Alcom-FT Technical Report Series
ALCOMFT-TR-03-181

How to certify in deterministic polynomial time the high chromatic number of instances of sparse random graphs

Sotiris Nikoletseas* Paul Spirakis*

Abstract

In this work we show how to certify in deterministic polynomial time that an instance G of the random graph $G_{n,p}$ with $p = \frac{c(n)}{n}$ (where $c(n) << n^\delta, \forall\delta > 0$ but $c(n) \to +\infty$ as $n \to +\infty$) has a high vertex chromatic number.

Our certifier is based on the following fact that we show here: Let the eigenvalues of the adjacency matrix A of G be $\lambda_1 = \lambda_{\max} \geq \lambda_2 \geq \cdots \geq \lambda_n = \lambda_{\min}$. Let $\lambda = \max_{i=2,\ldots,n} |\lambda_i|$ and $\nu = \frac{\lambda_1}{\lambda}$ be the *eigenvalue gap* of G. We show that $\nu \to +\infty$ almost surely in such graphs.

1 Introduction

Let $G_{n,p}$ be the class of random graphs of n vertices where each edge occurs independently with probability p. We concentrate here on *two classes of sparse random graphs*. Let the subclass C of $G_{n,p}$ for which $p = \frac{c(n)}{n}$ and $c(n)$ satisfies (1) $c(n) = o(\log n)$ and (2) $c(n) \to +\infty$ as $n \to +\infty$. Let also C_1 the class of $G_{n,p}$ with $c(n) = n^\delta$ for any fixed $\delta > 0$.

For such graphs it is well known (see e.g. [5], p. 274) that the vertex chromatic number of $G_{n,p}$ almost surely[1] satisfies

$$(1 + o(1))\frac{c(n)}{2\log c(n)} \leq \chi(G_{n,p}) \leq (1 + o(1))\frac{c(n)}{\log c(n)}$$

i.e. $\chi(G_{n,p}) \to +\infty$ as $n \to +\infty$.

However, in applications like cryptography, we would like to know *with certainty* for a *given* instance G of $G_{n,p}$ that e.g. $\chi(G) > 3$ (or e.g. $\chi(G) > 50$).

Let S be a *deterministic polynomial time* algorithm that when given an instance $G(V, E)$ (with $n = |V|$ sufficiently large) of the class C or the class C_1 and a fixed number $\xi > 0$ it (a) either certifies that $\chi(G) > \xi$ or (b) does not provide such an information. We want case (a) above to succeed almost surely i.e. for almost all instances G in C, or in C_1.

Definition 1 We call such an algorithm S a proper *verifier* for the high chromatic number of the class C (or for the class C_1).

The existence of such verifiers is extremely crucial when e.g. we base the success of an application (e.g. the strength of a cryptographic system) to the property that the instance G

*Computer Technology Institute and Department of Computer Engineering & Informatics, University of Patras, Greece. E-mails: `nikole@cti.gr, spirakis@cti.gr`.

[1]i.e. with probability tending to 1 as n tends to infinity. We denote this by "a.s."

(which can be used for e.g. key construction) satisfies $\chi(G) > 3$. If S fails to verify G, then we can draw another instance from the class C (or C_1). We know that, given that S is a proper verifier, "good" instances of C (and C_1) will be found after a few tests.

Note that here we pose a special case of a general problem which is how to certify *negations* of properties that are hard in general. (Our case in non ξ-colorability). Little is known for such problems. We are aware of the works of [6] and that of [7] for recognizing unsatisfiable instances of random k-SAT. Their methods require at least $m = n^{k/2}$ clauses for n variables (i.e. $n^{3/2}$ clauses for 3-SAT).

One could attempt to construct a proper verifier S that searches the graph G and outputs a clique of size at least $k_0 = \xi + 1$. However, the probability threshold for such fixed-size cliques is around $p = \frac{n^{1-\frac{1}{k_0}}}{n}$ (i.e. when $\binom{n}{k_0} p^{\binom{k_0}{2}} > 1$) and therefore no such verifier will be able to find k_0-cliques a.s. for $c(n) = o(n^{1-1/k_0})$. So, such a verifier will fail even for the class C_1 for $\delta < 1 - 1/k_0$. Thus, any attempt to contruct proper verifiers for non-colorability, based on finding subgraphs of G with a large chromatic number, seems hopeless.

