JOURNAL OF ALGORITHMS 10, 451–489 (1989)

The Solution of Some Random NP-Hard Problems in Polynomial Expected Time

M. E. DYER

Leeds University, Leeds, England

AND

A. M. FRIEZE

Carnegie-Mellon University, Pittsburgh, and Queen Mary College, London, England

Received October 13, 1986; revised September 30, 1987

The average-case complexity of recognising some NP-complete properties is examined, when the instances are randomly selected from those which have the property. We carry out this analysis for

(1) Graph k-colourability. We describe an $O(n^2)$ expected time algorithm for n-vertex graphs, with k constant.

(2) Small equitable cut. We describe an $O(n^3)$ expected time algorithm for finding *and verifying*, the minimum equitable cut in a $2n$-vertex graph G, condition on G having one with at most $(1 - \varepsilon)n^2/2$ edges.

(3) Partitioning a $2n$ vertex graph into two sparse vertex induced subgraphs of a given class. We describe an $O(n^3)$ expected time algorithm for computing such a partition.

(4) The number problem 3-PARTITION. We describe an $O(n^2)$ expected time algorithm for problems with $3n$ integers. © 1989 Academic Press, Inc.

1. INTRODUCTION

We examine the "average-case" computational complexity of some problems which are known to be NP-hard [3]. By "average-case" we mean that the inputs are selected randomly from some natural family of distributions parameterised by problem size.

The type of problem we consider is one in which the instances are known to have the property we are seeking, and our task is to exhibit a proof of this. From the worst-case point of view such problems are just as hard as

0196-6774/89 $3.00

those in which we do not know whether the instance has the property. For, suppose π is an NP-hard property, and we had an algorithm which would exhibit a proof that the instance had property π, given that it did, in polynomial time. It is easy to construct from this a polynomial time algorithm for deciding whether an arbitrary instance has π.

As a concrete example (see Section 3) consider 3-colouring the vertices of a graph. It is well known [3] that the decision problem is NP-complete. Our problem is, given a 3-colourable graph, colour it using only three colours. In this case our input distribution would be the uniform distribution on the set of all 3-colourable graphs on N vertices, for example. This type of problem for graph-colouring has been studied previously by Kucera [5] and Turner [8, 9]. We strengthen their results by exhibiting an algorithm which performs the colouring in expected polynomial time.

In Section 4 we examine the problem of "minimum cut into equal-sized subsets"—see also Bui, Chaudhuri, Leighton, and Sipser [1]. An interesting feature of this problem is that we present expected polynomial time algorithms not only for finding, but also for proving *optimality* of the minimum cut under a natural model.

In Section 5 we consider a partitioning problem on graphs of the type considered in [2]. In Section 6 we examine a non-graph problem, 3-partition. Finally, in Section 7 we comment briefly on other problems which fall within the scope of our approach.

2. Notation and Preliminaries

We denote an arbitrary graph by $G = (V(G), E(G))$, and we will also use $N = |V(G)|$, $M = |E(G)|$. For a vertex $v \in V(G)$, $\Gamma(v)$ will denote its set of adjacent vertices in G. By extension for $S \subseteq V(G)$ we will write $\Gamma(S) = \bigcup_{v \in S}\Gamma(v) - S$. (By convention $\Gamma(\varnothing) = V(G)$). We will also use $\delta_X(v)$ on occasion to mean $|\Gamma(v) \cap X|$ for some $X \subseteq V(G)$, i.e., $\delta_X(v)$ is the number of neighbours that v has in X. For any $X \subseteq V(G)$, $G[X]$ will denote the subgraph of G induced by X.

We will denote by $B(n, p)$ the binomial distribution with parameters n, p. We use the notation $=^d$ and $\leq^d$ to imply equality and dominance in distribution. Many of our results involve transformations between probability spaces, and to this end we will give the following two simple results here for future reference. The first concerns restricting or enlarging the sample space.

Lemma 2.1. *Let S_1 be a discrete sample space with a probability measure P. Suppose $S_2 \subseteq S_1$ and let $\bar{S}_2 = S_1 - S_2$. If $E_1 \subseteq S_1$ and $E_2 = E_1|S_2$ then*

$$P(E_1) \leq P(E_2) + P(\bar{S}_2)$$

and

$$P(E_2) \leq P(E_1)/P(S_2).$$

Proof. $P(E_1) = P(E_2)P(S_2) + P(E_1 \cap \bar{S}_2)$. Hence

$$P(E_1) \geq P(E_2)P(S_2) \qquad \text{and} \qquad P(E_1) \leq P(E_2) + P(\bar{S}_2). \ \square$$

Lemma 2.1 is used as follows. Suppose S_1 is, for example, a class of graphs with input distribution P, and E_1 is the event that at graph fails to have some property π. If we restrict it to a subclass S_2, then E_2 is the event that graphs in S_2 do not have π. Then $P(E_2)$ will be small if $P(E_1)/P(S_2)$ is small. Similarly, $P(E_1)$ is small if $P(E_2) + P(\bar{S}_2)$ is small. Thus, under these circumstances, we can add or delete parts of the sample space without significantly affecting probability results.

Our other transformation involves many–one mappings of the space. The following is not the most general result of this type, but is sufficient for our purposes.

LEMMA 2.2. *Let U_i be the uniform random variable on discrete sample space S_i $(i = 1, 2)$. Let f: $S_1 \to S_2$ be onto. Suppose $X_2 = g(U_2)$ is a non-negative random variable and $X_1 = g(f(U_1))$ is the random variable induced in S_1. Then*

$$\frac{E(X_2)}{E(X_1)} \leq \frac{1}{E(1/|f^{-1}f(U_1)|)}.$$

Proof.

$$E(X_2) = \sum_{u_2 \in S_2} g(u_2)/|S_2| \leq \sum_{u_2 \in S_2} |f^{-1}(u_2)| g(u_2)/|S_2|$$

(since f is onto and g is non-negative)

$$= \frac{\sum_{u_1 \in S} g(f(u_1))}{|S_1|} \cdot \frac{|S_1|}{|S_2|} = E(X_1) \cdot \frac{|S_1|}{|S_2|}$$

$$= E(X_1) \cdot \frac{1}{E(1/|f^{-1}f(U_1)|)}.$$

(The last equation follows from

$$E(1/|f^{-1}f(U_1)|) = \sum_{u_1 \in S_1} \frac{1}{|f^{-1}f(u_1)|} \cdot \frac{1}{|S_1|} = \frac{|S_2|}{|S_1|}. \ \square$$

COROLLARY 2.3. (a) $E(X_2)/E(X_1) \leq k/\Pr(|f^{-1}f(U_1)| \leq k)$ *for any integer* $k \geq 1$.

(b) $E(X_2)/E(X_1) \leq E(|f^{-1}f(U_1)|)$.

Proof. For any positive random variable X,

(a) $E(1/X) \geq \Sigma_{i=1}^{k}\Pr(X = i)/i \geq \Pr(X \leq k)/k$;

(b) $E(1/X) \geq 1/E(X)$, since $1/x$ is a convex function on $x > 0$ and use Jensen's inequality. □

Lemma 2.2 and its corollary are used as follows. Suppose S_1 is a sample space of pairs (graph, label), in which the same graph can appear more than once, but with a different label, and we have a uniform distribution on a sample space S_2 in which each such graph appears only once. (The label indicates the way the graph was chosen.) Under the mapping f which discards the label, $|f^{-1}f(U_1)|$ is the number of "occurrences" of a random graph in S_1. Then, provided either that $|f^{-1}f(U_1)|$ has a large enough probability of being 1 (unique occurrence) or has small enough expected value, then by Corollary 2.3 we deduce that events having small probabilities in S_1 will also have small probabilities in S_2. Note that unique occurrences is simply the case $k = 1$ of Corollary 2.3(a), but we will need the more general statement given in the Corollary in Section 5 below.

3. GRAPH COLOURING

We will describe a polynomial time (randomised) algorithm which always solves the problem of vertex colouring a graph with a fixed number of colours, k. Our input distribution for this result is the uniform distribution on all k-colourable graphs with N vertices. Thus our main result says that if we know a graph is k-colourable, then we can colour it in polynomial expected time under the assumption that all such graphs are equally likely. We proceed to this result indirectly, by considering a sequence of models, which are themselves of some intrinsic interest. We will first describe these. Let $N = |V(G)|$, $M = |E(G)|$. Our first model, Model 1, has k colour classes each having approximately the same number of $n = N/k$ of vertices, and all possible edges between different classes have the same probability $p(n)$ of being present, choices being made independently for each edge. The number $p(n)$ is called the edge-density. Here we will be principally concerned with $p(n)$ bounded away from zero. To avoid confusion we will call the colour classes used in the generation of G, the *blocks* of G. By approximately equal-sized blocks, we mean that each has size $\approx n$ as $N \to \infty$. Our second model, Model 2, again assumes fixed blocks, but we then select M edges at random for some given M.

Our third model has two variants, Models 3 and 3′. For a fixed M, Model 3 selects a graph uniformly from the following sample space. The distinct sample points are all ways of choosing the k blocks as a partition of $V(G)$ (of size N) and then selecting M inter-block edges. Since the colouring of such a graph may not always be unique, the same k-colourable graph with N vertices and M edges may occur more than once in the sample space for Model 3. By contrast, Model 3′ is the uniform distribution on the sample space obtained by removing all duplicates of the same graph.

Finally, Models 4 and 4′ allow M to vary and consider all graphs obtained as in Models 3, 3′ as equally likely. Thus Model 4′ is the true object of interest, the uniform distribution on all k-colourable graphs with N vertices. A random graph under Model i will be denoted G_i ($i = 1, 2, 3, 3', 4, 4'$). Kucera [5] and Turner [8, 9] have examined the graph colouring problem under one or more of these models and given "almost sure" algorithms. That is, their algorithms have a negligible probability of failure. However, in case of failures, there is no known algorithm which requires less than exponential time to colour G, and this, unfortunately, is too large in relation to the failure probability to give a polynomial expected running time. Thus, they have shown that we can "usually" colour G fast. In contrast we will show that we can always colour G fast "on average." We exhibit a randomised algorithm and prove its polynomial expected-time performance under each of the models described above, provided suitable conditions are imposed on the parameters of the model.

Before describing our algorithm, we will deal with an issue which is of great importance in relating our models. This is that of uniqueness of colouring. We prove this for Model 1. Turner [9] gives a weaker form of the following result as a by-product of his colouring algorithm. Here we will give a direct proof. We restrict ourselves to constant values of p and k, as $n \to \infty$, though the analysis extends to other cases. We also assume all blocks are of size exactly n. The modifications for blocks of size $n(1 + o(1))$ are trivial.

THEOREM 3.1. *Let k, p be constants. Then, under Model* 1, G, *almost surely has a unique k-colouring. Moreover, the expected number of different k-colourings of G, is* $1 + o(1)$.

Remark. Here, as elsewhere, we use the term "almost surely" to mean "with probability $1 - o(1)$ as $n \to \infty$." This usage, while at odds with practice elsewhere in probability theory, is common in random graph theory.

Proof. Denote the blocks of G_1 by B_i ($i = 1, \ldots, k$). Suppose A_i ($i = 1, \ldots, k$) is some alternative partition of $V(G_1)$. We will estimate the probability that this provides a proper colouring of G_1.

Let $a_{ij} = |B_i \cap A_j|$. Thus we have $\Sigma_{j=1}^k a_{ij} = n$ for $i = 1,2,\dots,k$. We will assume that the A_i are numbered such that

$$a_{ii} \geq \left(n - \sum_{j=1}^{i-1} a_{ij}\right) \Big/ (k - i + 1). \tag{3.1}$$

This can be achieved by re-indexing in a "greedy" manner. We choose the j maximising a_{1j} as A_1, then the j ($\neq 1$) maximising a_{2j} ($j \neq 1$) as A_2, etc. Now the probability that the A_i's are stable sets is $(1-p)^s$ where $S = \Sigma_{j=1}^k \Sigma_{i=1}^k \Sigma_{l=i+1}^k a_{ij} a_{lj}$.

Consider the following two cases. Suppose $\frac{1}{2} < \alpha < 1$.

(a) There are two of the $a_{ij} \geq n^\alpha$ for some j. Then clearly $S \geq n^{2\alpha}$. The number of possible partitions of $V(G_1)$ into k sets is less than k^{kn}, so the expected number of such stable partitions is $< k^{kn}(1-p)^S \leq k^{kn}(1-p)^{n^{2\alpha}}$, which approaches zero super-exponentially as $n \to \infty$ since $2\alpha > 1$.

(b) Case (a) does not hold. Thus $a_{1j} < n^\alpha$ ($j \neq 1$), since $a_{11} \geq n/k$ by construction (3.1). Therefore $a_{22} > (1/(k-1))(n - n^\alpha)$, which implies $a_{2j} < n^\alpha$ ($j \neq 2$) for large n, since $\alpha < 1$. Generally we will have $a_{ii} > (n - (i-1)n^\alpha)/(k - i + 1)$ which implies $a_{ij} < n^\alpha$ ($j \neq i$). Therefore we find that $a_{ij} < n^\alpha$ for all $j \neq i$ and hence $a_{ii} = n - \Sigma_{j \neq i} a_{ij} > n - (k-1)n^\alpha$ ($i = 1,2,\dots,k$).

