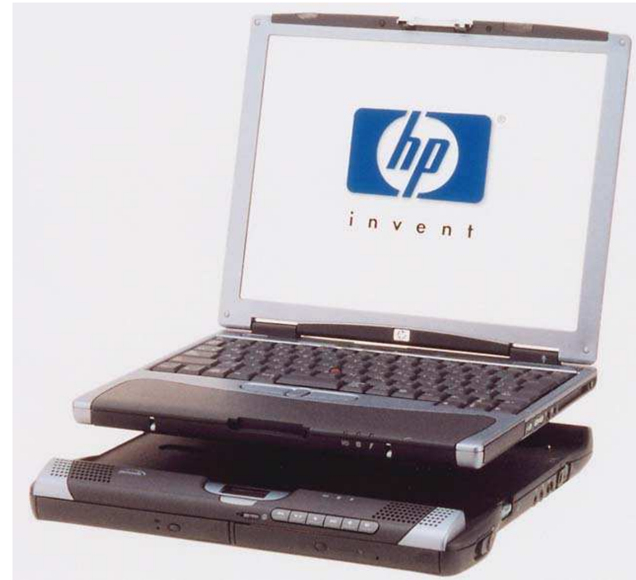
Alan Turing (1912-1954)

Computers Now and Then



ENIAC (1946)

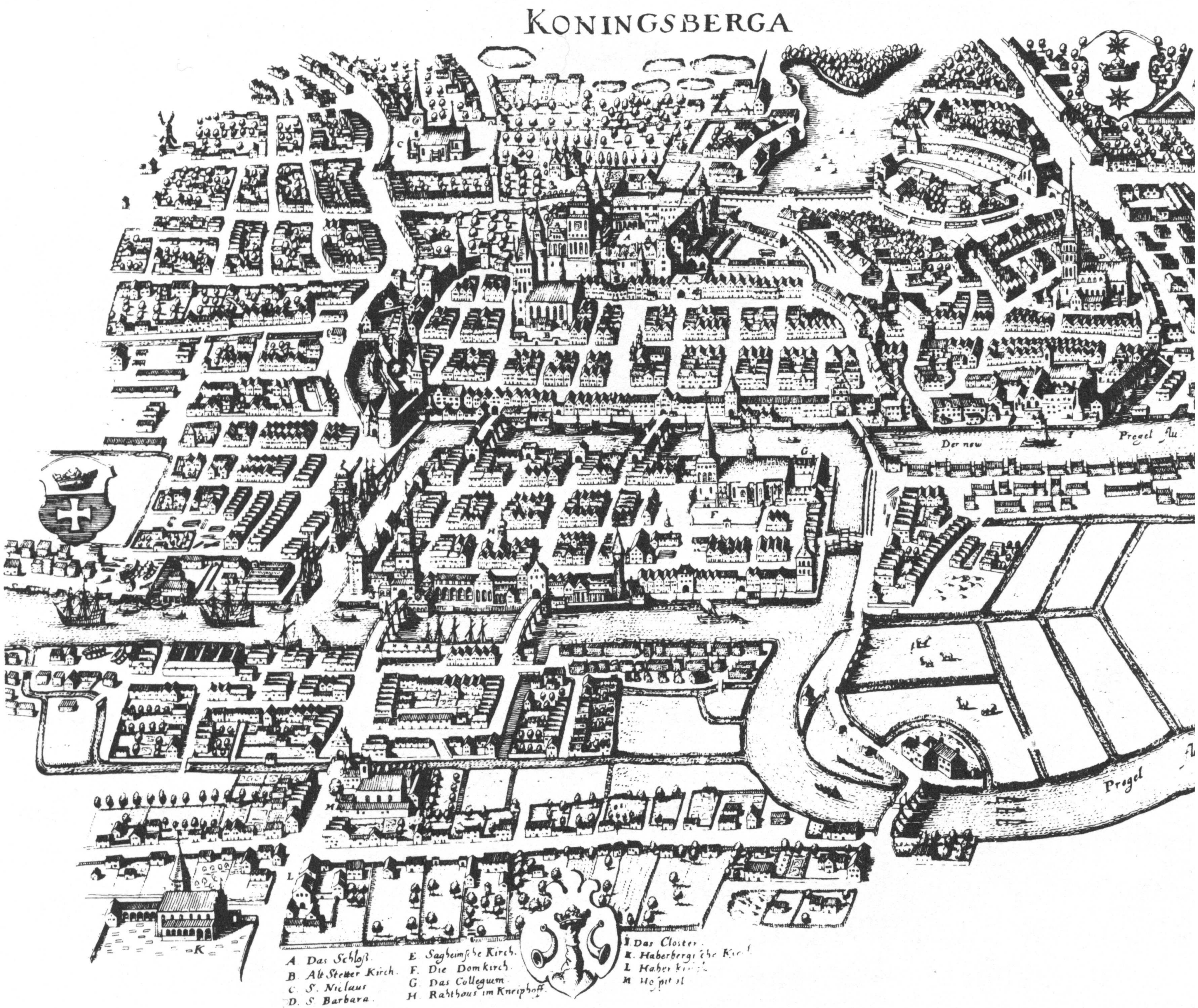
- 19000 tubes
- 35000 kg
- 175 kW
- 300 mult. per sec.



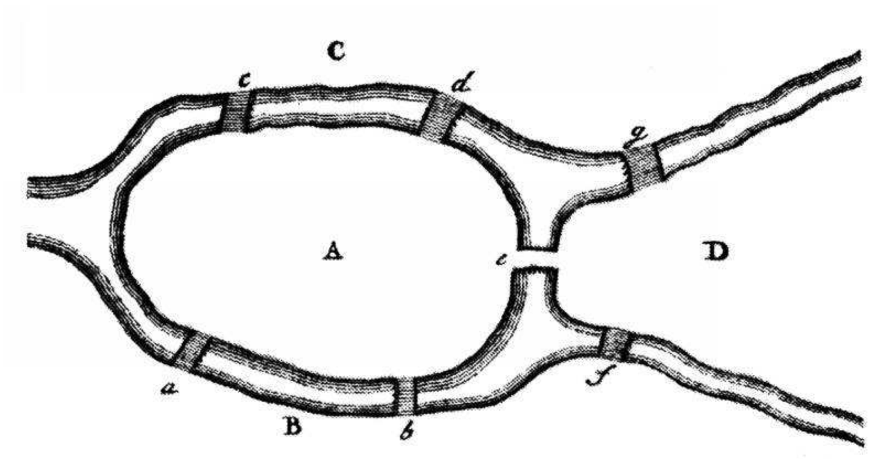
Omnibook 500 (2002)

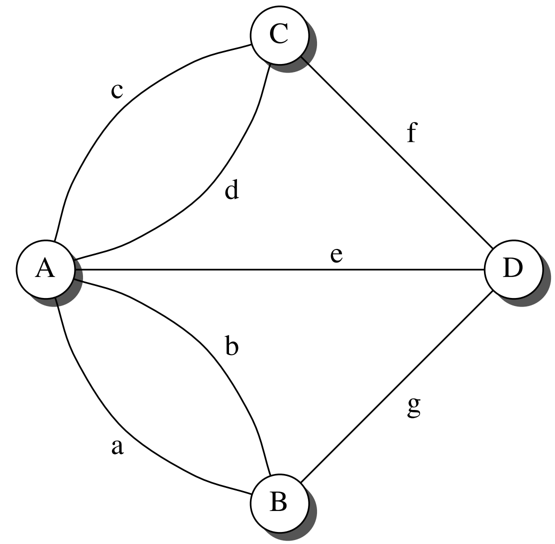
- > 10^8 transistors
- 1.5 Kg
- $<$ 60 W
- 10^9 mult. per sec.

Crossing Brigdes



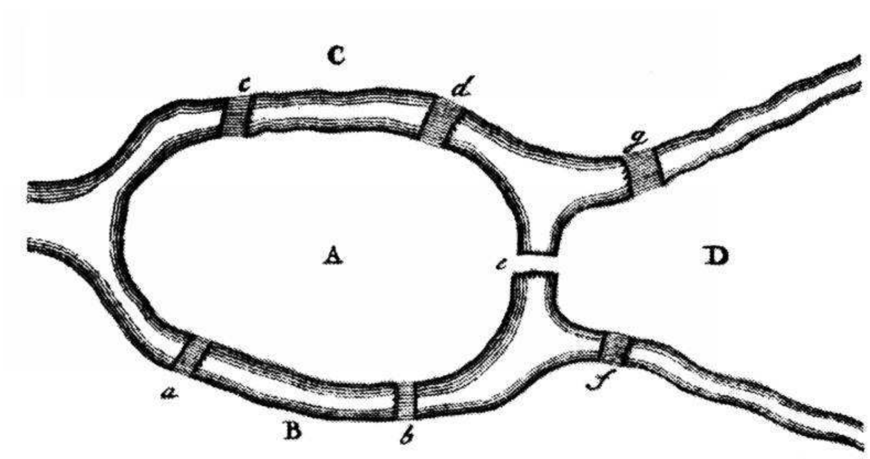
Königsberg Bridges

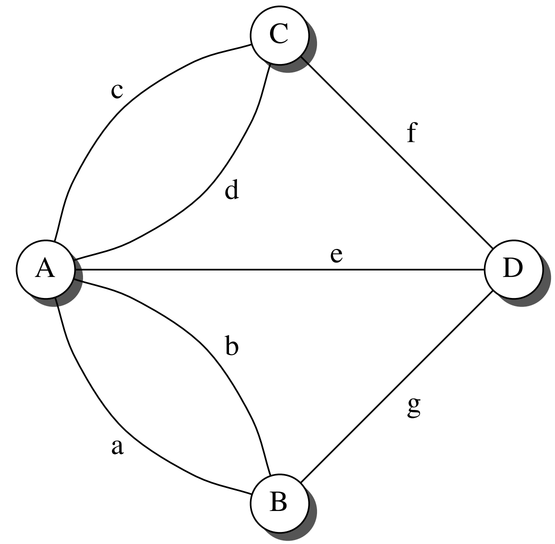




Leonhard Euler (1703–1783)

Königsberg Bridges

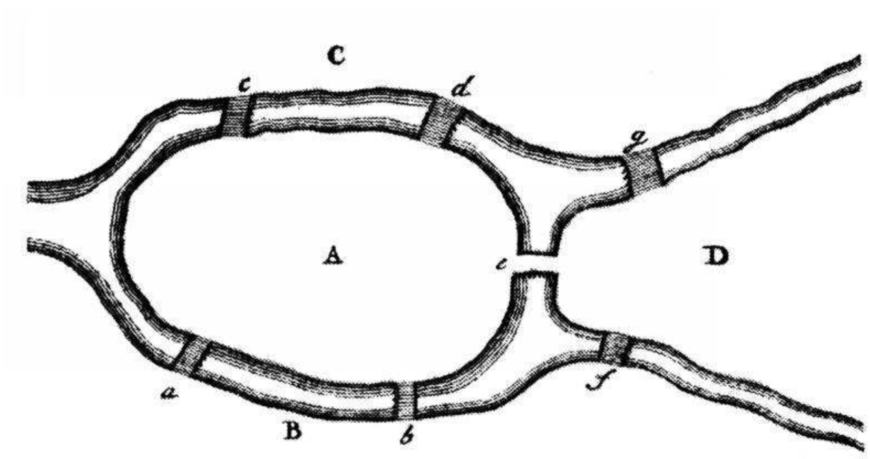


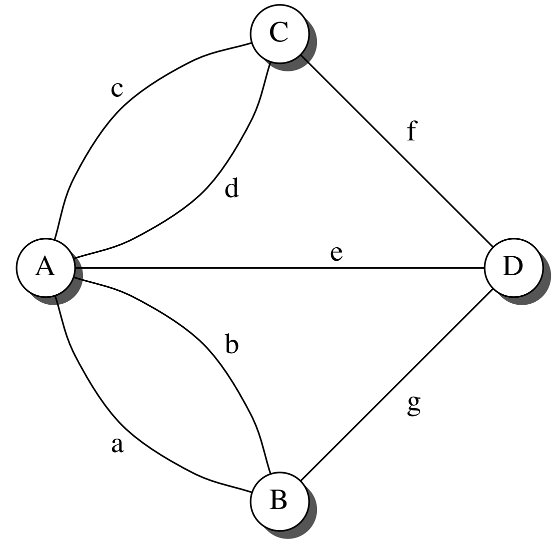


Leonhard Euler (1703–1783)

“As far as the problem of the seven bridges of Königsberg is concerned, it can be solved by making an ***exhaustive list*** *of possible routes, and then finding whether or not any route satisfies the conditions of the problem. Because of the number of possibilities, this method of solutions would be too difficult and laborious, and in other* ***problems with more bridges****, it would be* ***impossible****”.*

Königsberg Bridges



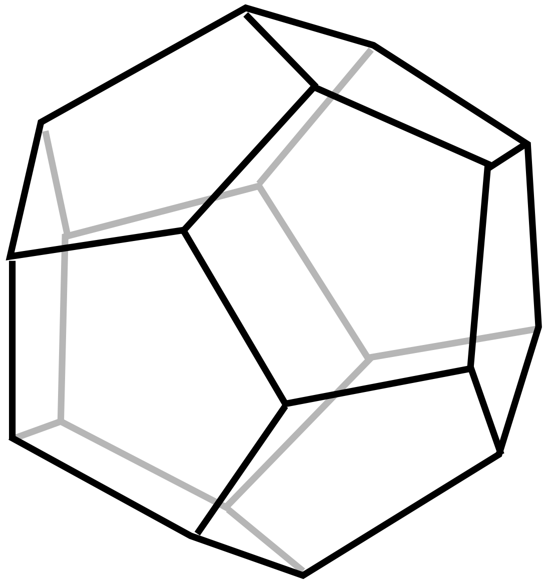


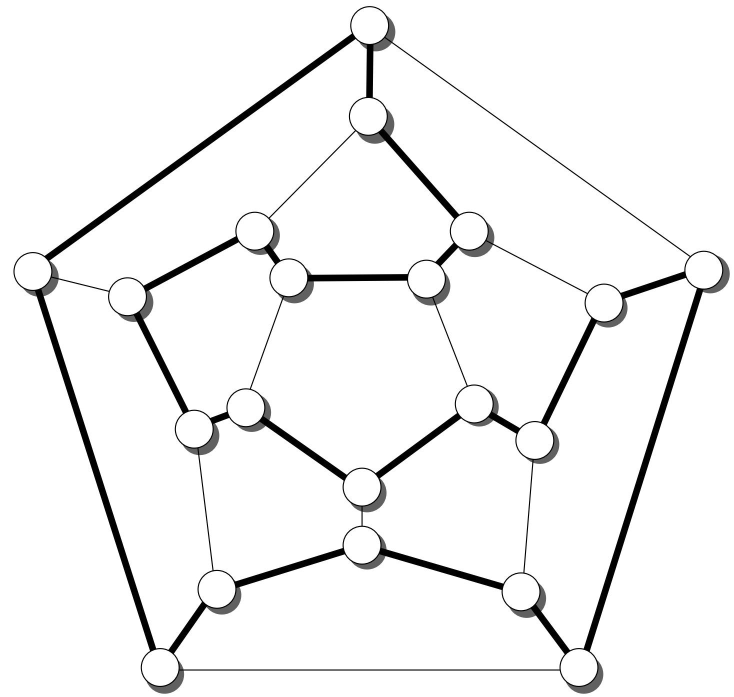
Leonhard Euler (1703–1783)

A cycle that traverses each edge of a graph excatly once is called an **Eulerian cycle**.

A connected graph G has an Eulerian cycle if and only if the degree of all vertices is even.

Intractable Itineraries

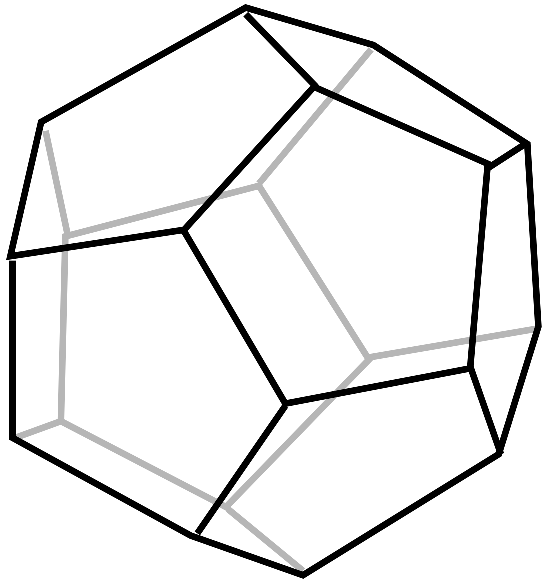


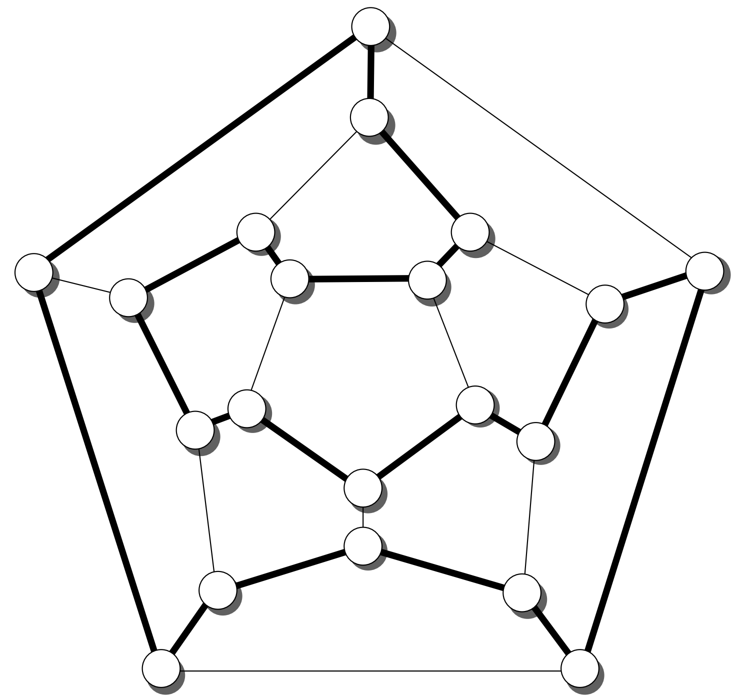


Sir William Rowan Hamilton (1805–1865)

A cycle that traverses each vertex of a graph excatly once is called an **Hamiltonian cycle**.

Intractable Itineraries





Sir William Rowan Hamilton (1805–1865)

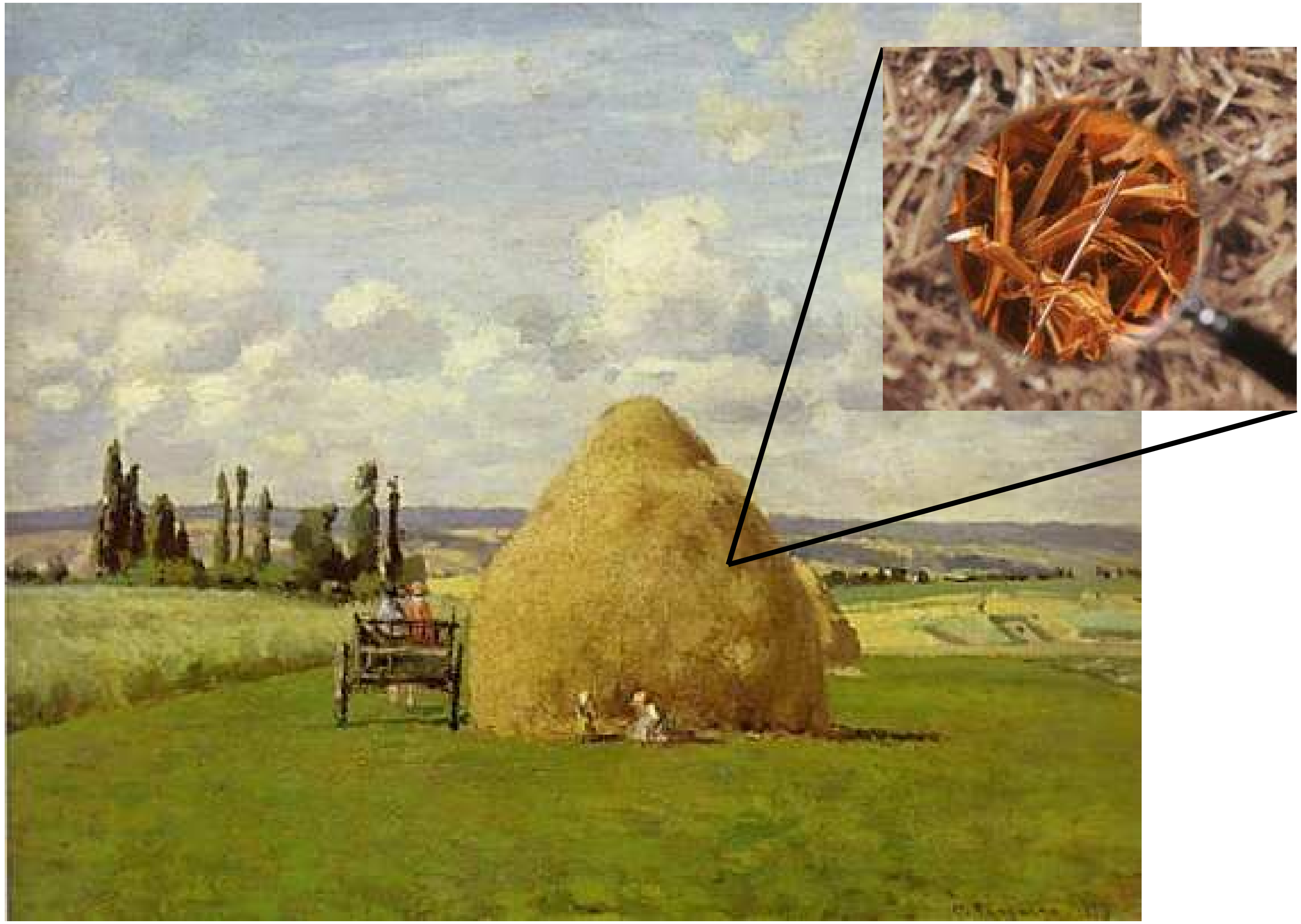
A cycle that traverses each vertex of a graph excatly once is called an **Hamiltonian cycle**.

?

