Small Clique Detection and Approximate Nash Equilibria

Lorenz Minder and Dan Vilenchik

Computer Science Division, University of California, Berkeley, CA 94720-1776
lorenz@eecs.berkeley.edu, danny.vilenchik@gmail.com

Abstract. Recently, Hazan and Krauthgamer showed [12] that if, for a fixed small ε, an ε-best ε-approximate Nash equilibrium can be found in polynomial time in two-player games, then it is also possible to find a planted clique in $G_{n,1/2}$ of size $C \log n$, where C is a large fixed constant independent of ε. In this paper, we extend their result to show that if an ε-best ε-approximate equilibrium can be efficiently found for arbitrarily small $\varepsilon > 0$, then one can detect the presence of a planted clique of size $(2+\delta)\log n$ in $G_{n,1/2}$ in polynomial time for arbitrarily small $\delta > 0$. Our result is optimal in the sense that graphs in $G_{n,1/2}$ have cliques of size $(2 - o(1))\log n$ with high probability.

1 Introduction

The computational complexity of finding a Nash equilibrium in a given game has been the focus of extensive research in recent years: The problem of finding a best Nash equilibrium (i.e., an equilibrium that maximizes the sum of the expected payoffs) in a two-player game has been shown to be NP-hard by Gilboa and Zemel [9] in 1989. The easier problem of computing an arbitrary equilibrium in a finite two-player game was shown to be PPAD-complete by Chen et al [4] and Daskalakis et al [6].

Given these results, it is unlikely that Nash equilibria can be computed in polynomial time. However, some positive results show that Nash equilibria can at least to some extent be approximated. The most recent result, following extensive work in the area, provides a polynomial time algorithm that computes a 0.3393-equilibrium [15]. Another algorithm due to Lipton et al computes an ε-equilibrium in quasi-polynomial time $N^{\log N/\varepsilon^2}$, where $N \times N$ is the dimension of the game matrix. The latter result also extends to the case of an ε-equilibrium that maximizes the sum of payoffs.

Having a quasi-polynomial time approximation algorithm probably means that finding ε-equilibria is not NP-hard. It is however still not known whether the problem has a polynomial time approximation scheme.

Recently, Hazan and Krauthgamer [12] showed that for sufficiently small yet constant ε the problem of computing an ε-equilibrium whose sum of payoffs is off by at most ε from the best Nash equilibrium (for short, we call this problem

I. Dinur et al. (Eds.): APPROX and RANDOM 2009, LNCS 5687, pp. 673–685, 2009.

ε-best ε-equilibrium) is at least as hard as finding a planted k-clique in the random graph $G_{n,1/2}$, where $k = c \log n$ [1], and $c \approx 10^6$ is a fixed large constant (by "hard" we mean the standard notion of polynomial – maybe randomized – reductions). The planted k-clique problem consists of finding a clique of size k that was planted into an otherwise random graph with density 1/2. This problem is a well-known notoriously hard combinatorial problem.

– Despite considerable efforts, the currently best known efficient algorithm to solve the planted clique problem [2] needs a clique size of $k = \Omega(\sqrt{n})$.
– The planted k-clique problem is (for certain values of k) related to the assumption that refuting low-density 3CNF formulas is hard on the average. This fact was used by Feige [7] to derive constant-factor hardness of approximation for several well-known problems.

1.1 Our Contribution

In this paper, we strengthen the result of Hazan and Krauthgamer in the following sense: We show that if a polynomial time approximation scheme exists that finds for any $\varepsilon > 0$ an ε-best ε-equilibrium, then for any $\delta > 0$ there is a polynomial time algorithm that detects the presence of a planted clique of size $(2 + \delta) \log n$ with high probability (*whp* for short).

Note that random graphs contain a clique of size $(2 - o(1)) \log n$. Hence the $2 \log n$ threshold that we achieve is a natural boundary implied by the problem statement. See in this context also the work of Juels and Peinado [11] for the planted clique problem when $k < 2 \log n$.