As in [6, 7], we here employ spectral methods. In particular, we base our method on the spectrum of the adjacency matric of G. It is well known that the eigenvalues of any real symmetric $n \times n$ matrix A can be found in time polynomial in n.

2 Previous Work

The important works of [6, 7] present proper verifiers for recognizing unsatisfiable instances of random $k-$SAT. Their methods are spectral and require at least $m = n^{k/2}$ clauses for n variables.

For the random graph model $G_{n,m}$ (all graphs of m edges equiprobable), the inspiring works of [11] as well as the PhD Thesis of [10] apply the first moment method in a clear way to show upper bounds to $r_3 = \frac{m}{n}$ above which the probability that $G_{n,m}$ is 3-colorable tends to zero. The best bound, due to [11], is $r_3 < 2.495$. The methods are non-constructive and do not lead to the finding of a proper verifier for non 3-colorability, however.

Important work for the establishment of the existence of a *threshold* $r_k = \frac{m}{n}$ for non k-colorability of random graphs is presened in [13] and [1].

3 Our Results

Let $\lambda_1 = \lambda_{\max} \geq \lambda_2 \geq \cdots \geq \lambda_n = \lambda_{\min}$ be the (sorted) eigenvalues (sorted) of the adjacency matrix A of the undirected graph G.

Definition 2 Let $\lambda = \max_{i=2,\ldots,n} |\lambda_i|$.

Definition 3 (eigenvalue gap) Let $\nu = \frac{\lambda_{\max}}{\lambda}$, called the *eigenvalue gap* of G.

We recall a nice theorem of Hoffman ([8]).

Theorem 1 (Hoffman, 1970) For every undirected graph G with at least one edge, its vertex-chromatic number $\chi(G)$ satisfies

$$\chi(G) \geq 1 + \frac{\lambda_{\max}}{-\lambda_{\min}}$$

A nice proof of the theorem of Hoffman can be found in [4], pp. 55-57.

Corollary 1 The above theorem implies that $\chi(G) \geq 1 + \nu$ (since $\lambda_{\min} < 0$ and $\lambda \geq -\lambda_{\min}$).

Our main result is to show that $\nu \to +\infty$ almost surely for $G \in C$. Then Hoffman's theorem and Corollary 1 immediately imply a proper verifier S for the class C. Given $\xi > 0$ and fixed (e.g. $\xi = 4$) algorithm S computes the eigenvalues of A of G. S then tests whether $\nu \geq \xi$. Our main result shows that this works almost surely for G in C.

The rest of the paper is devoted to proving that $\nu \to +\infty$ for $G \in C$ almost surely. In Section 4, we establish this for the weaker class C_1. In Section 5 we strengthen the convergence of $\nu(n)$ to $+\infty$ as $n \to +\infty$ for the class C.

Our work in section 4 extends a method of [6] to its limit i.e. to G in class C_1. Our work in section 5 which shows the result for class C is based on the work of Juhasz ([9]).

3.1 A basic result about λ_1

We start from a well-known fact (see e.g. [9]) which we also prove here.

Lemma 1 Let A be an $n \times n$ symmetric $(0,1)$ matrix in which the number of ones is $2m$. Then the largest eigenvalue λ_1 of A satisfies

$$\frac{2m}{n} \leq \lambda_1 \leq \sqrt{2m}$$

Proof: Let $e = (1 \cdots 1)$ be the n-dimensional all-one column vector. Then,

$$\lambda_1 \geq \frac{< e^T A e >}{< e^T e >}$$

So, $\lambda_1 \geq \frac{2m}{n}$.
Also,

$$trace(A^2) = \sum_{i=1}^{n} \lambda_i^2 = 2m$$

thus $\lambda_1 \leq \sqrt{2m}$ ◇

Consider now the random graph $G_{n,p}$ with $p = \frac{c(n)}{n}$. Its number of edges, m, is the binomial $B(\frac{n(n-1)}{2}, p)$ with expected value $E(m) \geq \frac{(n-1)c(n)}{2}$ and from Chernoff bounds we get:

Lemma 2 For $G_{n,p}$ and $p \geq c(n)/n, \forall \epsilon \in (0,1)$ it is

$$\Pr\left\{(1-\epsilon)\frac{(n-1)c(n)}{2} \leq m \leq (1+\epsilon)\frac{(n-1)c(n)}{2}\right\} \geq 1 - \exp\left(-\epsilon^2 \frac{(n-1)c(n)}{2}\right)$$

◇.