Hence $S > (n - (k-1)n^\alpha)\Sigma_{j=1}^k \Sigma_{i \neq j} a_{ij} \geq n - (k-1)n^\alpha$ since the A_i differ from B_i. However, the number of partitions of $V(G_1)$ into such sets A_i is now at most

$$\sum_{\{a_{ij}\}} \prod_{i=1}^k n^{\Sigma_{j \neq i} a_{ij}} < \prod_{i=1}^k n^{k+(k-1)n^\alpha} = n^{k^2 + k(k-1)n^\alpha}.$$

($n^{\Sigma_{j \neq i} a_{ij}}$ is an upper bound on the number of ways of partitioning B_i into blocks $B_i \cap A_j$ for $j = 1,2,\dots,k$ given the values of the a_{ij}.) Thus the expected number is at most $n^{k^2+k(k-1)n^\alpha}(1-p)^{n-(k-1)n^\alpha}$ which tends to zero exponentially fast as $n \to \infty$.

Thus, in either case, the probability of non-uniqueness is at least exponentially small. (In fact it is exactly exponentially small, since G_1 will have an isolated vertex with probability at least $(1-p)^{n(k-1)}$, in which case the colouring is certainly not unique.)

If $\gamma(G_1)$ is the number of different k-colourings of G_1, then using the estimates in (a), (b) above

$$\begin{aligned} E(\gamma) &\leq 1 + k^{kn}(1-p)^{n^{2\alpha}} + n^{k^2+k(k-1)n^\alpha}(1-p)^{n-(k-1)n^\alpha} \\ &= 1 + o(1). \end{aligned}$$

Clearly $E(\gamma) \geq 1$, giving the result. □

We will now describe our algorithm, COLOUR, to find a k-colouring of a graph G.

COLOUR

```
Apply COLOUR 1 below to $G$;
If COLOUR 1 fails then apply COLOUR 2 below to $G$;
If COLOUR 2 fails then try all possible $k$-colourings to colour $G$;
Stop Either $G$ is $k$-coloured or no such colouring exists.
```

We must describe the procedures COLOUR 1 and COLOUR 2. In order that our algorithm is reasonably fast on the average, we use a "greedy" procedure for COLOUR 1. The method is essentially that of Kucera [5].

COLOUR 1

```
for $i \leftarrow 1$ to $k - 1$ do
begin
   $X_i \leftarrow \varnothing$ (where $X_i$ is the set of vertices coloured $i$).
   $Y_i \leftarrow V(G) - \bigcup_{j<i} X_i$ (the uncoloured portion of $G$ which is available to be coloured $i$)
repeat
     Select $v \in Y_i$ such that $\delta_{Y_i}(v)$ is minimal. (If there is a tie choose arbitrarily.)
    $X_i \leftarrow X_i \cup \{v\}$, $Y_i \leftarrow Y_i - \{v\} - \Gamma(v)$.
until $Y_i = \varnothing$.
end;
If $X_k = V(G) - \bigcup_{j=1}^{k-1} X_i$ is stable then $X_1, \dots, X_k$ is a $k$-colouring else COLOUR 1 has failed.
```

Each repetition of the for-loop finds a stable set disjoint from previous ones by a "greedy minimum degree" choice. It can be implemented in time linear in the number M of edges in G by simply updating degree counts at each vertex of Y_i as vertices are deleted from it. The overall complexity will then be $O(kM) = O(N^2)$ for k constant. We could, alternatively, use the method of Turner [8] for COLOUR 1. For fixed k and p this would have the same expected time-complexity.

Before proving any properties of COLOUR 1, we will describe COLOUR 2. COLOUR 2 guesses large k-coloured subgraphs of G and uses an "only available colour" rule to colour most of G; then it uses complete enumeration on the remainder, provided this is small enough.

COLOUR 2

```
r $\leftarrow \lceil 8k^2 \log n / - \log(1 - p) \rceil$
repeat $2nr^{(k+4)/2}$ times
 begin
   Choose $W \subseteq V(G)$ at random with $|W| = kr$
   for each partition of $W$ into $k$ equal subsets $W_1, \dots, W_k$ do
   if $W_1, \dots, W_k$ is a $k$-colouring of $W$ then
   begin
     $X_i \leftarrow W_i$ $(i = 1, \dots, k)$
     for each $v \in V(G) - W$ do
```

```
      begin
        if $\delta_{W_i}(v) = 0$ for more than one $i$ then next $v$
        else let $j$ be such that $\delta_{W_j}(v) = 0$
        if no such $j$ then next partition of $W$
        else $X_j \leftarrow X_j \cup \{v\}$
      end;
      $Y \leftarrow V(G) - \bigcup_{i=1}^{k} X_i$;
      if $|Y| > kr$ then next partition of $W$;
      else for each ordered partition of $Y$ into $k$ sets $Y_1, \ldots, Y_k$ do
     if $\{X_i \cup Y_i$: $i = 1, \ldots, k\}$ is a $k$-colouring of $G$ then stop {success}
      end
      end
Stop: COLOUR 2 has failed.
```

We now show that COLOUR gives a polynomial expected-time algorithm under Model 1 with k, p constant.

LEMMA 3.2 (Kucera [5]). *If k, p are constant, then COLOUR 1 fails with probability at most e^{-n^β}, for any $0 < \beta < 1$, when G is a random graph selected using Model 1.*

Proof. Since Kucera [5] does not provide a proof for his claims, we will sketch the proof here.

It is sufficient to show that the first repetition of the for-loop in COLOUR 1 terminates with a block of G in X_1. If this is the case we are then effectively applying COLOUR 1 to a random graph generated by Model 1 and $k \leftarrow k - 1$. Multiplying the failure probability for phase 1 by k will then give the result.

Without loss assume that the first $v \in Y_1$ selected is in block B_1. It is necessary to proceed with a little care, since the minimum degree choice rule immediately conditions all of G. Let us use the phrase "high probability" to mean with probability at least $1 - e^{-n^\beta}$ for any $0 < \beta < 1$. Suppose $r \geq 1$ vertices have been selected in X_1 and suppose $X_1 \subseteq B_1$. Note that $Y_1 = V(G) - \Gamma(X_1) - X_1$. Let $r_0 = \lceil (\log k - \log p)/-\log(1-p) \rceil$.

If $r < r_0$, we can show using the Chernoff bound that, for any such set X_1 with r vertices, $|B_j - \Gamma(X_1)| \approx n(1-p)^r$ with high probability, for all $j \neq 1$. By the same method we show that with high probability, for all $j \neq i$, if $v \in B_j$ there will be $\approx n(1-p)^{r+1}$ vertices in $B_i - \Gamma(X_1 \cup \{v\})$. Also any vertex $v \in B_j$ $(j \neq 1)$ will have degree $\approx np$ in B_1 with high probability. It now follows that if $v \in B_1 \cap Y_1$ then $\delta_{Y_1}(v) \approx (k-1)[n(1-p)^r - n(1-p)^{r+1}] = (k-1)np(1-p)^r$. However, if $v \in B_j \cap Y_1$ $(j \neq 1)$ then $\delta_{Y_1}(v) \approx np + (k-2)np(1-p)^r$. The latter is always larger. Thus if $r < r_0$ we will select the next vertex from B_1 with high probability.

If $r \geq r_0$ we use a slightly different argument. Now $|B_j \cap Y_1|$ is at most $\approx n(1-p)^{r_0}$ for all $j > 1$ with high probability. Also if $v \in B_j \cap Y_1$

$(j > 1)$ then all its $\approx np$ neighbours in B_1 must still be in $B_1 \cap Y_1$. Then if $v \in B_1 \cap Y_1$ it must have $\delta_{Y_1}(v)$ at most $\approx (k-1)n(1-p)^{r_0}$, whereas if $v \in B_j \cap Y_1$ $(j > 1)$ it has at least $\approx np$ for $\delta_{Y_1}(v)$. The choice of r_0 now ensures that the latter is larger. Thus with high probability in this case also we select the next vertex for X_1 from B_1. Thus with high probability $X_1 = B_1$ after n steps. □

Lemma 3.2 and its proof extend to k growing quite rapidly with n (for p constant) or for p decreasing with n (k constant). We will not need this here, but see Kucera [5]. We know therefore that COLOUR 1 usually succeeds and gives us an almost sure solution algorithm. However, its failure probability is not small enough to allow us to enumerate the cases of failure and obtain expected polynomial-time behaviour.

We must show that COLOUR 2 has a small enough failure probability. We consider its running time subsequently.

LEMMA 3.3. *COLOUR 2 has failure probability at most $e^{-n \log n}$ for n large and G selected using Model 1 with k, p constant.*

Proof. If we select sets of size kr with $r = \lceil 8k^2 \log n / -\log(1-p) \rceil$ at random from $V(G)$, the probability that we select r from each B_i is

$$\frac{\binom{n}{r}^k}{\binom{kn}{kr}} \approx \frac{\sqrt{2\pi kr}}{(2\pi r)^{k/2}} \geq \frac{1}{r^{k/2}} \qquad \text{for large } n.$$

Now consider block B_1 and random r-sets $W_2, \ldots, W_k$ in $B_2, \ldots, B_k$. For any $v \in B_1$, the probability that it is not adjacent to at least one vertex in each W_j $(j = 2, \ldots, k)$ is less than $k(1-p)^r$. Thus the probability that there is a subset of size r in B_1 all of which fail to be adjacent to at least one W_j is at most $\binom{n}{r}(k(1-p)^r)^r \leq n^r(kn^{-8k^2})^r < n^{-6k^2 r}$ for large n.

Let us call $W_1, \ldots, W_k$ a *bad selection for* B_1 (otherwise *good*) if there is such a subset of size r in B_1. Now suppose B_i is partitioned into n/r subsets $B_{i1}, B_{i2}, \ldots$ $(i = 1, \ldots, k)$ each of size r. (We can assume all B_i have $|B_i| = n$ and $r | n$ for simplicity, the modifications otherwise being trivial but cumbersome.) Consider the n/r choices of $W_i = B_{it}$ $(i = 1, \ldots, k)$ for $t = 1, 2, \ldots, n/r$. The probability that a proportion more than $1/2k$ of these are bad is then, using the independence, at most $\binom{n/r}{n/2kr}(n^{-6k^2 r})^{n/2kr} < 2^{n/r} n^{-3kn} < n^{-2kn}$ for large n. Now let us call such an (ordered) partition of the B_i "defective" if it contains more than a proportion $1/2k$ of bad selections for B_1. There are less than n^{kn} partitions altogether, so the probability that there exists any defective partition is less than $n^{kn} n^{-2kn} = n^{-kn}$. Now the procedure of randomly selecting a partition, then randomly selecting a $W_1, \ldots, W_k$ from the partition in the prescribed manner is clearly equivalent, by symmetry, to a random choice of sets W_i from B_i $(i = 1, \ldots, k)$. Thus the probability that a random selection is bad for a given B_i is at most $1/2k$. The probability that a random selection is bad for any B_i is therefore at most $k(1/2k) = \frac{1}{2}$. Thus the probability that our random W contains r vertices from each block and a good selection is at least $1/2r^{k/2}$ at each sampling. But if W contains a good selection we will find it, since we enumerate all cases. Then all of $V(G)$, except for a subset of size at most r in each B_i, will be correctly coloured by the "only available colour" rule used in COLOUR 2. Thus $|Y| \leq kr$ and the final loop will complete the colouring by enumeration. Since sampling is independent, the probability that we fail to get a good selection in all trials is at most

$$\left(1 - \frac{1}{2r^{k/2}}\right)^{2nr^{(k+4)/2}} \leq e^{-nr^2} < e^{-n \log n} \qquad \text{for large } n. \ \square$$

The running time of the main loop of COLOUR 2 is dominated by the two enumerations of W and Y. These will take the $O(k^{kr})$ which is polynomial in n for fixed k, p. The number of repetitions of the main loop is polynomial, hence COLOUR 2 has polynomial overall running time. It may be noted that the exponent grows rather fast with k, i.e., $k^3 \log k$. A more complicated implementation of the same idea used in COLOUR 2 might reduce the exponent, but it appears we can only obtain polynomial behaviour for fixed k. (However, note that even if COLOUR 2 is non-polynomial, we may still be able to obtain a polynomial expected-time algorithm for COLOUR provided the failure probability is small enough).

THEOREM 3.4. *COLOUR has expected-time $O(n^2)$ under Model* 1 *with constant k, p.*

Proof. Let T be the running time of COLOUR, T_1 that of COLOUR 1 and T_2 that of COLOUR 2. Let A_i be the event that COLOUR i succeeds $(i = 1, 2)$. Then

$$\begin{aligned} E(T) &\leq T_1 \Pr(A_1) + T_2 \Pr(\overline{A_1 \cap A_2}) + k^{kn} \Pr(\bar{A}_1 \cap \bar{A}_2) \\ &\leq T_1 + T_1 \Pr(\bar{A}_1) + k^{kn} \Pr(\bar{A}_2). \end{aligned}$$

But $T_1 = O(n^2)$, T_2 is polynomial in n, $\Pr(\bar{A}_1) \leq e^{-\sqrt{n}}$, say, and $\Pr(\bar{a}_2) \leq e^{-n \log n}$. Thus $E(T) = T_1 + o(1)$, i.e., $E(T) = O(n^2)$. □

Thus COLOUR is not only polynomial expected-time, but has expected-time linear in the number of edges of G in this model.