Needle Problems

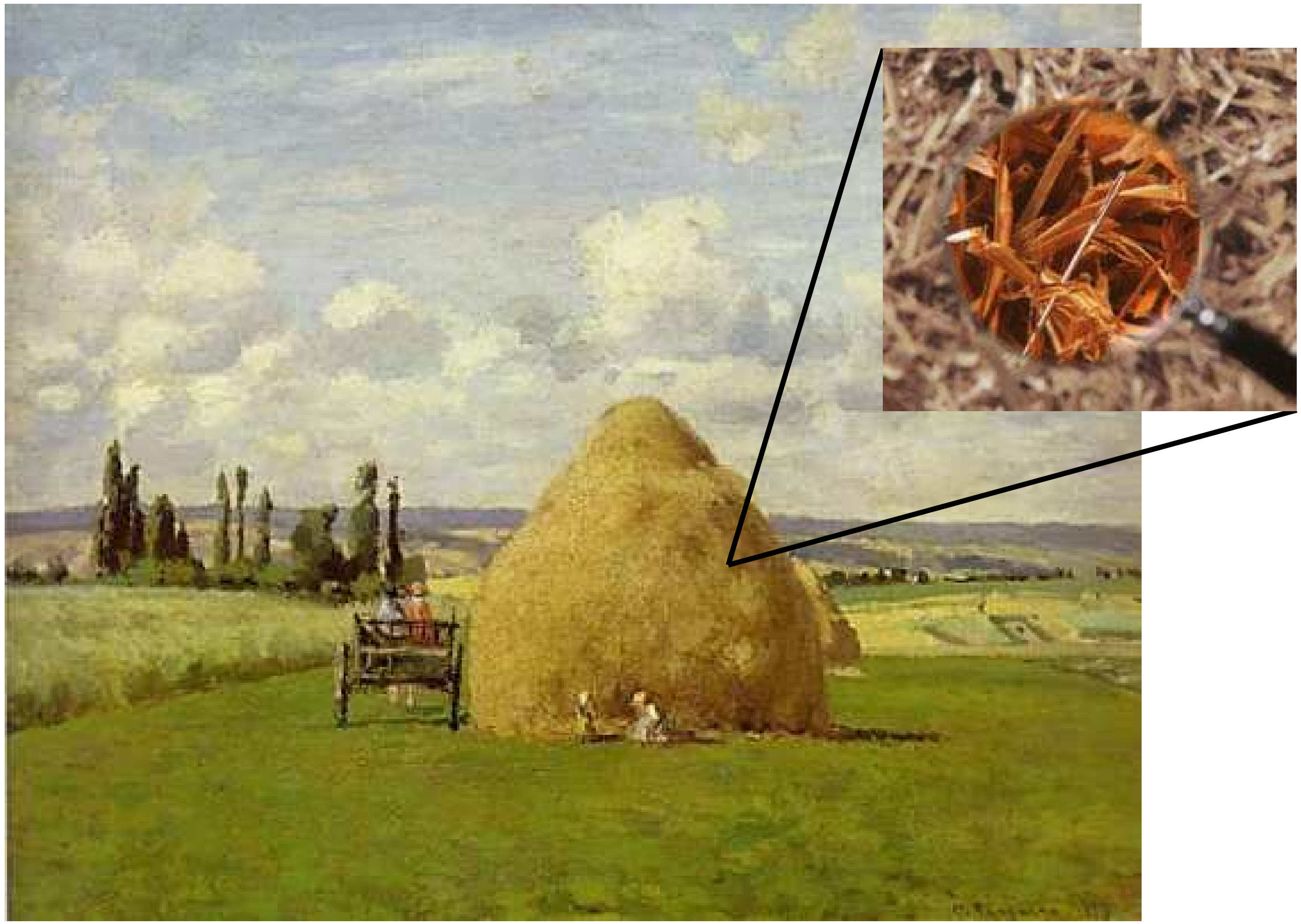
Camille Pissaro, *Haystack* (1873)

Needle Problems



Camille Pissaro, *Haystack* (1873)

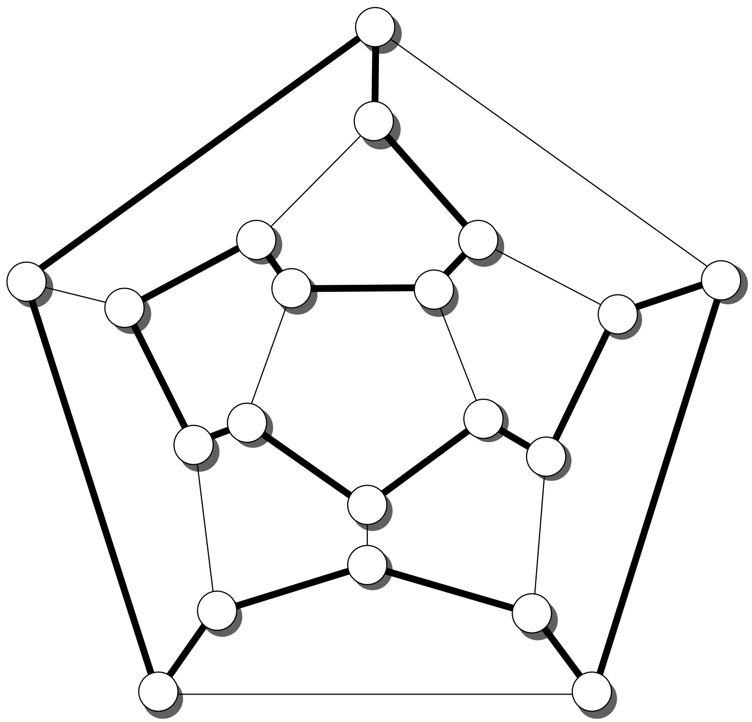
Needle Problems

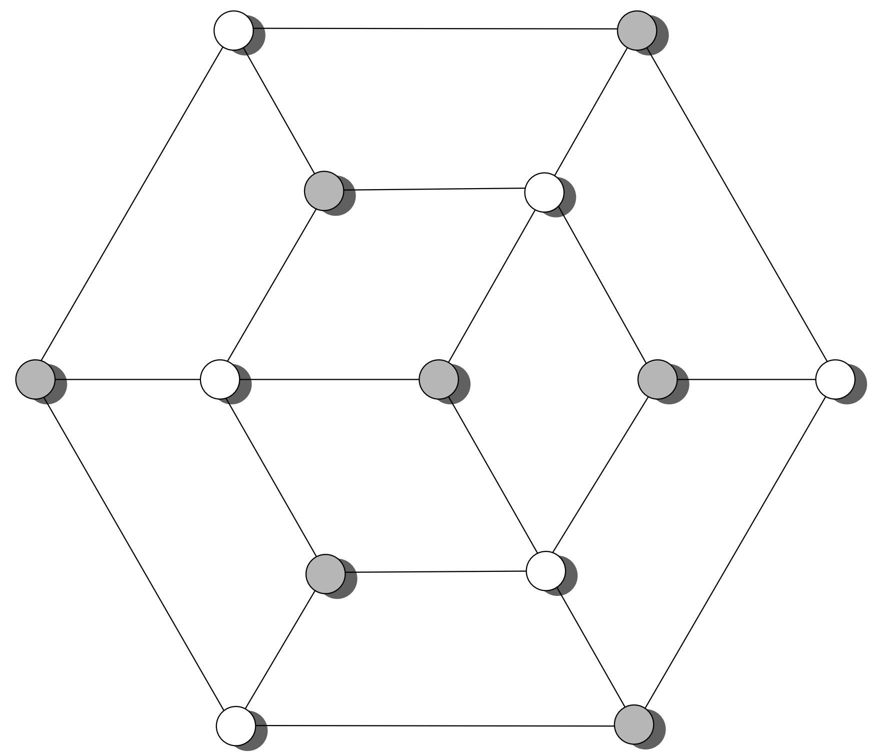


Camille Pissaro, *Haystack* (1873)

NP: nondeterministic polynomial

Yes-No Asymmetrie



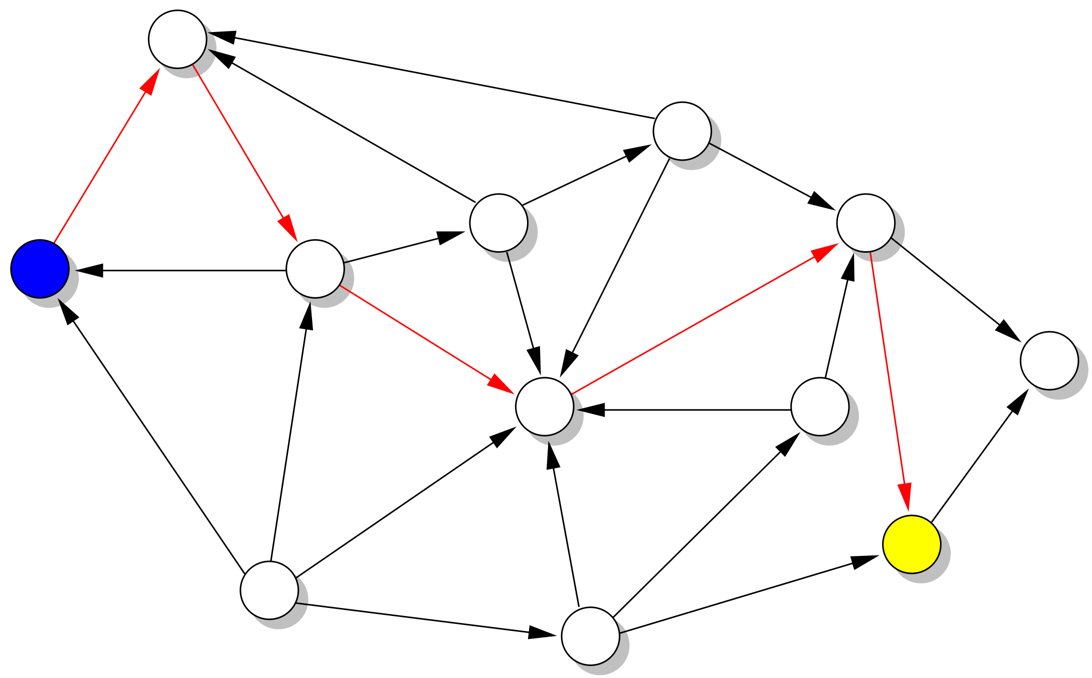


Hamiltonian Cycle ?

Decision Problems $\notin$ NP

Is there a winning strategy for white?

Getting There from Here



Reachability: Given a directed graph G and two vertices s and t. Is there a path that runs from s to t?

2-SAT

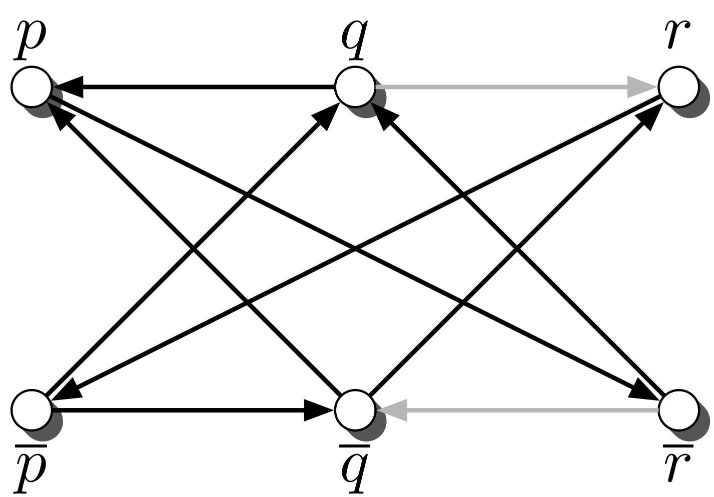
$$F_1(p,q,r) = (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q)$$

$$F_2(p,q,r) = (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q) \wedge (\overline{q} \vee r)$$

2-SAT

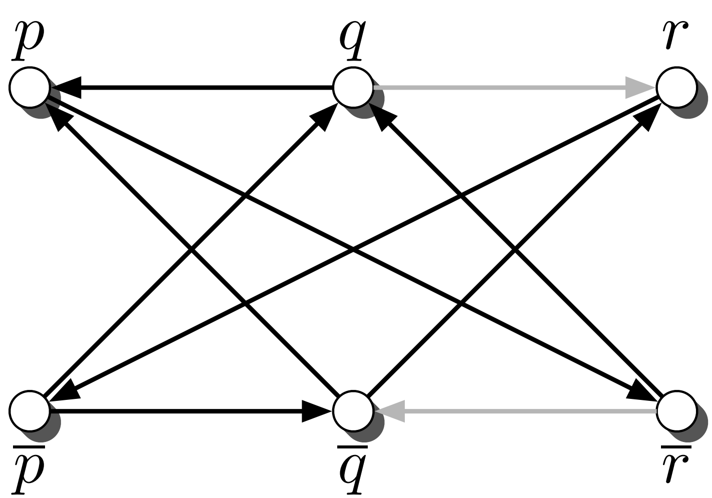
$$F_1(p,q,r) = (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q)$$

$$F_2(p,q,r) = (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q) \wedge (\overline{q} \vee r)$$



2-SAT

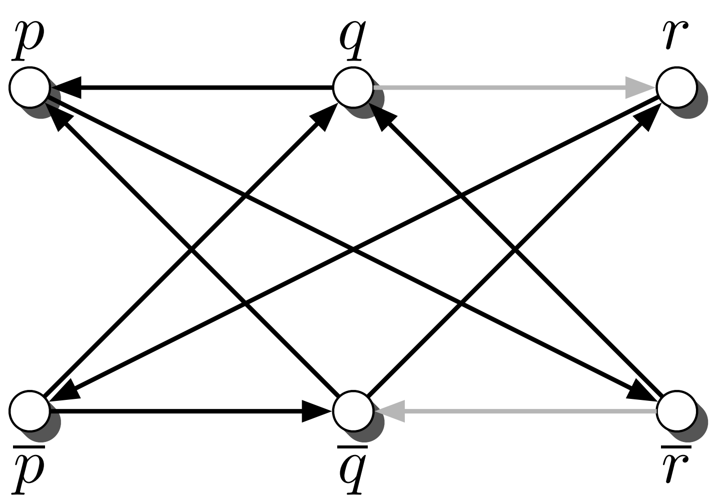
$$F_1(p,q,r) \;=\; (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q)$$
$$F_2(p,q,r) \;=\; (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q) \wedge (\overline{q} \vee r)$$



while *there is an unset variable* **do**
  Choose an unset variable x ;
  if *there is a path* $x \rightsquigarrow \overline{x}$ **then** set $x = \texttt{false}$;
  else if *there is a path* $\overline{x} \rightsquigarrow x$ **then** set $x = \texttt{true}$;
  else set x to any value you like ;
  while *there is a unit clause* **do**
    unit clause propagation ;
  end
end

2-SAT

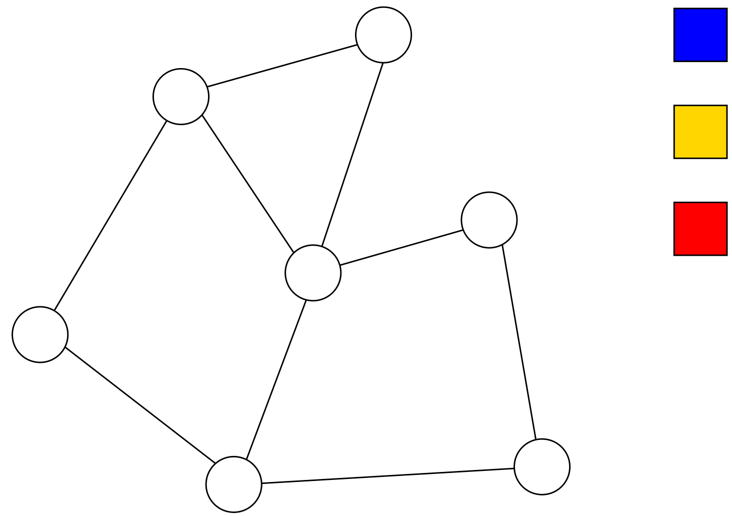
$$F_1(p,q,r) \;=\; (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q)$$
$$F_2(p,q,r) \;=\; (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \wedge (q \vee r) \wedge (p \vee q) \wedge (\overline{q} \vee r)$$



while *there is an unset variable* **do**
  Choose an unset variable x ;
  if *there is a path* $x \leadsto \overline{x}$ **then** set $x = \texttt{false}$;
  else if *there is a path* $\overline{x} \leadsto x$ **then** set $x = \texttt{true}$;
  else set x to any value you like ;
  while *there is a unit clause* **do**
    unit clause propagation ;
  end
end

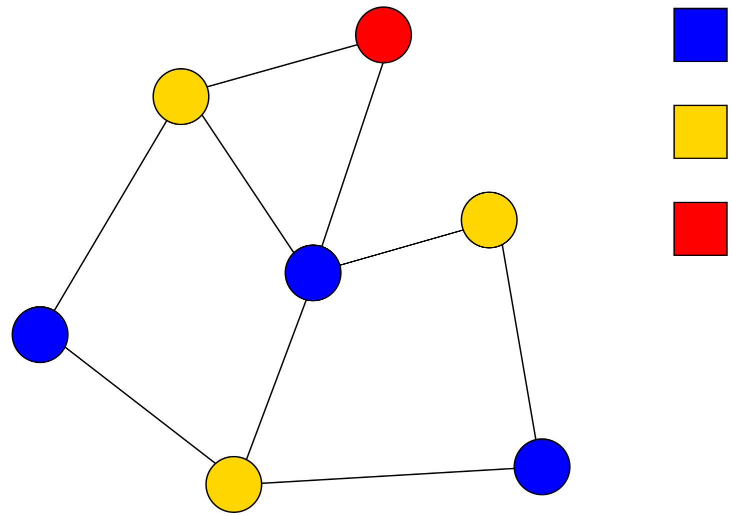
2-SAT $\leq$ Reachability

Coloring



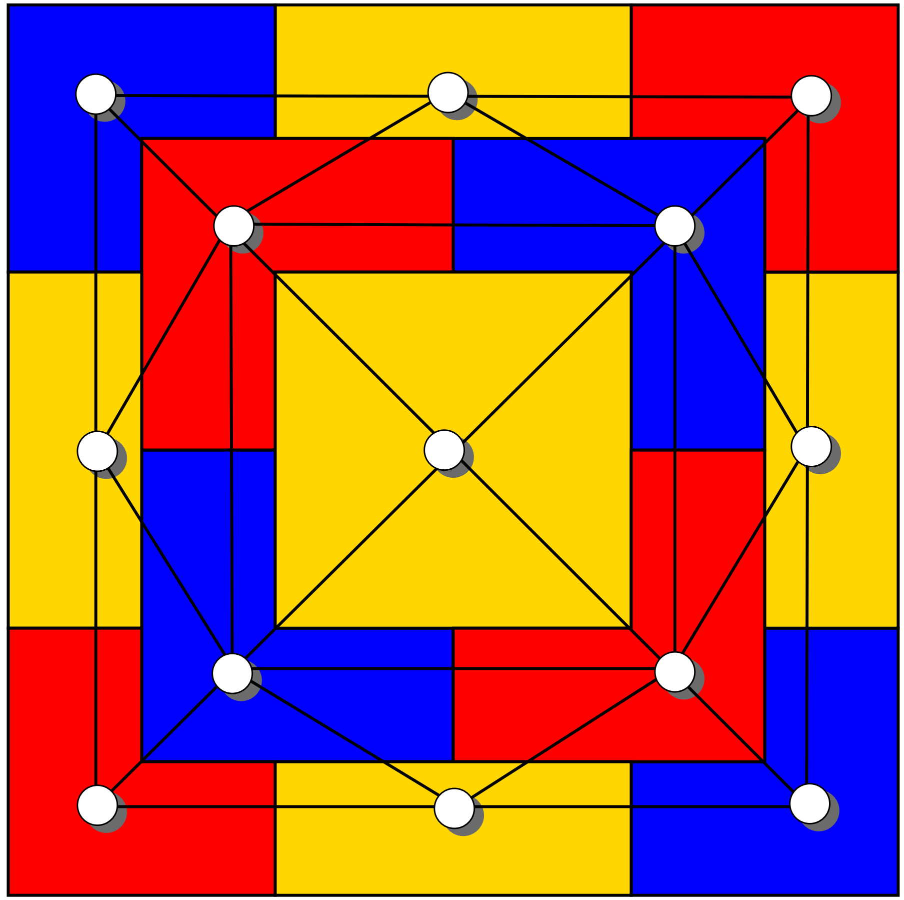
K-Coloring: Given a graph G and an integer K. Is there a coloring of the vertices of G using at most K different colors such that no two adjacent vertices have the same color?

Coloring



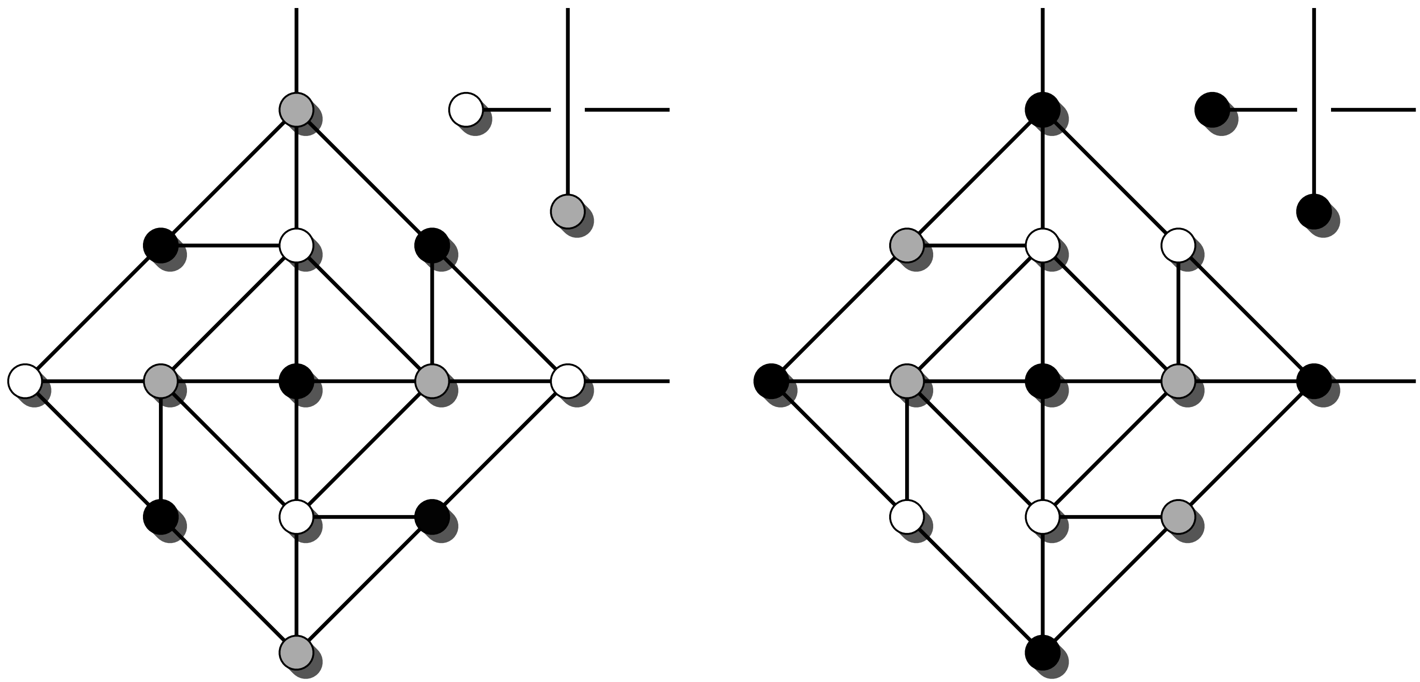
K-Coloring: Given a graph G and an integer K. Is there a coloring of the vertices of G using at most K different colors such that no two adjacent vertices have the same color?

Planar Coloring



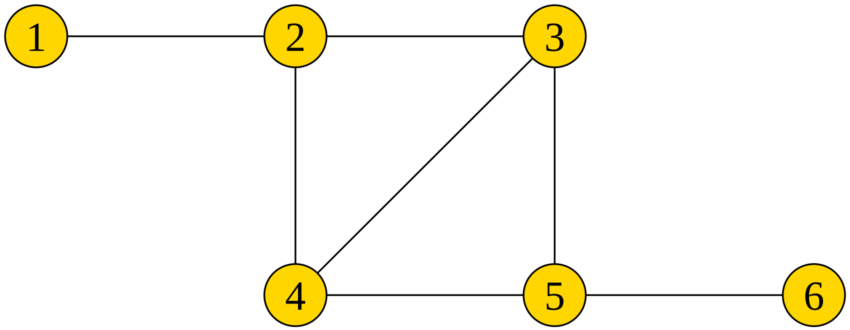
Planar-4-Coloring is easy

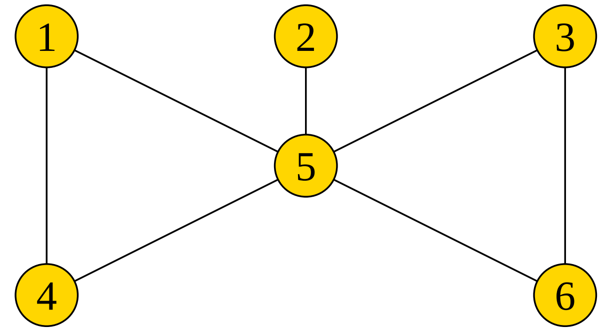
Planar Coloring



K-Coloring $\leq$ Planar-3-Coloring

Graph Isomorphism Problem





	1	2	3	4	5	6
1	0	1	0	0	0	0
2	1	0	1	1	0	0
3	0	1	0	1	1	0
4	0	1	1	0	1	0
5	0	0	1	1	0	1
6	0	0	0	0	1	0

	1	2	3	4	5	6
1	0	0	0	1	1	0
2	0	0	0	0	1	0
3	0	0	0	0	1	1
4	1	0	0	0	1	0
5	1	0	1	1	0	1
6	0	0	1	0	1	0