Combining Lemmas 1,2 we get:

Lemma 3 Let A be the adjacency matrix of $G_{n,p}$ where $p \geq c(n)/n$, $\epsilon \in (0,1)$. Then, with probabaility at least

$$1 - \exp\left(-\epsilon^2 \frac{(n-1)c(n)}{2}\right)$$

we have for the maximum eigenvalue of A that

$$(1-\epsilon)\left(\frac{n-1}{n}\right) c(n) \leq \lambda_1 \leq \sqrt{(1+\epsilon)(n-1)c(n)}$$

◇

Notice that Lemma 3 works even when $c(n)$ is constant. Notice also that [12] gives a tighter result, but Lemma 3 is enough for our purposes.

4 The trace method for the class C_1

We will show here the following.

Theorem 2 For any fixed $\mu > 0$, $\frac{\lambda_1}{\lambda} > \mu$ for $G \in C_1$, almost surely.

The whole section is devoted to the proof of Theorem 2.

We first establish a basic inequality:

For all *even* constant $k > 0$ $\forall i$ it is $\lambda_i^k \geq 0$ and we get

$$trace(A^k) = \sum_{k=1}^{n} \lambda_i^k \geq \lambda_1^k + \lambda^k$$

i.e.

$$E(\lambda^k) \leq E(trace(A^k)) - E(\lambda_1^k) \tag{1}$$

From Lemma 3, we have that with probability at least $1 - exp(-\epsilon^2 \frac{(n-1)}{2} c(n))$ that $\lambda_1 \geq (1-\epsilon)c(n) - o(1)$. Then

$$E(\lambda_1^k) \geq (1-\epsilon)^k c^k(n) - o(c^k(n)) \tag{2}$$

since the probability of failure in Lemma 3 is *exponentially low* in n and k is *constant*.

4.1 The expectation of the trace of A^k for large fixed k

We now calculate an upper bound to $E(trace(A^k))$ for k fixed, even and sufficiently large.

The calculation follows a method from [6].

For $\overrightarrow{\alpha} = (\alpha_0, \alpha_1, ..., \alpha_k = \alpha_0)$ let $W(\overrightarrow{\alpha}) = 1$ mean that the walk given by $\overrightarrow{\alpha}$ is possible in the random graph, i.e. all edges $\{\alpha_{i-1}, \alpha_i\}$ for $1 \leq i \leq k$ occur.

Then

$$E(trace(A^k)) = \sum_{\overrightarrow{\alpha}} \Pr\{W(\overrightarrow{\alpha}) = 1\} \tag{3}$$

We first highlight a technical lemma (also "burried" in [6]).

Lemma 4 For $G \in C_1$ it is

$$E(trace(A^k)) \leq c^k(n) + o(c^k(n))$$

Proof: We start from Equation 3 i.e. $E(trace(A^k)) = \sum_{\overrightarrow{\alpha}} \Pr\{W(\overrightarrow{\alpha}) = 1\}$ for all walks $\overrightarrow{\alpha}$. As in [7], there are three types of walks $\overrightarrow{\alpha}$:

A walk is *distinct* iff all edges in it are distinct. A walk is *duplicated* iff each edge $e_i = \{\alpha_{i-1}, \alpha_i\}$ occurs at least twice. All other walks are *quasi-distinct* iff some edges away from e_i occur at least twice and some only once.

For $\overrightarrow{\alpha}$ distinct, the expected number of such walks is bounded above by $n^k p^k = c^k(n)$.