More formally, our main result can be stated as follows.

Theorem 1. *There exists a positive constant ε_0 so that if there is a polynomial time algorithm that finds in a two-player game the ε-best ε-equilibrium, $0 < \varepsilon \leq \varepsilon_0$, then there is a probabilistic polynomial time algorithm that distinguishes whp between two graphs: $G \in G_{n,1/2}$ and H, an arbitrary graph on n nodes with a clique of size $(2 + 28\varepsilon^{1/8}) \log n$.*

As explained in Section 3.3, our analysis gives $\varepsilon_0 = 32^{-8}$, although this estimate is somewhat loose. The probability in the statement is taken over the choices of the algorithm and the distribution $G_{n,1/2}$.

Our result in particular implies that finding an ε-best ε-equilibrium is at least as hard as distinguishing between $G_{n,1/2}$ and $G_{n,1/2,k}$ (i.e., $G_{n,1/2}$ with a planted k-clique) for $k = (2 + 28\varepsilon^{1/8}) \log n$.

Let us also briefly mention that our analysis implies that for every fixed $\delta > 0$, given an efficient algorithm for finding an ε-best ε-equilibrium, one can efficiently *find* a planted clique of size $(3 + \delta) \log n$ in $G_{n,1/2}$. For details, see section 4.

In the next section we describe our technical contribution.

[1] In this paper, log denotes the base-2 logarithm.

1.2 Techniques

The main idea of the reduction, as put out by [12], is to incorporate the graph with the planted clique into a game so that the ε-best ε-equilibrium reflects in some useful sense that clique.

More formally, let G be a simple graph with self-loops added, and let A be its adjacency matrix. Construct the following game matrices R and C, composed of four blocks. $C = R^T$ so let us just describe R.

$$R = \begin{pmatrix} A & -B^T \\ B & \mathbf{0} \end{pmatrix}$$

Here, $\mathbf{0}$ stands for the all-0 matrix. The matrix B is constructed as follows. The constants $t \leq 2, p$ and s, whose values depend on ε, are chosen as in the proof of Proposition 1. B is an $n^s \times n$ matrix, each entry of which is a scaled Bernoulli random variable $B_{i,j}$ which takes the value t with probability p and 0 otherwise.

The difference from the construction in [12] is our different choice of parameters for the matrix B. The heart of the analysis outlined in [12] lies in proving that if a clique of size $c_1 \log n$ is planted in $G_{n,1/2}$ then a graph of size $c_2 \log n$, $c_2 \leq c_1$, with edge-density greater than, say, 0.55 can be recovered using the above construction and the ε-best ε-equilibrium which one assumes can be found efficiently. Since this graph is denser than what one expects in $G_{n,1/2}$, and the constant c_2 is sufficiently large, it has *whp* many edges in common with the planted clique. This fact can then be used to recover the clique. In [12], c_1 was a large constant, and so was c_2, and the question of how tight the gap between them can be was not considered. This is however exactly our main question. Our new choice of parameters and a refined analysis (based on [12]) allows us to get essentially the best possible ratio between c_1 and c_2 (which would be 1), and essentially the best value for c_1 (which would be 2). The "price" we pay for those optimal constants is that we are unable to find the planted clique, but rather distinguish between a random graph and a random graph with a slightly larger clique planted in it.

1.3 Notations

Let R and C (for "row" and "column") be two $N \times N$-matrices with entries in $\mathbb{R}$. Let x, y be in $\mathbb{R}^N$, with non-negative entries, and such that $\sum_{i=1}^N x_i = \sum_{i=1}^N y_i = 1$; such a pair (x, y) is called a pair of *mixed strategies*. The (expected) *payoff* of the row player is $x^T Ry$, and the one of the column player is $x^T Cy$.