The world of NP

planar-3-Coloring

Hamiltonian Cycle

3-SAT

SAT

3-Coloring

Graph Isomorphism

Factoring

Reachability

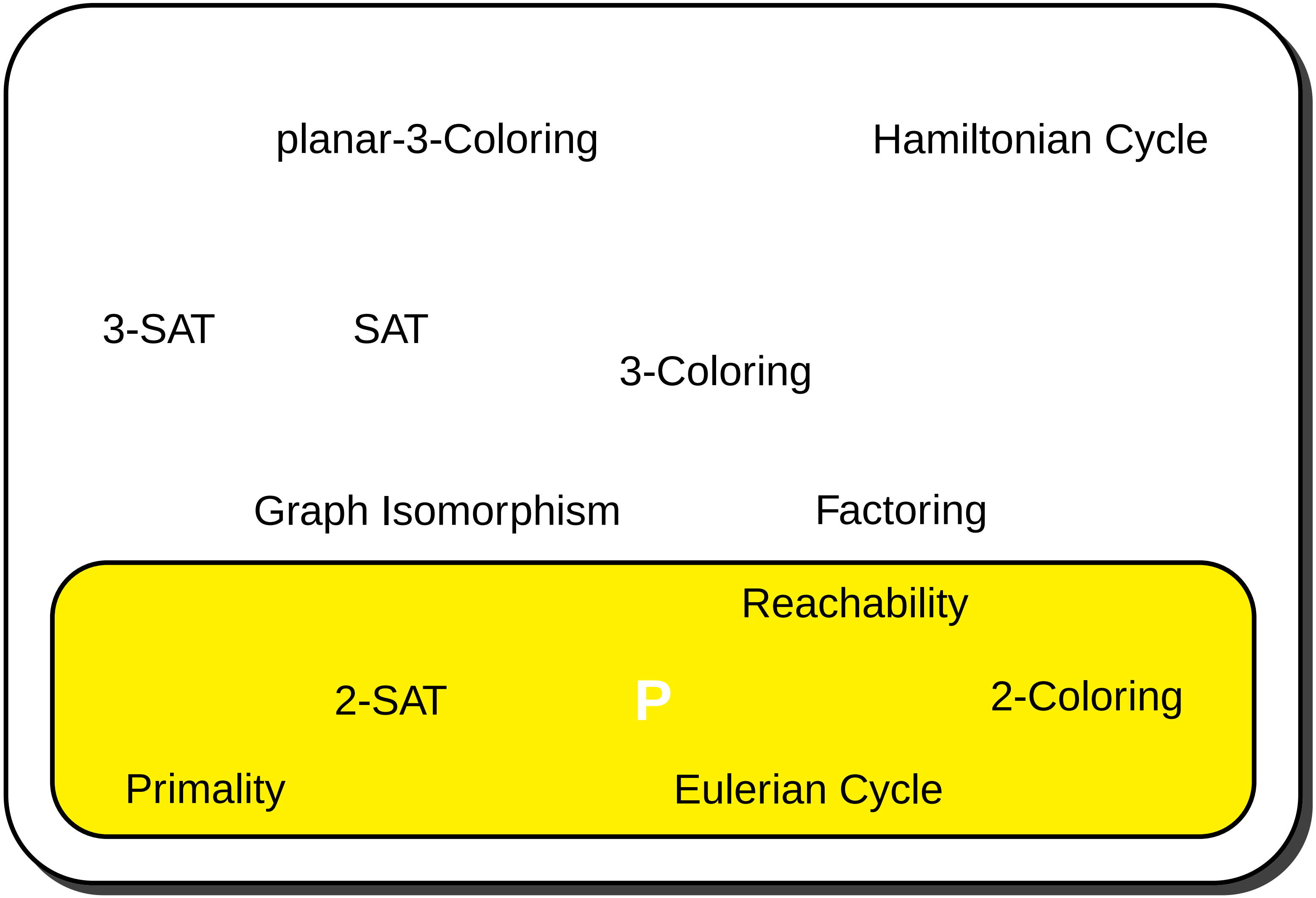
2-SAT

2-Coloring

Primality

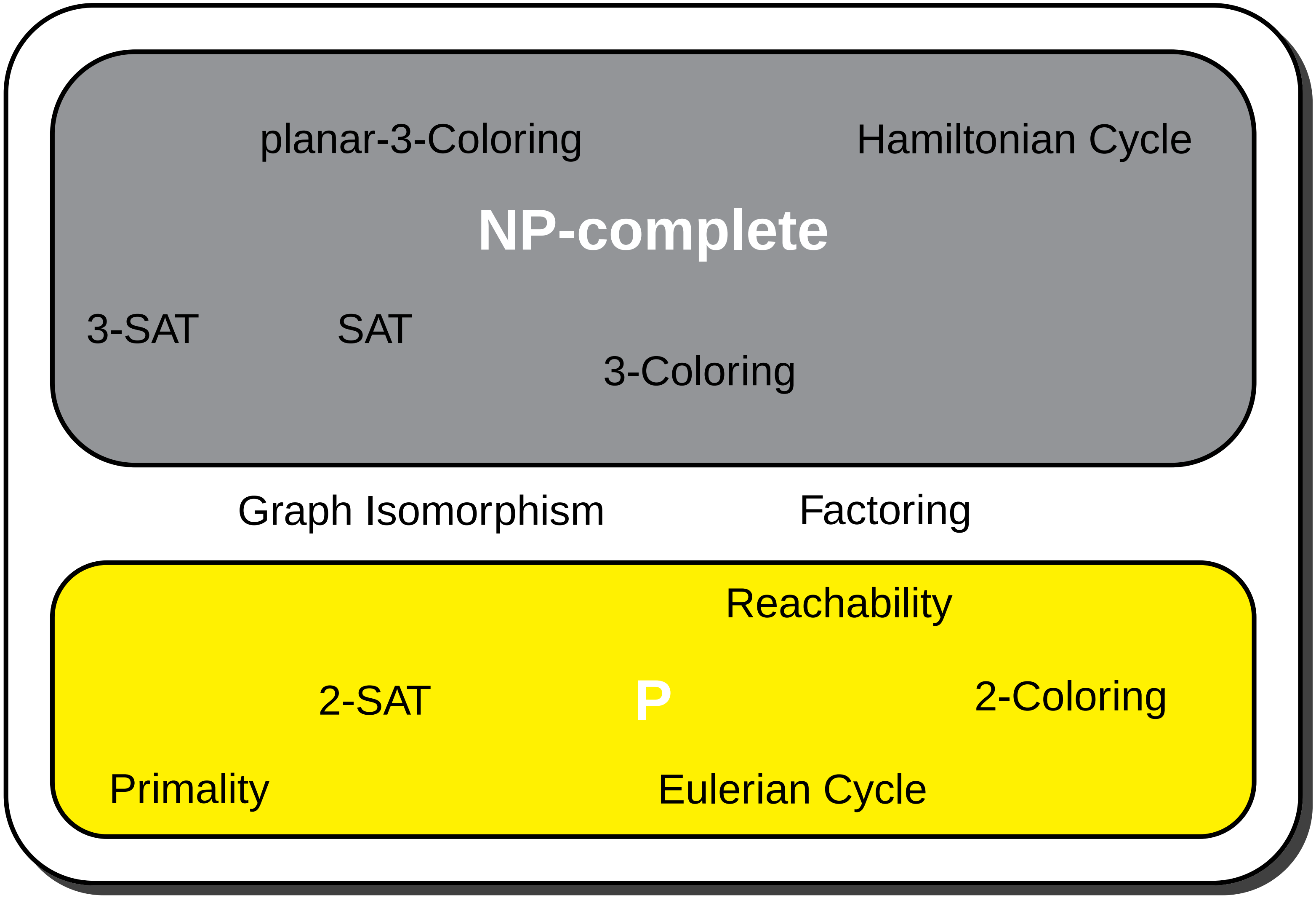
Eulerian Cycle

The world of NP



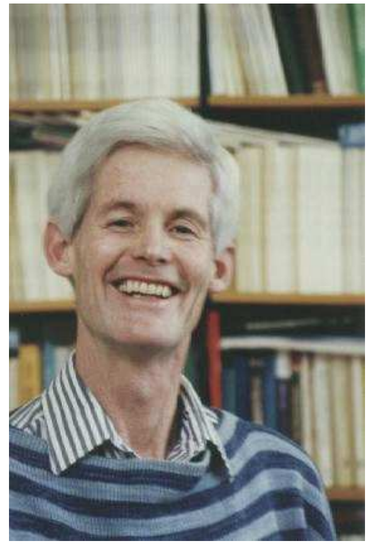
$P \neq NP$?

The world of NP



P $\neq$ NP ?

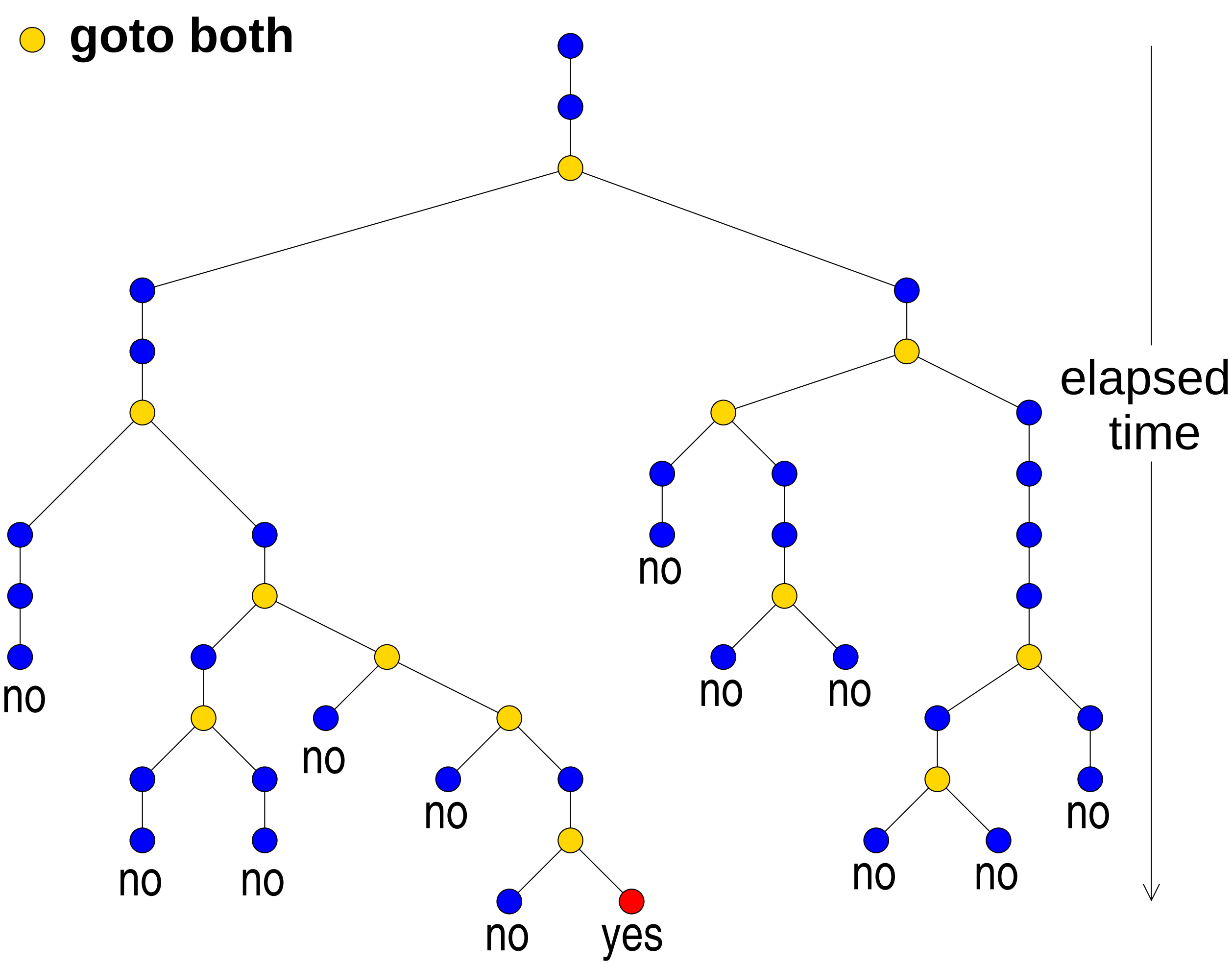
NP-completeness



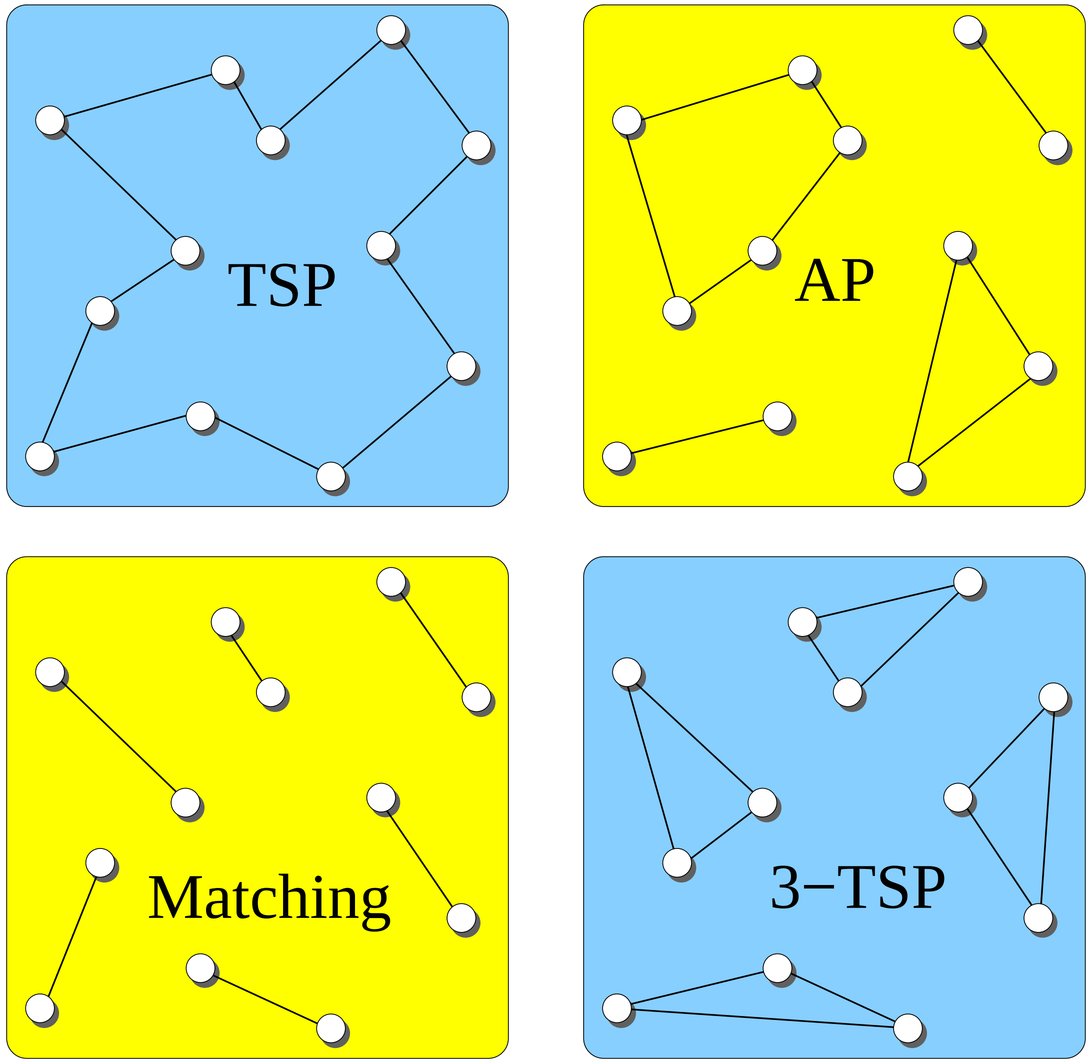
Theorem (Cook, 1971): All problems in NP are polynomially reducible to SAT:

$$\forall P \in \text{NP} : P \leq \text{SAT}$$

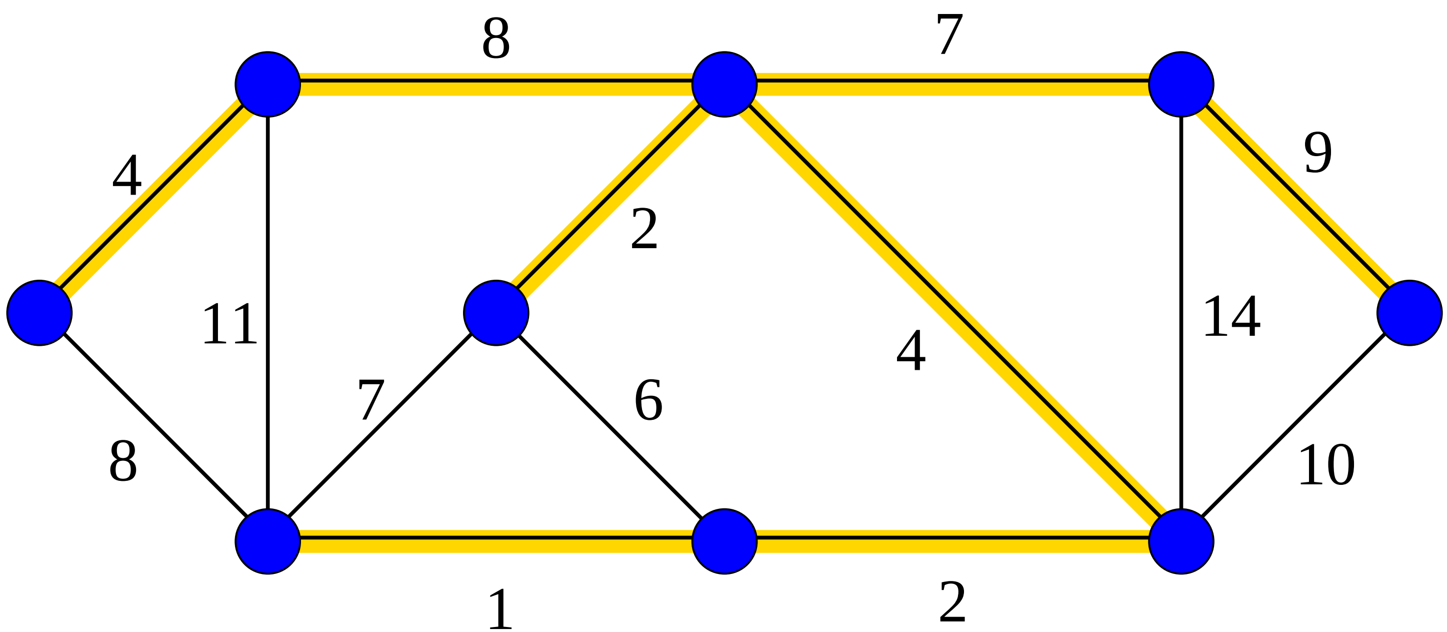
Nondeterministic Algorithm



Travelling Salesmen & Co



Minimum Spanning Tree



Given a graph $G = (V, E)$ with non-negative edge weights.

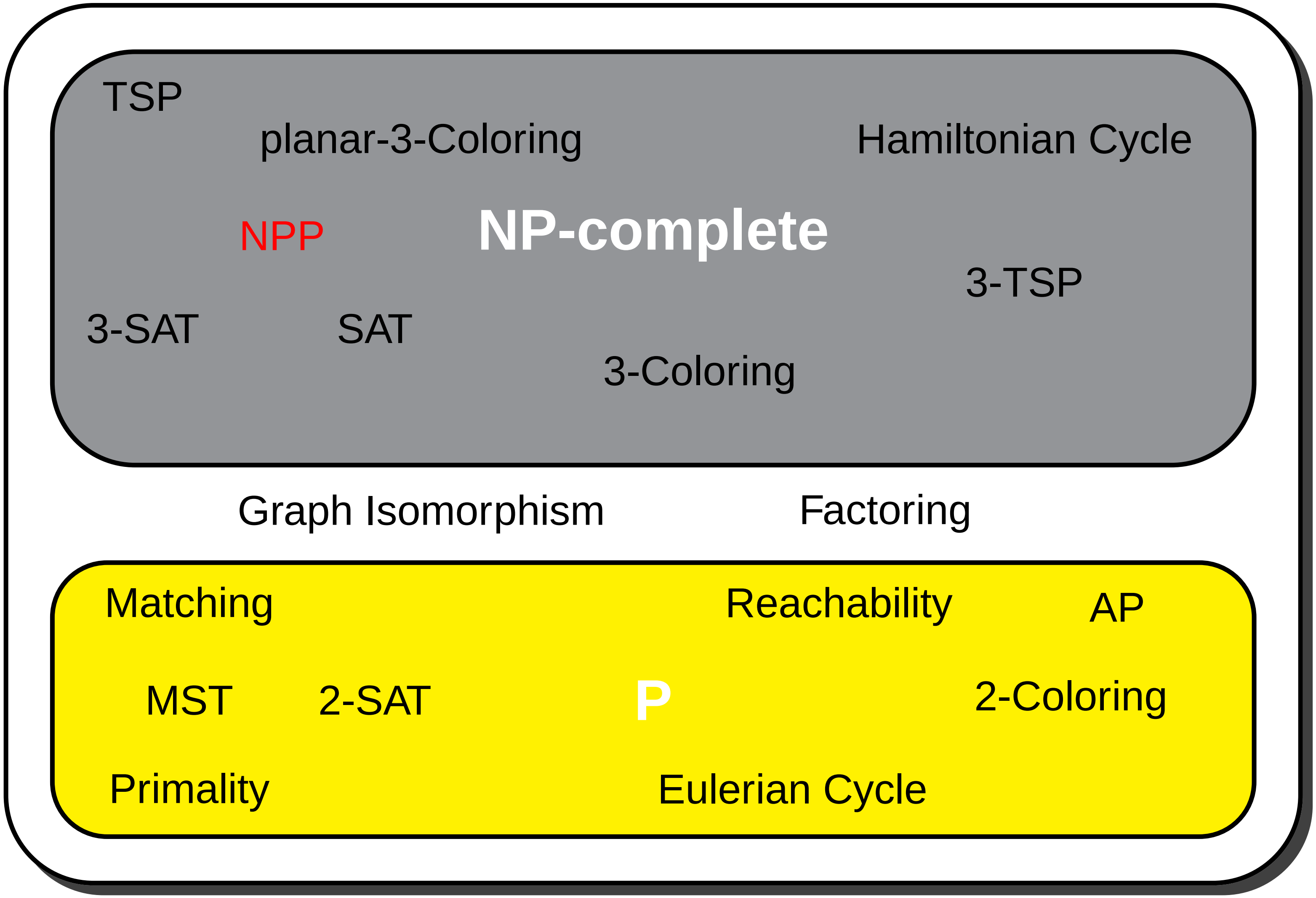
Find a spanning tree with minimal total weight.

Minimum Spanning Tree

Otakar Borůvka (1899-1995)

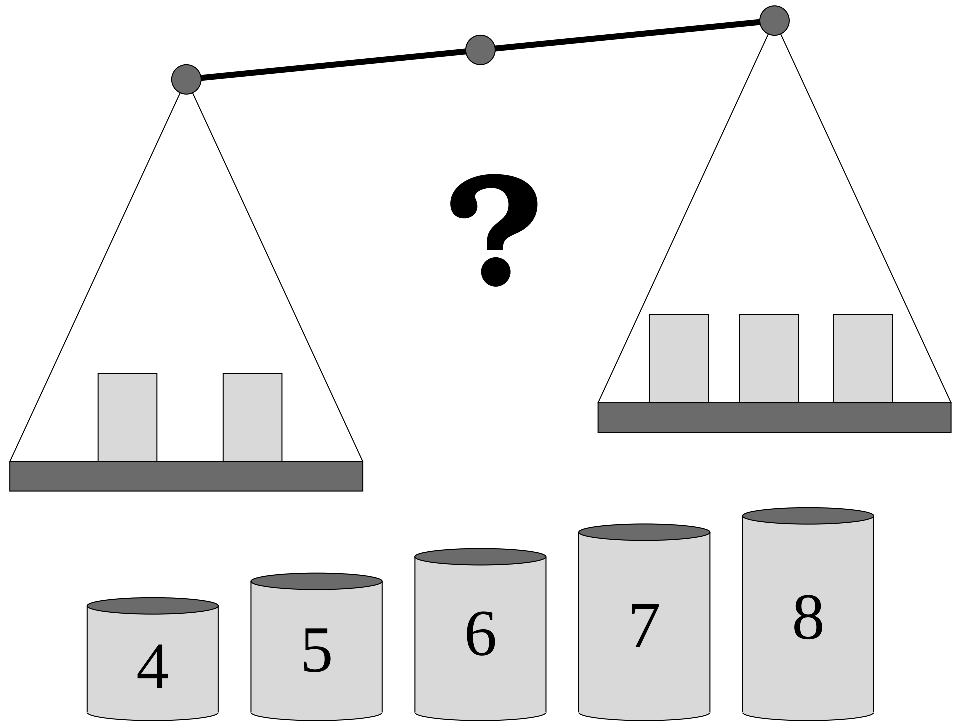
Insight: Let $G = (V, E)$ be a connected graph with positive edge weights. Let $U \subset V$ be a proper subset of the vertices of G, and let e be the edge with smallest weight that connects U and $V \setminus U$. Then e is part of a minimum spanning tree in G.

The world of NP

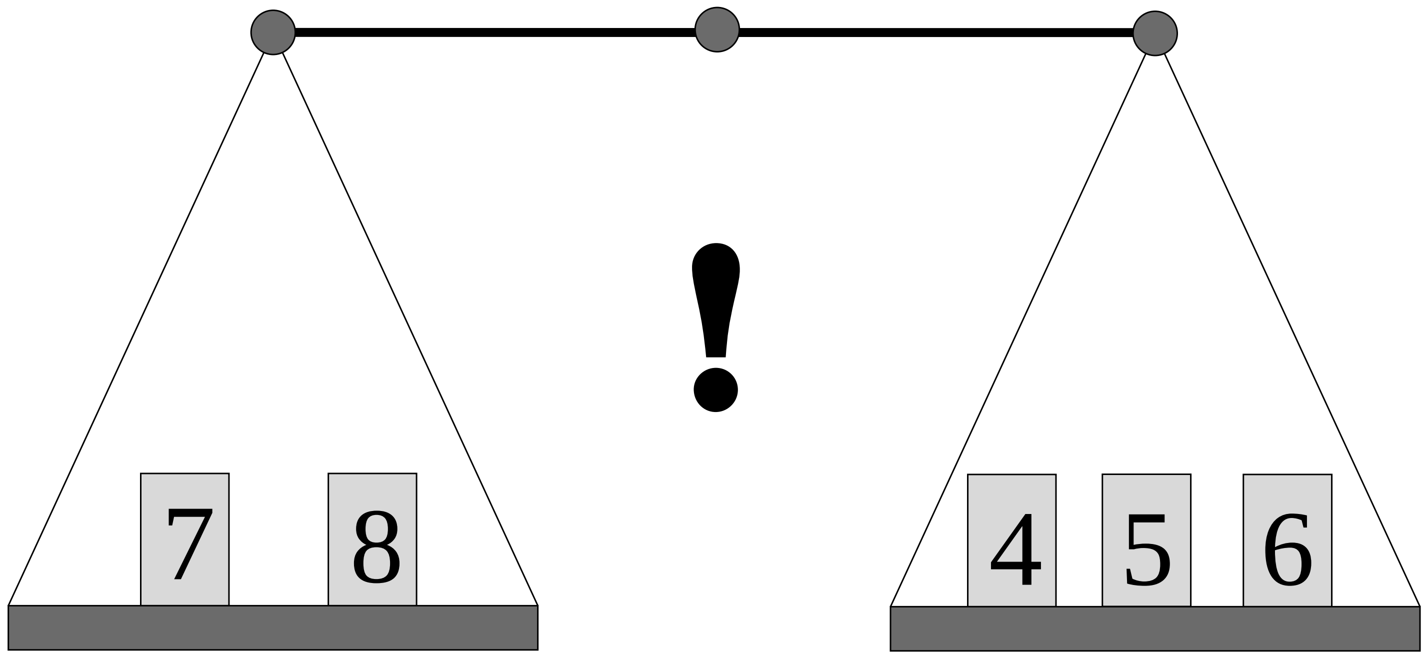


$P \neq NP$?