For $\overrightarrow{\alpha}$ duplicated let j be the number of distinct edges in $\overrightarrow{\alpha}$. Clearly $1 \leq j \leq \frac{k}{2}$ thus for the expected number of duplicated walks we get the upper bound B

$$B = \sum_{j=1}^{\frac{k}{2}} k^{2k} n^{j+1} p^j \leq \sum_{j=1}^{\frac{k}{2}} k^{2k} n^{j+1} \frac{c^j(n)}{n^j} \leq \frac{k}{2}\, k^{2k} n\, c^{\frac{k}{2}}(n).$$

Picking $k > \frac{2}{\delta}$ in the class C_1 implies $1 + \frac{\delta k}{2} < \delta k$, so

$$B \leq \frac{k}{2}\, k^{2k} n c^{\frac{k}{2}}(n) = o(n^{\delta k}) = o(c^k(n))$$

The bound for the case of quasi-distinct walks can be derived by first assuming that the last edge e_k is a unique edge of the walk. We get then a bound of $kk^{2k}c^{k-1}(n) = o(c^k(n))$ since $\delta(k-1) < \delta k$.

Summing up all cases we get $E(trace(A^k)) \leq c^k(n) + o(c^k(n))$. $\diamond$

4.2 The rest of the proof

Given this, Equation (1) and Equation (2) we have

$$E(\lambda^k) \leq E(trace(A^k)) - E(\lambda_1^k)$$

i.e.

$$E(\lambda^k) \leq c^k(n)[1-(1-\epsilon)^k] + o(c^k(n))$$

Since this holds $\forall \epsilon > 0$ we get then

$$E(\lambda^k) = o(c^k(n)) \tag{4}$$

Now $\forall\ \mu > 0$ fixed and $\forall\ k$ fixed, it is

$$\Pr\{\mu\lambda > \lambda_1\} = \Pr\{\mu^k\lambda^k > \lambda_1^k\} = \Pr\{\mu^k\lambda^k > \lambda_1^k \text{ given that } \lambda_1^k \geq [(1-\epsilon)c(n) - o(1)]^k\}\cdot$$

$$\cdot \Pr\{\lambda_1 \geq (1-\epsilon)c(n) - o(1)\} + \Pr\{\mu^k\lambda^k > \lambda_1^k \text{ given that } \lambda_1^k < [(1-\epsilon)c(n) - o(1)]^k\}\cdot$$

$$\begin{aligned}\cdot \Pr\{\lambda_1 < (1-\epsilon)c(n) - o(1))\} &\leq \Pr\{\mu^k\lambda^k > [\left(1-\epsilon\right)c(n) - o(1)]^k\} \left(1 - exp(-\epsilon^2 \tfrac{(n-1)}{2} c(n))\right) \\ &+ exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right) \\ &\leq \Pr\{\lambda^k > \left[\tfrac{(1-\epsilon)^k}{\mu^k} c^k(n) - \tfrac{o(1)}{\mu^k} / E(\lambda^k)\right] E(\lambda^k)\} \left(1 - exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right)\right) \\ &+ exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right)\end{aligned}$$

By the Markov inequality it is

$$\Pr\{\lambda^k > \alpha E(\lambda^k)\} < \frac{1}{\alpha}$$

So

$$\begin{aligned}\Pr\{\mu\lambda > \lambda_1\} &\leq \frac{E(\lambda^k)}{\frac{(1-\epsilon)^k}{\mu^k} c^k(n) - \frac{o(1)}{\nu^k}} \left(1 - exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right)\right) + exp(-\epsilon^2 \tfrac{(n-1)}{2} c(n)) \\ &\leq \frac{o(c^k(n))}{\left(\frac{1-\epsilon}{\mu}\right)^k c^k(n) - o(1)} \left(1 - exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right)\right) + exp\left(-\epsilon^2 \tfrac{(n-1)}{2} c(n)\right)\end{aligned}$$

Let $\beta(n)$ be the fastest growing of all the $o(c^k(n))$ terms till here.
Let $\gamma(n) = \frac{c^k(n)}{\beta(n)}$
Note that $\gamma(n) \to +\infty$ as $n \to +\infty$.
Then by the above it is

$$\Pr\{\mu\lambda_1 > \lambda_1\} \leq \frac{1}{\alpha\gamma(n)}$$

where $\alpha > 0$ a constant.

So

$$\Pr\{\mu\lambda \leq \lambda_1\} \geq 1 - \frac{1}{\alpha\gamma(n)}$$

This completes the proof of Theorem 2.