A possible criticism of our algorithm might be that p appears to have to be known, since it is used to define r in COLOUR 2. This is not necessary, since all we really require is a good lower bound on p. This can easily be obtained by counting the number of edges in G. If this is M, then for any $\varepsilon > 0$, $M/\left(\binom{k}{2}n^2(1+\varepsilon)\right)$ is a lower bound on p with probability at least $1 - O(e^{-\alpha n^2})$, where $\alpha = \frac{1}{3}\varepsilon^2\binom{k}{2}p$, using the Chernoff bound. Thus the probability of failure of this estimation procedure is small enough that we could afford to handle all graphs where it fails by complete enumeration.

We now "translate" Theorem 3.4 model by model in order to obtain our desired result. Thus we next consider Model 2, in which M inter-block edges are selected at random.

LEMMA 3.5. *COLOUR has $O(n^2)$ expected time behaviour if G is selected using Model 2 with $M = \Omega(n^2)$, k constant and all block sizes $\approx n$.*

Proof. Let $\hat{p} = M/\binom{k}{2}n^2$, then as $n \to \infty$ $\hat{p}$ is bounded below by a constant. Note that Model 2 is equivalent to Model 1 conditional on $|E(G)| = M$. But in Model 1 with $p = \hat{p}$,

$$\Pr(|E(G)| = M) \approx \frac{1}{\sqrt{2\pi\binom{k}{2}n^2\hat{p}(1-\hat{p})}},$$

using Stirling's formula to approximate $B\left(\binom{k}{2}n^2, \hat{p}\right)$. Thus $\Pr(|E(G)| = M) = \Omega(1/n)$. Now, using Lemma 2.1, we see that the events $\bar{A}_i$ of Lemma 3.4 will have essentially the same probabilities. □

We also have

LEMMA 3.6. *In Model 2, under the conditions of Lemma 3.5, the colouring is almost surely unique and the expected number of colourings is $1 + o(1)$.*

Proof. Same as Lemma 3.5 using Theorem 3.1. □

We now turn to Model 3. Here the block sizes are not fixed. Let $n_i = |B_i|$ $(i = 1, \dots, k)$. We then select M edges at random. There are $\binom{\sum_{i<j} n_i n_j}{M}$ ways of selecting M edges. Thus the total number of such graphs is

$$\sum_{\Sigma n_i = N} \frac{N!}{\prod_{i=1}^{k} n_i!} \binom{\sum_{i<j} n_i n_j}{M} = S(N, M), \qquad \text{say.} \tag{3.2}$$

We assume in Model 3 that G is chosen so that all $S(N, M)$ such graphs are equally likely. We first show that restricting to $n_i \approx n$, where $n = N/k$ makes no difference provided $M = \Omega(n^{3/2})$.

Lemma 3.7. *Suppose $|n_i - n| \leq n\ \delta > k$ for any i, then*

$$\frac{N!}{\prod_{i=1}^{k} n_i!}\binom{\sum_{i<j} n_i n_j}{M} < \left(1 - \frac{\delta^2}{k^2}\right)^M \frac{N!}{\prod_{i=1}^{k} t_i!}\binom{\sum_{i<j} t_i t_j}{M},$$

where all $t_i = \lfloor n \rfloor$ or $\lceil n \rceil$ and $\sum_{i=1}^{k} t_i = N$.

Proof. First note $\prod_{i=1}^{k} n_i! \geq \prod_{i=1}^{k} t_i!$ always. Thus it is only necessary to show

$$\binom{\sum_{i<j} n_i n_j}{M} < \left(1 - \frac{\delta^2}{k^2}\right)^M \binom{\sum_{i<j} t_i t_j}{M}.$$

We use the identity

$$\sum_{i<j} n_i n_j = \binom{k}{2} n^2 - \frac{1}{2}\sum_{i=1}^{k} (n_i - n)^2 \tag{3.3}$$

which is easily proved by direct expansion. This implies

$$\sum_{i<j} t_i t_j > \binom{k}{2} n^2 - \frac{1}{2}k, \qquad \text{since } |t_i - n| < 1 \text{ for all } i$$

and

$$\sum_{i<j} n_i n_j < \binom{k}{2} n^2 - \frac{1}{2} n^2 \delta^2,$$

and also

$$\sum_{i<j} n_i n_j \leq \sum_{i<j} t_i t_j.$$

Now observe that if $M \leq A \leq B$ for any integers M, A, B then

$$\binom{A}{M} \leq \left(\frac{A}{B}\right)^M \binom{B}{M}. \tag{3.4}$$

Putting $A = \sum_{i<j} n_i n_j$, $B = \sum_{i<j} t_i t_j$, we have

$$\frac{A}{B} < \frac{\binom{k}{2}n^2 - \frac{1}{2}n^2\delta^2}{\binom{k}{2}n^2 - \frac{1}{2}k} < 1 - \frac{\delta^2}{k^2} \qquad \text{provided } n\delta \geq k. \tag{3.5}$$

The result now follows from (3.4) and (3.5). □

LEMMA 3.8. *In Model* 3, *with* $M = \Omega(n^2)$ *and n large*,

$$\Pr\left(|n_i - n| < n^{3/4},\ i = 1,2,\ldots,k\right) \geq 1 - e^{-n^{4/3}}.$$

Proof. Putting $\delta = n^{-1/4}$ in Lemma 3.7 for large n each term of $S(N, M)$ not satisfying the condition $|n_i - n| < n^{3/4}$ for all i is at most

$$\left(1 - \frac{1}{k^2 n^{1/2}}\right)^{\Omega(n^2)} S(N, M) \leq e^{-\Omega(n^{3/2})} S(N, M).$$

Since there can be at most k^N such terms, the probability that there exists any i such that $|n_i - n| \geq n^{3/4}$ is at most $k^{kn} e^{-\Omega(n^{3/2})} \leq e^{-n^{4/3}}$ for large n. □

THEOREM 3.8. *If* $M = \Omega(n^2)$ *then COLOUR has expected time-complexity* $O(n^2)$ *under Model* 3, *with constant k*.

Proof. The difference between the sample spaces for Models 2 and 3 is an event of probability at most $e^{-n^{4/3}}$ in Model 3. This is sufficiently small that, even if COLOUR used complete enumeration on all graphs in this event, the expected running time would still be $O(n^2)$. □

LEMMA 3.10. *Colourings are almost surely unique in Model* 3, *with expected number* $1 + o(1)$.

Proof. Similar to Theorem 3.9, noting that no graph has more than k^N different colourings. □

Now, in view of Lemma 3.10 and Lemma 2.2, we see that all our results for Model 3 are unaffected if we modify it so that all graphs which do not possess a unique k-colouring are represented only once in the sample space. But this is Model 3′, the uniform distribution on k-colourable graphs with N vertices and M edges. We have, therefore,

THEOREM 3.11. *COLOUR has expected running time* $O(n^2)$ *under the model in which input graphs are chosen at random from the uniform distribution on all k-colourable graphs with N vertices, M edges provided* $M = \Omega(n^2)$.

Moreover, in this model almost all graphs are uniquely colourable, with expected number of colourings $1 + o(1)$.

Proof. Consider, for example, the event $\bar{A}_1$ from Lemmas 3.4, 3.5. Let $\Pr(\bar{A}_1)$ be the probability of $\bar{A}_1$ under Model 3 and $\Pr(\bar{A}_1)$ under Model 3′. Using Corollary 2.3, $\Pr'(\bar{A}_1)/\Pr(\bar{A}_1) \le 1 + o(1)$. Thus $\Pr'(\bar{A}_1) \le e^{-\sqrt{n}}(1 + o(1))$. The other results follow immediately. □

We finally turn to Model 4. We consider the sample space of $T(N) = \Sigma_M S(N, M)$ graphs generated as in Model 3, with all allowable values of M. We select uniformly from these $T(N)$ graphs. This gives Model 4, with Model 4′ then derived by omitting copies of non-uniquely colourable graphs.

LEMMA 3.12. *Let* $M_0 = \frac{1}{2}(k/2)n^2$ *and, for fixed* $\varepsilon > 0$, *let* $Q = \{M | M - M_0| \le \varepsilon M_0\}$. *Then, under Model* 4, $\Pr(M \in Q) < e^{-M_0\varepsilon^{2/3}}$ *for large* n.

Proof.

$$S(N, M) = \sum_{n_i} \frac{N!}{\prod_{i=1}^{k} n_i!} \binom{\sum_{i<j} n_i n_j}{M}$$

$$\le \sum_{n_i} \frac{N!}{\prod_{i=1}^{k} n_i!} \binom{2M_0}{M}, \qquad \text{since } \sum_{i<j} n_i n_j \le 2M_0$$

$$= k^N \binom{2M_0}{M}.$$

Thus

$$\sum_{M \in Q} S(N, M) \le k^N \sum_{M \in Q} \binom{2M_0}{M} = 2k^N \sum_{M < (1-\varepsilon)M_0} \binom{2M_0}{M}$$

$$< 2k^N e^{-\varepsilon^2 M_0/2} 2^{2M_0},$$

using the Chernoff bound.

But $T(N) > (N!(n!)^k)\binom{2M_0}{M_0}$, since this is a term of $S(M_0, N)$. Thus we obtain, using Stirling's approximation $T(N) > (k^N/n^k)2^{2M_0}/(M_0/2)$ for large enough n. Thus $\Pr(M \in Q) = \Sigma_{M \in Q} S(M, N)/T(N) < M_0 n^k e^{-\varepsilon^2 M_0/2} < e^{-\varepsilon^2 M_0/3}$ for large n. □

Thus, the probability that M is far from M_0 is vanishingly small. We use this to establish

THEOREM 3.13. *Under Model 4, COLOUR runs in $O(n^2)$ time. Also colourings are almost surely unique with expected number* $1 + o(1)$.

Proof. Let A be any event in Model 4. Then write $X = |E(G_4)|$. We have

$$\begin{aligned}\Pr(A) &= \sum_{M=0}^{2M_0} \Pr(A|X = M)\Pr(X = M)\\ &= \sum_{M \notin Q} \Pr(A|X = M)\Pr(X = M) + O(e^{-\varepsilon^2 M_0/3})\\ &\qquad\qquad\qquad\qquad \text{using Lemmas 3.12 and 2.1.}\\ &\leq \max_{M \notin Q} \Pr(A|X = M) + O(e^{-\varepsilon^2 M_0/3}).\end{aligned}$$

Thus any event having small probability in Model 3 will have small probability in Model 4. Applying this to the events A_i of Theorem 3.4 or the events of Theorem 3.1 gives the result. □

Finally we transfer this to Model 4′, to give

THEOREM 3.14. *For fixed k, COLOUR runs in $O(N^2)$ expected time under the model in which graphs are selected randomly from the uniform distribution on all k-colourable graphs with N vertices. Moreover, under this model, k-colourings are almost surely unique, with expected number* $1 + o(1)$.

Proof. Follows the same lines as Theorem 3.11. □

4. MINIMUM CUT

We consider the problem of determining the minimum number of edges in a cut which partitions the vertices of a graph into two equal-sized subsets. (See [1].) We will show that we can find, and prove we have found, the minimum cut, in polynomial expected time. Our eventual model here will be the uniform distribution on the set of all graphs G, of a given size $|V(G)|$, which have a "small" cut into two equal subsets, i.e., a cut containing at most $(\frac{1}{2} - \varepsilon)|E(G)|$ edges for some fixed $\varepsilon > 0$.

Again, as in Section 3, we approach this through a sequence of related models. Since some of the methods are similar to Section 3, we will omit details on occasion. Model 1 is the following. Let $V(G) = \{1,2,\dots,2m\}$. Randomly select $A \subseteq V(G)$ with $|A| = m$. Write $B = V - A$. Select, randomly and independently, edges joining vertices of A with those in B with probability p. Similarly, edges joining two vertices of A or B are selected with probabilities p_A, p_B, respectively. We assume $p_A \leq p_B$ without loss, and $2p < (p_A + p_B)$ so that the $A : B$ cut will tend to be small. We will suppose p, p_A, p_B, and $(p_A + p_B - 2p)$ remain bounded below as $m \to \infty$, though many of our results hold with these assumptions relaxed somewhat. We first show that $A : B$ is almost surely the minimum cut.

THEOREM 4.1. *Under Model* 1, $\Pr(A{:}B$ *is uniquely the minimum cut*$) = 1 - o(1)$ *as* $m \to \infty$.

Proof. Let A', B' be an arbitrary cut in G with $|A'| = |B'| = m$. Let $A_1 = A \cap B'$, $B_1 = B \cap B'$, $A_2 = A \cap A'$, $B_2 = B \cap A'$. Write $k = |A_1| = |B_2|$, and assume without loss that $k \leq \frac{1}{2}m$.

Let $\Delta = |A'{:}B'| - |A{:}B|$, so $\Delta < 0$ if $A'{:}B'$ is a smaller cut than $A{:}B$. Now $\Delta = |A_1{:}A_2| + |B_1{:}B_2| - |A_1{:}B_1| - |A_2{:}B_2|$ and $|A_1{:}B_1|$, $|A_2{:}B_2| =^d B(k(m-k), p)$, $|A_1{:}A_2| =^d B(k(m-k), p_A)$, $|B_1{:}B_2| =^d B(k(m-k), p_B)$ are independent random variables.