Balancing Numbers



Balancing Numbers



Number Partitioning Problem

Given positive numbers $\{a_1, a_2, \ldots, a_N\}$.

Find a partition $\sigma = \{\pm 1\}^N$ that minimizes

$$E(\sigma) = |\sum_{j=1}^{N} a_j \sigma_j|.$$

- $E^2(\sigma)$: mean field, antiferromagnetic Ising model
- NPP is NP-hard

Subset-Sum

Given positive numbers $\{a_1, a_2, \ldots, a_N\}$ and a number s. Is there a subset $\mathcal{A} \subset \{a_1, \ldots, a_N\}$ such that $\sum_{a_i \in \mathcal{A}} a_i = s$?

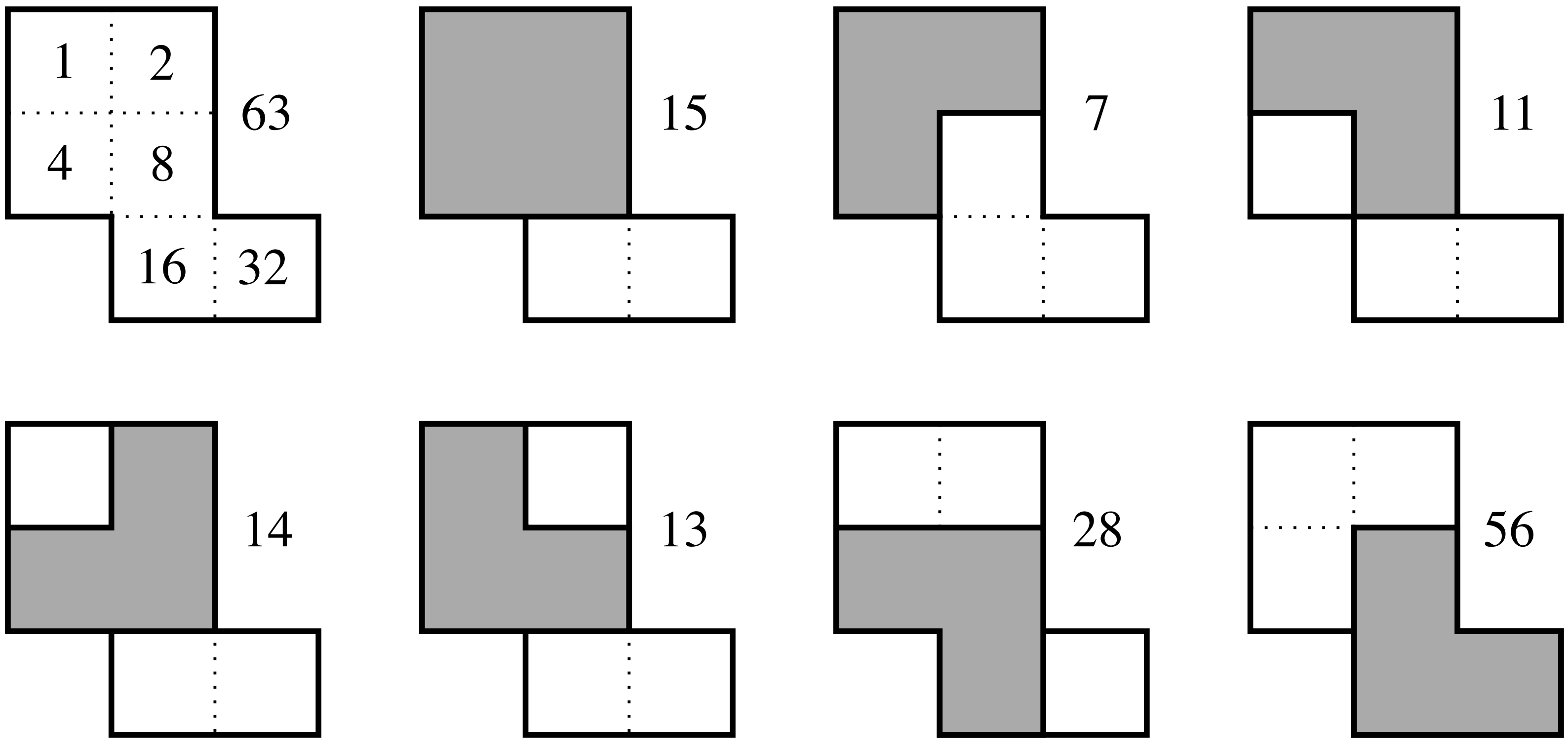
Lemma: Subset-Sum $\leq$ NPP

Proof: Wlog $2s \leq \sum a_i$. Define $a'_i = a_i$, $a'_0 = \sum a_i - 2s$.

$$\exists \sigma \text{ s.t. } \sum_{i=0}^{n} a'_i \sigma_i = 0 \qquad \Longleftrightarrow \qquad \exists \mathcal{A} \text{ s.t. } \sum_{a_i \in \mathcal{A}} = s$$

Hint: Set $\mathcal{A} = \{a_i : \sigma_i = \sigma_0\}_{i=1}^{N}$.

Tiling $\leq$ Subset-Sum



Worst Case vs. Typical Case

Heuristics: Greedy

Idea: keep the energy small all the time

- sort: $a_1 \geq a_2 \geq a_3 \geq \cdots \geq a_N$
- $S_1 := a_1$, $S_2 := 0$
- for $i := 2$ to N add a_i to min(S_1, S_2)
- print $|S_1 - S_2|$

Time complexity is $\mathcal{O}(N \log N)$, Quality is $\approx \min_i\{a_i\}$.

Heuristics: Differencing

Idea: reduce size of numbers[1].

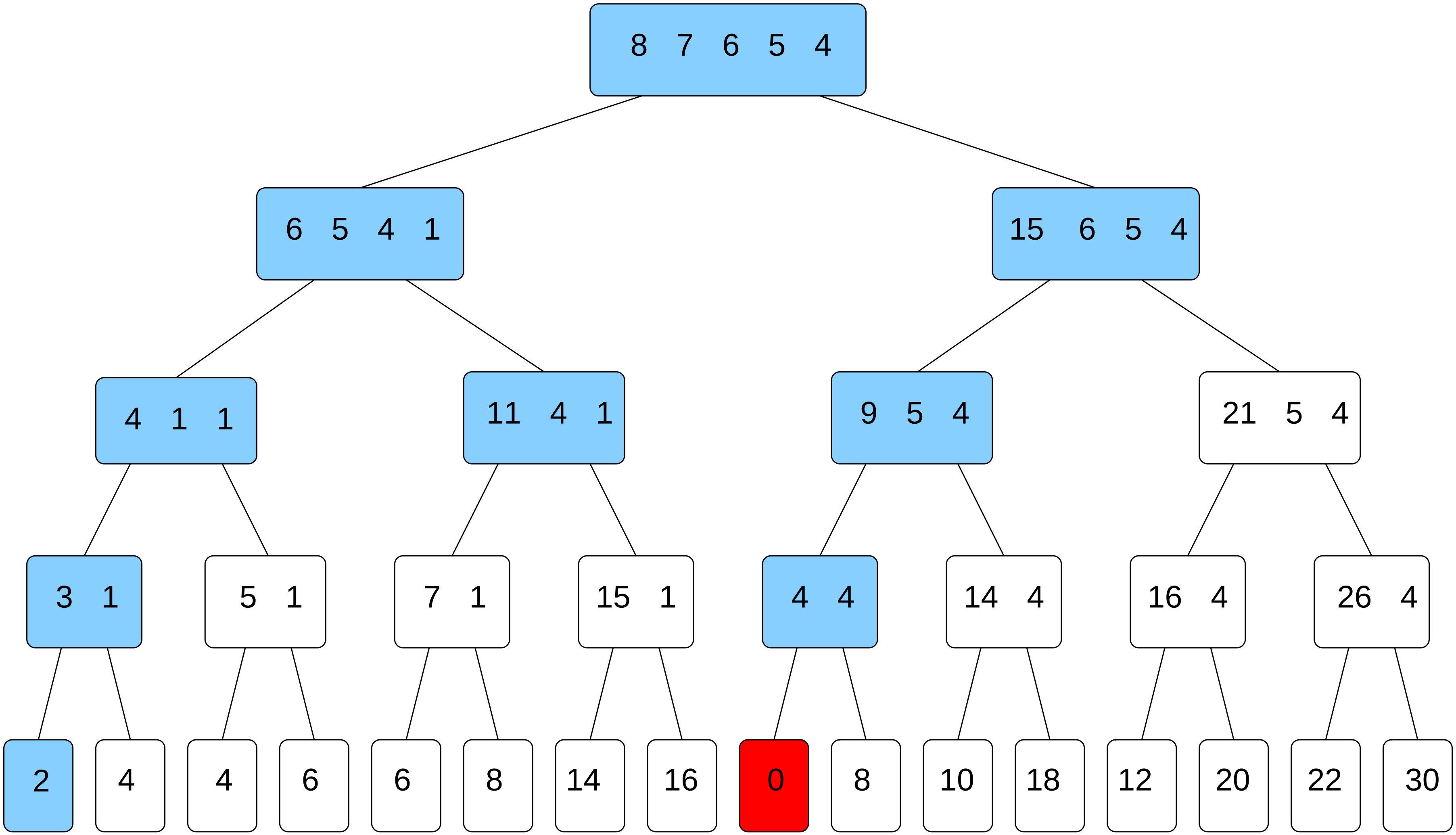
- $L := (a_1, \ldots, a_n)$
- while $|L| > 1$:
  - remove two two largest numbers a_j and a_k from L.
  - insert $|a_j - a_k|$ into L.
- print L

Time complexity is $\mathcal{O}(N \log N)$, Quality[2] is $\Theta(N^{-c \log N})$

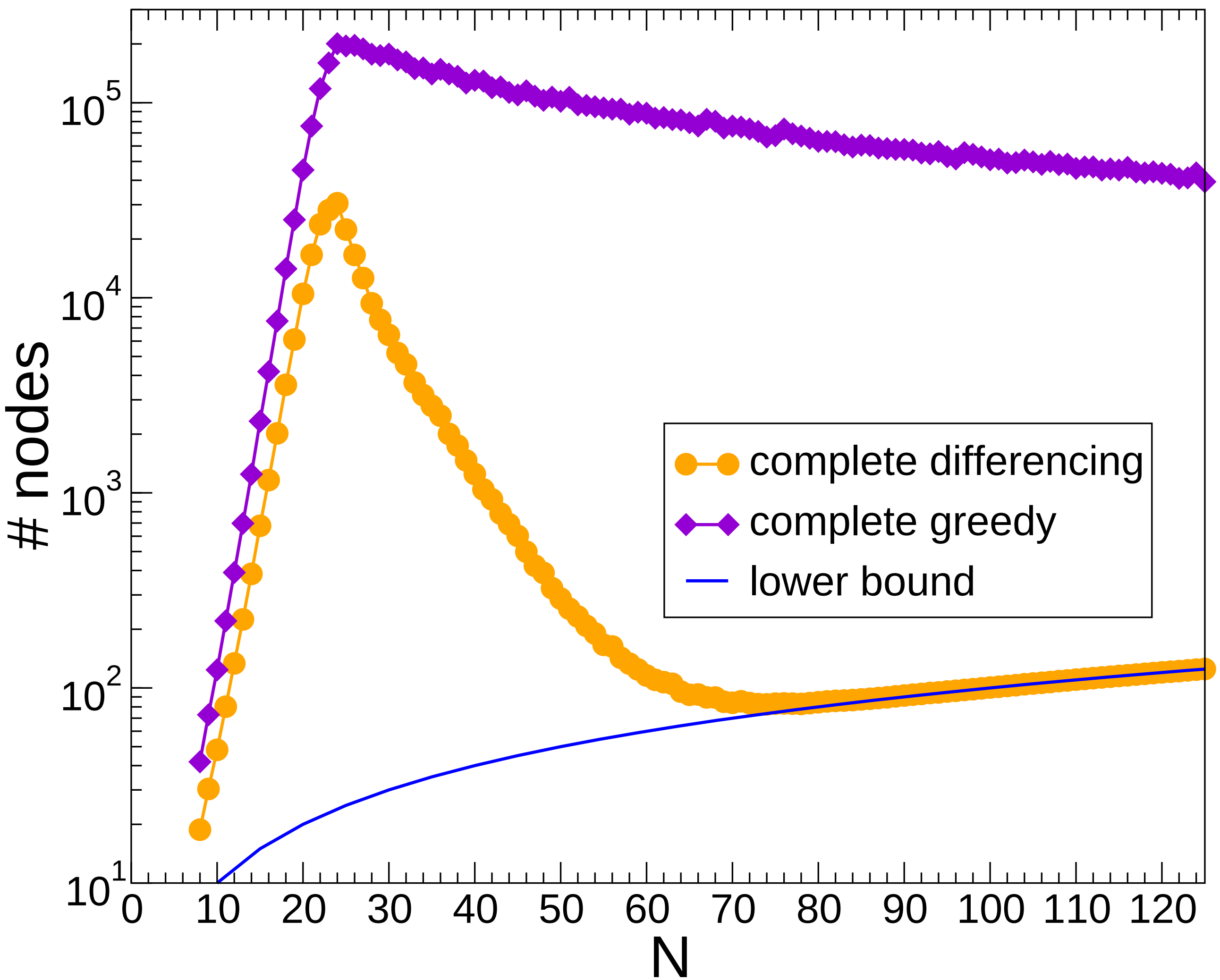
[1] Karmarkar, Karp (1982)

[2] Karmarkar, Karp, Lueker, Odlyzko (1986)

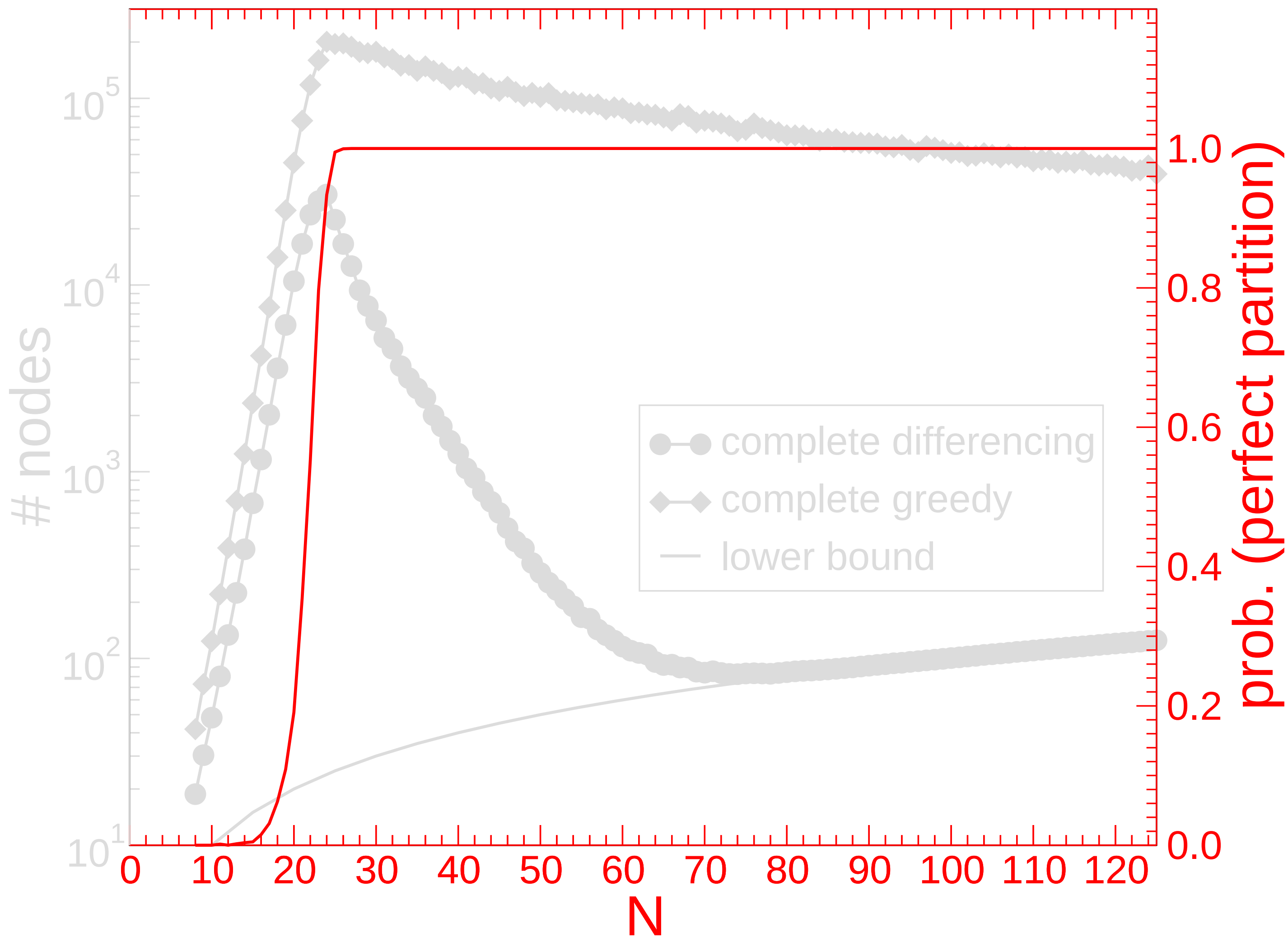
Complete Differencing



Running Times



Emergence of Perfect Partitions



Heuristic Argument

m bits

a_1: 1 0 1 0 0 1 1

a_2: 0 1 1 0 1 1 0

a_3: 1 1 0 1 1 1 1

$\vdots$

a_n: 1 0 0 1 0 1 1

$\sum a_i \sigma_i$: 0 0 0 0 0 0 0

2^{n-1} 2^{n-2} 2^{n-3}

Rigorous Argument

First Moment Bound: Prob$(Z > 0) \leq \mathbb{E}(Z)$

Second Moment Bound: Prob$(Z > 0) \geq \frac{\mathbb{E}(Z)^2}{\mathbb{E}(Z^2)}$

Rigorous Argument

First Moment Bound: Prob$(Z > 0) \leq \mathbb{E}(Z)$

Second Moment Bound: Prob$(Z > 0) \geq \frac{\mathbb{E}(Z)^2}{\mathbb{E}(Z^2)}$

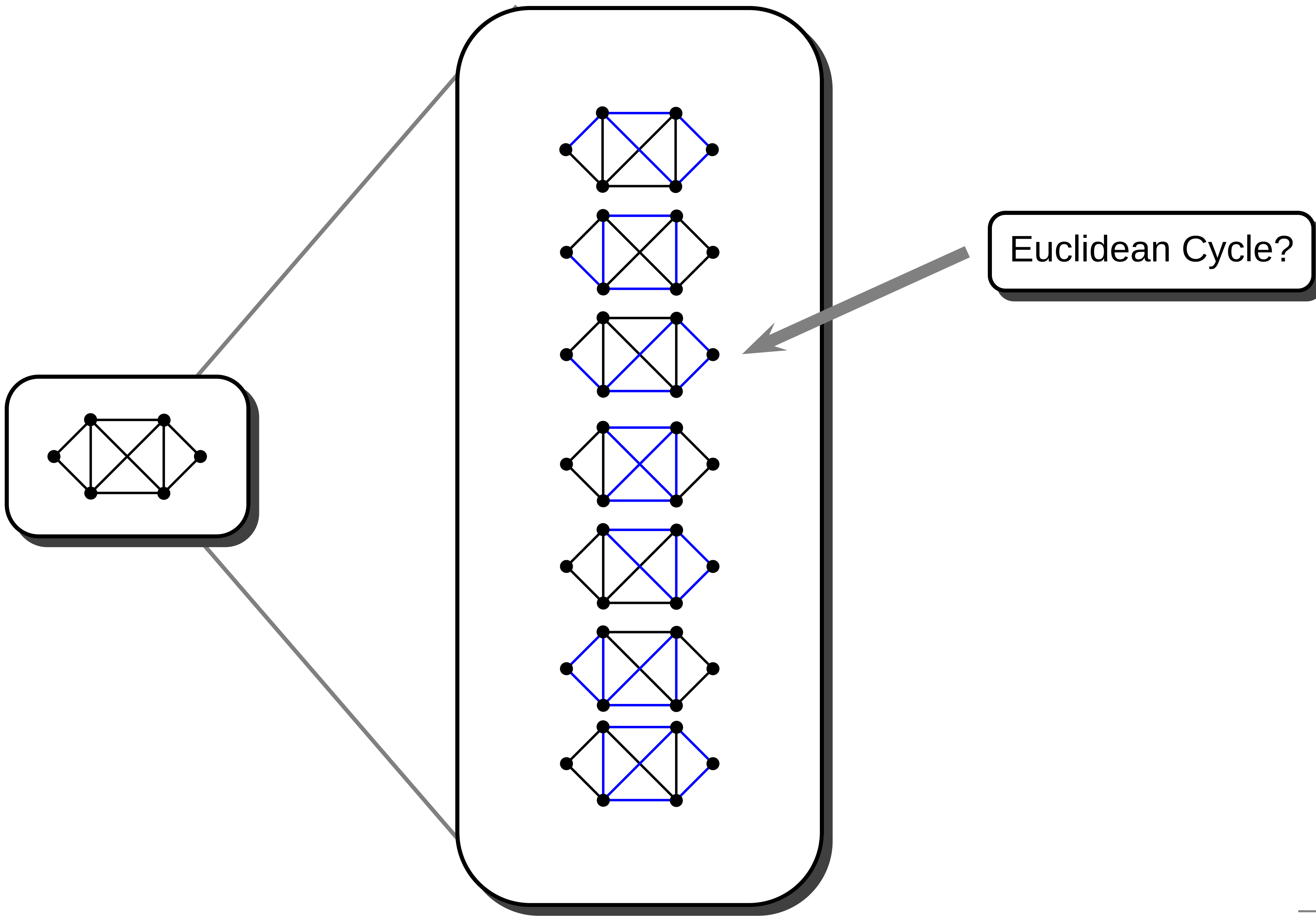
Here: Z := # of perfect partitions of m-bit iid integers.

$$\mathbb{E}(Z) \simeq 2^{n-m}\sqrt{\frac{3}{2\pi n}} \to 0 \text{ for } \kappa := \frac{m}{n} > 1$$

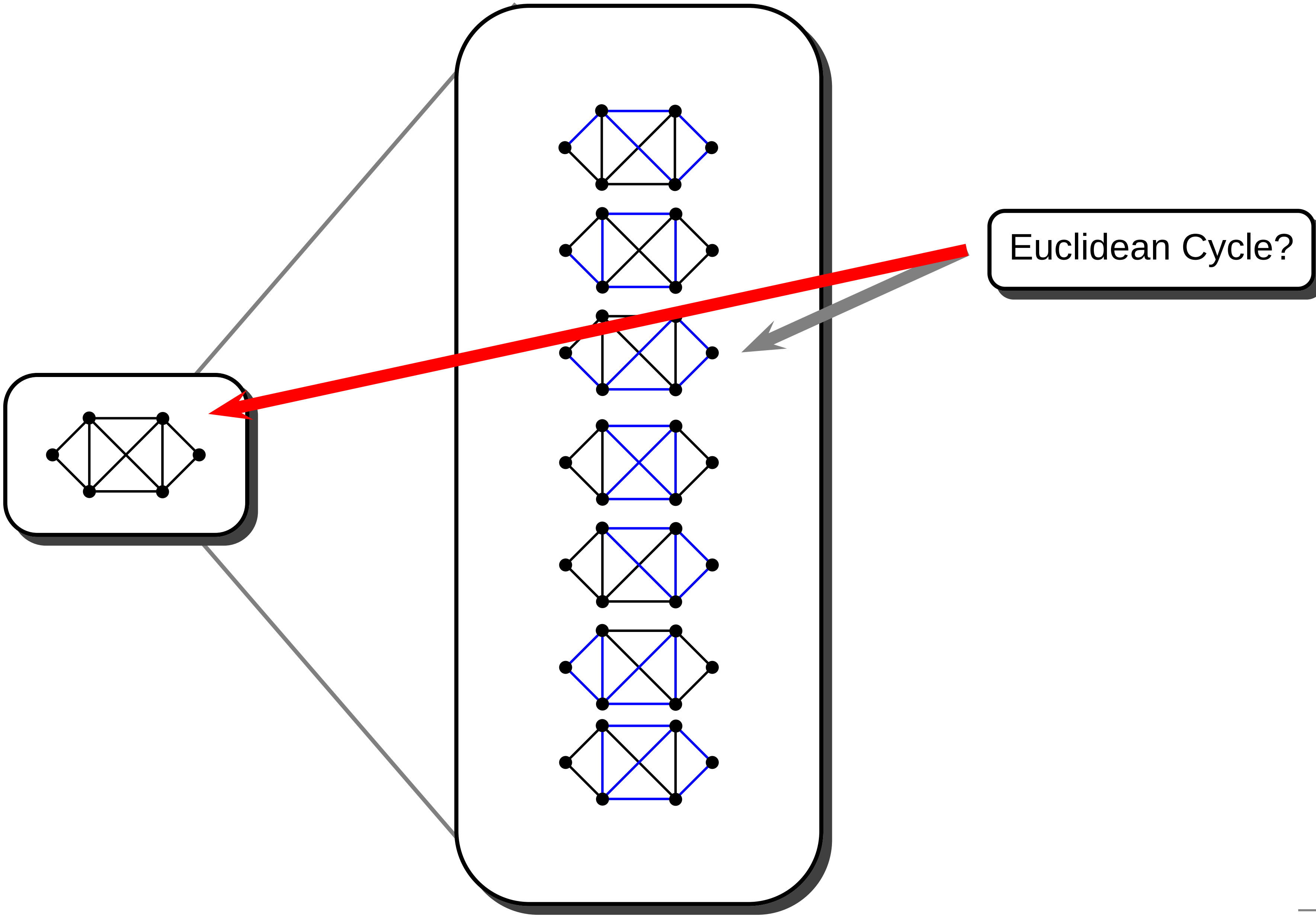
$$\frac{\mathbb{E}(Z)^2}{\mathbb{E}(Z^2)} \simeq 1 \text{ for } \kappa < 1$$

$$\Rightarrow \quad \lim_{n\to\infty} \text{Prob}(Z > 0) = \begin{cases} 1 & \kappa < 1 \\ 0 & \kappa > 1 \end{cases}$$

Mathematical Haystacks



Mathematical Haystacks



Mathematical Haystacks

74636649
31389813
34562189
73552552
31456321
46372280
20349548
43289010
74093204
31415926
05647308
89745638
80103341
31443277
45632831
21467430

31415926 ?

Level statistics of the NPP

$$g(E) = \mathbb{E}\left(\delta\left(E - |\sum a_j \sigma_j|\right)\right)_{a,\sigma} \simeq \sqrt{\frac{6}{N\pi}}\,\mathrm{e}^{-3E^2/2N}$$

Level statistics of the NPP

$$g(E) = \mathbb{E}\left(\delta\left(E - |\sum a_j\sigma_j|\right)\right)_{a,\sigma} \simeq \sqrt{\frac{6}{N\pi}}\,\mathrm{e}^{-3E^2/2N}$$

Sort energies: $0 < E_1 < E_2 < \cdots < E_{2^{N-1}}$.

$$\varepsilon_k(N) := \sqrt{\frac{6}{N\pi}}\,2^{N-1}\,E_k$$

Level statistics of the NPP

$$g(E) = \mathbb{E}\left(\delta\big(E - |\sum a_j \sigma_j|\big)\right)_{a,\sigma} \simeq \sqrt{\frac{6}{N\pi}}\,\mathrm{e}^{-3E^2/2N}$$

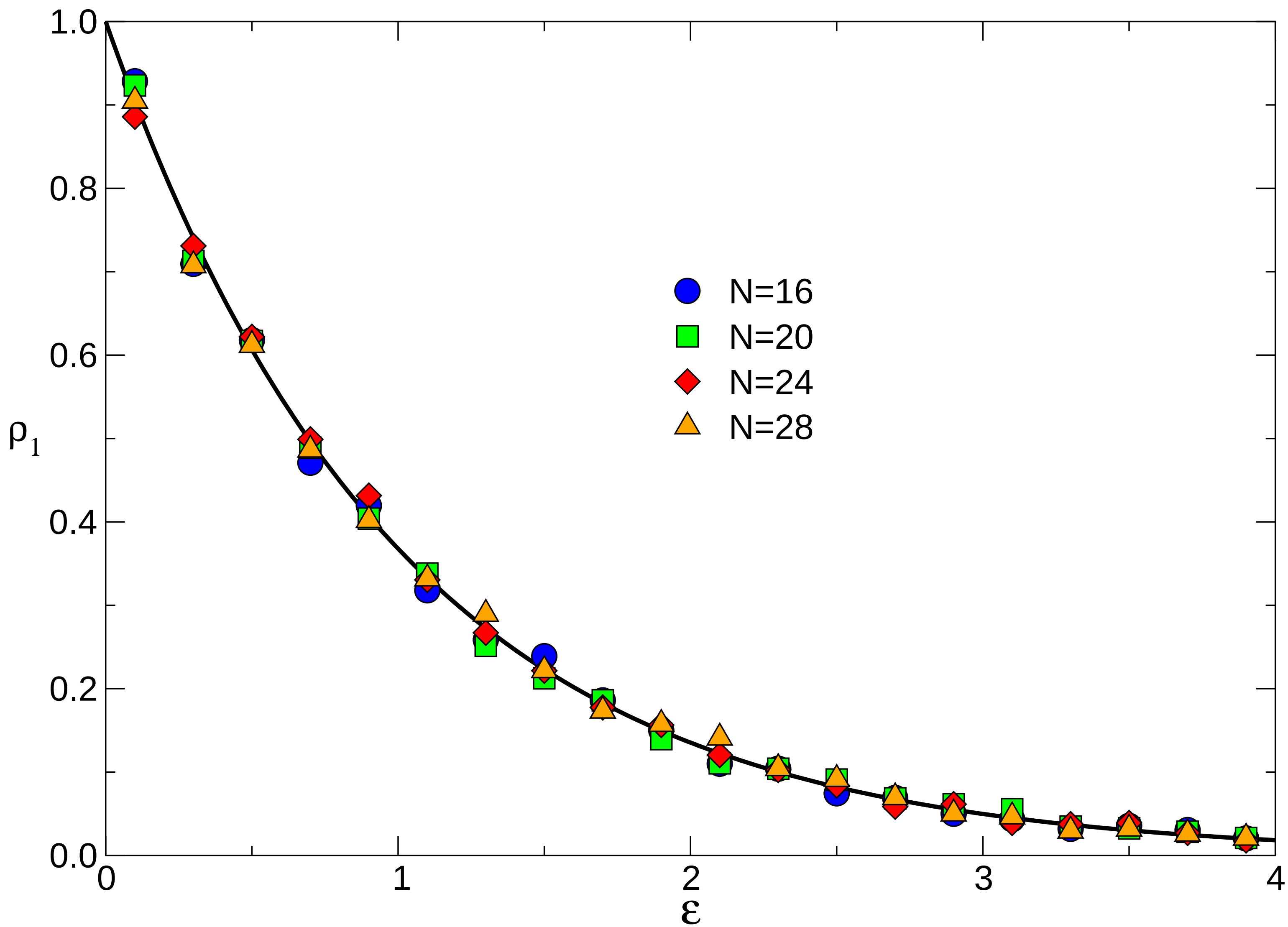
Sort energies: $0 < E_1 < E_2 < \cdots < E_{2^{N-1}}$.

$$\varepsilon_k(N) := \sqrt{\frac{6}{N\pi}}\,2^{N-1}\,E_k$$

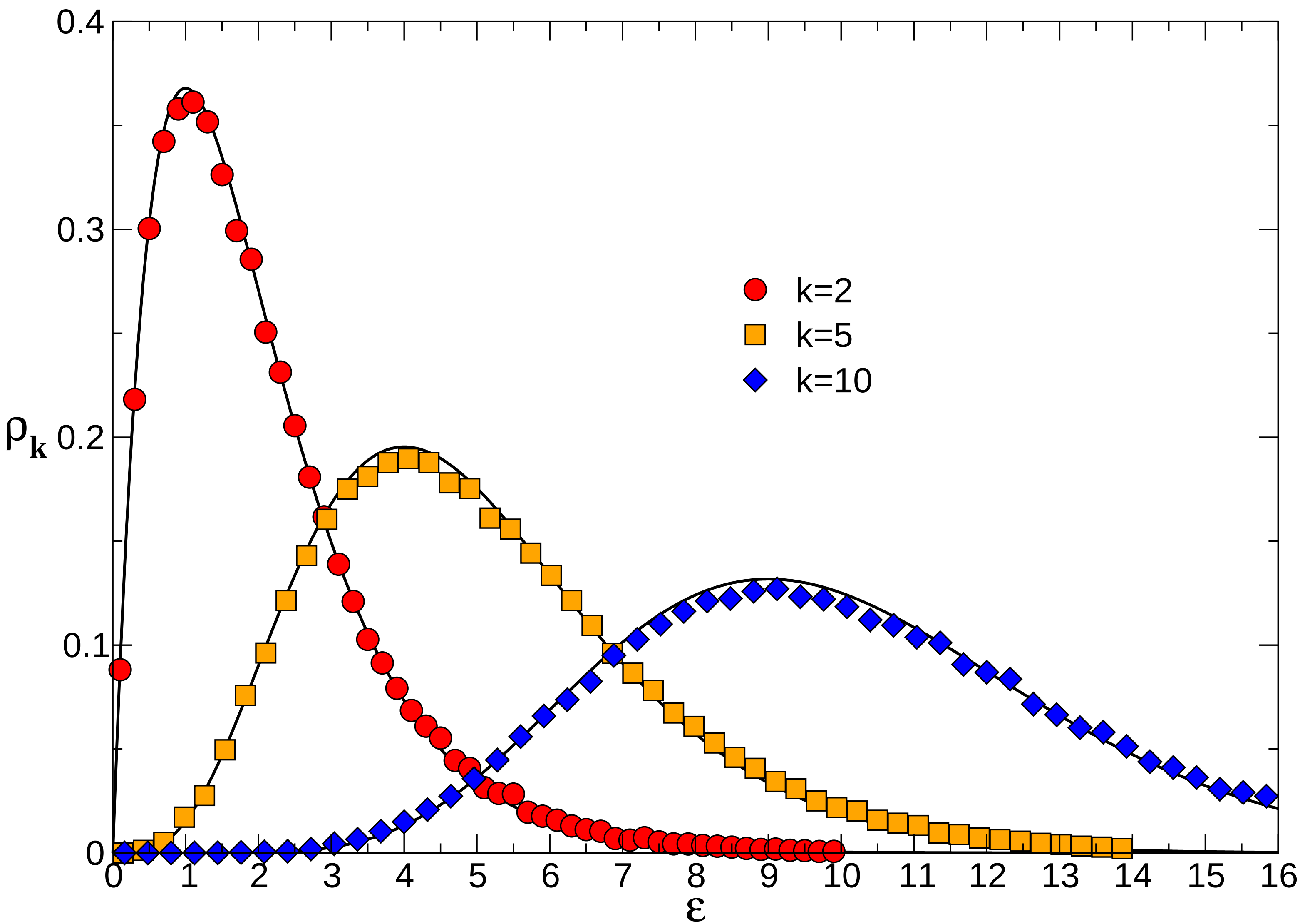
REM: Assume E_k are independent. Then

$$\lim_{N\to\infty} \rho_k(\varepsilon) = \frac{\varepsilon^{k-1}}{\Gamma(k)}\,\mathrm{e}^{-\varepsilon}$$

Testing the REM hypothesis



Testing the REM hypothesis



Configurations

Groundstate: $E(\sigma) = E_1$

1st excitation: $E(\sigma') = E_2$

$$q(\sigma, \sigma') = \frac{1}{N} \left| \sum_{i=1}^{N} \sigma_i \sigma_i' \right|$$

Configurations

Groundstate: $E(\sigma) = E_1$

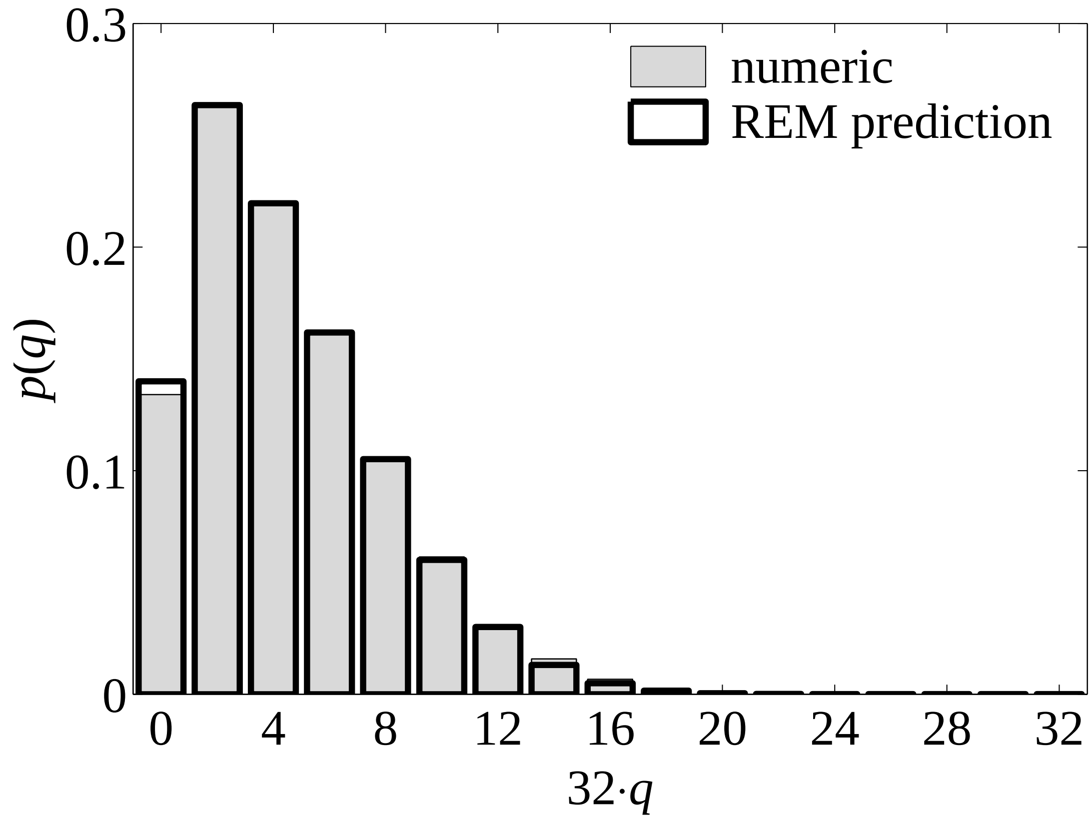
1st excitation: $E(\sigma') = E_2$

$$q(\sigma, \sigma') = \frac{1}{N} \left| \sum_{i=1}^{N} \sigma_i \sigma_i' \right|$$

REM: σ and σ' uncorrelated

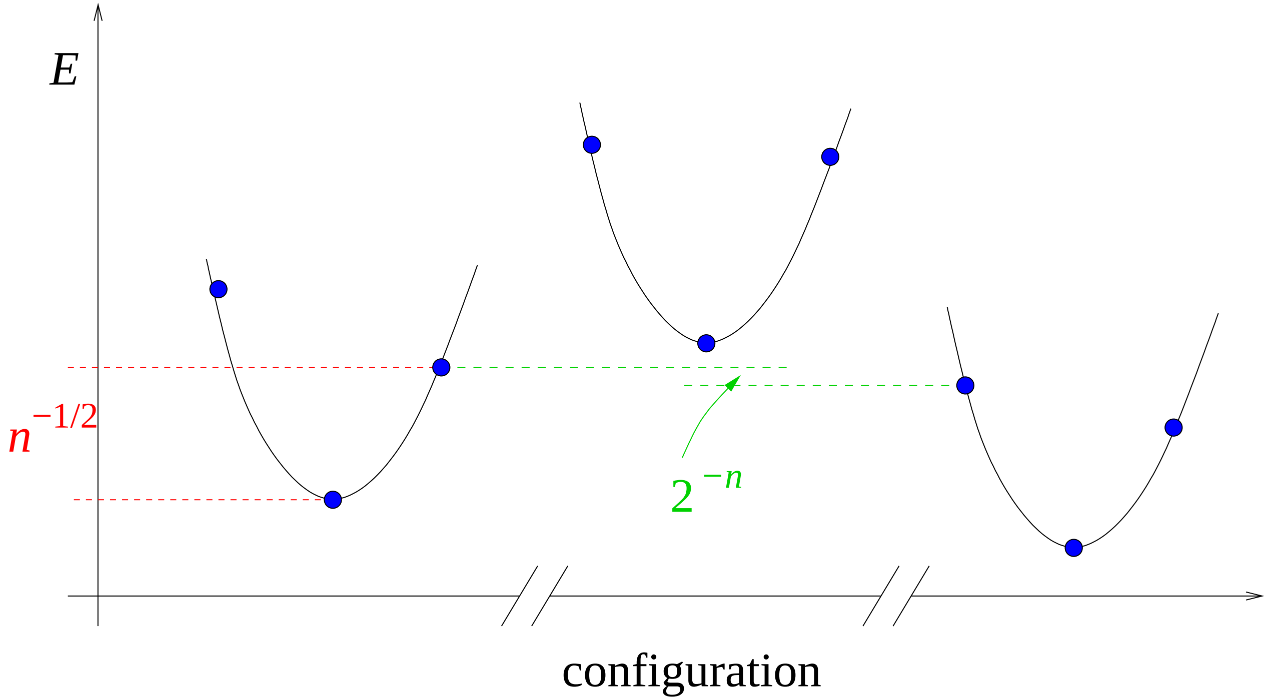
$$p(q) = \begin{cases} 2^{-N} \binom{N}{N/2} & \text{for } q = 0 \\ 2^{-N+1} \binom{N}{N(1-q)/2} & \text{for } q > 0 \, . \end{cases}$$

Configurations



Overlap q of ground state and first excited state ($N = 32$).

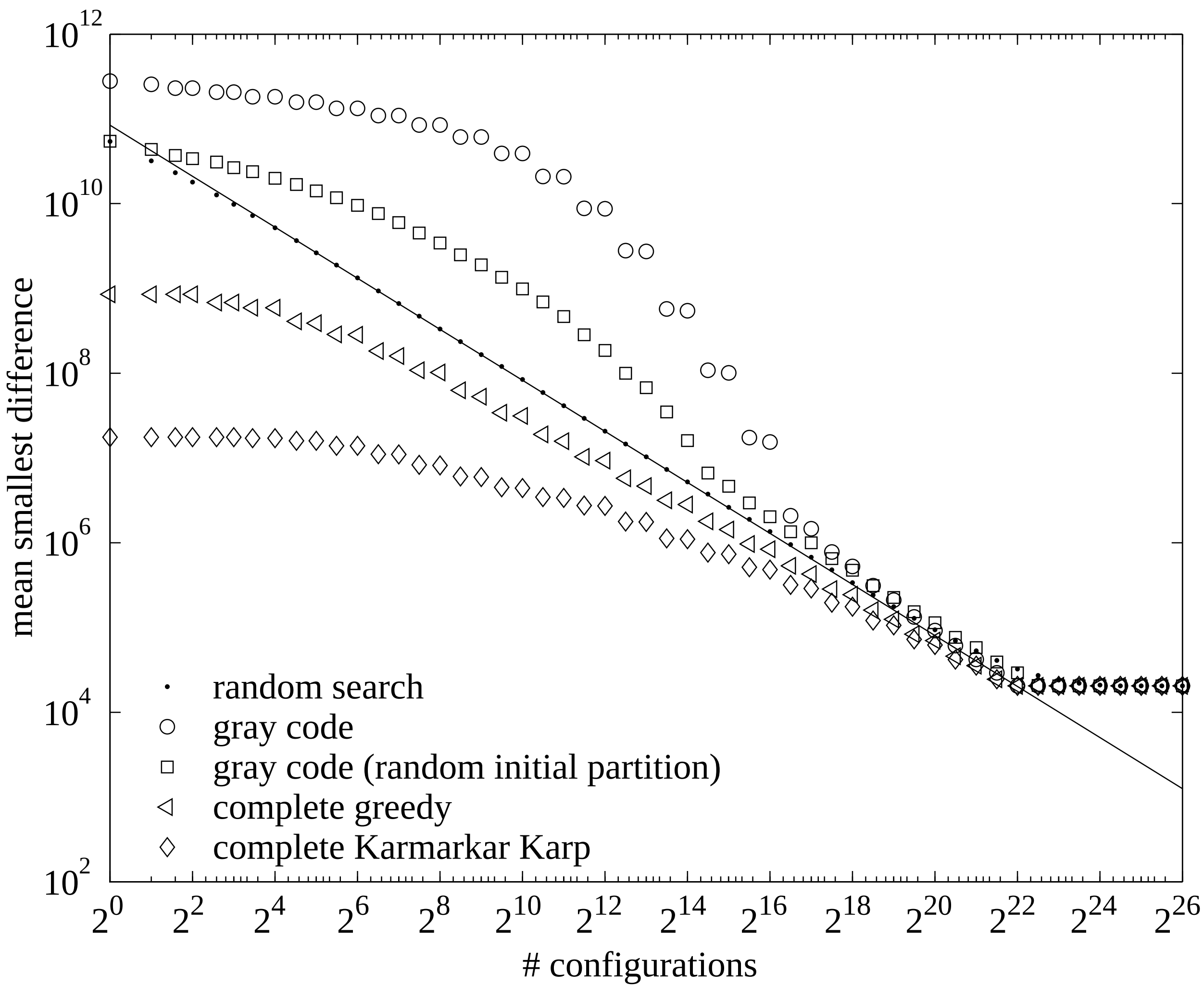
Energy Landscape



close in energy, close in config space

choose one

Lost in Space



Heuristic Explanation

Let a_i's be B-bit random numbers, $a_i \in \{0, 1, \ldots, 2^B - 1\}$.

$$E = -\sum_{i=1}^{N} a_i \sigma_i \in [-N2^B, N2^B]$$

Heuristic Explanation

Let a_i's be B-bit random numbers, $a_i \in \{0, 1, \ldots, 2^B - 1\}$.

$$E = -\sum_{i=1}^{N} a_i \sigma_i \in [-N2^B, N2^B]$$

- $B < N$: $\Delta E_r = E_{r+1} - E_r = 2$

Heuristic Explanation

Let a_i's be B-bit random numbers, $a_i \in \{0, 1, \ldots, 2^B - 1\}$.

$$E = -\sum_{i=1}^{N} a_i \sigma_i \in [-N2^B, N2^B]$$

- $B < N$: $\Delta E_r = E_{r+1} - E_r = 2$
- $B > N$: $\Delta E_r \simeq O(2^{B-N})$
  - ΔE_r determined by $B - N$ low order bits of J
  - σ controls only N high order bits J

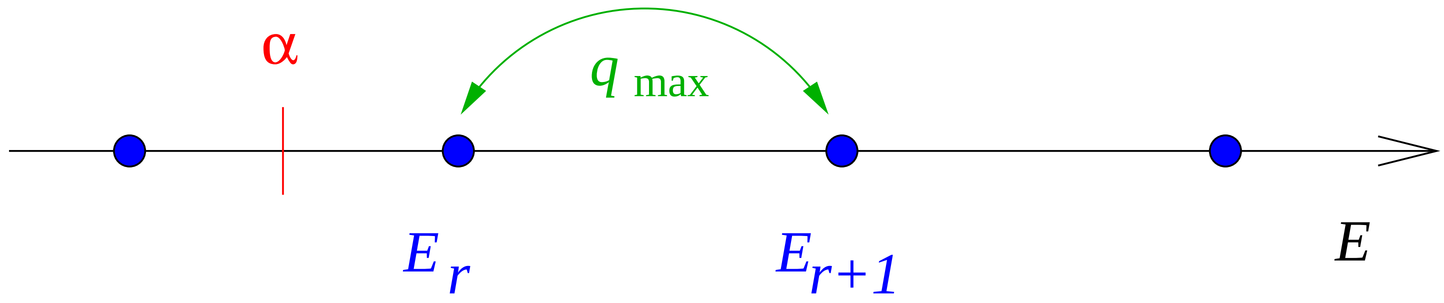
Heuristic Explanation

Let a_i's be B-bit random numbers, $a_i \in \{0, 1, \ldots, 2^B - 1\}$.

$$E = -\sum_{i=1}^{N} a_i \sigma_i \in [-N2^B, N2^B]$$

- $B < N$: $\Delta E_r = E_{r+1} - E_r = 2$
- $B > N$: $\Delta E_r \simeq O(2^{B-N})$
  - ΔE_r determined by $B - N$ low order bits of J
  - σ controls only N high order bits J
- local REM should depend on bit-entropy of the disorder