4.3 The limits of the method of traces

Unfortunately the method of traces works well only for as low a $c(n)$ as a subclass of C_1 allows:

Lemma 5 Let $p = \frac{c(n)}{n}$ and $c(n) \leq n^{\frac{1}{k}}$. Then

$$E(trace(A^k)) = \Omega\left(c^k(n)\right)$$

Proof: As in section 4.2,

$$E(trace(A^k)) \geq E(\#duplicated\, walks\, of\, length\, k) \geq f(k)\cdot n \cdot c^{\frac{k}{2}}(n)$$

where $f(k)$ an unbounded function of k.

To see this, consider e.g. a line segment of $\frac{k}{2}$ edges (i.e. $\frac{k}{2}+1$ vertices) and the duplicated walk that goes from the left end of the segment to the right and then all the way back. The expected number of such segments is at least

$$A = \left(\frac{k}{2}+1\right)!\binom{n}{\frac{k}{2}+1}\left(\frac{c(n)}{n}\right)^{\frac{k}{2}}$$

where there are $\binom{n}{\frac{k}{2}+1}$ ways to choose the $\frac{k}{2}+1$ vertices, then $\left(\frac{k}{2}+1\right)!$ ways to order them in a line and $\left(\frac{c(n)}{n}\right)^{\frac{k}{2}}$ is the probability for the $\frac{k}{2}$ edges to exist simultaneously. But $\binom{n}{\frac{k}{2}+1} = \frac{n!}{(\frac{k}{2}+1)!(n-\frac{k}{2}-1)!}$. So, by carrying out the calculation we get

$$A \geq \left(n^{\frac{k}{2}+1} - \left(\frac{k}{2}\right)^{\frac{k}{2}+1}\right)\left(\frac{c(n)}{n}\right)^{\frac{k}{2}} \geq nc^{\frac{k}{2}}(n) - \left(\frac{k}{2}\right)^{\frac{k}{2}+1} c^{\frac{k}{2}}(n) \geq nc^{\frac{k}{2}}(n) - o\left(nc^{\frac{k}{2}}(n)\right)$$

For any $c(n) \leq n^{\frac{1}{k}}$ i.e. $n \geq c^k(n)$ we get $nc^{\frac{k}{2}}(n) \geq nc^{\frac{3k}{2}}(n)$. So, $A = \Omega\left(c^k(n)\right)$. Thus $E(trace(A^k)) = \Omega\left(c^k(n)\right)$ $\diamond$

To get the result for the class C_1 we need stronger methods. We do this in the following section.

5 The class C and the Juhasz bound

Here we prove our stronger (and main) result:

Theorem 3 For any fixed $\mu > 0$ it is $\frac{\lambda_1}{\lambda} > \mu$ for $G \in C$, almost surely.

Proof: We carefully adapt the ideas from [9].

Consider the matrix

$$B_n = P_n A P_n$$

where P_n is the orthogonal projection parallel to the all-one vector $e = (1, \cdots, 1)$. The Courant-Fischer equalities (see e.g. [14], p. 159, Exercise 6.19) state that

$$m(B_n) = \max\{x^T B_n x\} \text{ over all } x : ||x|| = 1$$

where $m(B_n)$ is the maximum eigenvalue of B_n.

The same equalities, for the matrix A state that

$$\lambda_2 = \max\{x^T Ax\}$$

where $||x|| = 1$ and $x^T e_1 = 0$ with e_1 being the eigenvector corresponding to the first eigenvalue λ_1 (reminder: $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$). Since, $\lambda \leq \lambda_2$ we get $\lambda \leq \max\{x^T Ax\}$ where $||x|| = 1$ and $x^T e_1 = 0$. Let

$$E_1 = \{x : ||x|| = 1\} \text{ and } x^T e_1 = 0$$

and

$$E_2 = \{x : ||x|| = 1\}$$

Note that $E_1 \subseteq E_2$. By the definition of B_n then

$$\max_{x \in E_1}\{x^T Ax\} \leq \max_{x \in E_2}\{x^T B_n x\}$$

inplying $\lambda \leq m(B_n)$. In the sequel, for any real symmetric matrix E, we denote by $m(E)$ its maximum eigenvalue.

It is easy to see that

$$B_n = (b_{ij}), b_{ij} = a_{ij} - d_i - d_j + d$$

where nd_i is the number of 1's in the i^{th} row and $n^2 d$ the number of ones in A. We write

$B_n = C_n - R_n$,
$C_n = [c_{ij}]$, where $c_{ij} = a_{ij} - p(n)$ and
$R_n = [r_{ij}], r_{ij} = d_i + d_j - d - p(n)$
Then,

$$m(B_n) \leq m(C_n) + m(R_n) \leq m(C_n) + \left(\sum_{i=1}^{n} \sum_{j=1}^{n} r_{ij}^2 \right)^{\frac{1}{2}} \tag{5}$$

But

$$Var(d_i + d_j - d) = \frac{1}{n^4} Var\left(\sum_{k=1}^{n} \sum_{l=k+1}^{n} a_{kl} Pr\{a_{kl} = 1\} \right) \leq \frac{3p(n)(1 - p(n))}{n}$$

So

$$E\left(\sum_{i=1}^{n} \sum_{j=1}^{n} r_{ij}^2 \right) \leq n^2 \ \frac{3p(n)(1 - p(n))}{n}$$

$\Rightarrow E(m(R_n)) \leq \sqrt{3p(n)n(1 - p(n))} \leq \sqrt{3c(n)}$

Since $\forall_i \forall_j$ it is $E(c_{ij}) = 0$, by using Wigner's ([15]) theorem we again get $E(m(C_n)) = \Theta(\sqrt{c(n)})$

So, from Equation 5 we get that $\exists a_1 > 0$ a constant:

$$E(\lambda) \leq E(m(B_n)) \leq a_1 \sqrt{c(n)}$$

by linearity of expectation.

Now, by Markov's inequality and for any $\mu > 0$

$$\begin{aligned}
\Pr\{\mu\lambda > \lambda_1\} &= \Pr\{\mu\lambda > \lambda_1 \text{ given that } \lambda_1 > (1 - \epsilon)c(n) - o(1)\} \cdot \Pr\{\lambda_1 > (1 - \epsilon)c(n) - o(1)\} \\
&\quad + Pr\{\mu\lambda > \lambda_1 \text{ given that } \lambda_1 \leq (1 - \epsilon)c(n) - o(1)\} \cdot \Pr\{\lambda_1 \leq (1 - \epsilon)c(n) - o(1)\} \\
&\leq \Pr\{\mu\lambda > (1 - \epsilon)c(n) - o(1)\} + \Pr\{\lambda_1 \leq (1 - \epsilon)c(n) - o(1)\} \\
&\leq \Pr\left\{\lambda > \tfrac{(1-\epsilon)c(n) - o(1)}{\mu a_1 \sqrt{c(n)}} a_1 \sqrt{c(n)}\right\} + \Pr\{\lambda_1 \leq (1 - \epsilon)c(n) - o(1)\}
\end{aligned}$$

By the Markov inequality however and since $E(\lambda) \leq a_1\sqrt{c(n)}$ we get

$$\Pr\left\{\lambda > \frac{(1-\epsilon)c(n)-o(1)}{\mu a_1\sqrt{c(n)}}a_1\sqrt{c(n)}\right\} \leq \Pr\left\{\lambda > \frac{(1-\epsilon)c(n)-o(1)}{\mu a_1\sqrt{c(n)}}E(\lambda)\right\} \leq \frac{\mu a_1\sqrt{c(n)}}{(1-\epsilon)c(n)-o(1)}$$

So

$$\Pr\{\mu\lambda > \lambda_1\} \leq \frac{\mu a_1\sqrt{c(n)}}{(1-\epsilon)c(n)-o(1)} + \Pr\{\lambda_1 \leq (1-\epsilon)c(n)-o(1)\}$$

Notice that Lemma 2 holds also for the class C (even for $c(n) \geq c$ a constant). By Lemma 2

$$\Pr\{\lambda_1 \leq (1-\epsilon)c(n)-o(1)\} \leq exp\left(-\epsilon^2\frac{(n-1)}{2}c(n)\right)$$

So

$$\Pr\{\mu\lambda > \lambda_1\} \leq \frac{\mu a_1}{1-\epsilon}\frac{1}{\sqrt{c(n)}} + exp\left(-\epsilon^2\frac{(n-1)}{2}c(n)\right) \leq \frac{1+\epsilon}{1-\epsilon}\mu a_1\frac{1}{\sqrt{c(n)}}$$

This tends to zero as $n \to \infty$. So, we get our main result, which we restate more precisely here.

