An n-Colouring Problem (Bartels + W 94)

<u>Input</u> : Graph G on n vertices

<u>Output</u> : "Almost" random good n-colouring.

Simple Markov Chain

1) Start with good n-colouring
2) Pick vertex v, colour c at random.
   Colour v with colour c if its a good colouring.
3) Repeat

Simple irreducible <u>symmetric</u> Markov chain which converges to <u>uniform distribution</u> on all n-colourings of G.

<u>Question</u> Does it converge quickly?

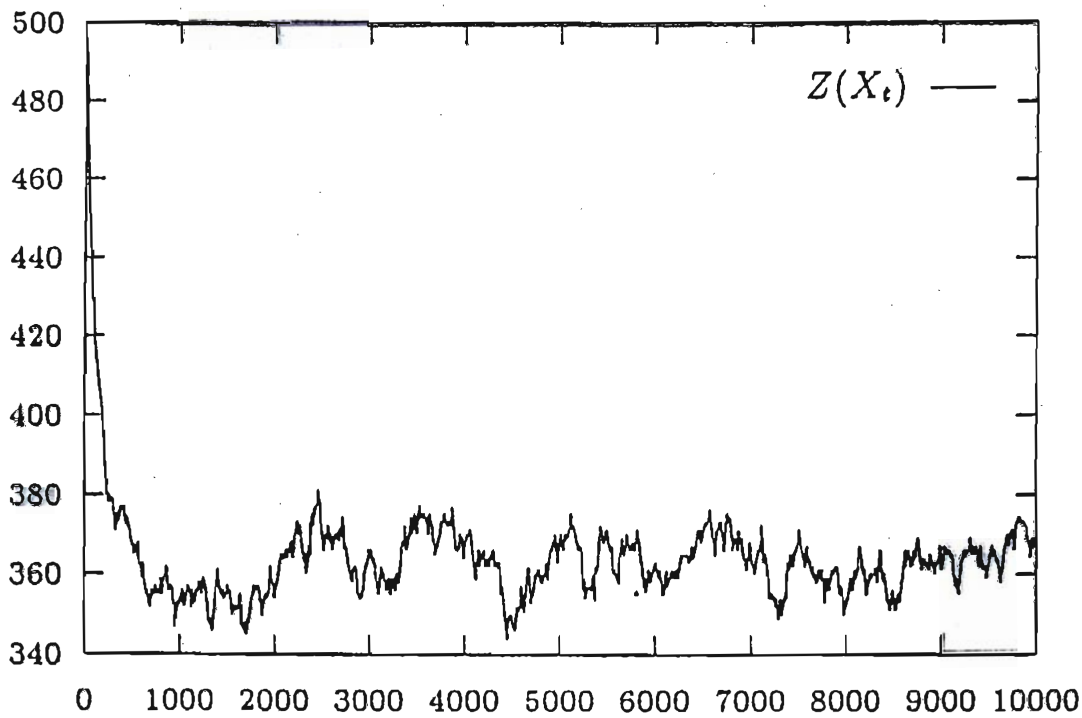


Fig. 1. A typical simulation for a random graph $G(500, 0.5)$. Number of colours versus time-steps.

$\mu(G)$ = Expected number of colours used in a good n-colouring

$$= E\left(\sum_{1}^{n} X_i\right) = n\,E(X_1)$$

where $X_i = \begin{cases} 1 & \text{if colour } i \text{ is used} \\ 0 & \text{otherwise} \end{cases}$

$$= n\left(1 - \frac{P(G;n-1)}{P(G;n)}\right)$$

Conjectures

(1) $\mu(G_n) \geq \mu(O_n)$ where O_n is empty graph

(2) $\mu(G_n) \geq \mu(G_n \setminus e)$ for some e

(3) $\mu(G_n) \geq \mu(G_n \setminus e)$ for all e

Seymour (1998) – $\mu(G_n)/n \geq 0.6321167883$

but $\mu(O_n)/n \to 0.632120558$

Dong (2000) Proves (1)