Maximum Overlap



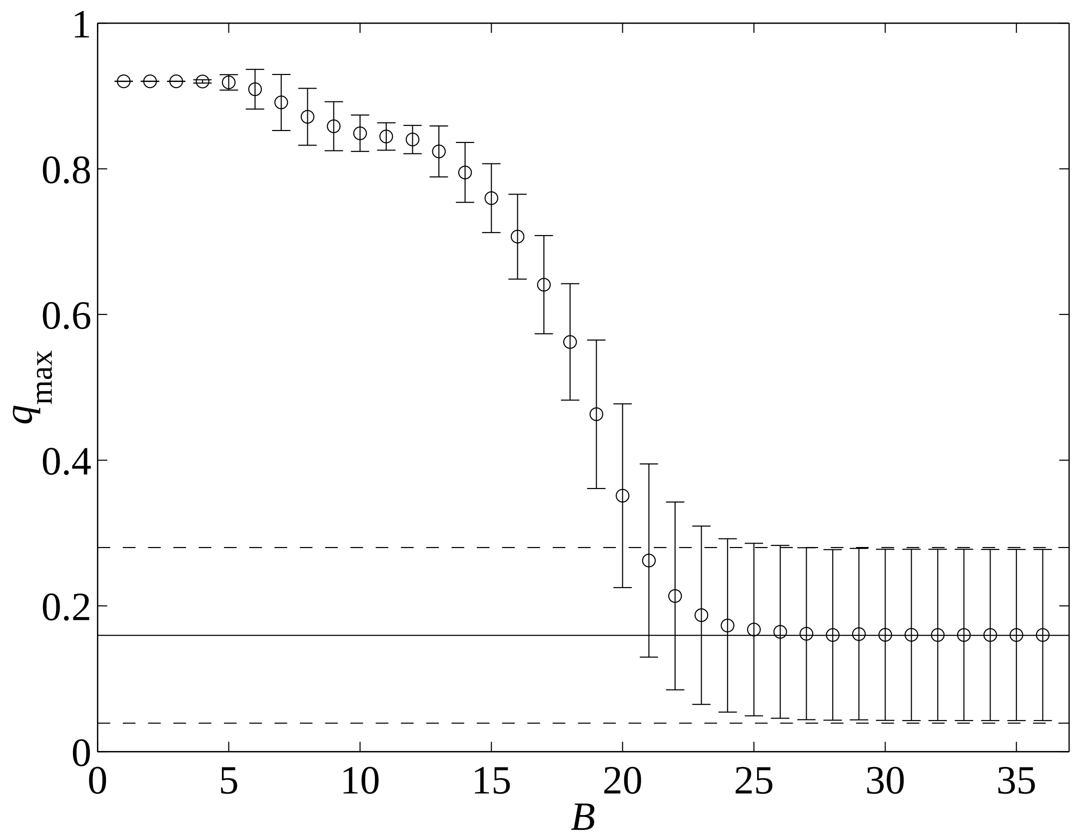
- $B \ll n$: levels are exponentially degenerated

$$q_{\max} \simeq 1 - \frac{2}{n}$$

- $B \gg n$: levels are non-degenerated

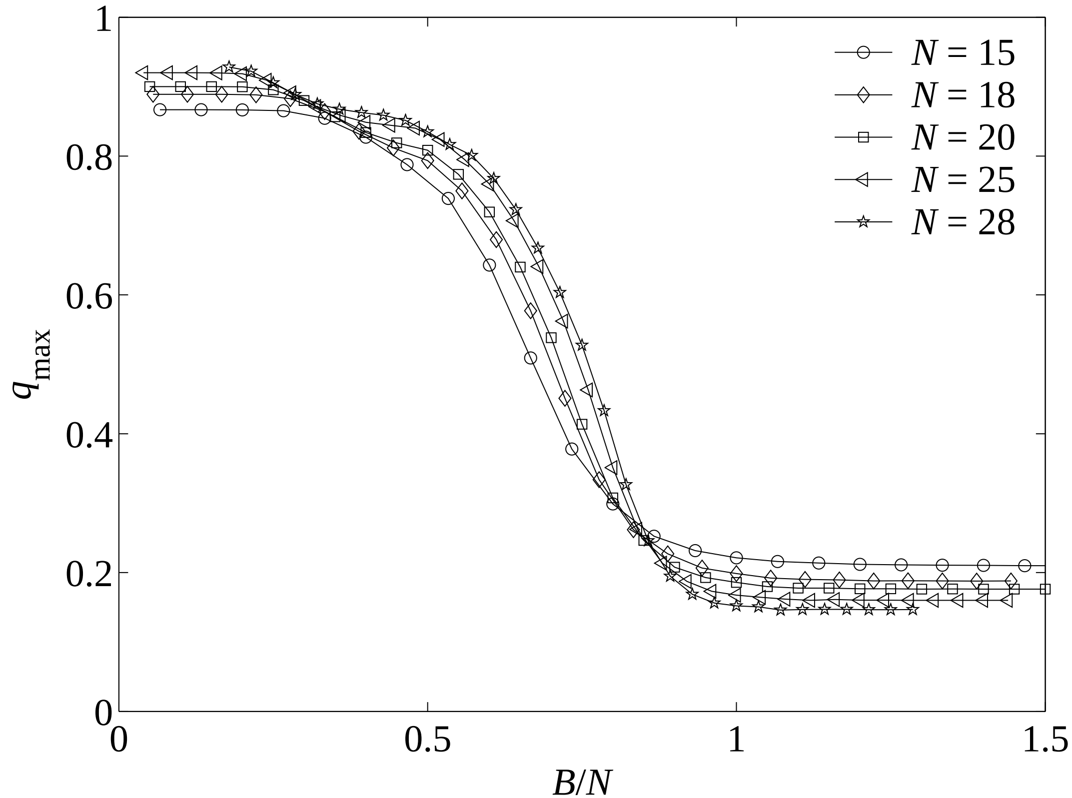
$$q_{\max} = q_{\text{random}}$$

Local Moves



Max. overlap of two energetically adjacent configurations.

Phase Transition



Maximum overlap between energetically adjacent configurations.

Universality

Heuristic explanation of local REM relies on

- $H(\sigma) = \sum a_j \sigma_j$
- max$|H(\sigma)| =$ poly(n)
- card$\{\sigma\} = \Theta(2^n)$

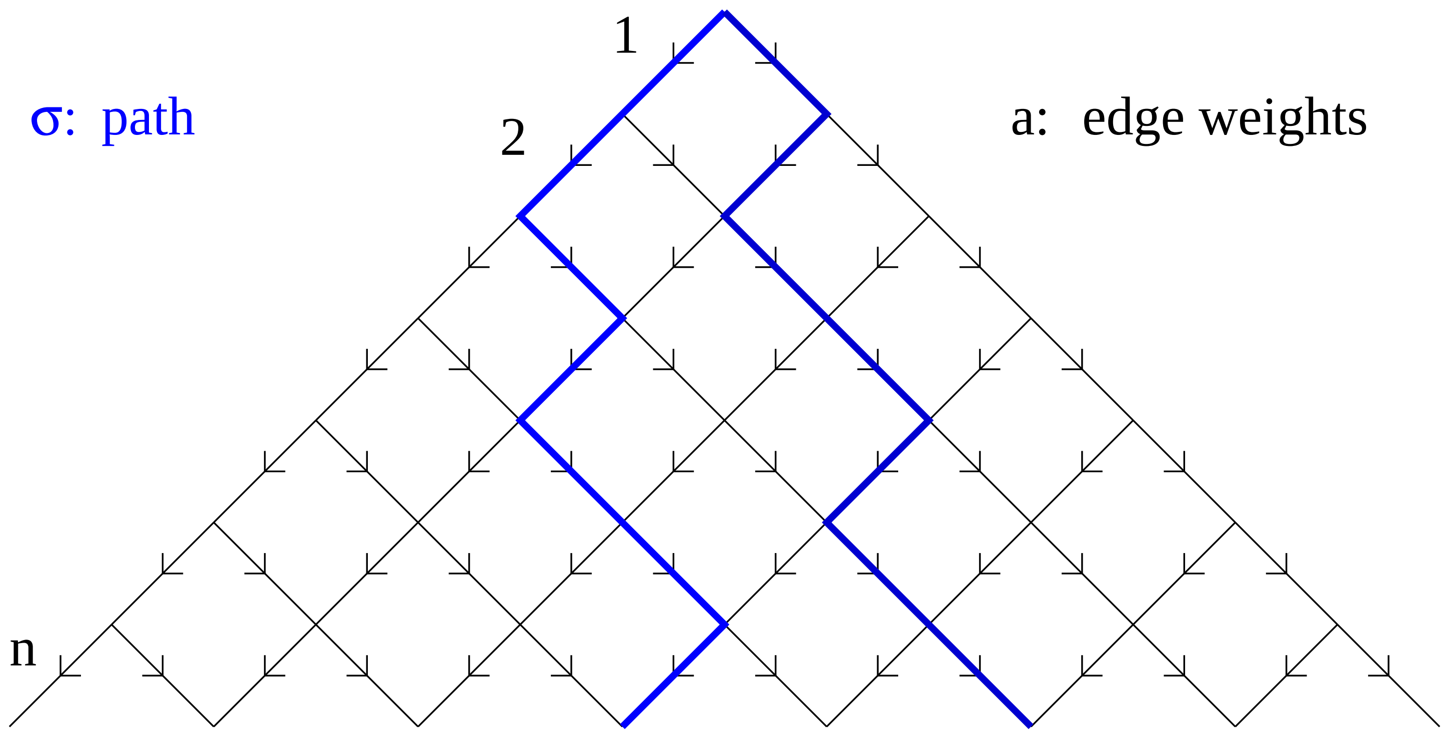
Universality

Heuristic explanation of local REM relies on

- $H(\sigma) = \sum a_j \sigma_j$
- max$|H(\sigma)| =$ poly(n)
- card$\{\sigma\} = \Theta(2^n)$

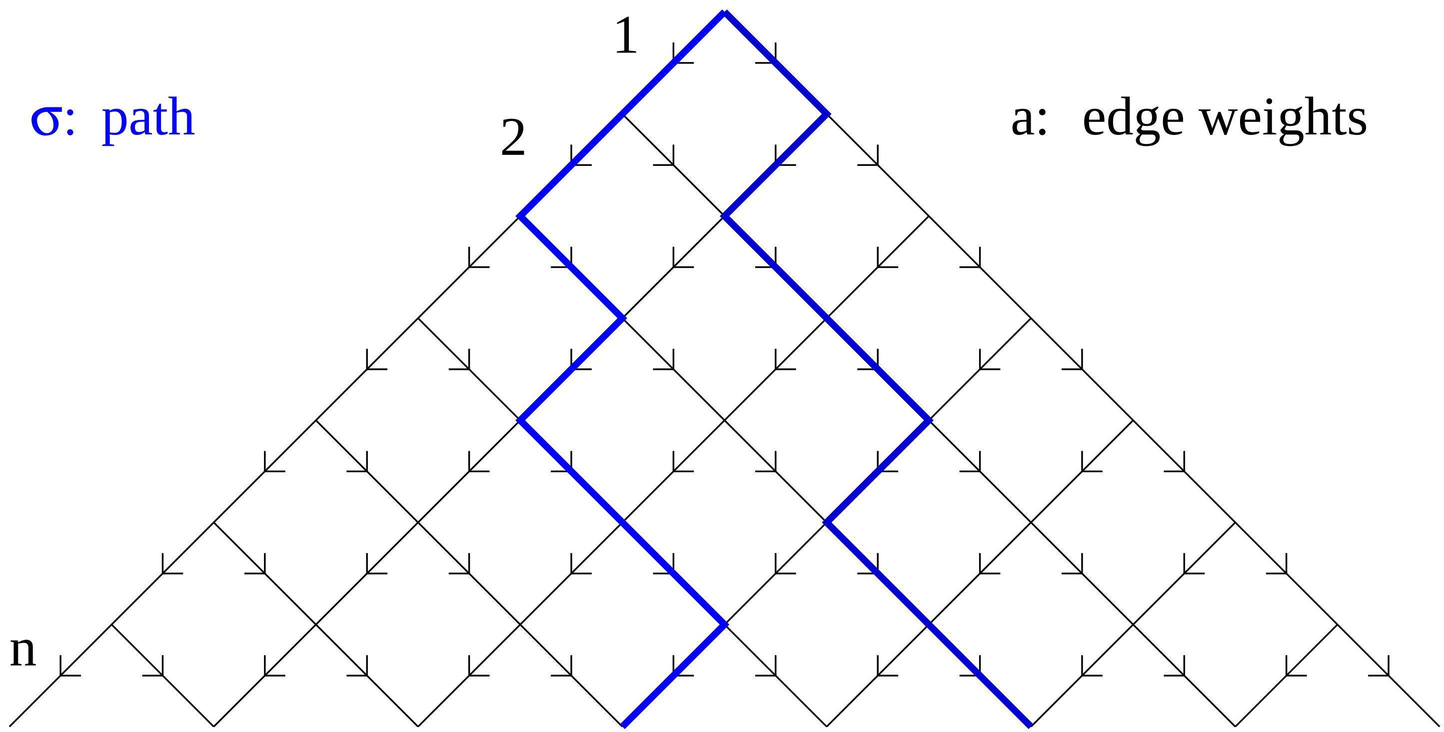
Local REM is a universal feature.

DPRM



Directed Polymer in Random Media

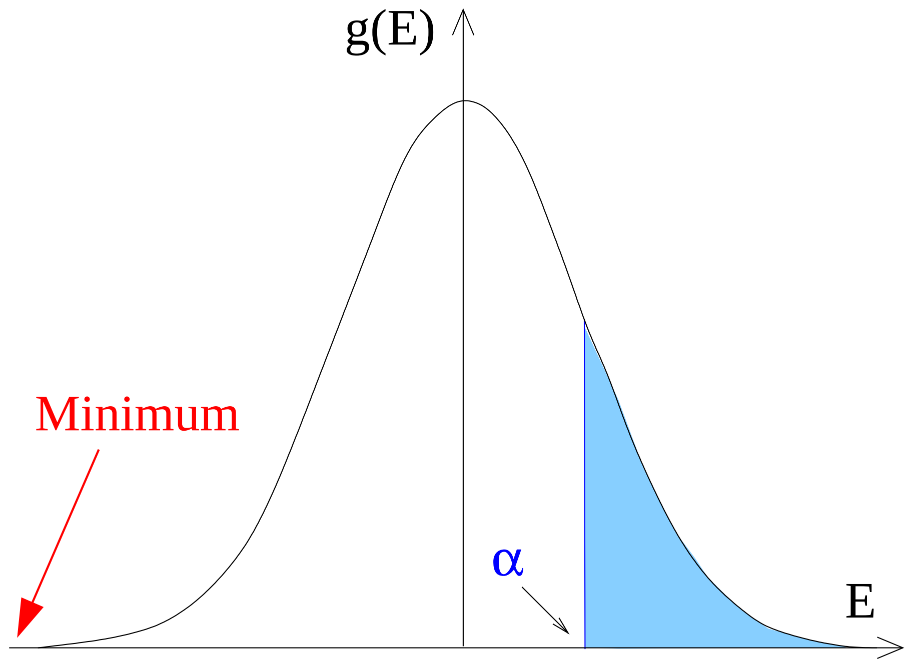
DPRM



Directed Polymer in Random Media

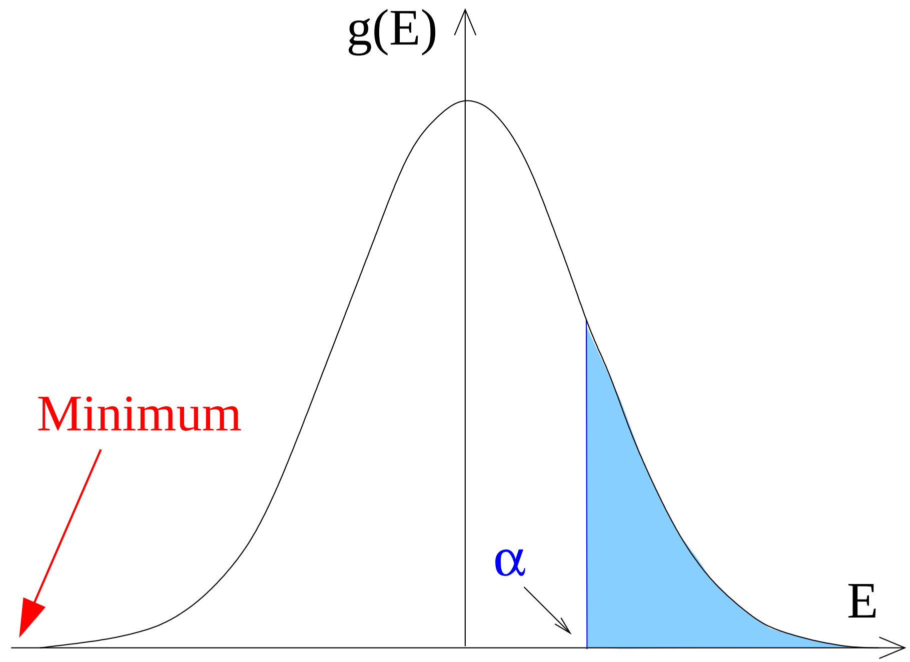
- single-source shortest-path problem
- solvable in polynomial time (Bellman-Ford)

Constrained DPRM



Find shortest path among all paths with length $\geq \alpha$.

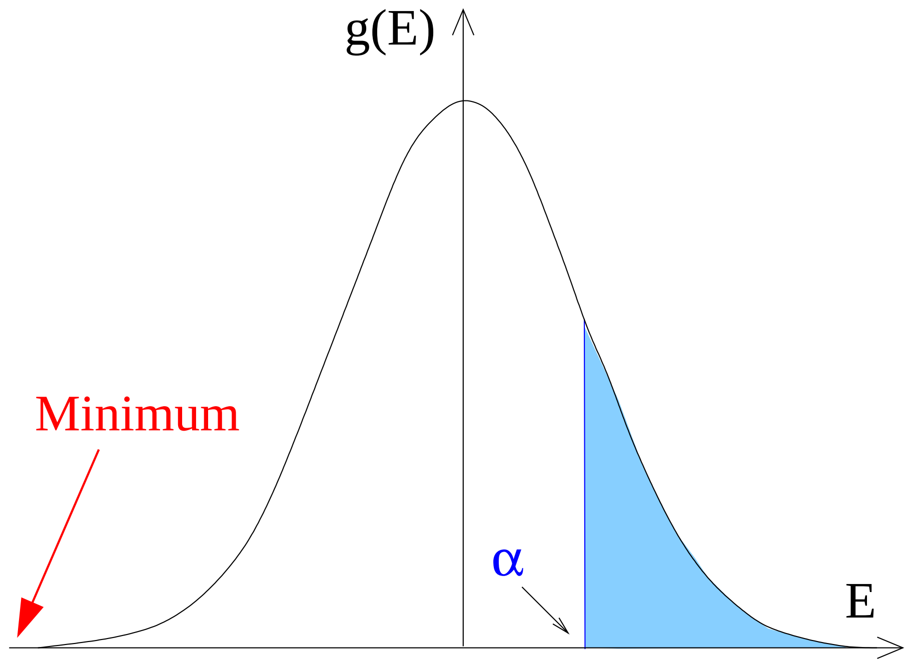
Constrained DPRM



Find shortest path among all paths with length $\geq \alpha$.

- cannot be easier than unconstrained case ($\alpha = -\infty$)

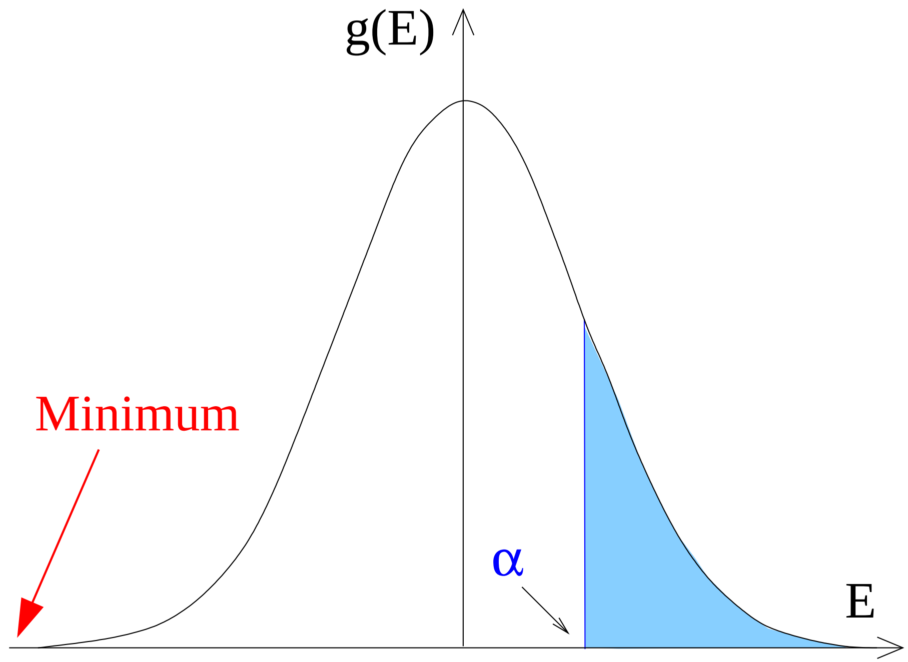
Constrained DPRM



Find shortest path among all paths with length $\geq \alpha$.

- cannot be easier than unconstrained case ($\alpha = -\infty$)
- is NP-hard

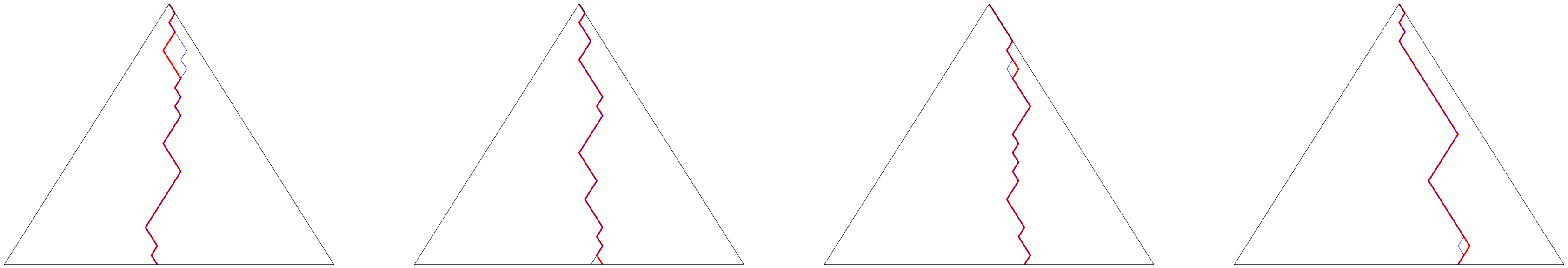
Constrained DPRM



Find shortest path among all paths with length $\geq \alpha$.

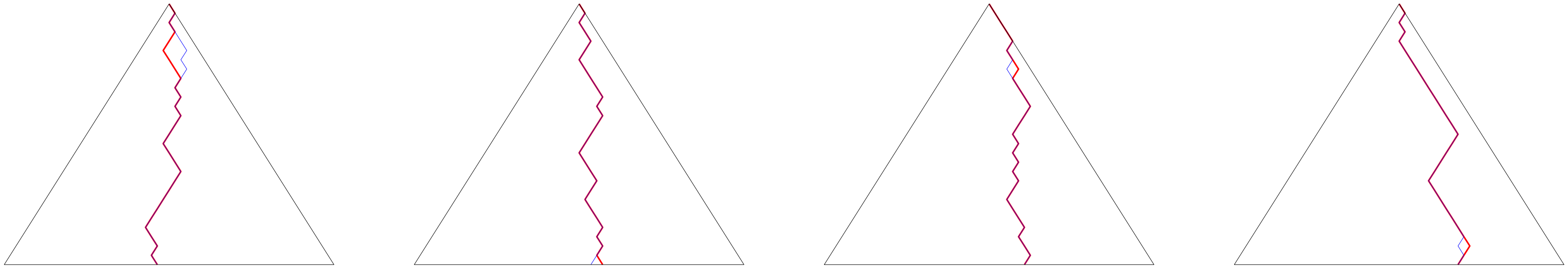
- cannot be easier than unconstrained case ($\alpha = -\infty$)
- is NP-hard
- has local REM property

Energetically Adjacent Paths

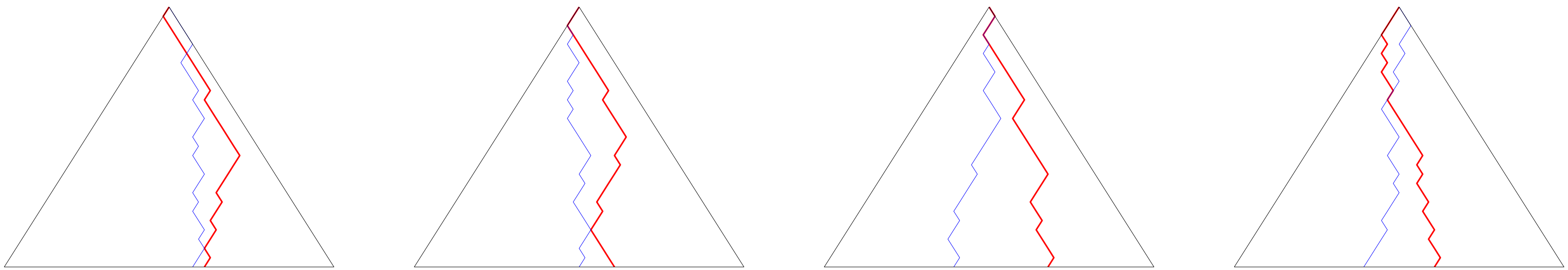


$$\alpha = -\infty$$

Energetically Adjacent Paths

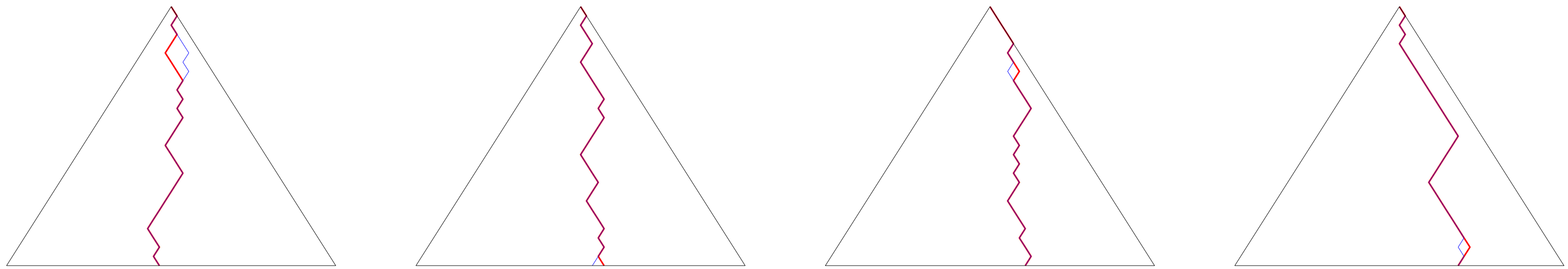


$$\alpha = -\infty$$

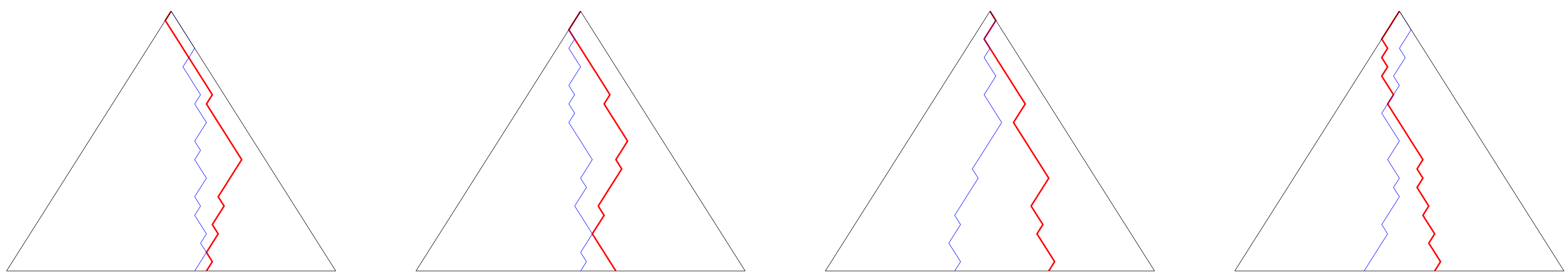


$$\alpha = 0$$

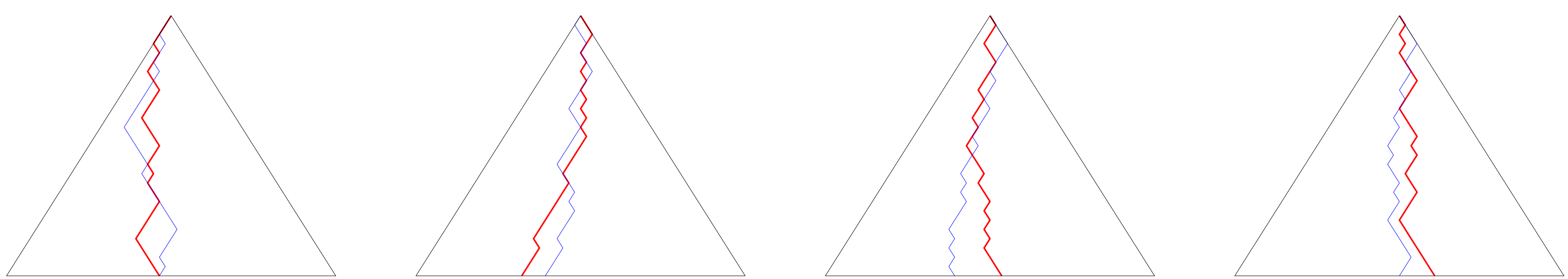
Energetically Adjacent Paths



$\alpha = -\infty$



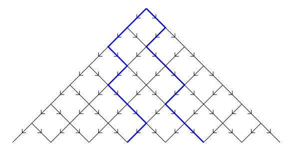
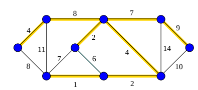
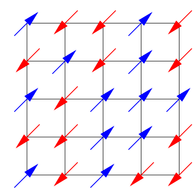
$\alpha = 0$



random

More Examples

Minimizing $H(\sigma)$ is polynomial for

- DPRM, shortest path 
- Minimum Spanning Tree 
- $1d$ and $2d$ Spin-Glasses 

Minimizing s.t. $H(\sigma) \geq \alpha$ is NP-complete
All problems have local REM property.

Experiments on Random 3-SAT

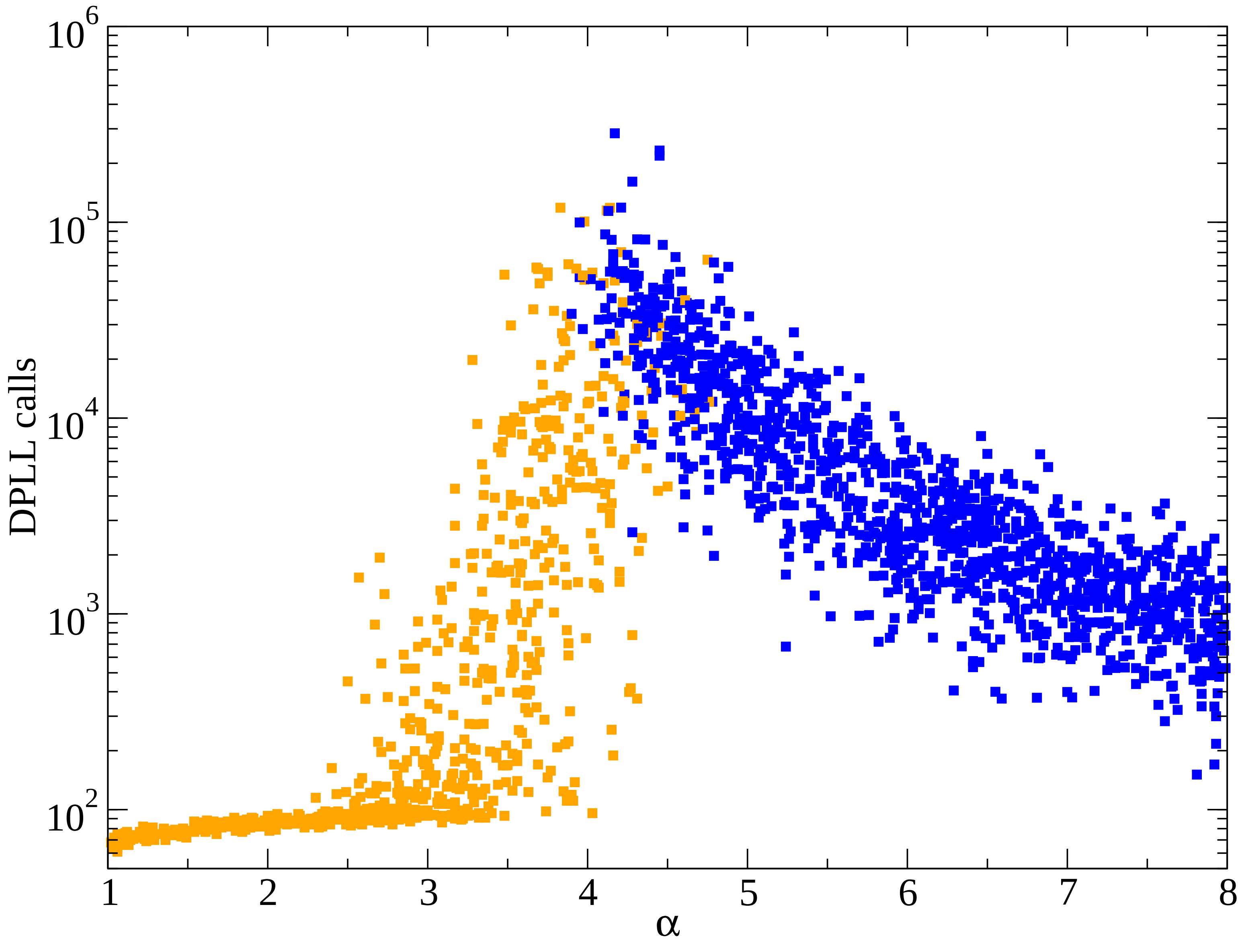
"If mathematics describes an objective world just like physics, there is no reason why inductive methods should not be applied in mathematics just the same as in physics."

Kurt Gödel (1951)

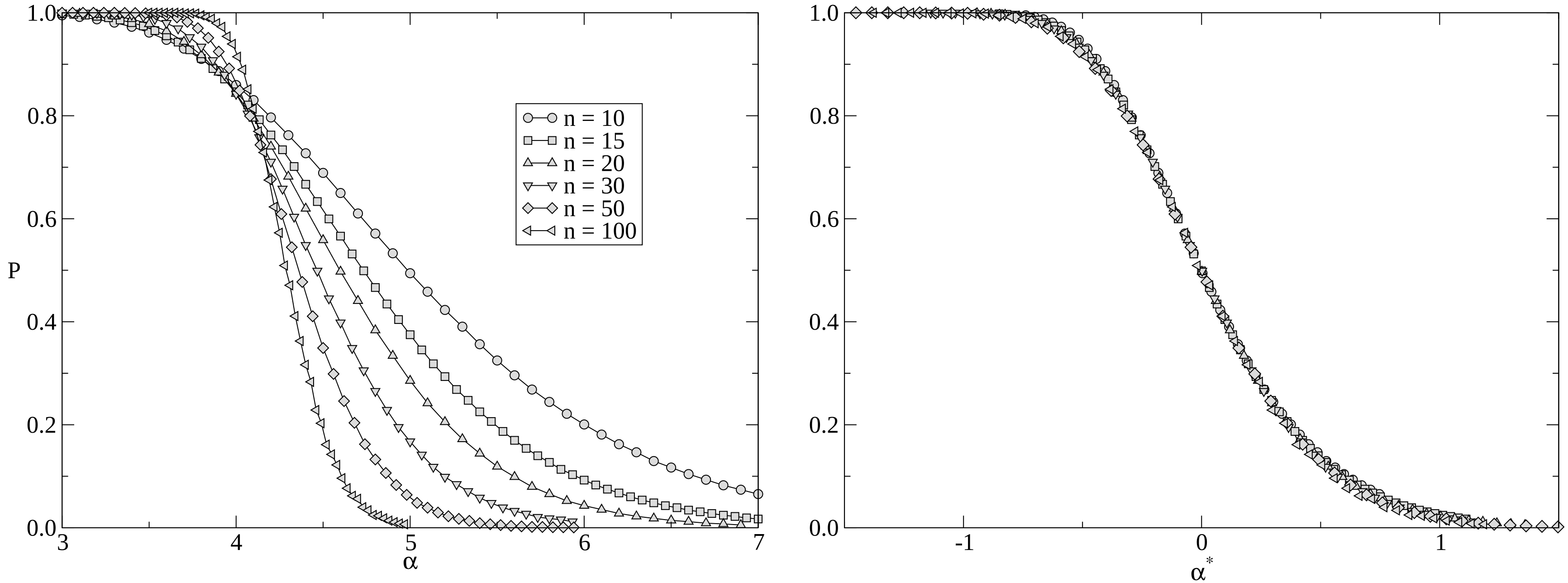
A Simple Algorithm

```
DPLL (F)
begin
    if F is empty then return SAT;
    if F contains empty clause then return UNSAT;
    select a literal ℓ ∈ F;
    F' := F(ℓ = true);
    if DPLL(F') = SAT then return SAT;
    F' := F(ℓ = false);
    if DPLL(F') = SAT then return SAT;
    return UNSAT
end
```

First Light



SAT-UNSAT Transition



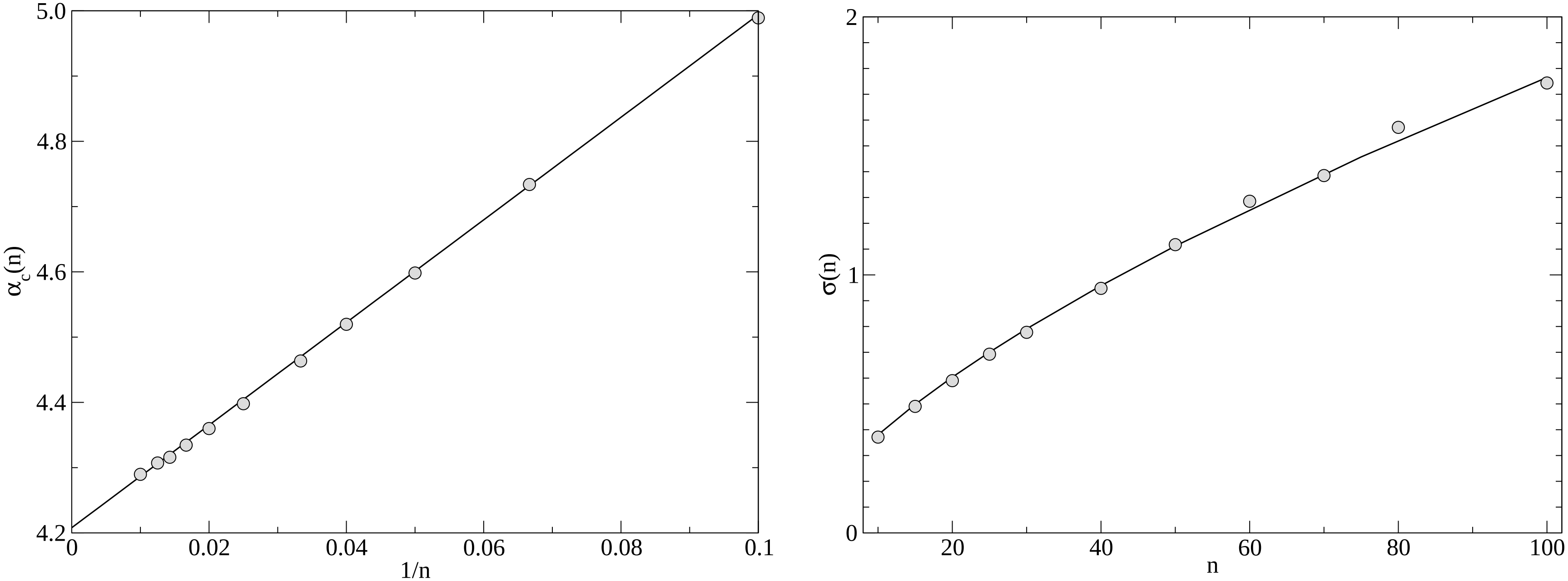
Finite Size Scaling

$$\alpha^\star = \sigma(n)[\alpha - \alpha_c(n)]$$

Data Collapse

$$P(\alpha) = \hat{P}\big(\sigma(n)[\alpha - \alpha_c(n)]\big)$$

Finite Size Scaling

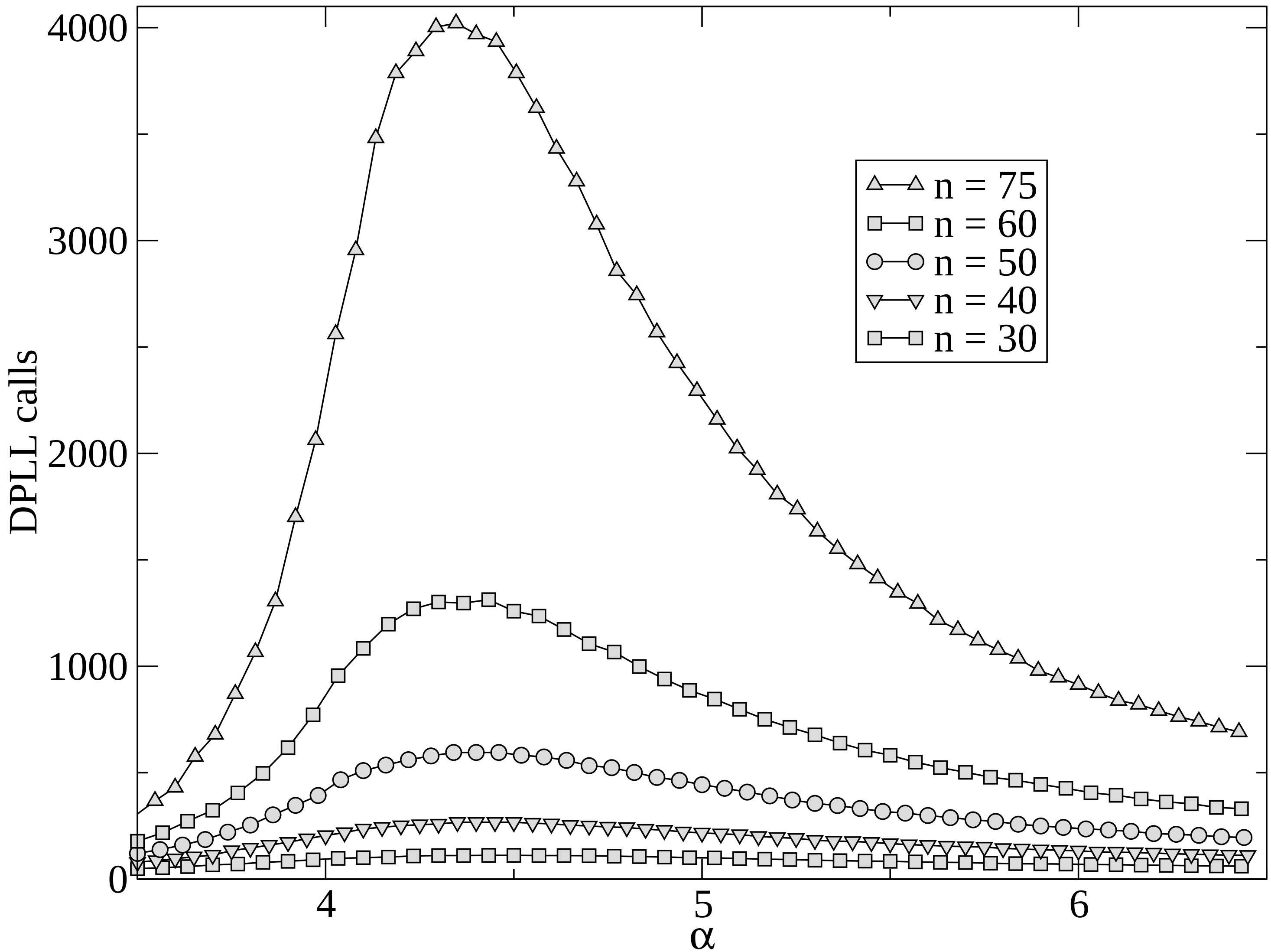


$$\alpha_c(n) = \alpha_c + \Theta(1/n)$$

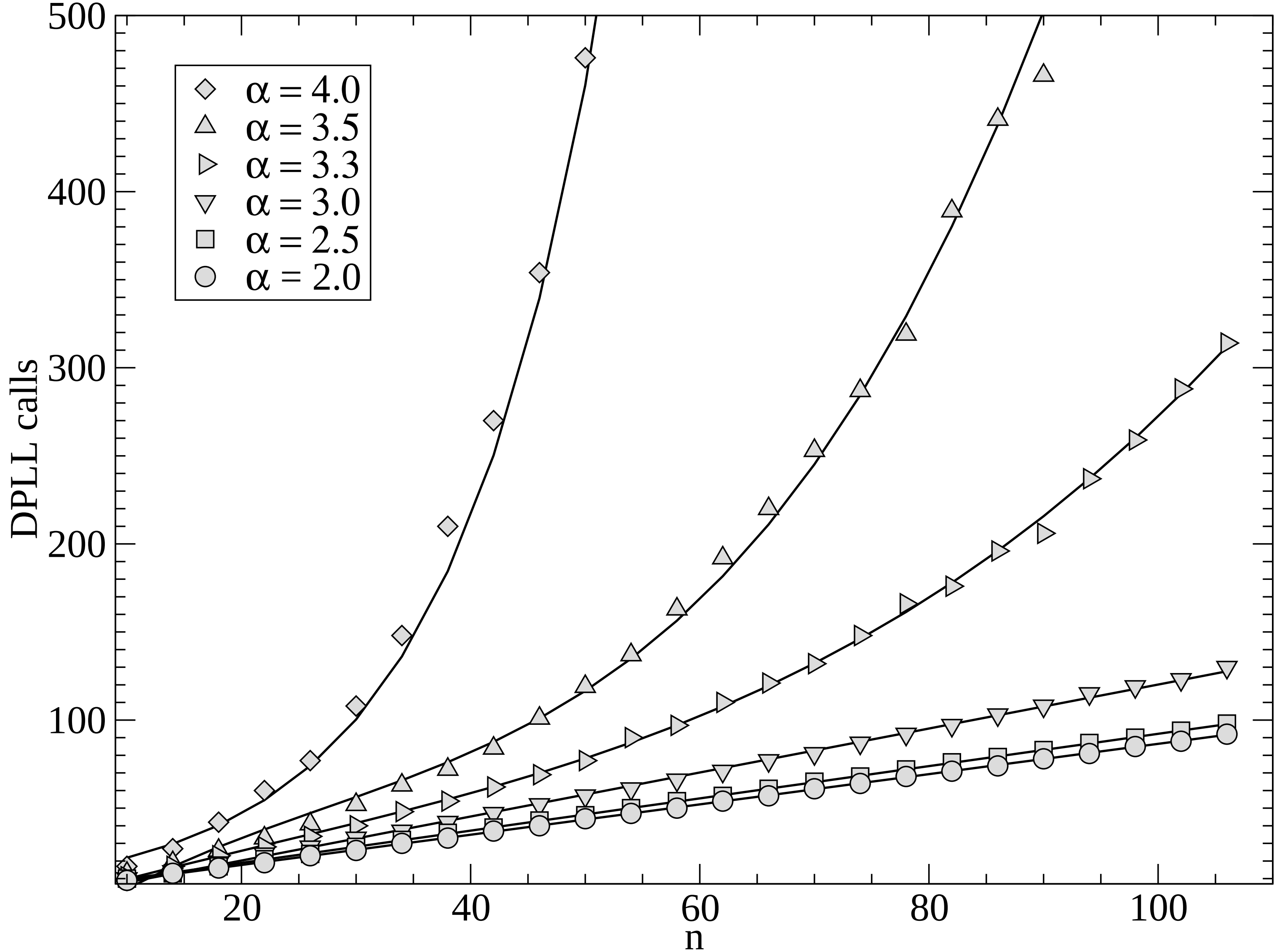
$$\sigma(n) = \Theta(n^{1/\nu})$$

k	α_c	ν
3	4.21 ± 0.05	1.5 ± 0.1
4	9.80 ± 0.05	1.25 ± 0.1
5	20.9 ± 0.1	1.10 ± 0.05
6	43.2 ± 0.2	1.05 ± 0.05

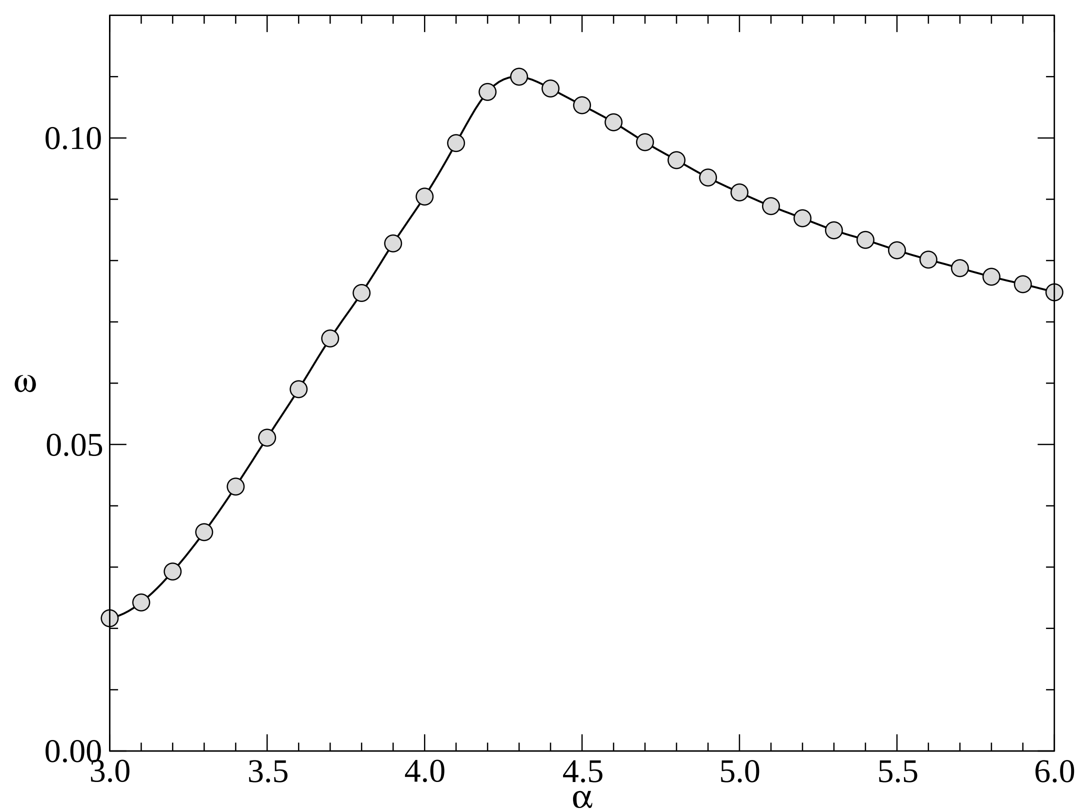
Algorithms on the Edge



Algorithms on the Edge



Algorithms on the Edge



$$\omega = \lim_{n \to \infty} \frac{1}{n} \mathbb{E}[\log(\text{\# DPLL calls})]$$

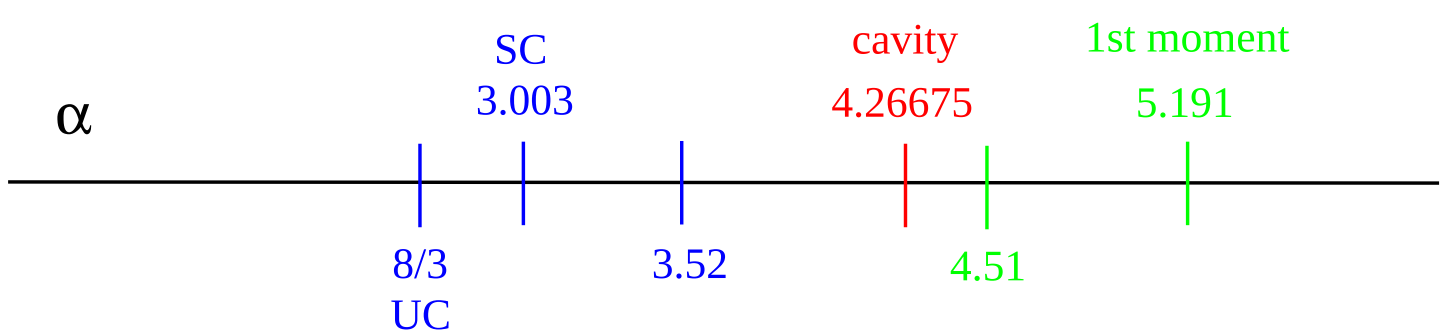
Rigorous Results

Theorem (Friedgut, 1999):

There is a function $\alpha_c(n)$ such that, for any $\varepsilon > 0$,

$$\lim_{n\to\infty} \text{Prob}\Big(F_3(n, m = \alpha n)\text{satisfiable}\Big) = \begin{cases} 1 & \alpha < (1-\varepsilon)\alpha_c(n) \\ 0 & \alpha > (1+\varepsilon)\alpha_c(n) \end{cases}$$

lower and upper Bounds:



Unit Clause Heuristics

UC

begin

while F *contains unsatisfied clauses* **do**

if F *contains a unit clause* $c = (x)$ *or* $c = (\overline{x})$ **then**

Set x to the value that satisfies c ;

else

Choose x uniformly from among the unset variables ;

Set x to a random value ;

Remove or shorten the clauses containing x ;

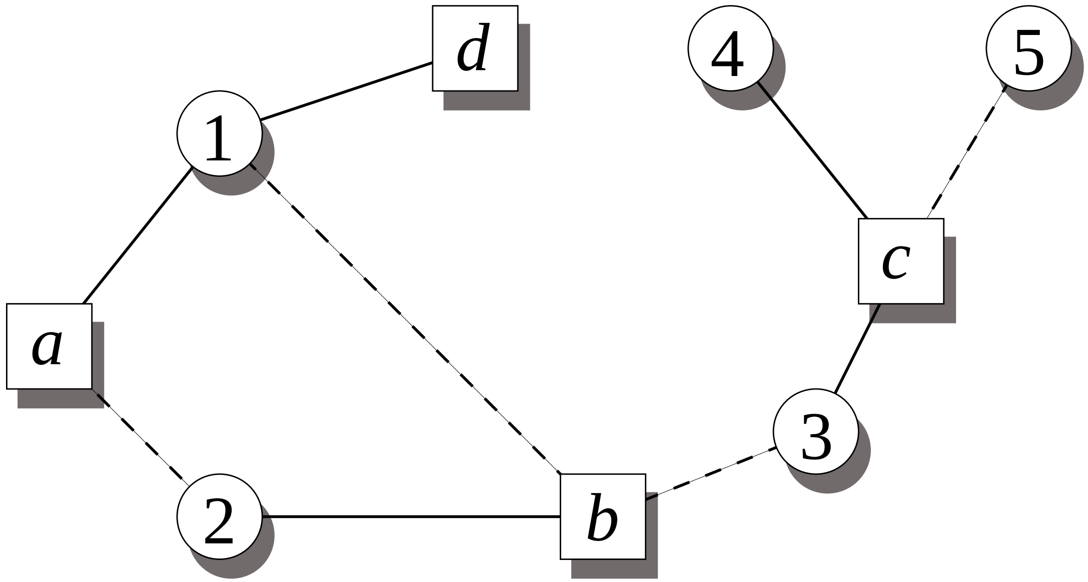
if F *contains an empty clause* **then return** *don't know* ;

end

return *SAT*;

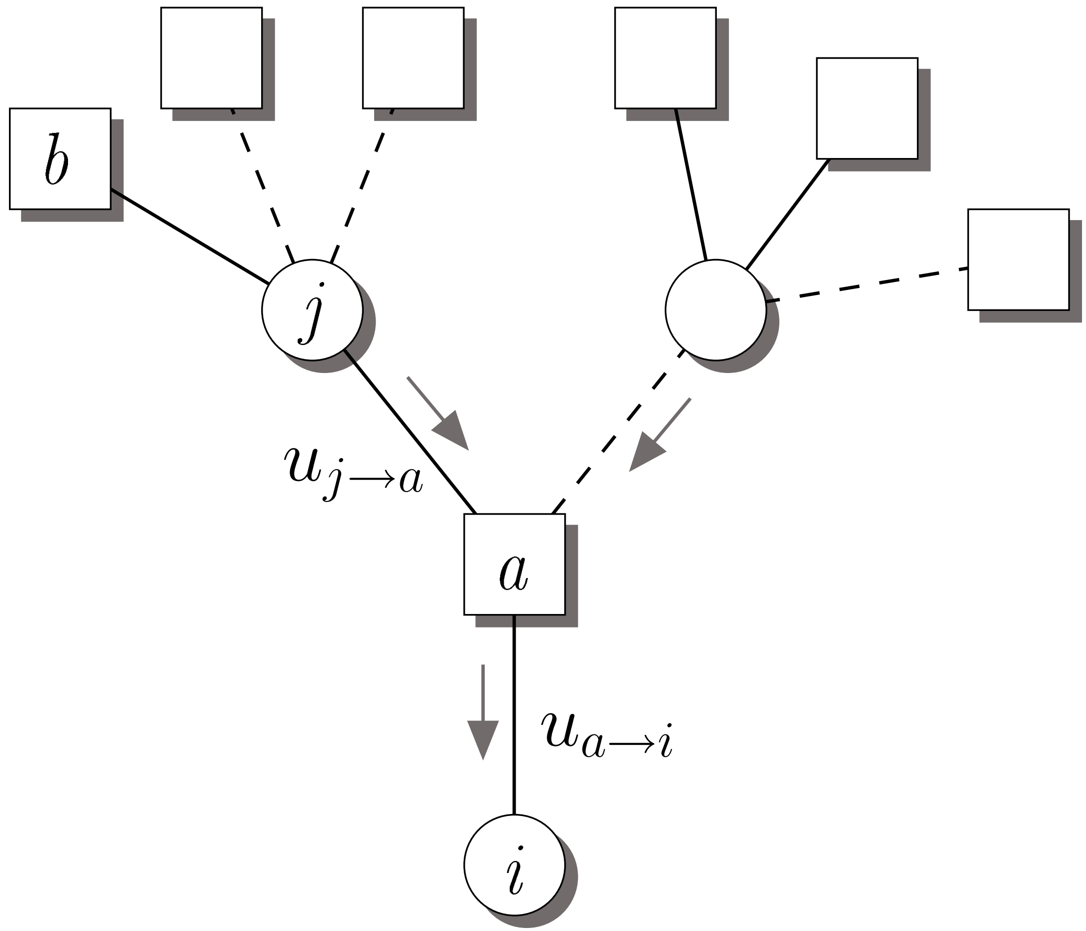
end

Factor Graph

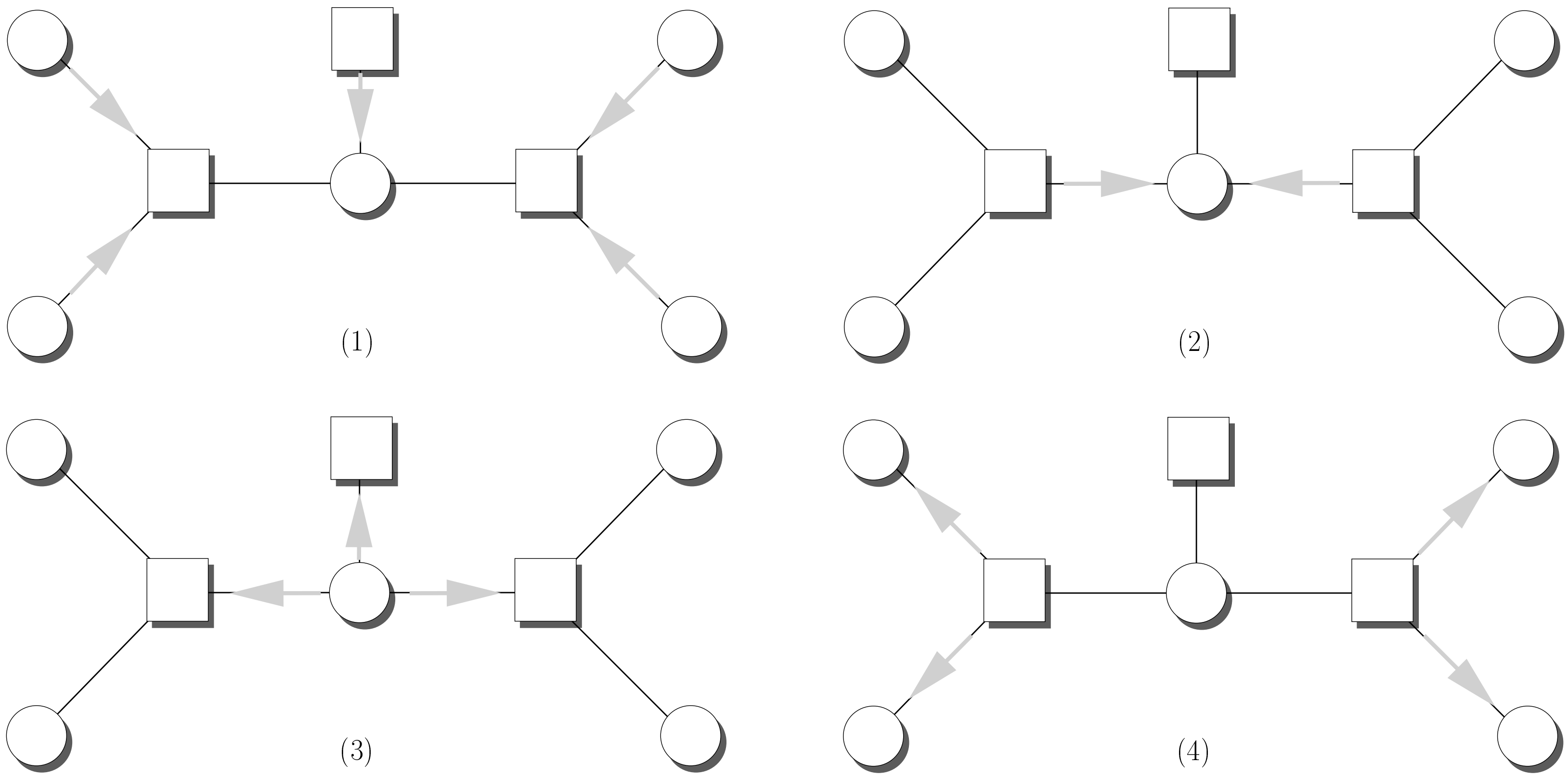


$$\underbrace{(x_1 \vee \overline{x}_2)}_{a} \wedge \underbrace{(\overline{x}_1 \vee x_2 \vee \overline{x}_3)}_{b} \wedge \underbrace{(x_3 \vee x_4 \vee \overline{x}_5)}_{c} \wedge \underbrace{(x_1)}_{d}$$

Warning Propagation



Warning Propagation



Belief Propagation

- $\mu_{a\to i}(x_i)$: prob. a is sat, given i has value x_i
- $\mu_{i\to a}(x_i)$: prob. i takes value x_i when a is absent

Marginals:

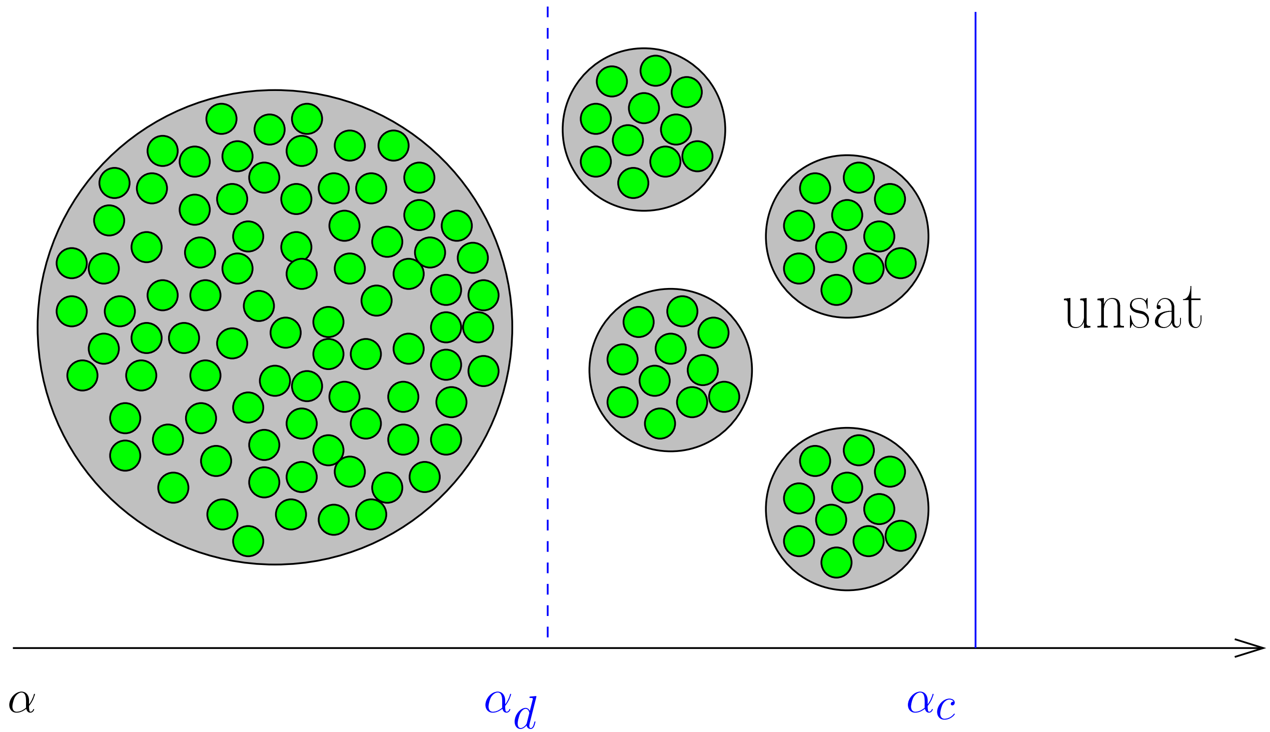
$$p_i(x_i) = c_i \prod_{b\in V(i)} \mu_{b\to i}(x_i) \qquad p_a(X_a) = c_a f_a(X_a) \prod_{i\in V(a)} \mu_{i\to a}(x_i)$$

BP-equations:

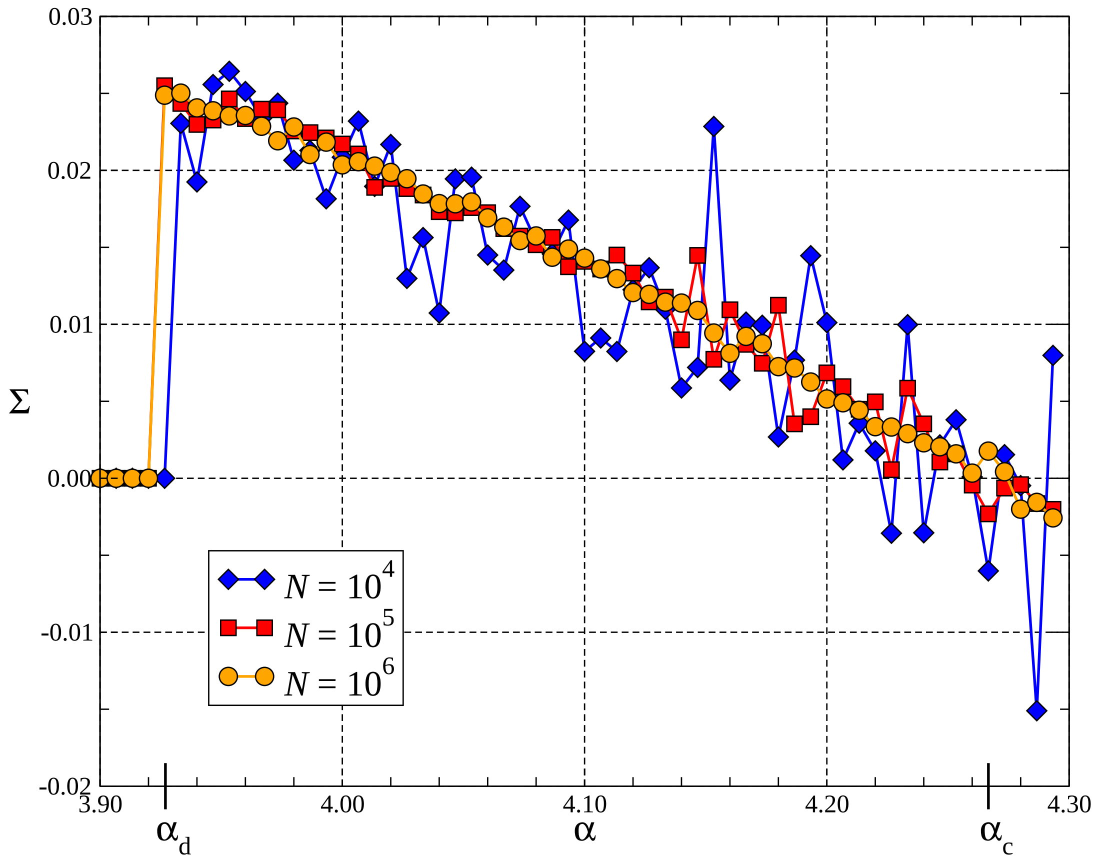
$$\mu_{i\to a}(x_i) = C_{i\to a} \prod_{b\in V(i)\setminus a} \mu_{b\to i}(x_i)$$

$$\mu_{a\to i}(x_i) = \sum_{x_j(j\neq i)} f_a(X_a) \prod_{j\in V(a)\setminus i} \mu_{j\to a}(x_j)$$

Clustering



Complexity



$$\alpha_c(3) = 4.26675 \pm 0.00015$$

SAT-UNSAT Threshold

$$2^{-K}\alpha_c(K) = \ln(2) + \sum_{i=1}^{M} \hat{\alpha}_i 2^{-iK} + o(2^{-MK})$$

$$\hat{\alpha}_1 = -\frac{1+\ln(2)}{2}$$

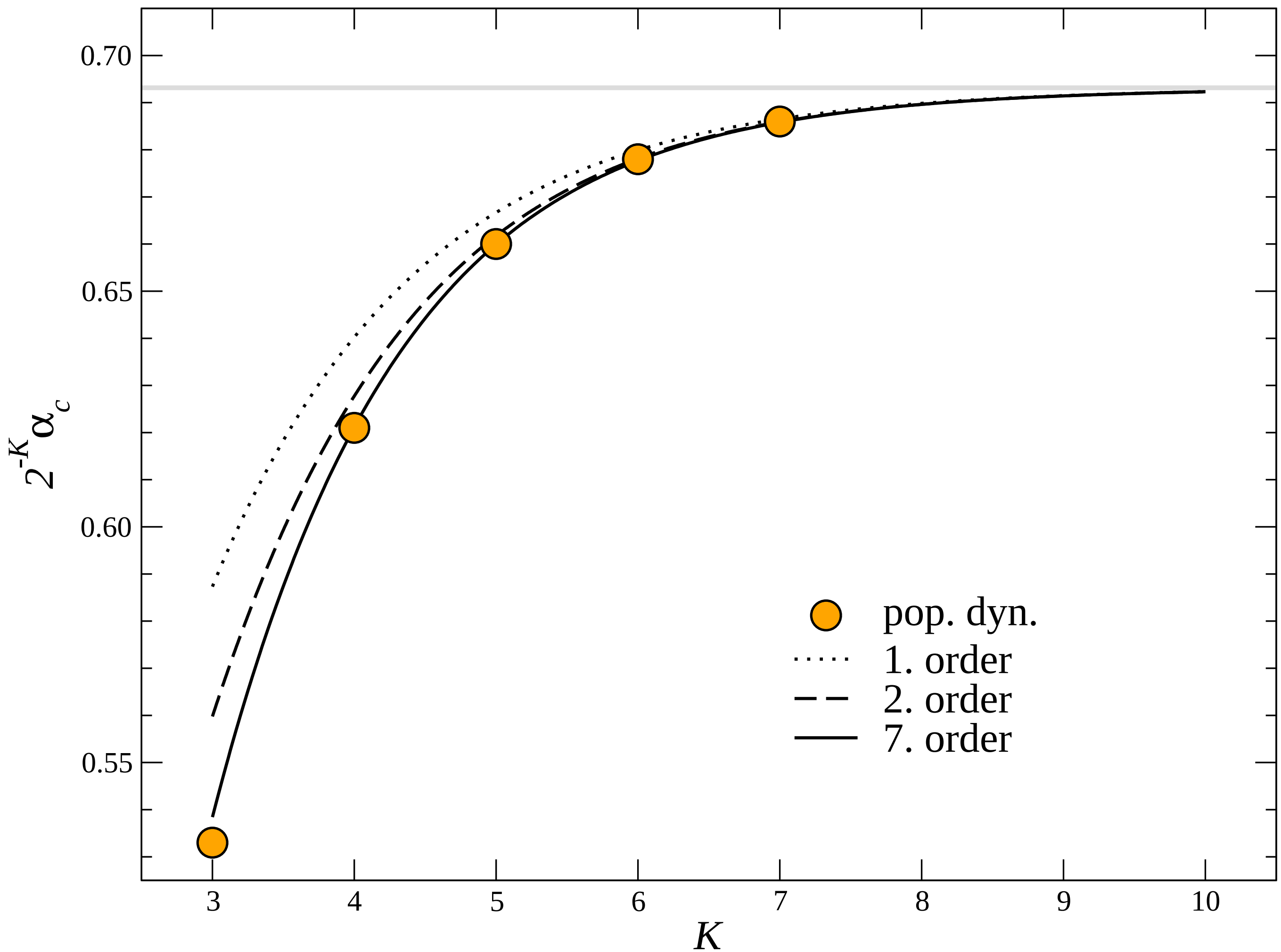
$$\hat{\alpha}_2 = \frac{1}{8} - \frac{\ln(2)}{12} + \frac{3\ln(2)-2}{8}K - \frac{\ln(2)+2\ln^2(2)}{8}K^2$$

$\hat{\alpha}_1, \ldots, \hat{\alpha}_7$ known.

Rigorous Bounds:

$$\begin{aligned} 2^{-K}\alpha_{\mathrm{LB}}(K) &\simeq \ln(2) - 2^{-K}\left(\frac{K+1}{2}\ln(2) + 1 + o(1)\right) + \mathcal{O}(2^{-2K}) \\ 2^{-K}\alpha_{\mathrm{UB}}(K) &\simeq \ln(2) - 2^{-K}\frac{1+\ln(2)}{2} + \mathcal{O}(2^{-2K}) \end{aligned}$$

Series Expansion



Further Reading

- S.M., Computational Complexity for Physicists, *Computing in Science and Engineering* vol.4, no.3, May/June 2002, pp. 31-47
- `http://www.uni-magdeburg.de/mertens`