Lemma 6 *$\forall\ \mu > 0$, μ fixed and $\forall\ \epsilon > 0\ \exists\ a_1$ fixed $a_1 > 0$ so that*

$$\mu \leq \frac{\lambda_1}{\lambda}$$

with probability at least

$$1 - \frac{1+\epsilon}{1-\epsilon}\mu a_1\frac{1}{\sqrt{c(n)}}$$

for all $c(n)$: $G_{n,\frac{c(n)}{n}} \in C$.

This completes the proof of Theorem 3. ◇

6 Conclusions and Open Problems

The results of section 5 imply together with Hoffman's theorem that:

Corollary 2 *$\forall\mu > 0$ fixed and for G in the class C:*

$$\chi(G) \geq 1 + \frac{\lambda_{\max}}{-\lambda_{min}} \geq 1 + \mu$$

almost surely.

This gives the proper verifier for class C by computing the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of the adjacency matrix A of G in polynomial time.

What happens, however, for $c(n)$ constant? Our techniques are unable to get so down for the $c(n)$ values. We leave this as an important open problem.

In particular, although our result provides a verifier for non 3-colorability of $G \in G_{n,p}$ with $p = \frac{c(n)}{n}$ and $c(n)$ anything but constant, it fails to do so for $c(n)$ constant.

Acknowledgement. We wish to thank Andreas Goerdt who motivated us to work on this problem during his visit to Patras University and CTI.

References

[1] D. Achlioptas and E. Friedgut : A sharp threshold for k-colorability. In *Journal of Random Structures and Algorithms 14, pp. 63 - 70*, (1999).

[2] L. Arnold: On the asymptotic distribution of eigenvalues of random matrices. In *J. of Math. Analysis Appl. 20, pp. 262 - 268*, (1967).

[3] L. Arnold: Deterministic version of Wigner' s semi-circle law for the distribution matrix eigenvalues . In *Linear Algebra and its Appl. 13, pp. 185 - 199*, (1976).

[4] N. Biggs: Algebraic Graph Theory. 2nd Edition, Cambridge University Press, (1993).

[5] B. Bollobás, "Random Graphs", Academic Press, 1985.

[6] J. Friedman and A. Goerdt: Recognizing More Unsatisfiable Random 3-SAT Instances Efficiently. In *ICALP 2001, pp. 310 - 321*, (2001).

[7] A. Goerdt and M. Krivelevich: Efficient recognition of random unsatisfiable k-SAT instances by spectral methods. In *STACS 2001*, (2001).

[8] A. J. Hoffman, On Eigenvalues and Colorings of Graphs In *Graph Theory and its Applications, pp. 79 - 92*, Academic Press, NY (1970).

[9] F. Juhasz: On the Spectrum of a Random Graph. In *Algebraic Methods in Graph Theory*, Colloquia Mathematica Societatis Janos Bolyai, Szeged, Hungary, (1978).

[10] A. Kaporis: Limit phenomena for phase transition in combinatorial problems. *PhD Thesis, Dept of Computer Engineering and Informatics, Univ. of Patras*, (2003).

[11] A. Kaporis, L. Kirousis and Y. Stamatiou: A note on the non-colorability threshold of a random graph. In *Electronic Journal of Combinatorics 7 (1) R 29*, (2000).

[12] M. Krivelevich and B. Sudakov: The largest eigenvalue of sparse random graphs. In *Math Dept Technical Report, TEl Aviv Univ.*.

[13] T. Luczak: Size and connectivity of the k-core of a random graph. In *Discrete Mathematics 91, pp. 61 - 68*, (1991).

[14] R. Motwani and P. Raghavan, Randomized Algorithms. Cambridge University Press.

[15] E. P. Wigner: Characteristic vectors of bordered matrices with infinite dimensions. In *Ann. of Math. 62, pp. 548 - 564*, (1955).

[16] E. P. Wigner: On the distribution of roots of certain symmetric matrices with infinite dimensions. In *Ann. of Math. 67, pp. 325 - 327*, (1958).