Complexity of Counting

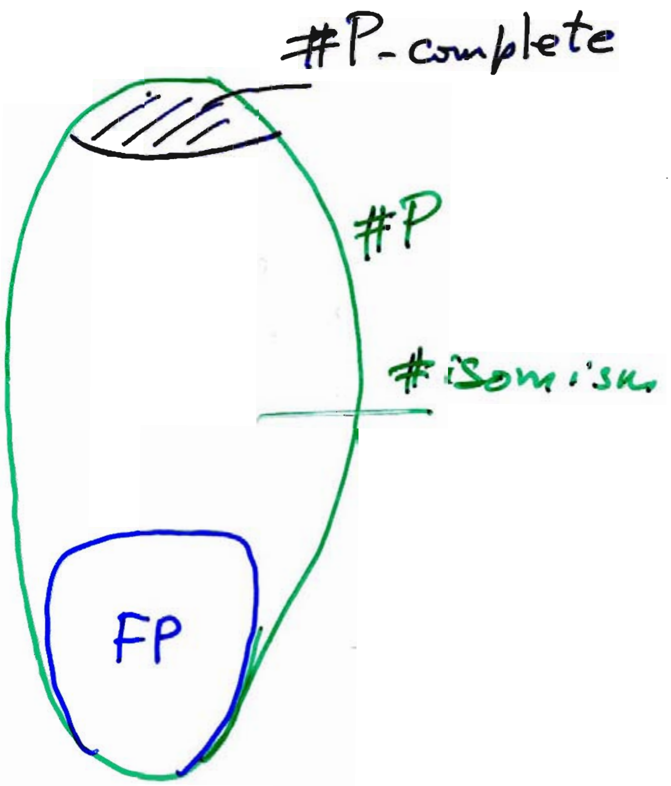
Valiant (1980)

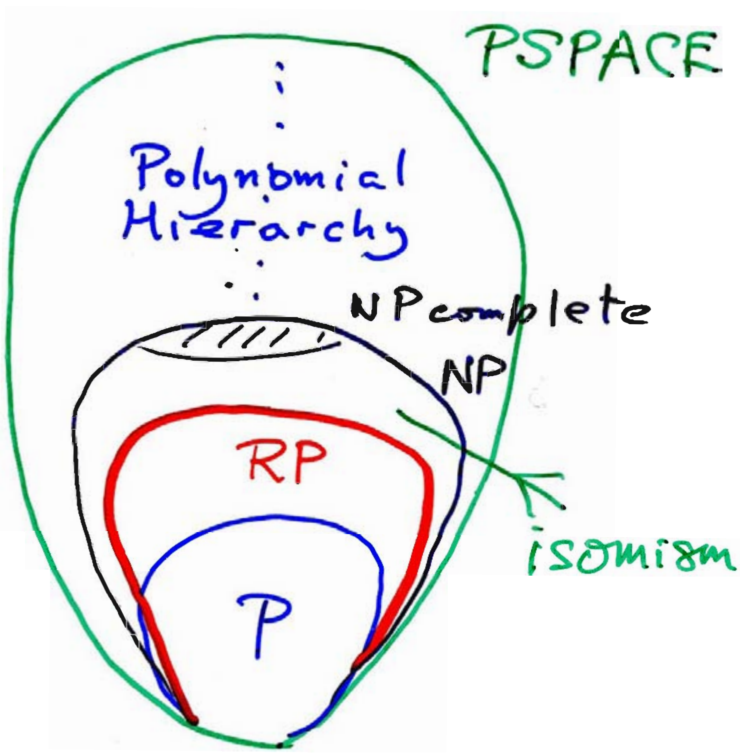
#P = { functions f : f counts objects which can be recognised in polynomial time }

Examples Number of cliques, Hamilton cycles, trees, spanning trees, isomorphisms, forests of a graph.

Not known to be in #P

Number of Hamiltonian subgraphs of a graph.





Observations (not facts)

1) Very few counting functions in FP.

2) If counting fn is in FP it is an "evaluation" of a determinant.

3) Most natural counting functions are #P-complete

4) # ISOMORPHISMS / AUTOMORPHISMS are special.

Randomised Approximation

A randomised approximation scheme for a counting problem $f : \Sigma^* \to \mathbb{N}$ is a randomised algorithm that takes an instance $x \in \Sigma^*$ and an error tolerance $\epsilon > 0$ and outputs a number (random variable) N such that

$$\Pr\left\{ 1-\epsilon \leq \frac{N}{f(x)} \leq 1+\epsilon \right\} \geq \frac{3}{4}.$$

Note: $3/4$ could be replaced by any number in $(\frac{1}{2}, 1)$.

It is a fully polynomial randomised approximation scheme (FPRAS) if its running time $\leq$ poly(n, ϵ^{-1}).
(n = size of instance x)

Impossible to Approximate

Claim: Unless NP = RP there is no fpras for counting k-colourings in a graph for $k \geq 3$.

Proof: Existence of fpras would give p-time algorithm for deciding k-colourability which is NP complete.

Note: Can replace k-colourings by anything which has an NP-complete decision problem.

SAMPLE Proposition

If $NP \neq RP$ there is no fpras for number of cycles in a graph.

Proof idea:

Given graph G replace each edge by

to get graph G_k.

For k sufficiently large, fpras for number of cycles in G_k will show whether or not G has a Hamilton cycle.

Generating / Sampling at Random

An <u>almost uniform sampler</u> (AUS) of a space Ω is a randomised algorithm which produces a random variable Z s.t. the <u>variation distance</u> between the uniform dist^n on Ω and the distribution of Z is less than a prescribed δ.

It is <u>fully polynomial</u> giving an FPAUS if the running time of the algorithm is bounded by

$$\mathrm{poly}(n, \log(1/\delta)).$$

Fundamental Theorem

(Jerrum Valiant Vazirani 1986)

Provided we are dealing with self reducible problem there exists an FPRAS iff there exists an FPAUS

Note: "Most" natural problems seem to be self reducible.

Definition: Markov chain is rapid mixing if its mixing time

$$\tau(\epsilon) = \text{poly}\left(n, \log\left(\frac{1}{\epsilon}\right)\right)$$

Methods of Proving Rapid Mixing

1. Second eigenvalue (≡ spectral gap).

2. Conductance

3. Canonical paths

4. Geometric – such as embed into approximating a volume

5. Coupling.

Coupling

Given a MC Z_t, a coupling is a pair of chains (X_t, Y_t) s.t.

(i) marginally X_t and Y_t are copies of Z_t

(ii) once $X_t = Y_t$ then $X_s = Y_s$ $\forall s > t$.

More precisely (i) can be stated:

(X_t, Y_t) has transition probabilities

$$\Pr\{X_1 = x' \mid X_0 = x, Y_0 = y\} = \Pr(Z_1 = x' \mid Z_0 = x)$$

$$\Pr\{Y_1 = y' \mid X_0 = x, Y_0 = y\} = \Pr\{Z_1 = y' \mid Z_0 = y\}$$

The Coupling Lemma

If T is such that regardless of initial states x_0, y_0

$$P\{X_T \neq Y_T \mid X_0 = x_0, Y_0 = y_0\} \leq \epsilon$$

then the mixing time of the MC satisfies

$$\tau(\epsilon) \leq T.$$

Alternative form

If T^{ij} is the coupling time from initial state (i,j) then

$$\tau\left(\frac{1}{2e}\right) \leq 2e \max_{i,j} E(T^{ij}).$$

Theorem (Jerrum 95)

For connected graph G with max degree Δ and $k \geq 2\Delta + 1$ there exists an fpras for counting k-colourings with running time

$$O^*(n m^2 \epsilon^{-2})$$

on a graph with n vertices + m edges.

Proof method

Use coupling to design an FPAUS via a Markov chain Z_t on k-colourings having mixing time

$$\tau(\epsilon) \leq \frac{k - \Delta}{k - 2\Delta} n \ln\left(\frac{n}{e}\right).$$

Proof Outline

Start with 2 proper k-colourings X_0, Y_0 — Note possible by Brooks Th^m.

At time t:

Choose vertex v colour c uar.

Compute permutation σ on colour set by (complicated) algorithm CHOOSE

Recolour v in X_t with c to get X_t'

" v in Y_t with $\sigma(c)$ " Y_t'

If X_t' is proper colouring $X_{t+1} = X_t'$

" Y_t' " " " $Y_{t+1} = Y_t'$

Else $X_{t+1} = X_t$, $Y_{t+1} = Y_t$ resp.

Now show that if D_t denotes number of vertices where X_t, Y_t differ

$$\Pr\{|D_t| > 0\} \leq n e^{-t(k-2\Delta)}$$

giving

$$\Pr\{D_t \neq 0\} \leq \epsilon$$

provided

$$t \geq a^{-1} \ln(n\epsilon^{-1})$$

where $\quad a = \dfrac{k-2\Delta}{(k-\Delta)n}.$

$\Rightarrow$ Mixing time

$$T(\epsilon) \leq \frac{(k-\Delta)}{(k-2\Delta)} n \ln\left(\frac{n}{\epsilon}\right)$$

by Coupling Lemma.

$\square$

Illustrative Proposition (Jerrum 1998)

Suppose we have AUS for k-colourings ($k > \Delta$) with running time $T(n, \delta)$. Then there exists RAS for number of k-colourings with running time

$$O\left(\frac{m^2}{\epsilon^2} T\left(n, \epsilon/6m\right)\right)$$

on a graph with n vertices and m edges.

[δ, ϵ are respective tolerance bounds]

Proof Outline

Let $G = G_m > G_{m-1} > \cdots > G_0 = (V, \emptyset)$ where G_i is got from G_{i+1} by removing an edge.

So number of k-colourings $|\Omega(G)|$

$$= \frac{|\Omega(G_m)|}{|\Omega(G_{m-1})|} \cdot \frac{|\Omega(G_{m-1})|}{|\Omega(G_{m-2})|} \cdots |\Omega(G_0)|$$

$$|\Omega(G_0)| = k^n$$

So need to estimate

$$\rho_i = |\Omega(G_i)| \big/ |\Omega(G_{i-1})|$$

Combinatorial argument gives

$$\tfrac{1}{2} \leq \rho_i \leq 1$$

Then set

$$\delta = \epsilon / 6m$$

Each ρ_i needs $\frac{75m}{\epsilon^2}$

samples from the AUS

There are m such ρ_i

and this gives required running time.

$\square$

Coupling on a Metric Space

Let d be arbitrary integer valued metric on Ω.

Let $0 < \rho < 1$.

We say pair of states $(x,y) \in \Omega^2$ is ρ-decreasing if there exists a coupling s.t.

$$E\left(d(X_1, Y_1) \mid X_0 = x, Y_0 = y \right) \le \rho\, d(x,y).$$

Coupling Theorem (another version)

If every $(x,y) \in \Omega^2$ is ρ-decreasing then mixing time

$$\tau(1/4) \le \frac{2 \log d_{max}}{1-\rho}$$

where $d_{max} = \max d(x,y)$, $x, y \in \Omega$.

Path Coupling (Bubley-Dyer)

Regard Ω as the set of vertices of a graph and let $S \subseteq \Omega \times \Omega$ be a set of 'edges' such that (Ω, S) is a connected graph.

Define metric d on Ω by

$d(x,y)$ = shortest distance in graph (Ω, S) between x, y.

Path Coupling Lemma

If every $(x,y) \in S$ is ρ-decreasing then

$$\tau(1/4) \leq \frac{2}{1-\rho} \log d_{max}$$

Theorem Let Δ = max degree of G and $k > 3\Delta$. Then mixing time

$$\tau(1/4) \leq 2nk\log(n)$$

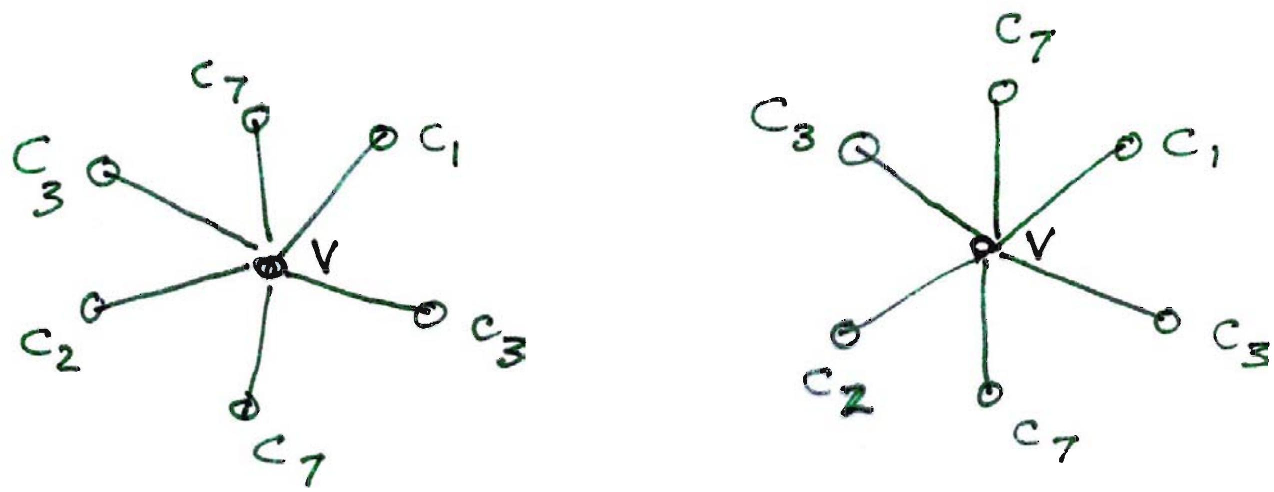
This and next proof are Frieze + Vigoda (2007)

Proof Let Ω = space of all k-colourings

The distance $d(X, Y)$ between two colourings is the number of vertices at which they differ.

Coupling is the identity coupling where a vertex z and colour c are picked at random and both chains try to update z to colour c.

Suppose X_t and Y_t differ only at one vertex v.



$X_t(v) = c_X$ $\qquad$ $Y_t(v) = c_Y$

Update fails in X_t but succeeds in Y_t iff z is neighbour of v and $c = c_X$

Similarly fails in Y_t but succeeds in X_t iff $z \in \partial(v)$ and $c = c_Y$

So $\Pr\{D_{t+1} = D_t + 1\} \leq \dfrac{2\Delta}{kn}$

How do we decrease distance?

Pick $z = v$ and c one of 'good' colours.

So $\Pr\{D_{t+1} = D_t - 1\} \geq \dfrac{1}{n} \dfrac{k-\Delta}{n}$

Hence

$$E\left[d(X_{t+1}, Y_{t+1}) - d(X_t, Y_t) \mid X_t, Y_t\right]$$

$$\leq \frac{1}{kn}\left(2\Delta - (k-\Delta)\right) \leq -\frac{1}{kn}$$

for $k \geq 3\Delta + 1$.

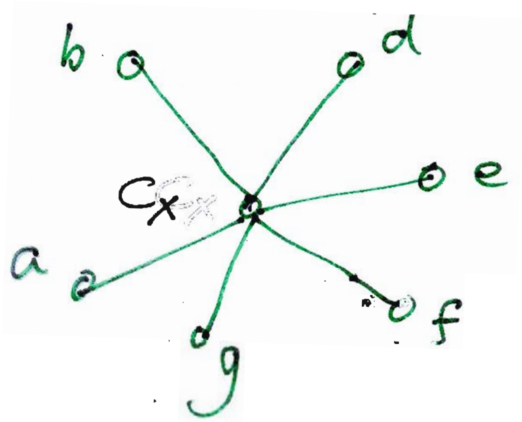
Path coupling lemma gives result since $d_{max} = n$ $\square$

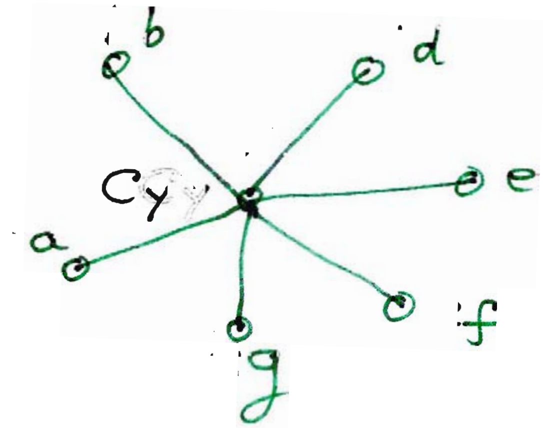
Extend to Prove Jerrum's $2k+1$ result.

Modify coupling

If X_t tries to recolour neighbour w of v to c_X (c_Y)
then Y_t tries to recolour w to c_Y (c_X)

Otherwise do same in both chains.





Only update which can increase distance is if z is neighbour of v and c is c_Y.

So $\Pr\{D \to D+1\} \leq \frac{1}{k} \frac{\Delta}{n}$

$$\Pr\{D \to D-1\} \geq \frac{k-\Delta}{kn}$$

$$\therefore E\big(d(X_{t+1}, Y_{t+1}) - d(X_t, Y_t) \mid X_t, Y_t\big)$$

$$\leq \frac{1}{kn}\big(\Delta - (k-\Delta)\big)$$

$$\leq -\frac{1}{kn} \quad \text{provided } k \geq 2\Delta+1.$$

$\square$.

Theorem (Vigoda 2000) There exists fpras for k-colourings for $k \geq 11\Delta/6$

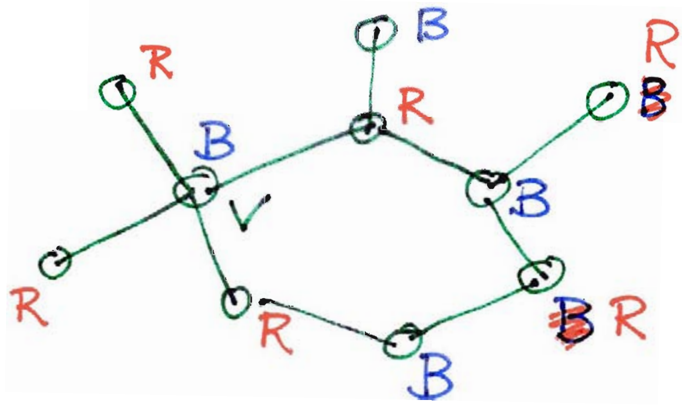
Idea MC on set of all proper k-colourings

Move = flip of an alternating cluster

Given a state = k-colouring σ

Pick vertex v colour c at random

This specifies an alternating cluster



c = RED

$\sigma(v)$ = BLUE

Note All 'boundary' vertices are neither Red nor BLUE

Properties of chain

1) aperiodic 2) symmetric

3) irreducible provided $k \geq \Delta + 2$ and $p_1 > 0$

Key parameters $\{p_j\}$

Here p_j/j is probability of flipping a cluster size j

Choosing

$$p_1 = 1, \quad p_2 = \frac{13}{42}, \quad p_3 = \frac{1}{6}$$

$$p_4 = \frac{2}{21}, \quad p_5 = \frac{1}{21}, \quad p_6 = \frac{1}{84}$$

$$p_j = 0 \quad j > 6$$

gives Vigoda's theorem!

Open Problems

Can you generate (almost) uniformly at random in polynomial time (or show very unlikely)

1) 4 colouring of a planar graph

Note: This is not a self-reducible situation.

2) A planar (or any nontrivial adjective) subgraph of a graph.

3) A tree or forest of given size in a graph.

4) A set of columns of a matrix over the binary field which are linearly independent.