Thus Δ is a sum of $k(m-k)$ random variables, independently and identically distributed between -2 and $+2$ and having expectation $(p_A + p_B - 2p)$. It follows from Hoeffding [4, Theorem 2] that

$$\Pr(\Delta < 0) \leq e^{-k(m-k)(p_A+p_B-2p)^2/16}.$$

Thus $\Pr(A{:}B$ is not minimum$) \leq \sum_{k=1}^{\lfloor m/2 \rfloor} \binom{m}{k}^2 e^{-k(m-k)\lambda^2}$, where $\lambda = (p_A + p_B - 2p)/4 > 0$. It follows that $\Pr(\Delta < 0) = O(m^2 e^{-m\lambda^2})$ which tends rapidly to zero with m. Note that λ could approach zero as fast as $\sqrt{c \log m/m}$ for any $c > 2$ and the conclusion of the lemma would still hold. □

It is worth noting that when p_A, p_B, p are constant, Theorem 4.1 only guarantees an exponentially small probability that $A{:}B$ is not the minimum cut. It is necessary to take account of this in our algorithm. Our algorithm is again three-phase, similar to that of Section 3.

```
CUT
Apply CUT 1 below to $G$;
If CUT 1 fails to produce a provably minimum cut then apply CUT 2 below to $G$;
If CUT 2 fails to produce the proven minimum then Try all $O(2^{2m})$ equitable cuts and choose
the minimum.
Stop
```

The difference between this and the colouring case will be apparent. We not only have to produce a cut here, but we have to devise a proof procedure which is also fast enough. Thus there are two ways the algorithm can fail at each stage, by failing to find the minimum cut or by finding it and failing to prove it.

```
CUT 1
Choose the vertex $w \in V(G)$ of maximum degree. $W \leftarrow \Gamma(w)$.
for all $v \in V(G)$ do $d(v) \leftarrow \delta_W(v)$;
$k \leftarrow m$th largest $d(v)$;
$C \leftarrow \{v: d(v) \leq k\}$, such that $|C| = m$;
Output cut $C: V - C$
Stop
```

We first note that it is easy to implement CUT 1 to run in $O(|E|) = O(m^2)$ time. It succeeds because W is likely to be large, with $|W \cap A|$ significantly larger than $|W \cap B|$, assuming $w \in A$. Vertices in A will then have significantly larger d values than vertices in B.

LEMMA 4.2. *Under Model* 1, Pr(CUT 1 *finds* $A:B$) $= 1 - O(e^{-\beta m})$ *for some* $\beta > 0$.

Proof. If $a \in A, b \in B$, then $\Pr(\delta_V(a) > \delta_V(b)) \leq e^{-(m-1)(p_B - p_A)^2/4}$ using Hoeffding [4, Theorem 2] in a manner similar to Lemma 4.1. Thus $\Pr(w \notin B) < me^{-(m-1)(p_B - p_A)^2/4}$. Hence if $p_B \neq p_A$, we may assume that $w \in B$, since this failure probability is small enough. If $p_B = p_A$ we will assume without loss that $w \in B$.

Now for any $a \in A$, $b \in B$, let us suppose at first that $w \in B$ is chosen arbitrarily, so G is unconditioned by this step. Let $t = \frac{1}{2}(p^2 + p_B^2 - pp_A - pp_B)) \geq \frac{1}{8}(p_A + p_B - 2p)^2 > 0$.

Now, again using Hoeffding's Theorem 2,

$$\Pr(\delta_W(a) > m(pp_A + pp_B + t)) < 2e^{-mt^2/4}$$

and

$$\Pr\big(\delta_W(b) < m\big(p^2 + p_B^2 - t\big)\big) < 2e^{-mt^2/4}.$$

Thus $\Pr(\exists a \in A: \delta_W(a) > m(pp_A + pp_B + t)) < 2me^{-mt^2/4}$ and $\Pr(\exists b \in B: \delta_W(b) < m(p^2 + p_B^2 - t)) < 2me^{-mt^2/4}$. Hence, using the value of t,

$$\Pr\big(\exists a \in A, b \in B: \delta_W(a) > \delta_W(b)\big) < 4me^{-mt^2/4}.$$

Finally, $\Pr(\exists a \in A; b, w \in B: \delta_W(a) > \delta_W(b)) < 4m^2e^{-mt^2/4}$. Thus, almost surely $C \leftarrow A$ in CUT 1. □

We note in passing that the threshold for success in CUT 1 could be reduced to $(p_A + p_B - 2p) = 5(\log m/m)^{1/4}$ by the same calculation.

Before turning to the optimality-verification algorithm associated with CUT 1, we will describe CUT 2, which does more work but has a higher probability of success. For constant p_A, p_B, p, it is possible to derive such an algorithm which works in polynomial time by a similar method to COLOUR 2 of Section 3. There is a technical problem with lack of independence if we proceed in exactly the same manner, but we can resolve this as follows. We randomly split the graph into two $O(m)$ times. With high probability one such split will contain exactly half of A and half of B in each half of the split. For each split we take repeated "small" random subsets from each half. We use the random subsets to determine the A: B partition of the other half of the split by counting degrees in the subset of external vertices. The "partition" argument used to justify COLOUR 2 can now be used to show a high probability of success in polynomial time. However, we will not do this here, for two reasons. First, our proof procedure in this case does not work in polynomial time and hence there is little advantage when we require proof of optimality. Second, the above-outlined procedure requires knowledge of p_A, p_B, p, and, unlike COLOUR 2, we cannot give a simple estimation procedure, with a high enough success probability, for these parameters. Thus the procedure we describe is rather crude, but nonetheless effective. It randomly chooses a set U of size $m^{2/3}$ and checks each possibility for $U \cap A, (X =)U \cap B$, by complete enumeration. The great majority of vertices in B should then have a high value of $\delta_X(v)$, and so the vertices with the $m - |X|$ largest δ_X values are added to X to produce C (our guess for B). There is then a final check to account for a few "misplaced" vertices.

```
CUT 2
min ← $\infty$;
repeat $m^2$ times
 begin
  Select a random subset $U \subseteq V(G)$ with $|U| = \lceil m^{2/3} \rceil$
 for each subset $X \subseteq U$ do
 begin
  for each $v \in V - U$ do $d(v) \leftarrow \delta_X(v)$ od
  $k \leftarrow (m - |X|)$th largest value of $d(v)$
  $C \leftarrow \{v : d(v) \geq k\} \cup X$, such that $|C| = m$; $\bar{C} \leftarrow V - C$;
  for each subset $Y \subseteq C$ with $|Y| \leq 2\lceil m^{2/3} \rceil$ do
  begin
   for each subset $\bar{Y} \subseteq \bar{C}$ with $|\bar{Y}| = |Y|$ do
   $C' \leftarrow (C - Y) \cup \bar{Y}$
   $\bar{C}' \leftarrow (\bar{C} - \bar{Y}) \cup Y$
   if $|C' : \bar{C}'| <$ min then
   begin
    $C_0 \leftarrow C'$, min $\leftarrow |C' : \bar{C}'|$
   end
  end
 end
end
Output $C_0 : V - C_0$
Stop
```

The running time of CUT 2 is $O(2^{\lceil m^{2/3}\rceil}\binom{m}{2\lceil m^{2/3}\rceil}^2 m^p)$ for some integer constant $p > 0$. This is $O(2^{m^{3/4}})$.

LEMMA 4.3. *Under Model* 1, Pr(CUT 2 *fails to find the minimum cut*) $= O(e^{-m^{5/4}})$.

Proof. Suppose $A': B'$ is the minimum cut. First observe that the probability that $A':B'$ differs greatly from $A:B$ is very small. Suppose $|A_1| = |A \cap B'| > m^{2/3}$, then the proof of Theorem 4.1 shows

$$\Pr\left(|A_1| > m^{2/3}\right) \le \sum_{k=\lceil m^{2/3}\rceil}^{\lfloor m/2\rfloor} \binom{m}{k}^2 e^{-k(m-k)\lambda^2},$$

where $\lambda = (p_A + p_B - p)/4 > 0$. Thus,

$$\Pr\left(|A_1| > m^{2/3}\right) = O\left(e^{-m^{3/2}}\right), \qquad \text{say.}$$

Now the probability that CUT 2 fails to produce some subset U with $|U \cap B| \ge \lceil \frac{1}{2}m^{2/3}\rceil$ is $O(2^{-m^2})$ in view of the m^2 repetitions. Thus we may suppose that CUT 2 determines some X with $X \subseteq B$ and $|X| \ge \lceil \frac{1}{2}m^{2/3}\rceil$. Let $0 < \varepsilon < (p_B - p)/(p_B + p)$. Then, using the Chernoff bound, for any $a \in A - U, b \in B - U$,

$$\Pr\left(\delta_X(a) > (1+\varepsilon)|X|p\right) < e^{-m^{2/3}\varepsilon^2 p/6}$$

$$\Pr\left(\delta_X(b) < (1-\varepsilon)|X|p_B\right) < e^{-m^{2/3}\varepsilon^2 p_B/4}$$

and these are independent for all such a, b.

Let $S = \{a \in A - U: \delta_X(a) > (1+\varepsilon)|X|p\}$, $T = \{b \in B - U: \delta_X(b) < (1-\varepsilon)|X|p_B\}$ then $\Pr(|S| > m^{2/3}) < \binom{m}{\lceil m^{2/3}\rceil} e^{-m^{4/3}\varepsilon^2 p/6} = O(e^{-m^{5/4}})$. Similarly, $\Pr(|T| > m^{2/3}) = O(e^{-m^{5/4}})$.

Let E_1 be the event that the vertices with the $(m - |X|)$ largest values of $d(v)$ in CUT 2 contain more than $m^{2/3}$ from A. Since by choice of ε, $(1-\varepsilon)|X|p_B > (1+\varepsilon)|X|p$, $E_1 \subseteq (|S| > m^{2/3}) \cup (|T| > m^{2/3})$. Hence, $\Pr(E_1) = O(e^{-m^{5/4}})$.

Now let E_2 be the event that C contains more than $m^{2/3}$ vertices from A. Since $X \subseteq B$, we have $\Pr(E_2) = O(e^{-m^{5/4}})$. Thus, with probability $1 - O(e^{-m^{5/4}})$, we find a set C which differs from B by at most $m^{2/3}$ vertices. But B' differs from B by at most $m^{2/3}$ vertices with probability $1 - O(e^{-m^{3/2}})$. Thus we have $C' \leftarrow B'$ at some stage in CUT 2 with probability $1 - O(e^{-m^{5/4}})$. □

We now turn to proving optimality. We first consider CUT 1.

THEOREM 4.4. *Let $\beta < 1$ be chosen arbitrarily. There exists an $O(m^3)$ time deterministic algorithm which*

(i) *has failure probability $O(e^{-m^\beta})$ under Model* 1;

(ii) *if it succeeds, constructs a correct proof of optimality for the cut produced by* CUT 1.

Proof. The algorithm is quite simple, and will be described informally in our proof. First, in calculating probabilities we may assume that CUT 1 finds $A{:}B$, by Lemma 4.2. Thus in the following $A{:}B$ means the cut produced by CUT 1, but will mean the underlying cut $A{:}B$ where probability calculations are involved.

We split the argument into two cases. Let $A'{:}B'$ be any cut, and let other quantities be as defined in the proof of Theorem 4.1. The two cases are then as follows:

Let $0 < \gamma < \frac{1}{2}(1 - \beta)$ and $1 - \frac{1}{2}\gamma < \alpha < 1$ be chosen.

(i) $k = |A_1| = |B_2| \leq m^\alpha$

(ii) $m^\alpha < k \leq \frac{1}{2}m$.

Define the following quantities:

$$\bar{p}_A = \min_{v \in A} \delta_A(v)/m, \ \bar{p}_B = \min_{v \in B} \delta_B(v)/m,$$

$$\bar{p} = \min\left\{\min_{v \in A} \delta_B(v), \min_{v \in B} \delta_A(v)/m\right\}$$

$$\bar{p}' = \max\left\{\max_{v \in A} \delta_B(v), \max_{v \in B} \delta_A(v)/m\right\}.$$

Case (i). We consider $\Delta = |A_1{:}A_2| + |B_1{:}B_2| - |A_1{:}B_1| - |A_2{:}B_2|$. However, $|A_1{:}A_2| \geq \Sigma_{v \in A_1} \delta_A(v) - 2\binom{k}{2} \geq km\bar{p}_A - k(k-1)$. Similarly, $|B_1{:}B_2| \geq km\bar{p}_B - k(k-1)$. Also $|A_1{:}B_1| \leq \Sigma_{v \in A_1} \delta_B(v) \leq km\bar{p}'$ and $|A_2{:}B_2| \leq km\bar{p}'$. Hence $\Delta \geq k(m(\bar{p}_A + \bar{p}_B - 2\bar{p}') - 2(k-1)) > 0$ provided

$$k < k_1 = \left\lceil \tfrac{1}{2}m(\bar{p}_A + \bar{p}_B - 2\bar{p}') + 1 \right\rceil.$$

We can compute k_1 in $O(m^3)$ time by straightforward vertex-counting. Let $0 < \varepsilon < (p_A + p_B - 2p)/(p_A + p_B + 2p)$. Then a standard argument using the Chernoff bound shows that

$$k_1 > \tfrac{1}{2}m((1-\varepsilon)p_A + (1-\varepsilon)p_B - 2(1+\varepsilon)p) = \Omega(m)$$

with probability $1 - O(e^{-c_1 m})$ for some $c_1 > 0$. Thus $k_1 > m^\alpha$ with high enough probability for the conclusion of the theorem.