The strategies (x, y) is an *ε-equilibrium* if none of the players can increase his payoff by more than ε by changing his strategy. In other words, the pair (x, y) is an ε-equilibrium if for all strategies $\tilde{x}$ and $\tilde{y}$, we have

$$\tilde{x}^T Ry \leq x^T Ry + \varepsilon \qquad \text{and} \qquad x^T C\tilde{y} \leq x^T Cy + \varepsilon.$$

(For the definition of approximation we use the following conventional assumptions: the value of the equilibrium lies in $[0, 1]$ and the approximation is additive). A 0-equilibrium is more succinctly called a *Nash equilibrium*.

A Nash equilibrium is *best* if it maximizes the average payoff of the players, i.e., if it maximizes its *value*

$$\frac{1}{2}x^T(R+C)y.$$

A pair of strategies (x, y) is an ε*-best* ε*-equilibrium* if it is an ε-equilibrium and its value is at least as large as the value of the best Nash equilibrium minus ε, i.e.,

$$\left(\max_{\tilde{x},\tilde{y}} \frac{1}{2}\tilde{x}^T(R+C)\tilde{y}\right) - \varepsilon \leq \frac{1}{2}x^T(R+C)y,$$

where $(\tilde{x}, \tilde{y})$ runs over the Nash equilibria of the game.

2 Preliminaries: Properties of the Matrix B

In this section we describe several properties that the matrix B has *whp*, which play a crucial role in our proof. We remind the reader that the entries of B are scaled Bernoulli variables of some scale t and probability p, i.e.,

$$B_{i,j} = \begin{cases} 0 & \text{with probability } 1-p, \\ t & \text{with probability } p, \end{cases}$$

where t and p are parameters to be selected.

Proposition 1. *Fix small enough $\beta > 0$, and let $c_1 = 2+7\beta^{1/2}$, $c_2 = 2+6\beta^{1/2}$. There exists parameters t, p and s such that the matrix B of size $n^s \times n$, filled with independent and identically distributed scaled Bernoulli-variables of scale t and parameter p, enjoys the following properties whp:*

(i) Fix a set $I \subseteq [1, n]$ of $c_1 \log n$ indices (independently of B). For every row i of B,

$$\frac{1}{c_1 \log n}\sum_{j\in I} B_{i,j} \leq 1.$$

(ii) For every set $J \subseteq [1, n]$ of $c_2 \log n$ indices, there exists a row $i = i(J)$ in B so that $B_{i,j} \geq 1 + 9\beta$ for every $j \in J$.

The proof uses the following variant of the Chernoff bound. If $X_1, \ldots, X_m$ are m independent Bernoulli variables of scale t and parameter p, then

$$\Pr\left(m^{-1}\sum_{i=1}^{m} X_i \geq tp(1+\delta)\right) \leq e^{mp[\delta-(1+\delta)\ln(1+\delta)]}, \tag{1}$$

for any $\delta > 0$.

Proof. **The c_1-calculation.** Write $m = c_1 \log n$, and fix a row j. Using (1), we see that

$$\Pr\left(m^{-1}\sum_{i=1}^{m} A_{j,i} \geq 1\right) \leq \exp\left(\frac{m[1-tp+\ln(tp)]}{t}\right).$$

Hence using the union bound over all the rows, the first property does not hold with probability at most

$$n^{s+c_1[1-tp+\ln(tp)]/(t\ln 2)}.$$

So the first property holds with high probability if

$$s < \frac{c_1}{t\ln 2}[tp-1-\ln(tp)]. \tag{2}$$

The c_2-calculation. For the second property to hold, we need $t \geq 1+9\beta$.

Fix a set $I = \{i_1, \ldots, i_{c_2 \log n}\} \subset [n]$ of $c_2 \log n$ indices. Then for a fixed row j, the probability that $B_{j,i} \geq t$ for every $i \in I$ is $p^{c_2 \log n}$, so the probability that there is no good row for the indices I is

$$(1-p^{c_2 \log n})^{n^s},$$

hence by the union bound, the probability that there is a set of indices with no good row is at most

$$\binom{n}{c_2 \log n}(1-p^{c_2 \log n})^{n^s} \leq \exp\left(c_2 \log n \ln n + n^s \ln(1-p^{c_2 \log n})\right),$$

which tends to 0 with $n \to \infty$ if

$$n^s \ln(1-p^{c_2 \log n}) < -c_2 \log n \ln n.$$

i.e., if $-n^{s-c_2\log(p^{-1})} < -c_2 \log n \ln n$. So, for the second property to hold, it suffices to require that

$$s > c_2 \log(p^{-1}), \tag{3}$$

in which case $n^s \ln(1-p^{c_2 \log n})$ goes polynomially fast to $-\infty$.

Choice of p and t. We can now deduce a sufficient condition by combining (2) and (3), which gives

$$\frac{c_1}{t\ln 2}[tp-1-\ln(tp)] > c_2 \log(p^{-1}).$$

Plugging in the values for c_1 and c_2 we obtain the following condition on p and t.

$$\frac{2+7\beta^{1/2}}{2+6\beta^{1/2}} > \frac{t\ln(p^{-1})}{tp-1-\ln(tp)}.$$

Now, the limit of the right hand side as $p \to 0$ equals t, hence if we set $t = 1+9\beta$, we see that the right hand side is indeed smaller than the left hand side for sufficiently small (yet constant) p, provided that

$$(2 + 7\beta^{1/2}) - (1 + 9\beta)(2 + 6\beta^{1/2}) > 0.$$

The left hand side of the above is a polynomial in $\beta^{1/2}$ with no constant term and whose dominant term, the coefficient in $\beta^{1/2}$, is positive (in fact, equal to one). Hence this polynomial is positive for small positive values.

3 Proof of Theorem 1

Before giving the actual details let us outline the proof in general lines.

3.1 Proof Outline

For the graph H (with the clique of size $(2+28\varepsilon^{1/8}) \log n$) we show that *whp* the game has a Nash equilibrium of social welfare at least 1. Then, given an ε-best ε-equilibrium, we show that a 3ε-best 7ε-equilibrium can be efficiently calculated whose support lies entirely on A (this is very similar to [12]). Then we show how to efficiently extract a very-dense subgraph D from that strategy (here our density is much higher than [12], we need this higher density as we don't have slackness in the size of the planted clique). On the other hand, we prove that $G \in G_{n,1/2}$ *whp* does not contain such subgraph, causing the algorithm to fail at some point. The graph D then allows us to distinguish H from G.

3.2 Formal Proof

In this section, we assume that the matrix B satisfies the properties of Proposition 1, which is the case *whp*. We assume that c_1 and c_2 are chosen according to Proposition 1, that is $c_1 = 2 + 7\beta^{1/2}, c_2 = 2 + 6\beta^{1/2}$.

Proposition 2. *If A represents a graph H with a clique of size at least $c_1 \log n$, then every equilibrium that maximizes the utilities of the players has value at least 1.*

Proof. Let C be a clique of H of size $c_1 \log n$. Consider the following strategies for both players: each player puts probability $|C|^{-1}$ on every row (column) of that clique. The value of that strategy is clearly 1 for both players. The first property of Proposition 1 guarantees that none of the players has an incentive to defect, thus ensuring that the strategies we chose indeed constitute a Nash equilibrium.

Proposition 3. *If (x, y) is a δ-equilibrium of value at least $1 - \delta$ then every player has at least $1 - 2\delta$ of his probability mass on A.*

Proof. The sum of payoffs of both players from the entries outside A is 0. If one player has more than 2δ of his probability mass outside A, then the value of the game cannot exceed (observing that the maximal entry in A is 1)

$$\frac{1}{2}(1+(1-2\delta)) = 1-\delta.$$

This contradicts our assumption on the value of the game.

Proposition 4. *Given a δ-equilibrium of value $1-\delta$ one can efficiently compute a 7δ-equilibrium of value at least $1-3\delta$ whose support is entirely on A.*

Proof. Given a δ-equilibrium (x, y), define (x', y') as follows: take the probabilities outside A in both x and y and spread them arbitrarily over A. Let us consider the row player (the column player is symmetric). The maximal entry outside A has value at most 2 (since $t \leq 2$), hence the payoff of the row player from the entries outside A is (in absolute value) at most $2\delta \cdot 2 = 4\delta$. The gain of relocating 2δ-probability to A is at most $1 \cdot 2\delta$ (he does not gain from the upper-right part of the matrix). Thus (x', y') is a $\delta + 4\delta + 2\delta = 7\delta$-equilibrium. As for its new total value, the total probability mass relocated for both players is 4δ, thus gaining at most $0.5 \cdot 4\delta \cdot 1 = 2\delta$ (0.5 factor comes from the definition of game-value, and the 1 is the maximal entry in A. The game outside A is zero-sum, so is disregarded).

Proposition 5. *Let (x, y) be a 7δ-equilibrium played entirely on A. Suppose also that the matrix B is generated with parameter $\beta \in [\delta, 1/9]$. Then every subset of the rows Σ whose probability in x is at least $1-\beta$ satisfies $|\Sigma| \geq c_2 \log n$. The same applies for y.*

Proof. We shall prove for the column player, the proof of the row player is symmetric. For contradiction, say there exists a set Σ of columns whose total probability is at least $1-\beta$ but $|\Sigma| \leq c_2 \log n$ (recall: $c_2 = (2 + 6\beta^{1/2})$). By the second property of B in Proposition 1, there exists a row in B in which all corresponding entries have value at least $1 + 9\beta$. If the row player relocates all his probability mass to that row, his new payoff is at least $(1 + 9\beta)(1-\beta) > 1 + 7\beta \geq 1 + 7\delta$ (the last inequality is true for our choice of β). His current payoff is at most 1 (as all entries in A are bounded by 1), and so he will defect, contradicting the 7δ-equilibrium.

For two sets of vertices (not necessarily disjoint), we let $e(V, W)$ be the number of edges connecting a vertex from V with a vertex from W. We use $e(V)$ as a shorthand for $e(V, V)$. It is easy to see that the maximal number of edges is

$$K(V, W) = |V| \cdot |W| - \binom{|V \cap W|}{2}. \tag{4}$$

The density of the two sets is defined to be

$$\rho(V, W) = \frac{e(V, W)}{K(V, W)}. \tag{5}$$

Proposition 6. *Assume we are given a* 7δ*-equilibrium of value* $1-3\delta$ *played entirely on* A*, and the matrix* B *was generated with* $\beta = 16\delta^{1/4}$*. One can efficiently find two sets of vertices* S_1, S_2 *that enjoy the following properties:*

- $|S_1|, |S_2| \geq (2 + 6\beta^{1/2}) \log n$,
- $\rho(S_1, S_2) > 1 - \beta$.

Proof. First observe that if the value of the game (played on A) is $1 - 3\delta$, then each player's payoff is at least $1 - 6\delta$ (as the maximum payoff on A is 1). Let $e_i \in \mathbb{R}^n$ be the unit vector whose entries are 0 except the i^{th} which is 1. Consider the following set of columns:

$$\Gamma_t = \{i : x^T A e_i \geq t\}, \qquad \bar{\Gamma}_t = \{i : x^T A e_i < t\}. \tag{6}$$

Since the payoff of the column player is at least $1-6\delta$ (and in particular at least $1 - 6\delta^{1/2}$), $\Gamma_{1-6\delta^{1/2}} \neq \emptyset$. We now claim that the total probability mass of y on the columns in $\bar{\Gamma}_{1-7\delta^{1/2}}$ is at most $16\delta^{1/2}$. If not, by relocating $16\delta^{1/2}$-probability from $\bar{\Gamma}_{1-7\delta^{1/2}}$ to $\Gamma_{1-6\delta^{1/2}}$ the gain is at least $(7-6)\delta^{1/2} \cdot 16\delta^{1/2} = 16\delta > 7\delta$, which contradicts the 7δ-equilibrium. Thus, by Proposition 5,

$$|\Gamma_{1-7\delta^{1/2}}| \geq (2 + 6\beta^{1/2}) \log n$$

(we can use Proposition 5 since $1 - 16\delta^{1/2} \geq 1 - \beta = 1 - 16\delta^{1/4}$).

For a set T of vertices, let $U_T \in \mathbb{R}^n$ be the uniform distribution over T and 0 elsewhere. The condition of Γ_t implies that (this is just a simple averaging argument)

$$x^T A U_{\Gamma_{1-7\delta^{1/2}}} \geq 1 - 7\delta^{1/2}. \tag{7}$$

Now define a set of rows Σ according to:

$$\Sigma = \{j : e_j^T A U_{\Gamma_{1-7\delta^{1/2}}} \geq 1 - 8\delta^{1/4}\}. \tag{8}$$

We claim that $\sum_{j \in \Sigma} x_j \geq 1 - \delta^{1/4}$. If not,

$$x^T A U_{\Gamma_{1-7\delta^{1/2}}} \leq \left(1 - \delta^{1/4}\right) \cdot 1 + \delta^{1/4} \cdot (1 - 8\delta^{1/4}) = 1 - 8\delta^{1/2}.$$

This contradicts (7). Applying Proposition 5 once more yields $|\Sigma| \geq (2 + 6\beta^{1/2}) \log n$. Equation (8) implies (again, averaging argument):

$$U_\Sigma^T A U_{\Gamma_{1-7\delta^{1/2}}} \geq 1 - 8\delta^{1/4}. \tag{9}$$

Finally we show how this gives the subgraph of correct density. Set $S_1 = \Sigma, S_2 = \Gamma_{1-7\delta^{1/2}}$. They are both of the required size, denoted s_1, s_2 respectively. The number of edges is (by $d_S(v)$ we denote the degree of v in the set S):

$$e(S_1, S_2) = \left(\sum_{v \in S_1} d_{S_2}(v) \right) - e(S_1 \cap S_2).$$

Here, $\sum_{v\in S_1} d_{S_2}(v)$ is just the total number of one-entries in the sub-matrix of A corresponding to $S_1 \times S_2$, which, by Equation (9), is at least $(1-8\delta^{1/4})s_1 s_2$, and we subtract the number of edges in the intersection (since they were counted twice). Thus,

$$e(S_1,S_2) \geq (1-8\delta^{1/4})s_1 s_2 - e(S_1 \cap S_2).$$

Recalling the definition of the density $\rho(S_1,S_2)$, Equation (5), we get

$$\begin{aligned}\rho(S_1,S_2) &= \frac{e(S_1,S_2)}{K(S_1,S_2)}\\ &\geq \frac{(1-8\delta^{1/4})s_1 s_2 - e(S_1\cap S_2)}{s_1 s_2 - \binom{|S_1\cap S_2|}{2}}\\ &\geq \frac{(1-8\delta^{1/4})s_1 s_2 - \binom{|S_1\cap S_2|}{2}}{s_1 s_2 - \binom{|S_1\cap S_2|}{2}}.\end{aligned}$$

This in turn equals

$$1 - \frac{8\delta^{1/4} s_1 s_2}{s_1 s_2 - \binom{|S_1\cap S_2|}{2}}.$$

Observing that $s_1 s_2 - \binom{|S_1\cap S_2|}{2} \geq s_1 s_2/2$, we get

$$\rho(S_1,S_2) \geq 1 - 2\cdot 8\delta^{1/4} = 1 - 16\delta^{1/4} = 1-\beta.$$

Finally we present the property of $G_{n,1/2}$ that we require.

Proposition 7. *The following assertion holds whp for $G_{n,1/2}$. For no $0 \leq \alpha \leq 1/8$, there exist two sets of vertices S_1, S_2 of size at least $(2+6\alpha)\log n$ each and such that $e(S_1,S_2) \geq (1-\alpha^2)K(S_1,S_2)$.*

Proof. The proof idea is as follows. The expected number of such sets S_1, S_2 is at most (summing over all possible sizes for S_1 and S_2 and intersection size)

$$\mu \leq \sum_{y,z\geq(2+6\alpha)\log n} \sum_{x=0}^{\min\{y,z\}} \binom{n}{x}\binom{n}{y-x}\binom{n}{z-x} 2^{-K} \sum_{i=0}^{\alpha^2 K}\binom{K}{i}$$

where $K = K(S_1,S_2)$. The first term accounts for choosing the intersection vertices, then completing each of S_1 and S_2. Next choose which edges are present and finally multiply by the probability for edges/non-edges. We need to show that $\mu = o(1)$, and then the claim follows from Markov's inequality.

Define

$$f(x,y,z) = \binom{n}{x}\binom{n}{y-x}\binom{n}{z-x} 2^{-K} \sum_{i=0}^{\alpha^2 K}\binom{K}{i}, \tag{10}$$

so that

$$\mu \leq \sum_{y,z\geq(2+6\alpha)\log n} \sum_{x=0}^{\min(y,z)} f(x,y,z). \tag{11}$$

Our first goal is to estimate the sum $\sum_{i=0}^{\alpha^2 K} \binom{K}{i}$. We start out with the standard estimate

$$\sum_{i=0}^{\rho K} \binom{K}{i} \leq 2^{Kh(\rho)} \qquad \text{for } 0 \leq \rho \leq 1/2,$$

where $h(\rho) = -\rho \log(\rho) - (1-\rho)\log(1-\rho)$ is the binary entropy function. In the range of interest $0 \leq \rho = \alpha^2 \leq 1/64$, we get

$$h(\rho) \leq \rho(-\log(\rho) + 64 \log(64/63)),$$

by bounding $\log(1-\rho)$ by the appropriate linear function.

Now, studying the first and second derivatives of $-\alpha^2 \log(\alpha^2)$, we see that this function is increasing in the range $0 \leq \alpha \leq 1/8$ and reaches its maximal slope in this range at $\alpha = 1/8$. The maximal slope is less than 1.2. Therefore,

$$h(\alpha^2) \leq 1.2\alpha + 64 \log\left(\frac{64}{63}\right)\alpha^2 \leq \left(1.2 + 8\log\left(\frac{64}{63}\right)\right)\alpha \leq \frac{3}{2}\alpha,$$

and so

$$\sum_{i=0}^{\alpha^2 K} \binom{K}{i} \leq 2^{\frac{3}{2}K\alpha}.$$

Going back to (10), bounding $\binom{n}{t}$ by n^t and recalling that $K = yz - \binom{x}{2}$, we get

$$\begin{aligned}\log f(x,y,z) &\leq (y+z-x)\log n - K\left(1 - \frac{3}{2}\alpha\right) \\ &= (y+z)\log n - yz\left(1-\frac{3}{2}\alpha\right) - x\log n + \left(1 - \frac{3}{2}\alpha\right)\frac{x^2}{2}.\end{aligned}$$

The maximum of the function $x \mapsto -x\log n + (1-\frac{3}{2}\alpha)x^2/2$ in the range $x \in [0, \min\{y,z\}]$ is reached at the boundary $x = \min\{y,z\}$, which, assuming wlog $y \geq z$, is at $x = z$. Thus,

$$\begin{aligned}\log f(x,y,z) &\leq (y+z)\log n - yz\left(1-\frac{3}{2}\alpha\right) - z\log n + \left(1-\frac{3}{2}\alpha\right)\frac{z^2}{2} \\ &= y\log n - \left(1-\frac{3}{2}\alpha\right)\left(yz - \frac{z^2}{2}\right).\end{aligned}$$

Observe that $yz - z^2/2 \geq yz/2$, and hence

$$\log f(x,y,z) \leq y\log n - \left(1-\frac{3}{2}\alpha\right)\frac{yz}{2} \leq y\left(\log n - \frac{z}{2}\left(1 - \frac{3}{2}\alpha\right)\right).$$

Recall our choice of z: $z \geq (2+6\alpha)\log n$ (and the same goes for y). Since $(1-\frac{3}{2}\alpha)(2+6\alpha) \geq 2$ for our values of α,

$$\log f(x,y,z) = -\Omega(\log^2 n).$$

Plugging this into (11) one obtains

$$\mu \le \sum_{y,z \ge (2+6\alpha)\log n} \sum_{x=0}^{\min\{y,z\}} 2^{-\Omega(\log^2 n)} \le n^3 \cdot n^{-\Omega(\log n)} = o(1).$$

The proposition follows by Markov's inequality.

3.3 The Distinguishing Algorithm

Let $\mathcal{A}$ be a polynomial time algorithm that finds the ε-best ε-equilibrium in a two player game. We shall show that there exists an algorithm $\mathcal{B}$ that runs in polynomial time and distinguishes *whp* between a graph randomly chosen from $G_{n,1/2}$ and an arbitrary graph with a clique of size $c_1 \log n$.

The algorithm $\mathcal{B}$ does the following on an input graph G, which is either a graph from $G_{n,1/2}$ or a graph containing a clique of size at least $(2+28\varepsilon^{1/8})\log n$.

1. If any of the below steps fails, return "G belongs to $G_{n,1/2}$".
2. Generate the game matrix with parameter $\beta = 16\varepsilon^{1/4}$ in the matrix B.
3. Run $\mathcal{A}$ to receive an ε-best ε-equilibrium of that game.
4. Calculate a 7ε-equilibrium of value at least $1-3\varepsilon$ whose support lies entirely on $A(G)$ (according to the procedure in the proof of Proposition 4).
5. Use this equilibrium to find two sets S_1 and S_2 satisfying $|S_1|, |S_2| \ge (2+6\beta^{1/2})\log n$ and $\rho(S_1, S_2) \ge 1-\beta$ (use the procedure in the proof of Proposition 6).
6. If succeeded, return "G does not belong to $G_{n,1/2}$".

We shall analyze the algorithm for $\varepsilon \le \varepsilon_0$. ε_0 is determined by the constraint of Proposition 7. Specifically, for the algorithm to answer correctly on $G_{n,1/2}$, it suffices if step 5 fails. For this we want to choose β so that *whp* $G_{n,1/2}$ does not contain two sets S_1, S_2 of the prescribed size and density. This is achieved by plugging $\alpha = \beta^{1/2}$, that is $\alpha = 4\varepsilon^{1/8}$, in Proposition 7, which translates to $\varepsilon_0 = (4 \cdot 8)^{-8}$.

It remains to prove that the algorithm answers correctly when G has a clique of size $\ge c_1 \log n$. Assume that the matrix B satisfies Proposition 1, which is the case *whp*. Propositions 2 and 4 then guarantee that Step 4 succeeds, and Step 5 succeeds by Proposition 6. Thus again the correct answer is returned.

4 Finding a Clique of Size $3\log n$

Let $\beta = 16\varepsilon^{1/4}$ as in the proof of Theorem 1, and let $H \in G_{n,1/2,k}$ with $k \ge (3+14\beta^{1/2})\log n$. Let C be the vertices of the planted clique. Observe that in no place in Section 1 did we use the actual size of the planted clique, just the "separation" properties as given by Proposition 1. Proposition 1 can be restated easily with $c_1 \ge (3+14\beta^{1/2})$ and $c_2 = (3+13\beta^{1/2})\log n$. Therefore by the same arguments as in the Proof of Theorem 1, we are guaranteed to efficiently find two sets S_1, S_2 of size at least $c_2 \log n$ each and density $1-\beta$. Our first goal is to show that $S_1 \cup S_2$ must intersect the planted clique on many vertices. