

ADIABATIC

COMPUTATION:

UNIVERSALITY

&

TOOLS

DORIT AHARONOV (HEBREW U)

JOINT WORK WITH

AMNON TA-SHMA (TEL-AVIV U)

PAPER ON QUANT-PH

QUANTUM ALGORITHMS

DISCRETE LOG

FACTORING

PELL'S EQUATION

QUADRATIC RESIDUOSITY



HSP

SHIFTED LEGENDRE SYMBOL

GI ?
LATTICES ?



ADIABATIC COMPUTATION [FARHI et al 2001]

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

es: $|\psi(t)\rangle = e^{-iEt} |\psi_0\rangle$
(UNITARY)



ADIABATIC THEOREM (KATO '81)

$$|\psi_0\rangle = |GS(0)\rangle \longrightarrow |\psi_T\rangle = |GS(T)\rangle$$

DELAY SCHEDULE.

$$i\hbar \frac{d}{ds} |\psi(s)\rangle = \tau(s) H(s) |\psi(s)\rangle$$

$s \in [0, 1]$

ADIABATIC CONDITION:

$$\tau(s) \gg \left| \frac{d}{ds} H(s) \right| / \Delta^2(H(s))$$

MOST PAPERS: STRAIGHT LINE

$$H(s) = (1-s)H_0 + sH_1$$

H_0

H_1

BACKGROUND - ADIABATIC

• NUMERICAL RESULTS FOR NPC PROBLEMS

[FARHI, GUTMANN, GOLDSTONE, SEPSEDER, LAPAN, LANDGREEN, PREDA, ... 2000-2001]

• LOWER BOUNDS

[VAN DAM, MOSCA, VAZIRANI 2001]

• GROVER'S SPEED UP ADIABATICALLY

[V. DAM, MOSCA, VAZIRANI 2001
ROLAND, CERF 2001]

• ADIABATIC VS. SIMULATED ANNEALING

[FARHI, GOLDSTONE, SEPSEDER 2002]

HOW POWERFUL IS ADIABATIC COMPUTATION? WHAT CAN BE DONE?

OUR ADIABATIC RESULTS

1)

ADIABATIC \equiv CIRCUIT MODEL

WHAT PROBLEMS? STATE GENERATION

2)

SZK \longleftrightarrow QSAMPLING

$\sum_i \sqrt{p_i} |c_i\rangle$

WHAT STATES CAN WE GENERATE?

MARKOV CHAINS & APPROX COUNTING

3)

APPROX COUNTING \Rightarrow QSAMPLING

TOOLS:

WHAT HAMILTONIANS?

THE "SPARSE HAMILTONIAN" LEMMA:

- PERFECT MATCHING
- CONVEX BODY

H SPARSE, ROW-COMPUTABLE \Rightarrow SIMULATABLE

HOW TO GUARANTEE LARGE Δ ?

THE "JAGGED ADIABATIC PATH" LEMMA:

ADIABAT ON



$\langle \alpha_i | \alpha_{i+1} \rangle > \frac{1}{\text{poly}(n)}$

ADIABATIC \equiv CIRCUIT MODEL [A. 02]

GIVEN: U_1, \dots, U_T (GATES)
 x_1, \dots, x_n (INPUT STRING)

$|x, 0\rangle \xrightarrow{\text{ADIABAT}} U_T \dots U_1 |x, 0\rangle$

$$H_0 = \Pi |x, 0\rangle^\perp$$

$$H_1 = \Pi U_T \dots U_1 |x, 0\rangle^\perp = U_T \dots U_1 H_0 U_1^\dagger \dots U_T^\dagger$$

LITTLE LEMMA:

$$\Pi |\alpha\rangle^\perp \longrightarrow \Pi |\beta\rangle^\perp$$

$$\Delta_{\min} = |\langle \alpha | \beta \rangle|$$

BUT THIS MIGHT BE 0!

ADIABATIC \equiv CIRCUIT MODEL (CONT'D)

GIVEN: $U_1 \dots U_T$ (GATES)

$x_1 \dots x_n$ (INPUT STRING)

INSTEAD:

$$|x, 0\rangle \longrightarrow |h_x\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^T U_t \dots U_1 |x\rangle \otimes |t\rangle$$

$$H_0 = (I - |xx\rangle\langle x|) \otimes I + I \otimes (I - |0x0\rangle\langle 0x0|)$$

$$H_1 = (I - |xx\rangle\langle x|) \otimes |0x0\rangle\langle 0x0| + H_{\text{prop}}$$

$$H_{\text{prop}} = \frac{1}{2} \sum_t \left[I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^\dagger \otimes |t-1\rangle\langle t| \right]$$

LITTLE LEMMA 2:

NON NEGLIGIBLE $\Delta \Rightarrow$ PROJECTION

BUT WHY IS $\Delta(H_{\text{prop}})$ NON NEGLIGIBLE?

ADIABATIC \equiv CIRCUIT MODEL (CONT)

$$H_{\text{prop}} = \frac{1}{2} \sum_t \left[I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^\dagger \otimes |t-1\rangle\langle t| \right]$$

$$H'_{\text{prop}} = I \otimes \begin{pmatrix} 1 & -\frac{1}{2} & & & 0 \\ -\frac{1}{2} & 1 & & & \\ & & \ddots & & \\ & & & 1 & -\frac{1}{2} \\ 0 & & & -\frac{1}{2} & 1 \end{pmatrix} = I \otimes (I - M)$$

M IS MARKOV CHAIN MATRIX

FOR RANDOM WALK ON $[0, \dots, T]$



RANDOM WALKS MIX TO LIMITING DIST.

THM: MIXING TIME $\sim \frac{1}{1-\lambda_2}$
[ALON]

MIX IN TIME $O(T^2) \rightarrow \Delta > \frac{1}{T^2}$

ADIABATIC \equiv CIRCUIT MODEL (CONT'D)

LITTLE LEMMA 1: (TWO PROJECTIONS)

$$H(s) = (1-s)(I - K\alpha\alpha^\dagger) + s(I - V\beta\beta^\dagger)$$

$$\rightarrow \Delta(H(s)) \geq |K\alpha|V\beta|$$

LITTLE LEMMA 2: (HAMILTONIAN \rightarrow PROJECTION)

IF H CAN BE SIMULATED,

AND $\Delta(H)$ NON NEGLIGIBLE

\Downarrow

$I - |g\rangle\langle g| = \Pi_{\bar{g}}$ CAN BE SIMULATED

TO FINISH PROOF:

$H_{\text{prop}} \xrightarrow{2} \Pi_{\text{prop}} \xrightarrow{1} \Delta(H_1)$ IS N.N

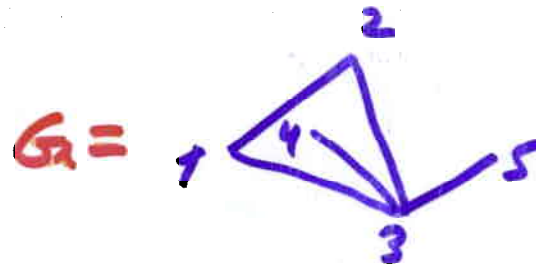
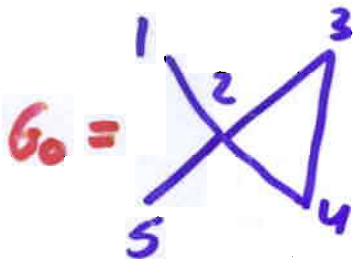
$\Delta(H_{\text{prop}} + s\Pi_{\text{prop}}) \text{ N.N.} \xleftarrow{\Pi_{\text{prop}}} \Pi_{\text{prop}} \xrightarrow{2}$

WHAT
PROBLEMS
TO
ATTACK

ADIABATICALLY ?



GRAPH ISOMORPHISM



$$A_{G_0} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$A_{G_1} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

INPUT: G_0, G_1 on n nodes

OUTPUT: IS THERE $\sigma \in S_n$ s.t. $\sigma(G_0) = G_1$?

REDUCIBLE TO:

INPUT: $|G\rangle$

OUTPUT: $|G\rangle |\alpha_G\rangle$

$$|\alpha_G\rangle = \frac{1}{\sqrt{n!}} \sum_{\sigma \in S_n} |G(\sigma)\rangle$$

SIMPLE ALGORITHM:

$$A_0 \rightarrow |\alpha_0\rangle$$

$$A_1 \rightarrow |\alpha_1\rangle$$

$$\langle \alpha_0 | \alpha_1 \rangle = ?$$

$$\frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \xrightarrow{A} \frac{|0\rangle |\alpha_0\rangle + |1\rangle |\alpha_1\rangle}{\sqrt{2}}$$

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad |0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\rightarrow \frac{(|0\rangle + |1\rangle) |\alpha_0\rangle + (|0\rangle - |1\rangle) |\alpha_1\rangle}{2}$$

$$= |0\rangle \left(\frac{|\alpha_0\rangle + |\alpha_1\rangle}{2} \right)$$

$$+ |1\rangle \left(\frac{|\alpha_0\rangle - |\alpha_1\rangle}{2} \right)$$

$$\text{Pr}(0) = \left| \frac{|\alpha_0\rangle + |\alpha_1\rangle}{2} \right|^2 = \frac{1 + \langle \alpha_0 | \alpha_1 \rangle}{2}$$

SIMPLE ALGORITHM?

HOW TO GENERATE

$$|\alpha_G\rangle = \sum_{G \in S_n} |G(G)\rangle \quad ?$$

CAN SAMPLE A RANDOM $G(G)$!

CAN GENERATE

$$\sum_{G \in S_n} |G\rangle \otimes |G(G)\rangle$$

HOW TO FORGET ?

QUANTUM SAMPLING

INPUT: C (A CIRCUIT)

ON UNIFORMLY DISTRIBUTED

x'

$$C(x') = x \sim \pi(x).$$

WANTED: $|C\rangle = \sum \sqrt{\pi(x)} |x\rangle$



THE QUANTUM SAMPLING
OF THE DISTRIBUTION π .

QUANTUM SAMPLING & SZK

GROUP MEMBERSHIP

DISCRETE LOG

QUADRATIC RESIDUACITY

GRAPH ISOMORPHISM

CLOSEST VECTOR IN A LATTICE

AND

ANY PROBLEM IN SZK

QUANTUM
SAMPLING

A diagram consisting of several orange arrows pointing from the list of problems on the left towards the text 'QUANTUM SAMPLING' on the right. The arrows originate from the right side of each problem name and converge towards the 'QUANTUM SAMPLING' text.

SZK \Rightarrow QSAMPLING

WHAT KIND OF
STATES CAN WE
GENERATE ?

WHAT
DISTRIBUTIONS
?

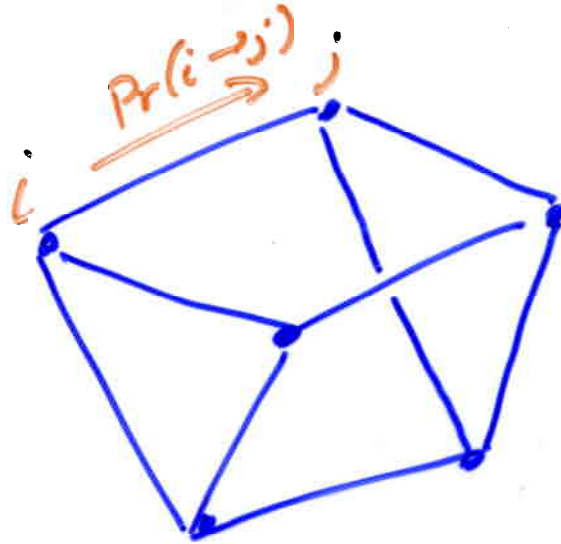


APPROXIMATE COUNTING \Rightarrow Q SAMPLING

CAN EFFICIENTLY APPROXIMATE

- ALL PERFECT MATCHINGS IN A BIPARTITE GRAPH G
- $\sum \sqrt{\pi(a)} |a\rangle$ IF $\pi(a)$ IS LOG CONCAVE AND EASY TO COMPUTE
- ALL GRID POINTS INSIDE A CONVEX BODY IN HIGH DIM
- ALL EXTENSIONS OF A GIVEN PARTIAL ORDER
- SUPER POSITION OVER THE GIBBS DISTRIBUTION FOR VARIOUS STAT. MECH. MODELS (POTTS ISING, ETC...)

MARKOV CHAINS



STATE SPACE = Ω

$$|\Omega| = \text{EXP}(n)$$

M_{ij} = TRANSITION MATRIX

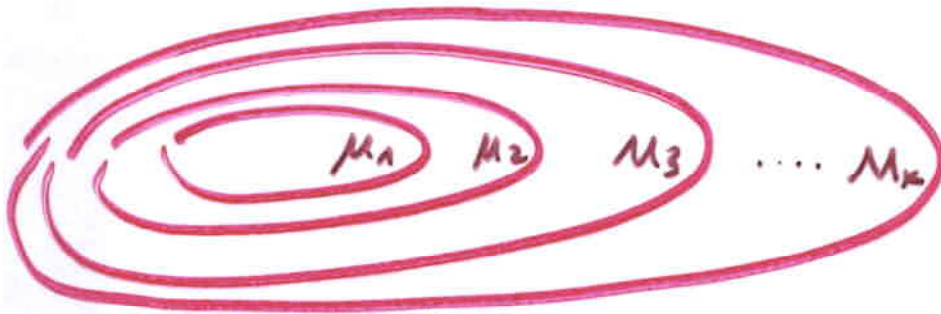
$$P_t = M P_{t-1}$$

π = LIMITING DISTRIBUTION

$$\pi = \lim_{t \rightarrow \infty} M^t P_0 \quad \forall P_0$$

RAPID MIXING IF $\lambda_2 < 1 - \frac{1}{n^c}$
(LARGE SPECTRAL GAP)

APPROXIMATE COUNTING



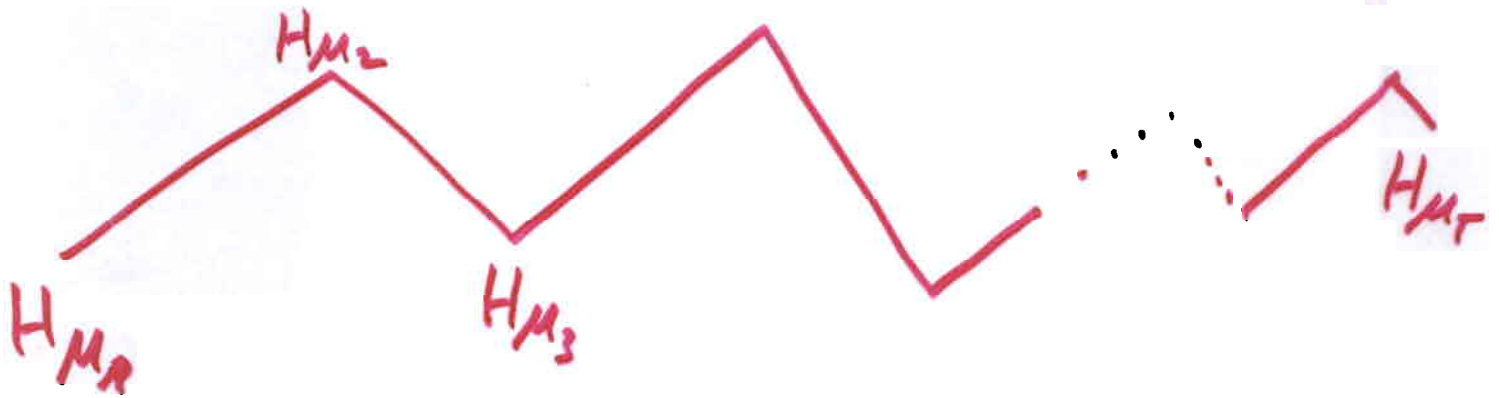
SEQUENCES OF RAPIDLY
MIXING MARKOV CHAINS

THM:

APPROX COUNTING \rightarrow QSAMPLING

MARKOV CHAINS ARE "STRONGLY SAMPLABLE"
(SPARSE, ROW COMPUTIBLE, REVERSIBLE,
& EASY TO CALCULATE $\pi(i)/\pi(j)$)

PROOF OF THEOREM:



WALK ADIABATICALLY ON THE
BROKEN LINE CONNECTING THE H_{μ_i}
IN HAMILTONIAN SPACE

IF 1) Δ_{\min} poly big

2) $\frac{dH}{ds}$ poly big

3) CAN APPLY $e^{iH(s)\Delta t}$ BY A QC

HAMILTONIANS FROM MC'S

HAMILTONIAN : HERMITIAN MATRIX

$$H \longleftrightarrow M$$

$$\pi(i) M_{ij} = \pi(j) M_{ji} \quad \text{REVERSIBLE}$$

$$\begin{pmatrix} \frac{1}{\sqrt{\pi_i}} & 0 \\ 0 & \frac{1}{\sqrt{\pi_j}} \end{pmatrix} M \begin{pmatrix} \sqrt{\pi_i} & 0 \\ 0 & \sqrt{\pi_j} \end{pmatrix}$$

$$H = I - \frac{1}{\sqrt{\pi}} M \sqrt{\pi}$$

$$\lambda \longleftrightarrow 1 - \lambda$$

$$\sum \sqrt{\pi(x)} |x\rangle \longleftrightarrow \pi \text{ LIMITING DIST}$$

GROUND
STATE

THE SPARSE HAMILTONIAN LEMMA

H IS SPARSE, $\forall i$ $H_{ij} \neq 0$ CAN
BE COMPUTED EFFICIENTLY



e^{iHt} CAN BE APPROXIMATED
TO WITHIN POLY ACCURACY
EFFICIENTLY

(IMPLICATIONS TO QWALKS ETC.)

PROOF (OF APPLYING A SPARSE H)

1. WRITE $H = \sum_{b=1}^{\text{poly}} H_b.$

TROTTER: $e^{i(A+B)} \approx (e^{i\frac{A}{r}} e^{i\frac{B}{r}})^r$

$$e^{iH\Delta t} = e^{i \sum_{b=1}^{\text{poly}} H_b \Delta t} \approx \left[\prod_{b=1}^{\text{poly}} e^{i \frac{H_b \Delta t}{r}} \right]^r$$

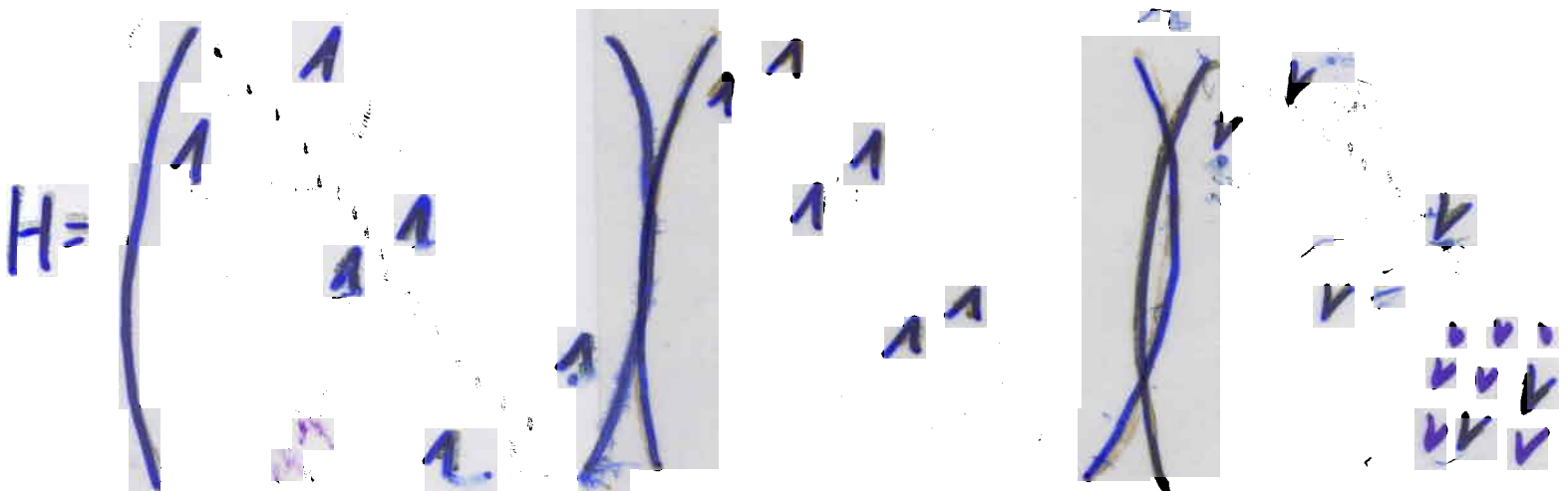
$H = \begin{pmatrix} \text{1} & & & & & & & & \\ & \text{1} & & & & & & & \\ & & \text{1} & & & & & & \\ & & & \text{1} & & & & & \\ & & & & \text{1} & & & & \\ & & & & & \text{1} & & & \\ & & & & & & \text{1} & & \\ & & & & & & & \text{1} & \\ & & & & & & & & \text{1} \end{pmatrix}$

PROOF (OF APPLYING A SPARSE H)

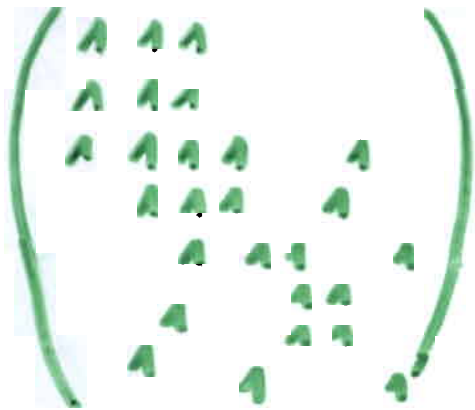
1. WRITE $H = \sum_{b=1}^{\text{poly}} H_b.$

TROTTER: $e^{i(A+B)} \approx (e^{i\frac{A}{r}} e^{i\frac{B}{r}})^r$

$$e^{iH\Delta t} = e^{i \sum_{b=1}^{\text{poly}} H_b \Delta t} \approx \left[\prod_{b=1}^{\text{poly}} e^{i \frac{H_b \Delta t}{r}} \right]^r$$



DECOMPOSING H



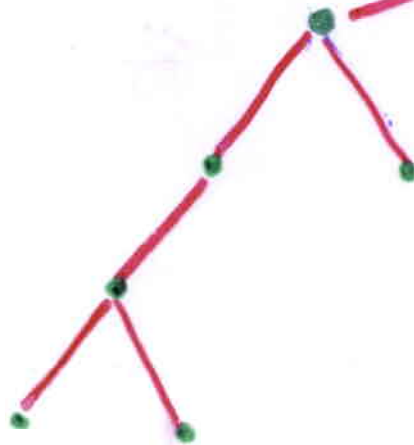
$\text{deg} = d$
 $\# \text{ colors} = d^5$

EACH ELEMENT $H_{r,l}$ PICKS A
 RANDOM COLOR $b \in [1, \dots, d^5]$

$H_1 + H_2 + \dots + H_{d^5} = H$

The equation shows the decomposition of matrix H into a sum of matrices H_1, H_2, \dots, H_{d^5} . Each H_i is shown in large parentheses and contains a sparse pattern of green '1's and blue '0's. A red arrow points from the text 'WHAT IS THE SIZE OF A BLOCK?' to the H_{d^5} matrix.

WHAT IS THE SIZE OF A BLOCK?



BRANCHING PROCESS ; $\Pr(\# \text{ sons} = j) < \frac{1}{C^j}$

LAST DETAIL: HASH FUNCTIONS

PROBLEM: COLORS CANNOT BE
CHOSEN RANDOMLY

INCONSISTENCY, DECOHERENCE, EXP MANY...

SOLUTION: CHOOSE A RANDOM HASH

$$\text{For } \exists X \rightarrow \text{Tr} \left(\sum_{i=1}^{d \cdot 10} C_i X^i \right) \in [1, \dots, 9]$$



CONCLUSIONS & OPEN PROBLEMS

- **ADIABATIC UNIVERSAL**

NEW TOOLS ?

PHYSICISTS METHODS...

LOCAL UNIVERSALITY ?

(FAULT TOLERANCE,

K-COLORABILITY EQMA)

- **IMPORTANCE OF Q SAMPLING**

NEW ALGORITHMS ?

OLD ALGORITHMS ?

- **TOOLS**

OTHER TOOLS ?

PHYSICS,

MARKOV CHAINS: CONDUCTANCE,

LOG SUBLEV,

FLOWS...