Case (ii). We make use of some recent results of Thomason [6, 7] on "jumbled" or "pseudo-random" graphs. By a straightforward calculation using the Chernoff bound, we know that, with probability $1 - O(e^{-m^\beta})$,

$$\delta_A(a) \geq mp_A\left(1 - \tfrac{1}{5}m^{-\gamma}\right) \qquad \text{for all } a \in A$$

and

$$\delta_A(a_1, a_2) \leq mp_A^2\left(1 + \tfrac{1}{5}m^{-\gamma}\right) \qquad \text{for all } a_1, a_2 \in A.$$

We are using the notation $\delta_A(a_1, a_2)$ to denote the number of common neighbours of a_1, a_2 in A, i.e., $\delta_A(a_1, a_2) = |\Gamma(a_1) \cap \Gamma(a_2) \cap A|$. Thus, with probability $1 - O(e^{-m^\beta})$, $\bar{p}_A \geq p_A(1 - \frac{1}{5}m^{-\gamma})$ and hence

$$\delta_A(a_1, a_2) \leq m\bar{p}_A^2(1 + m^{-\gamma}) \leq m\bar{p}_A^2 + m^{1-\gamma}.$$

Consider these two properties of the graph $G[A]$:

(a) $\delta_A(a) \geq m\bar{p}_A$. This always holds, by choice of $\bar{p}_A$, for all $a \in A$.

(b) $\delta_A(a_1, a_2) \leq m\bar{p}_A^2 + m^{1-\gamma}$. This holds, with probability $1 - O(e^{-m^\beta})$, for all pairs $a_1, a_2 \in A$.

The condition (b) can be checked in $O(m^3)$ time by edge-counting. If it fails for any pair a_1, a_2 we report failure of the proof procedure.

Now conditions (a), (b) imply, by Theorem 1.1 of [6], that all subgraphs of $G[A]$ have approximately the number of edges we would expect if $G[A]$ were a random graph with edge probability $\bar{p}_A$. Specifically, if H is a subgraph of $G[A]$ with h vertices and e edges,

$$\begin{aligned} \left|e - \bar{p}_A\binom{h}{2}\right| &\leq \left(\left(m\bar{p}_A + (m-1)m^{1-\gamma}\right)^{1/2} + \bar{p}_A\right)h \\ &\leq 2m^{1-\gamma/2}h \qquad \text{for } m \geq 4. \end{aligned} \tag{4.1}$$

A similar conclusion holds for $G[B]$, using $\bar{p}_B$. For the bipartite graph $G[A,B]$ with edge set $A{:}B$ we also have analogous properties to (a), (b) above, using $\bar{p}$. Note that all these conditions, for $G[A]$, $G[B]$, and $G[A, B]$, can be checked in $O(m^3)$ time, and if the condition (b) fails for any pair of vertices we report failure of our proof procedure. The failure probability thus far is clearly $O(e^{-m^\beta})$.

Now, for $G[A, B]$ another theorem of Thomason [7] then implies that for any bipartite subgraph $G[X, Y]$ of $G[A, B]$ with $|X| = x$, $|Y| = y$

and $|X:Y| = e$,

$$\begin{aligned}|e - \bar{p}xy| &\leq x\left(\frac{y(m-y)}{mx}\left(m^{1-\gamma}(x-1) + \bar{p}(1-\bar{p})m\right)\right)^{1/2}\\ &\leq x\left(\frac{m^{2-\gamma}}{4} + \frac{m^2}{16x}\right)^{1/2}\\ &\leq xm^{1-\gamma/2} \qquad \text{if } x > m^{\gamma},\end{aligned} \tag{4.2}$$

which is certainly true if $x > m^{1-\gamma/2}$, which is the case we shall require.

Now from (4.2), we obtain, putting $X = A_1$, $Y = B_1$,

$$\begin{aligned}|A_1:B_1| &\leq k(m-k)\bar{p} + km^{1-\gamma/2}\\ &\leq k(m-k)\bar{p} + \tfrac{1}{2}m^{2-\gamma/2}, \text{ since } k \leq \tfrac{1}{2}m.\end{aligned} \tag{4.3}$$

Similarly,

$$|A_2:B_2| \leq k(m-k)\bar{p} + \tfrac{1}{2}m^{2-\gamma/2}. \tag{4.4}$$

Writing $E(X)$ for the edge set of $G[X]$ we have, from (4.1),

$$|E(A_1)| \leq \binom{k}{2}\bar{p}_A + 2km^{1-\gamma/2} \leq \binom{k}{2}\bar{p}_A + m^{2-\gamma/2}$$

$$|E(A_2)| \leq \binom{m-k}{2}\bar{p}_A + 2(m-k)m^{1-\gamma/2} \leq \binom{m-k}{2}\bar{p}_A + 2m^{2-\gamma/2}.$$

Also $|E(A)| \geq \binom{m}{2}\bar{p}_A$, always. Thus

$$|A_1:A_2| = |E(A)| - |E(A_1)| - |E(A_2)| \geq k(m-k)\bar{p}_A - 3m^{2-\gamma/2}. \tag{4.5}$$

Similarly,

$$|B_1:B_2| \geq k(m-k)\bar{p}_A - 3m^{2-\gamma/2}. \tag{4.6}$$

Hence from (4.3)–(4.6) we get

$$\Delta \geq k(m-k)(\bar{p}_A + \bar{p}_B - 2\bar{p}) - 7m^{2-\gamma/2} \tag{4.7}$$

from which it follows that $\Delta > 0$ if

$$k > k_2 = \frac{1}{2}m\left(1 - \sqrt{1 - \frac{7}{\lambda m^{\gamma/2}}}\right),$$

where $\bar{\lambda} = (\bar{p}_A + \bar{p}_B - 2\bar{p})/4 > 0$. (If $\bar{\lambda} \le 0$ we report failure of the proof procedure.)

Note that

$$k_2 = \frac{7m^{1-\gamma/2}}{2\bar{\lambda}} \bigg/ \left(1 + \sqrt{1 - \frac{7}{\bar{\lambda} m^{\gamma/2}}}\right).$$

and can be evaluated in $O(m^2)$ time, the main task being the evaluation of $\bar{p}_A, \bar{p}_B, \bar{p}$.

Again a standard calculation shows that $\bar{\lambda} = \Omega(1)$ with probability $1 - O(e^{-c_2 m})$ for some $c_2 > 0$. Thus, with probability $1 - O(e^{-c_2 m})$, $k_2 = O(m^{1-\gamma/2})$ so $k_2 = o(m^\alpha) = o(k_1)$. Thus there will be no values of k for which $A' : B'$ could be better than $A : B$ with probability $1 - O(e^{-m^\beta})$ as required.

Algorithmically, we must determine k_1, k_2 and check that $k_1 > k_2$ in $O(m^2)$ time. In addition, we must check the conditions (b) above for $G[A]$, $G[B]$, and $G[A, B]$ in $O(m^3)$ time. Thus we have established the claims of the theorem. □

Thus, to summarise, CUT 1 and its proof procedure take $O(m^3)$ time and have failure probability $O(e^{-m^\beta})$ for any $\beta < 1$. We now turn to CUT 2.

THEOREM 4.5. *There exists an* $O(2^{m^{3/4}})$ *time deterministic algorithm which*

(i) *has failure probability* $O(e^{-m^{5/4}})$ *under Model* 1,

(ii) *and, if it succeeds, constructs a proof of optimality for the cut produced by* CUT 2.

Proof. Again we will describe the algorithm informally with our proof. First, we may assume that the cut $A^* : B^*$, say, produced by CUT 2 is optimal, by Lemma 4.3. Second, we may assume that $|A \cap B^*| < m^{1/3}$ with the requisite probability—see Lemma 4.3.

We start the proof procedure by enumerating all cuts with $|A^* \cap B'| \le m^{2/3}$ and counting the number of edges in each cut. We can do this in $O(m^2 \binom{m}{\lceil m^{2/3} \rceil}^2) = O(2^{m^{3/4}})$ time, as in CUT 2.

If we find a better cut than $A^* : B^*$ we report failure for the proof procedure. Otherwise we know that any better cut $A' : B'$ must have $|A^* \cap B'| > m^{2/3}$. We continue by selecting all possible pairs of disjoint subsets $S_1, S_2 \subseteq A^*$ such that $\frac{1}{2}\lceil m^{2/3} \rceil \le |S_i| \le \lceil m^{2/3} \rceil$, $i = 1, 2$. Let

$$\hat{p}_A = \min_{S_1, S_2} |S_1 : S_2| / (|S_1| \cdot |S_2|).$$

This can be calculated in $O(m^2 \binom{m}{\lceil m^{2/3} \rceil}^2) = O(2^{m^{3/4}})$ time. Similarly, we calculate $\hat{p}_B$ by choosing $S_1, S_2 \subseteq B^*$. We also determine, by choosing $S_1 \subseteq A^*, S_2 \subseteq B^*$,

$$\hat{p} = \max_{S_1, S_2} |S_1 : S_2| \big/ (|S_1| \cdot |S_2|).$$

The total time for these computations is $O(2^{m^{3/4}})$. Now each $S_i \subseteq A^*$ $(i = 1, 2)$ contains, with the required probabilty, at least $(|S_i| - m^{1/3})$ vertices from A. Thus $S_1 : S_2$ contains $\hat{p}_A |S_1| \cdot |S_2|(1 - o(1))$ edges from $G[A]$. Hence

$$\begin{aligned} \Pr(\exists S_1, S_2 \subseteq A^* : |S_1 : S_2| &< (1 - \varepsilon) p_A |S_1| \cdot |S_2|) \\ &< \binom{m}{\lceil m^{2/3} \rceil}^2 e^{-\varepsilon^2 m^{4/3} p_A / 16} \text{ for large } m, \end{aligned}$$

and hence,

$$\Pr(\hat{p}_A < p_A(1 - m^{-\alpha})) < e^{-m^{5/4}} \qquad \text{for } \alpha < \tfrac{1}{24}.$$

A similar lower bound on $\hat{p}_B$ and upper bound on $\hat{p}$ can be derived, with the same probability.

Now, letting $A_1 = A^* \cap B'$ etc., in notation similar to the proof of Theorem 4.1, but with $A^* : B^*$ playing the role of $A : B$, for some disjoint sets S_i $(i \in I)$, we have $A_1 = \bigcup_{i \in I} S_i$ with $\frac{1}{2}\lceil m^{2/3} \rceil \leq |S_i| \leq \lceil m^{2/3} \rceil$, since $|A_1| > m^{2/3}$.

Also, similarly, $A_2 = \bigcup_{j \in J} S_j'$ with $\frac{1}{2}\lceil m^{2/3} \rceil \leq |S_j'| \leq \lceil m^{2/3} \rceil$, since $|A_2| \geq \frac{1}{2}m$. Hence

$$\begin{aligned} |A_1 : A_2| &= \sum_{i \in I} \sum_{j \in J} |S_i : S_j'| \geq \sum_{i \in I} \sum_{j \in J} \hat{p}_A |S_i| \cdot |S_j'| \\ &= \hat{p}_A \sum_{i \in I} |S_i| \cdot \sum_{j \in J} |S_j'| = \hat{p}_A |A_1| \cdot |A_2| \end{aligned}$$

Similarly, $|B_1 : B_2| \geq \hat{p}_B |B_1| \cdot |B_2| = \hat{p}_B |A_1| \cdot |A_2|$. Also $|A_i : B_i| \leq \hat{p} |A_i| \cdot |B_i| = \hat{p} |A_1| \cdot |A_2|$ $(i = 1, 2)$, by similar reasoning. Hence $\Delta \geq |A_1| \cdot |A_2|(\hat{p}_A + \hat{p}_B - 2\hat{p}) > 0$, provided $\hat{p}_A + \hat{p}_B - 2\hat{p} > 0$. Thus the proof of optimality now simply involves checking whether $\hat{p}_A + \hat{p}_B > 2\hat{p}$. If so, we have proved the optimality of $A^* : B^*$. Otherwise, we report failure. Now, with probability $1 - O(e^{-m^{5/4}})$,

$$\begin{aligned} \hat{p}_A + \hat{p}_B - 2\hat{p} &> p_A(1 - m^{-\alpha}) + p_B(1 - m^{-\alpha}) \\ &\qquad -2p(1 + m^{-\alpha}) \qquad \text{for } \alpha < \tfrac{1}{24} \\ &> 0 \qquad\qquad\qquad\qquad \text{for large } m. \end{aligned}$$

Thus CUT 2 and its proof procedure require $O(2^{m^{3/4}})$ time and have failure probability $O(e^{-m^{5/4}})$. □

THEOREM 4.6. *Under Model* 1, CUT *and its proof procedures run in* $O(m^3)$ *expected time.*

Proof. From Theorem 4.1, Lemmas 4.2 and 4.3, and Theorems 4.4 and 4.5, if T is the running time, then

$$\begin{aligned} E(T) &\le O(m^3) + O(2^{m^{3/4}}) \cdot O(e^{-m^{\beta}}) + O(2^{2m}) \cdot O(e^{-m^{5/4}}) \\ &= O(m^3) \qquad \text{choosing } \beta > 3/4. \ \square \end{aligned}$$

We now go through our "result translation" procedure. We first consider Model 2 for this problem; we randomly select A, B as in Model 1. Then we randomly select M_A edges between vertices of A, M_B between vertices of B, and M between A and B. We require the existence of a constant C such that M, M_A, M_B, and $M_A + M_B - M \ge Cm^2$ for all large enough m.

LEMMA 4.7. *Under Model* 2, CUT *and its proof procedures run in* $O(m^3)$ *expected time. Moreover, for some* $\beta > 0$, *the minimum cut is unique with probability* $1 - O(e^{-\beta m})$.

Proof. Set $\hat{p}_A = M_A/\binom{m}{2}$, $\hat{p}_B = M_B/\binom{m}{2}$, $\hat{p} = M/m^2$. Then the existence of C implies that $\hat{p}_A$, $\hat{p}_B$, $\hat{p}$, and $\hat{p}_A + \hat{p}_B - 2\hat{p}$ are bounded away from zero. We now use the same method of proof as in Lemmas 3.5 and 3.6. □

Model 3 is now the following. We allow M_A, M_B, M (as in Model 2) to vary, but we require the existence of a constant $\delta > 0$ such that $M_A + M_B \ge (1 + \delta)M$. Then all graphs which can be chosen in this way are equally likely. Let

$$S(M) = \sum_{M_A + M_B \ge (1+\delta)M} \binom{\binom{m}{2}}{M_A}\binom{\binom{m}{2}}{M_B},$$

$$T' = \sum_{M=0}^{m^2} \binom{m^2}{M} S(M) \qquad \text{and} \qquad T = \binom{2m}{m} T'.$$

Then Model 3 selects from the uniform distribution on a sample space of T graphs.

LEMMA 4.8. *Let E be the event that a graph selected randomly according to Model* 3 *fails to satisfy the conditions of Model* 2 *with*

$$C = \frac{1}{16}\min\left\{\frac{1}{8}, \frac{\delta}{1+\delta}\right\}.$$

Then, for some $\gamma > 0$, $\Pr(E) = O(e^{-\gamma m^2})$.

Proof. Let $M_0 = \left\lfloor \frac{1}{2}\binom{m}{2}/(1+\delta) \right\rfloor$ and $S' = 2^{m(m-1)}$. Then it is easily shown that $\frac{3}{4}S' \leq S(M) \leq S'$ for $M \leq M_0$. Then

$$\sum_{M=0}^{\lfloor M_0/2 \rfloor} \binom{m^2}{M_0} S(M) < S' \binom{m^2}{M_0} 3^{-M_0/2}$$

by a straightforward calculation. But

$$T' > \binom{m^2}{M_0} S(M_0) \geq \binom{m^2}{M_0} \frac{3}{4} S'.$$

Hence $\Pr(M \leq \frac{1}{2}\mathrm{M}_0) < \frac{4}{3}3^{-M_0/2}$. Thus $M \geq \frac{1}{8}m(m-1)/(1+\delta)$ with probability $1 - O(e^{-\gamma_1 m^2})$ for some $\gamma_1 > 0$. Hence $M_A + M_B \geq \frac{1}{8}m(m-1)$ and $M_A + M_B - M \geq \delta m(m-1)/\delta(1+\delta)$. Thus for $m \geq 2$, M and $M_A + M_B - M$ satisfy the conditions of Model 2 with $C = \delta/16(1+\delta)$. Let

$$H(K) = \sum_{M_A=0}^{K} \binom{\binom{m}{2}}{M_A} \binom{\binom{m}{2}}{K - M_A},$$

so $S(M) = \sum_{k=\lceil(1+\delta)M\rceil}^{m(m-1)} H(K)$.

Now for $k \geq \frac{1}{8}m(m-1)$, it is straightforward to show that if

$$H'(K) = \sum_{M_A=\lceil K/8 \rceil}^{\lfloor 7K/8 \rfloor} \binom{\binom{m}{2}}{M_A} \binom{\binom{m}{2}}{K - M_A},$$

then

$$\begin{aligned} H(K) &= H'(K)\left(1 + O(6^{-K/8})\right) \\ &= H'(K)\left(1 + O(e^{-\gamma_2 m^2})\right) \qquad \text{for some } 0 < \gamma_2 < \gamma_1. \end{aligned}$$

It follows that $\Pr(M_A < \frac{1}{64}m(m-1)) = O(e^{-\gamma_2 m^2})$, and similarly for M_B. Thus M_A, M_B satisfy the conditions of Model 2, with $C = \frac{1}{128}$, for $m \geq 2$. Thus

$$C = \min\left\{\frac{1}{128}, \frac{\delta}{16(1+\delta)}\right\}$$

and $\gamma = \gamma_2$ satisfy the lemma. □

THEOREM 4.9. *Under Model* 3, CUT *and its proofs run in* $O(m^3)$ *expected time, and the cut is unique with probability* $1 - O(e^{-\beta m})$ *for* $\beta > 0$.

Proof. Follows directly from Lemma 4.8 and Lemma 4.7 in the same way as Theorem 3.12 was proved. □

Model 3′ is now Model 3 with copies of the same graph deleted. Note that the condition $M_A + M_B \geq (1 + \delta)M$ is equivalent to $M \leq 1/(2 + \delta)|E(G)| = (\frac{1}{2} - \varepsilon)|E(G)|$ for $\varepsilon = \delta/(2 + \delta)$.

THEOREM 4.10. *For $\varepsilon > 0$, let G_ε be the set of all $2m$-vertex graphs for G possessing an equitable cut of size at most $(\frac{1}{2} - \varepsilon)|E(G)|$. Then, if G is chosen uniformly from G_ε,* CUT *and its proof procedures run in $O(m^3)$ expected time and the minimum cut is almost surely unique.*

Proof. Follows from Theorem 4.9, by the same method of proof as Theorem 3.10. □

This result is that claimed in the introduction to this section. By refining the analysis it would appear that we could let ε tend slowly to zero as $m \to \infty$ and Theorem 4.10 would remain true. However, we will not consider this further here.

5. Graph Partitioning

We consider the following problem. Let $\mathscr{C}_A, \mathscr{C}_B$ be two classes of graphs which

(i) can be recognised in polynomial time. For simplicity below we will assume recognition in time $O(m^2/\log m)$. Otherwise the running time of our algorithms is dominated by the recognition steps.

(ii) have $|E(G)| < c|V(G)|$ for all $G \in \mathscr{C}_A, \mathscr{C}_B$ and some constant c. (We could assume different c_A, c_B but then obviously $c = \max(c_A, c_B)$ suffices.)

Thus $\mathscr{C}_A, \mathscr{C}_B$ could be, for example, trees ($c = 1$), planar graphs ($c = 3$), or $2c$-regular graphs. These can all be recognised in $O(m)$ time if $m = |V(G)|$.

We are given a graph G with $|V(G)| = 2m$ and the problem is to partition $V(G)$ into subsets A, B with $|A| = |B| = m$ such that $G[A] \in \mathscr{C}_A, G[B] \in \mathscr{C}_B$, or prove that this is impossible. For most common classes, $\mathscr{C}_A, \mathscr{C}_B$ this problem is NP-hard. See Dyer and Frieze [2] for further information.

Here we will prove the following. Let Γ be the class of $2m$-vertex graphs which have a partition into $G_A \in \mathscr{C}_A, G_B \in \mathscr{C}_B$. Then, if G is chosen uniformly at random from Γ, we can partition G into graphs $G'_A \in \mathscr{C}_A, G'_B \in \mathscr{C}_B$ in $O(m^3)$ expected time. Note that the partition is not always unique here, but we will show that there are almost always $O(1)$ such partitions.

Again we approach this result through a sequence of models. Model 1 is the following: We have an arbitrary $G_A \in \mathscr{C}_A$, $G_B \in \mathscr{C}_B$, with $|V(G_A)| = |V(G_B)| = m$. The vertices of $V(G_A) \cup V(G_B)$ are labelled as a random permutation of $\{1, 2, \ldots, 2m\}$. Thus we may take $A = V(G_A)$, $B = V(G_B)$, where A, B are as in Section 4. We will write $G_A = (A, E_A)$, $G_B = (B, E_B)$. Now, for p constant, we randomly select the edges in $A : B$, with probability p, from the m^2 possible edges.

Consider the following algorithm. The idea behind it is to guess an edge (s, t) with $s \in A$, $t \in B$ and decide whether $v \in A$ or $v \in B$ by counting neighbours in $\Gamma(s)$, $\Gamma(t)$. Apart from a few vertices (U) with large degree in their own graphs, this is likely to yield a correct decision. Then U can be dealt with by enumeration, provided it is small.

```
FIND 1
Determine the average degree $\bar{d}$ in $G$.
$U \leftarrow \{v \in V: \delta_V(v) > \bar{d}(1 + \bar{d}/4m)\}$
if $|U| \geq \log\log m$ then FIND 1 fails else
begin
 select $Z \subseteq E(G)$ with $|Z| = m$ at random;
 for each edge $(s, t) \in Z$ do
 begin
  $S \leftarrow \Gamma(s)$; $T \leftarrow \Gamma(t)$; $X \leftarrow S - T, Y \leftarrow T - S$
  for each $v \notin S \cup T$ do
  begin
   determine $\delta_S(v)$; $\delta_T(v)$;
   if $\delta_S(v) < \delta_T(v)$ then $X \leftarrow X \cup \{v\}$ else $Y \leftarrow Y \cup \{v\}$
  end;
  for each $v \in S$ do
  begin
   if $\delta_Y(v) < \delta_X(v)$ then $X \leftarrow X - \{v\}$, $Y \leftarrow Y \cup \{v\}$
  end;
  for each $v \in T$ do
  begin
   if $\delta_X(v) < \delta_Y(v)$ then $Y \leftarrow Y - \{v\}$, $X \leftarrow X \cup \{v\}$
  end;
  $X \leftarrow X - U$, $Y \leftarrow Y - U$;
  for each $W \subseteq U$ with $|W| = m - |X|$ do
  begin
   $X_1 \leftarrow X \cup W$; $Y_1 \leftarrow Y \cup (U - W)$;
   if $G[X_1] \in \mathscr{C}_A, G[Y_1] \in \mathscr{C}_B$
   or $G[Y_1] \in \mathscr{C}_A, G[X_1] \in \mathscr{C}_B$
   then output partition, stop {success}
  end
 end
end
Stop Find 1 has failed.
```

The time-complexity of FIND 1, implemented in a straightforward manner is easily checked to be $O(m^3)$.

THEOREM 5.1. *Under Model* 1, Pr(FIND 1 *fails*) $= O(e^{-m^\beta})$ *for any* $\beta < 1$.

Proof. Fix β and let $0 < \gamma < \frac{1}{2}(1-\beta)$. Then for $v \in A, \delta_V(v) \geq mp(1 - m^{-\gamma}) + \delta_A(v)$ with probability $1 - O(e^{-m^\beta})$ and similarly for $v \in B$. Thus $\bar{d} \geq mp(1 - m^{-\gamma}) + 2c$ with probability $1 - O(e^{-m^\beta})$.

Also for $v \in A$, $\delta_V(v) \leq mp(1 + m^{-\gamma}) + \delta_A(v)$ with similar probability. Thus, almost surely, $\delta_V(v) \geq \bar{d}(1 + \bar{d}/2m)$ implies

$$\begin{aligned} &mp(1 + m^{-\gamma}) + \delta_A(v) \\ &\qquad \geq (mp(1 - m^{-\gamma}) + 2c)\left(1 + \tfrac{1}{2}p(1 - m^{-\gamma}) + \frac{c}{m}\right), \end{aligned}$$

i.e.,

$$\delta_A(v) \geq \tfrac{1}{2}mp^2(1 - o(1)).$$

So for large m, certainly $\delta_A(v) > \frac{1}{3}mp^2$. Similarly for $v \in B$. Thus U contains only vertices with degree at least $\frac{1}{3}mp^2$ in their own graph G_A or G_B, except for probability $O(e^{-m^\beta})$. However, since G_A, G_B have at most cm edges, it follows by simple counting that $|U| < 12c/p^2$ almost surely, and hence $|U| < \log\log m$.

Now, again by counting, G_A, G_B have at least $\lceil \frac{1}{2}m \rceil$ vertices each of degree at most $4c$. Thus, with probability $1 - O(e^{-m^\beta})$ there are at least $\frac{1}{4}m^2p(1 - o(1))$ edges joining vertices of degree at most $4c$ in their own graphs. Since G has at most $m^2(1 + o(1))$ edges altogether, the probability that Z fails to contain an edge joining two vertices of degree at most $4c$ is $O(e^{-mp/4})$, by a straightforward calculation. Therefore we can assume FIND 1 (if it has not already partitioned G) discovers an edge $(s, t) \in Z$ with $s \in A$, $t \in B$, and $\delta_A(s), \delta_B(t) \leq 4c$.

However, the probability that for any $a \in A, \delta_B(a) < \frac{2}{3}mp$ is $O(e^{-m^\beta})$ and similarly for $\delta_A(b), b \in B$. Thus S almost surely contains at least $\frac{2}{3}mp$ vertices in B and at most $4c$ in A. Similarly for T. Now consider $v \notin S \cup T$. If $v \in A$ then, since the edges adjacent to v are unconditioned (except for $(v, t) \notin E(G)$), we have $\delta_S(v) \geq \frac{4}{9}mp^2$ with the required probability and $\delta_T(v) \leq \delta_A(v) + 4c$. Hence v will be put in the tentative A set Y, unless $\delta_A(v) + 4c > \frac{4}{9}mp^2$. For large m this implies $\delta_A(v) > \frac{1}{3}mp^2$ and hence $v \in U$. Thus, almost surely, the only vertices misclassified are in U.

Now we turn to examining S, which lies in the tentative B set, X. Suppose $a \in S \cap A$. Note that

$$|X \cap B| \geq m - |U| - 4c \qquad \text{and} \qquad |X \cap A| \leq |U| + 4c$$

with a corresponding statement for Y. Thus, with the required probability, we can argue a priori that

$$\delta_X(a) \geq mp(1 - m^{-\gamma}) - |U| - 4c$$

and

$$\delta_Y(a) \leq \delta_A(a) + |U| + 4c.$$

Now a will be removed to Y unless $\delta_A(a) \approx mp$ and hence $a \in U$. Thus, at the end of the phase, the only vertices misclassified are almost surely in U. We now remove U from X and Y and consider all possible ways of assigning them to give $|X_1| = |Y_1| = m$. Clearly one of these must yield $X_1 = B$, $Y_1 = A$, almost surely. □

If FIND 1 fails we take the following approach. Choose a large set U, and consider all possible guesses at $U \cap A, U \cap B$. Sort the values $\delta_X(v)$ for $v \notin U$, and put the vertices with small δ_X value in with X. Finally check for a few misplacements.

FIND 2

```
begin
 Select $U \subseteq V(G)$ with $|U| = \lceil m^{2/3} \rceil$, at random
 for all $X \subseteq U$ do
 begin
  for all $v \in V(G) - U$ do determine $d(v) \leftarrow \delta_X(v)$ od
  $k \leftarrow (m - |X|)$th smallest $d(v)$;
  $C \leftarrow \{v : d(v) \leq k\} \cup X$ such that $|C| = m$; $\bar{C} \leftarrow V - C$
  for all $S \subseteq C$ with $|S| \leq \lceil m^{2/3} \rceil$ do
  begin
   for begin
   determine $\delta_S(v)$; $\delta_T(v)$;
   if $\delta_S(v) < \delta_T(v)$ then $X \leftarrow X \cup \{v\}$ else $Y \leftarrow Y \cup \{v\}$
  end;
  for each $v \in S$ do
  begin
   if $\delta_X(v) < \delta_Y(v)$ then $Y \leftarrow Y - \{v\}$, $X \leftarrow X \cup \{v\}$
  end;
  $X \leftarrow X - U$, $Y \leftarrow Y - U$;
  for each $W \subseteq U$ with $|W| = m - |X|$ do
  begin
   $X_1 \leftarrow X \cup W$; $Y_1 \leftarrow Y \cup (U - W)$;
   if $G[X_1] \in \mathscr{C}_A$, $G[Y_1] \in \mathscr{C}_B$
   or $G[Y_1] \in \mathscr{C}_A$, $G[X_1] \in \mathscr{C}_B$
   then output partition, stop {success}
  end
 end
end
Stop Find 1 has failed.
```

The time-complexity of FIND 1, implemented in a straightforward manner is easily checked to be $O(m^3)$.

THEOREM 5.1. *Under Model* 1, Pr(FIND 1 *fails*) $= O(e^{-m^\beta})$ *for any* $\beta < 1$.

Proof. Fix β and let $0 < \gamma < \frac{1}{2}(1-\beta)$. Then for $v \in A$, $\delta_V(v) \geq mp(1 - m^{-\gamma}) + \delta_A(v)$ with probability $1 - O(e^{-m^\beta})$ and similarly for $v \in B$. Thus $\bar{d} \geq mp(1 - m^{-\gamma}) + 2c$ with probability $1 - O(e^{-m^\beta})$. Also for $v \in A$, $\delta_V(v) \leq mp(1 + m^{-\gamma}) + \delta_A(v)$ with similar probability. Thus, almost surely, $\delta_V(v) \geq \bar{d}(1 + \bar{d}/2m)$ implies

$$mp(1 + m^{-\gamma}) + \delta_A(v)$$
$$\geq \left(mp(1 - m^{-\gamma}) + 2c\right)\left(1 + \tfrac{1}{2}p(1 - m^{-\gamma}) + \frac{c}{m}\right),$$

i.e.,

$$\delta_A(v) \geq \tfrac{1}{2}mp^2(1 - o(1)).$$

So for large m, certainly $\delta_A(v) > \frac{1}{3}mp^2$. Similarly for $v \in B$. Thus U contains only vertices with degree at least $\frac{1}{3}mp^2$ in their own graph G_A or G_B, except for probability $O(e^{-m^\beta})$. However, since G_A, G_B have at most cm edges, it follows by simple counting that $|U| < 12c/p^2$ almost surely, and hence $|U| < \log\log m$.

Now, again by counting, G_A, G_B have at least $\lceil \frac{1}{2}m \rceil$ vertices each of degree at most $4c$. Thus, with probability $1 - O(e^{-m^\beta})$ there are at least $\frac{1}{4}m^2p(1 - o(1))$ edges joining vertices of degree at most $4c$ in their own graphs. Since G has at most $m^2(1 + o(1))$ edges altogether, the probability that Z fails to contain an edge joining two vertices of degree at most $4c$ is $O(e^{-mp/4})$, by a straightforward calculation. Therefore we can assume FIND 1 (if it has not already partitioned G) discovers an edge $(s, t) \in Z$ with $s \in A$, $t \in B$, and $\delta_A(s), \delta_B(t) \leq 4c$.

However, the probability that for any $a \in A$, $\delta_B(a) < \frac{2}{3}mp$ is $O(e^{-m^\beta})$ and similarly for $\delta_A(b)$, $b \in B$. Thus S almost surely contains at least $\frac{2}{3}mp$ vertices in B and at most $4c$ in A. Similarly for T. Now consider $v \notin S \cup T$. If $v \in A$ then, since the edges adjacent to v are unconditioned (except for $(v, t) \notin E(G)$), we have $\delta_S(v) \geq \frac{4}{9}mp^2$ with the required probability and $\delta_T(v) \leq \delta_A(v) + 4c$. Hence v will be put in the tentative A set Y, unless $\delta_A(v) + 4c > \frac{4}{9}mp^2$. For large m this implies $\delta_A(v) > \frac{1}{3}mp^2$ and hence $v \in U$. Thus, almost surely, the only vertices misclassified are in U.

Now we turn to examining S, which lies in the tentative B set, X. Suppose $a \in S \cap A$. Note that

$$|X \cap B| \geq m - |U| - 4c \qquad \text{and} \qquad |X \cap A| \leq |U| + 4c$$

with a corresponding statement for Y. Thus, with the required probability, we can argue a priori that

$$\delta_X(a) \geq mp(1 - m^{-\gamma}) - |U| - 4c$$

and

$$\delta_Y(a) \leq \delta_A(a) + |U| + 4c.$$

Now a will be removed to Y unless $\delta_A(a) \approx mp$ and hence $a \in U$. Thus, at the end of the phase, the only vertices misclassified are almost surely in U. We now remove U from X and Y and consider all possible ways of assigning them to give $|X_1| = |Y_1| = m$. Clearly one of these must yield $X_1 = B$, $Y_1 = A$, almost surely. □

If FIND 1 fails we take the following approach: choose a large set U and consider all possible guesses for $U \cap A$, $U \cap B$. Sort the values of $\delta_X(v)$ for $v \notin U$ and put the vertices with small δ_X values in with X. Finally, check for a few misplacements.

FIND 2

```
begin
 Select $U \subseteq V(G)$ with $|U| = \lceil m^{2/3} \rceil$, at random
 for all $X \subseteq U$ do
 begin
  for all $v \in V(G) - U$ do determine $d(v) \leftarrow \delta_X(v)$ od
  $k \leftarrow (m - |X|)$th smallest $d(v)$;
  $C \leftarrow \{v : d(v) \leq k\} \cup X$ such that $|C| = m$; $\bar{C} \leftarrow V - C$
  for all $S \subseteq C$ with $|S| \leq \lceil m^{2/3} \rceil$ do
  begin
   for all $T \subseteq \bar{C}$ with $|T| = |S|$ do
   begin
    $X_1 \leftarrow (C - S) \cup T$; $Y_1 \leftarrow (\bar{C} - T) \cup S$
    if $G[X_1] \in \mathscr{C}_A$ and $G[Y_1] \in \mathscr{C}_B$ or vice versa
    then output partition: stop fi
   end
  end
 end
Stop FIND 2 has failed.
```

LEMMA 5.2. FIND 2 *takes* $O(2^{m^{3/4}})$ *time and has failure probability* $O(e^{-m^{5/4}})$ *under Model* 1.

Proof. The running time is easily established. The failure probability calculations are rather similar to those in Lemma 4.3. The only point to note is that the only vertices misclassified by the $d(v)$ calculations are those which either (i) have very high degree in their own graph or (ii) have very low degree in the $A : B$ cut.

We bound the number of type (i) by counting and of type (ii) by their probability. The enumerated loops will then, with very high probability find the A, B partition if FIND 2 has not already partitioned G. The details will be left to the reader. □

If FIND 2 fails we use complete enumeration to partition G in $O(2^{2m})$ time. The three-phase algorithm FIND then partitions G with certainty.

THEOREM 5.3. *Under Model* 1, FIND *has expected running time* $O(m^3)$.

Proof. Similar to that of Theorem 4.6. □

Model 2 selects M edges randomly from the $A : B$ cut, with $M + \Omega(m^2)$.

LEMMA 5.4. *Under Model* 2, FIND *has expected running time* $O(m^3)$.

Proof. Similar to that of Lemma 3.5. □

Model 3 allows M to vary in Model 2 and chooses uniformly.

LEMMA 5.5. *Under Model* 3, FIND *has expected running time* $O(m^3)$.

Proof. There are $\binom{2m}{m}\sum_{M=0}^{m^2}\binom{m^2}{M}$ graphs in the sample space. It is easy to show that $\Pr(M \leq \frac{1}{4}m^2) = O(e^{-m^2/8})$. The proof then follows the lines of Theorem 3.12. □

We now wish to move to Model 3′ in which duplicates of Model 3 graphs are deleted. To do this we return to Model 1. Note that, since FIND 1 almost surely works, there are almost surely at most $2^{|U|}$ ways of partitioning G, where U is as in FIND 1. But we showed in the proof of Lemma 5.1 that $|U| < 12c/p^2$, almost surely. It follows that there are almost surely $O(1)$ ways of partitioning G. This conclusion transfers to Model 2 (since the failure probability is small) and hence to Model 3 and similarly to Lemmas 5.4 and 5.5 above. Thus in Model 3, there exists some constant K such that G almost surely has at most K different partitions.

THEOREM 5.6. *Let* Γ *be the class of graphs on* $2m$ *vertices which admit a partition into* $G_A \in \mathscr{C}_A, G_B \in \mathscr{C}_B$. *Then if* G *is chosen uniformly at random from* Γ, *FIND will partition* G *in* $O(m^3)$ *expected time.*

Proof. We use Corollary 2.3(a) on the (Model 3) failure probabilities for FIND 1 and FIND 2 as in Theorem 3.10, but with $k = K$ (as defined above), rather than $k = 1$. Since K is a constant and the probability that the number of partitions exceeds k is $o(1)$, all probabilities are inflated by only $K(1 + o(1))$, and these remain small. It remains only to observe that Model 3′ is that described in the theorem. □

This is the result we claimed earlier. Note that it is trivial to extend Theorem 5.6 to non-uniform distributions on $\mathscr{C}_A, \mathscr{C}_B$. Note also $\mathscr{C}_A, \mathscr{C}_B$ could each consist of a single graph provided we can find its isomorphs in polynomial time.

6. 3-Partition

The 3-PARTITION problem is defined as follows. Given non-negative integers $B_1, B_2, \ldots, B_{3m}$ and an integer B, can we partition $I = \{1, 2, \ldots, 3m\}$ into subsets $T_1, T_2, \ldots, T_m$ such that $|T_i| = 3$ and $\Sigma_{j \in T_i} B_j = B$ $(i = 1, \ldots, m)$? Clearly $mB = \Sigma_{j=1}^{3m} B_j$ is necessary for the problem to be non-trivial. It is well known [3] that this problem is strongly (unary) NP-complete when $B = \Omega(m^4)$.

We eventually consider the following model of a random 3-partitionable instance. Let $\overline{B}(m) = \omega m^2$, where $\omega = \omega(m) \to \infty$ with m, be an integer-valued function of m. Now consider the uniform distribution on all 3-partitionable instances of 3-PARTITION with $B \leq \overline{B}(m)$, for given m. Then, as $m \to \infty$, we can almost surely solve a random instance drawn from this distribution in $O(m^2)$ expected time. Note that the requirement that $\overline{B} = \omega m^2$ includes all instances *known* to be NP-hard, by taking $\overline{B} = \Omega(m^4)$. Whether there are NP-hard instances of 3-PARTITION with B as small as, say, $m^{2+\varepsilon}$ for all $\varepsilon > 0$ is, as far as we know, an open problem.

Our result here is not quite as strong as in previous sections since we give only almost sure, rather than polynomial expected time, solutions. This is because the error probabilities are much too small to permit methods like those used earlier, except in the extreme case where $\overline{B}$ grows exponentially fast with m. However, the result here does show that our methods have wider application than graph problems.

In this section Model 1 is as follows. Let $R_1, R_2, \ldots, R_m$ be a random partition of I such that $|R_i| = 3$ $(i = 1, \ldots, m)$. For each $R_i = \{p, q, r\}$, say, generate (B_p, B_q, B_r) uniformly from the set of all triples of non-negative integers satisfying $B_p + B_q + B_r = B$, where B is a fixed integer. Thus each instance is certainly 3-partitionable.

Consider the following algorithm.

```
PART
comment We first determine the set LIST of all triples $\{i, j, k\}$, $i < j < k$, such that
$B_i + B_j + B_k = B$. We do this in $O(m^2 + |\text{LIST}|)$ time by a process analogous to merging
two sorted lists.//
Sort the $\{B_i\}$ so that $B_1 \leq B_2 \leq \cdots \leq B_{3m}$.
LIST ← $\varnothing$
for $i \leftarrow 1$ to $3m$ do
begin
 $j \leftarrow 1$; $k \leftarrow 3m$
  while $j \leq 3m$, $k \geq 1$ do
  begin
   if $B_j + B_k > B - B_i$ then $k \leftarrow k - 1$
   else if $B_j + B_k < B - B_i$ then $j \leftarrow j + 1$
   else $l \leftarrow k$, $t \leftarrow j$
   while $B_{l-1} = B_k$ do $l \leftarrow l - 1$ od
```

```
    while $B_{t+1} = B_j$ do $t \leftarrow t + 1$ od
    for $p \leftarrow \max(l + 1, i + 1)$ to $k$ do
      for $q \leftarrow \max(p + 1, j)$ to $t$ do
        add $T = \{i, p, q\}$ to LIST
  end
  $k \leftarrow l - 1$, $j \leftarrow t + 1$
end
comment We now search the list of triples, removing any which are "forced" by having an element which appears only in that triple, hoping to construct a 3-partition.//
$S \leftarrow \varnothing$
for $k \leftarrow 1$ to $m$ do
begin
  Search LIST to determine any $i$ such that
    $i \in T$ for a unique triple $T$;
    if no such $i, T$ then stop, PART has failed
    $S \leftarrow S \cup \{T\}$.
  for $j \in T$ do
    for $T' \in$ LIST do
    if $j \in T'$ then delete $T'$ from LIST
end
stop, $S$ contains the required 3-partition.
```

It is not difficult to implement PART so that it runs in $O(m^2 + m|\text{LIST}|)$ time. It is evident that, if PART succeeds in constructing a solution, then the solution is unique, since all triples used are forced. Thus, proving that PART almost surely works automatically proves that solutions are almost surely unique.

THEOREM 6.1. *Under Model* 1,

(i) *If $B = \omega m^2$ then PART almost surely succeeds, runs in $O(m^2)$ time and solutions are almost surely unique.*

(ii) *If $B = o(m^2)$ then PART almost surely fails, and solutions are almost surely not unique.*

Proof. (i) First note that, if $i, j \in R_k$ for some k,

$$\Pr(B_i = x, B_j = y) = \frac{2}{(B+1)(B+2)} \qquad (0 \le x + y \le B) \quad (6.1)$$

$$\Pr(B_i = x) = \frac{2(B - x + 1)}{(B+1)(B+2)} \qquad (0 \le x \le B). \quad (6.2)$$

Let us call i, j (or B_i, B_j) *related* if $\{i, j\} \subset R_k$ for some k, otherwise unrelated. Unrelated variables are independent in Model 1, so for unrelated i, j,

$$\Pr(B_i = B_j) = \frac{2(2B+3)}{3(B+1)(B+2)} < \frac{4}{3B} \quad (6.3)$$

by a simple calculation using (6.2).

Let us call a triple $T = \{p, q, r\} \subseteq I$ *bad* if $T \neq R_k$ for any k and $B_p + B_q + B_r = B$. Let Q be the event that there exists k and a bad triple T such that $|T \cap R_k| = 2$. Let $\{p\} = T - R_k, \{q\} = R_k - T$. Then Q implies $B_p = B_q$ with p, q unrelated. Thus

$$\begin{aligned}\Pr(Q) &\leq \Pr(\exists p, q \text{ unrelated with } B_p = B_q)\\ &\leq 3^2\binom{m}{2}\frac{4}{3B} < \frac{6m^2}{B} = o(1), \text{ using (6.3).}\end{aligned}$$

Thus we may assume that $\overline{Q}$ occurs.

Suppose PART fails during the construction of the solution set S. Let LIST refer to the undeleted triples at this stage. We show there exists a sequence $T_1, T_2, \dots, T_k$, $k \geq 2$, of disjoint bad triples where $T_i = \{p_i, q_i, r_i\} \in$ LIST for $i = 1, 2, \dots, k$ and

$$q_i \text{ and } p_{i+1} \text{ are related for } i = 1, 2, \dots, k-1. \tag{6.4a}$$

$$q_k \text{ is related to } \textit{one} \text{ element of } \bigcup_{i=1}^{k-1} T_i. \tag{6.4b}$$

$$\begin{gathered}\text{Any pair of elements from } \bigcup_{i=1}^{k} T_i \text{ not mentioned}\\ \text{in (6.4a), (6.4b) are unrelated.}\end{gathered} \tag{6.4c}$$

Now LIST must contain at least one bad triple, else all the triples in LIST are forced. Let T_i be any such bad triple. Suppose now that we have succeeded in constructing $T_1, T_2, \dots, T_s$ where $s = 1$ or (6.4a) and (6.4c) hold with $k = s$ and suppose that (6.4b) does not hold. Let $q_s \in R_j = \{q_s, a, b\}$, where $a, b \notin \bigcup_{i=1}^{s} T_i$ by assumption. Let $p_{s+1} = a$.

LIST must contain another bad triple containing a, else R_j is forced. Let $T_{s+1} = \{a, x, y\}$ be this triple. If either of x, y are related to a previous element then with the appropriate choice of x or y for q_{s+1}, we have satisfied (6.4) with $k = s + 1$. (Note that $\overline{Q}$ prevents x being related to a or y.) Otherwise the process continues.

Clearly, after no more than |LIST| steps (6.4b) will be satisfied. Now the number of ways of choosing elements satisfying (6.4) is no more than

$$\binom{m}{k-1}6^{k-1}\binom{m-k+1}{k+1}3^k(2k) < 3^{2k-1}2^k k m^{2k}.$$

$$\left\{\begin{matrix}\binom{m}{k-1}6^{k-1} \text{ ways of choosing } q_2, p_3, q_3, \dots, q_{k-1}, \\ \text{then } \binom{m-k+1}{k+1}3^{k+1} \text{ ways of choosing} \\ p_1, r_1, r_2, \dots, r_k, \text{ then } 2k \text{ ways of choosing } q_k\end{matrix}\right\}.$$

The probability that such a choice satisfies $B_{p_i} + B_{q_i} + B_{r_i} = B$ for $i = 1, 2, \ldots, k$ is less than $(2B)^k$. To see this, first note that given the values B_{p_i}, B_{q_i} for $i = 1, 2, \ldots, k-2$, the probability that $B_{r_i} = B - B_{p_i} - B_{q_i}$ for $i = 1, 2, \ldots, k-2$ is at most $(2/(B+2))^{k-2}$ by (6.2). Given this and the values of $B_{p_{k-1}}, B_{r_{k-1}}, B_{q_k}, B_{r_k}$, the probability that $B_{q_{k-1}} = B - B_{p_{k-1}} - B_{r_{k-1}}$ and $B_{p_k} = B - B_{q_k} - B_{r_k}$ is $2/(B+1)(B+2)$ by (6.1). Hence

$$\Pr((6.4)\text{ holds}) \leq \sum_{k=2}^{\infty} \frac{k(6m)^{2k}}{B^k} = O(m^4/B^2).$$

and so

$$\Pr(\text{PART fails}) \leq \Pr(Q) + O(m^4/B^2) = o(1).$$

To show that PART runs in $O(m^2)$ expected time we show that $E(|\text{LIST}|) = m + o(m)$ after the triple construction phase. But if BAD = {bad triples} then (6.1) and (6.2) imply that $E(|\text{BAD}|) = O(m^3/B) = o(m)$ and the result follows.

(ii) We now consider briefly $B = o(m^2)$. Let U be the event that there exist unrelated i, j with $B_i = B_j$. If U occurs, the solution is clearly not unique. Moreover, PART will fail since, if $i \in R_h = \{i, p, q\}$ and $j \in R_k = \{j, r, s\}$, the set of triples, $R_h, R_q, \{j, p, q\}, \{i, r, s\}$ cannot be resolved (because every index appears twice). So we need only show that U almost surely occurs. We do this by the standard second moment method. Let X be the number of unrelated pairs i, j such that $B_i = B_j$. It is easy to show that

$$E(X) \approx 6m^2/B \qquad \text{and} \qquad E(X^2) \approx 36m^4/B^2 + 6m^2/B$$

Now, $\Pr(U) = \Pr(X > 0) \geq E(X)^2/E(X)^2$. Hence $\Pr(U) \geq (1 - o(1))/(1 + B/6m^2) = 1 - o(1)$ if $B = o(m^2)$. □

Theorem 6.1 provides a "weak threshold" for both unique solutions and the success of PART, under Model 1. It leaves only the case $B = \Theta(m^2)$ unresolved. We would not like to guess what happens here. It is clear that the event U of Theorem 6.1 can have probability bounded away from either 0 or 1. It is possible that we always have, as $m \to \infty$, Pr(unique solutions) → Pr(PART succeeds) → Pr(U), which would be "typical" behaviour for thresholds of this type, but this looks a little doubtful.

Model 1 may be regarded as selecting uniformly from a sample space of

$$\frac{1}{m!}\frac{(3m)!}{(3!)^m}\binom{B+2}{2}^m$$

different instances. Model 1′ will be the model given by deleting repetitions of the same instance, i.e., copies of instances not possessing a unique 3-partition.

LEMMA 6.2. *Under Model* 1′, *with* $B = \omega m^2$, *solutions are almost surely unique and PART almost surely succeeds.*

Proof. Uses Corollary 2.3(a) in a standard way. □

We finally move to Model 2, in which B can vary in Model 1, with Model 2′ being given by deleting copies. We assume $0 \le B \le \bar{B} = \omega m^2$.

LEMMA 6.3. *In Model* 2, *PART almost surely succeeds and solutions are almost surely unique.*

Proof. We select uniformly from

$$T = \frac{(3m)!}{(3!)^m} \sum_{B=0}^{\bar{B}} \binom{B+2}{2}^m$$

instances. Now

$$\Pr\left(B \le \frac{1}{2}\bar{B}\right) = \sum_{B=0}^{\lfloor \bar{B}/2 \rfloor} \binom{B+2}{2}^m \Bigg/ \sum_{B=0}^{\bar{B}} \binom{B+2}{2}^m = O\left(\frac{1}{2^{2m}}\right)$$

by a straightforward calculation. Thus, almost surely, $B = \omega m^2$ and the lemma follows from Theorem 6.1. □

Moving finally to Model 2′, we have

THEOREM 6.4. *If* $B = \omega m^2$ *and instances are randomly selected uniformly from all partitionable instances of* 3-*PARTITION with given m and* $0 \le B \le \bar{B}$, *the PART will almost surely construct the* (*almost surely unique*) 3-*partition.*

This is the result we claimed.

7. CONCLUSIONS

We have shown that, under fairly natural models, various NP-hard problems can be solved rapidly on average if we are guaranteed that the instances possess the property we are seeking. We have shown this for graph k-colourability, a small equitable cut, partitioning into sparse graphs, and 3-PARTITION. This probabilistic result is in contrast to the worst-case conclusion, which is that such guarantees are computationally worthless.

We believe that our results indicate that it is quite difficult to disguise structure, and instances of a given structure are usually apparent to rapid investigations. This clearly has implications for the design of heuristics for solving NP-hard problems. An interesting case is crytography, where randomness is often deliberately used in a attempt to hide a structure (the message) which is known to be present.

Finally, we believe that our approach is quite general, and corresponding models of other NP-complete problems can be developed. Among graph problems we might approach large stable set or dominating set by similar methods. These yield to very easy algorithms based on vertex degrees. For non-graph problems, satisfiability problems can be approached in a similar way. Perhaps of greater interest is an extension of results like those of Section 4 to NP-hard optimisation problems, for example to find the largest stable set and *prove* we have found it in expected polynomial time.

References

1. T. Bui, S. Chaudhuri, T. Leighton and M. Sipser, Graph bisection algorithms with good average case behaviour, *in* "Proceedings, 25th IEEE Symposium on the Foundations of Computer Science, 1984, pp. 181–192.
2. M. E. Dyer and A. M. Frieze, On the complexity of graph partitioning problems, *Discrete Appl. Math.* **10** (1983), 139–153.
3. M. R. Garey and D. S. Johnson, "Computers and Intractability," Freeman, San Francisco, 1979.
4. W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Statist. Assoc.* **58** (1963), 13–30.
5. L. Kucera, Expected behaviour of graph colouring algorithms, *in* "Fundamentals of Computation Theory, 1977," Lecture Notes in Computer Science, Vol. 56, pp. 447–451, Springer-Verlag, New York/Berlin, 1977.
6. A. Thomason, Pseudo-random graphs, *Ann. of Discrete Math.*, in press.
7. A. Thomason, Dense expanders, to appear.
8. J. S. Turner, On the probable performance of graph colouring algorithms, *in* "Proceedings, 1984 Allerton Conference on Communications, Control and Computing, pp. 281–290.
9. J. S. Turner, Almost all k-colorable graphs are easy to color, *J. Algorithms* **9** (1988), 63–82.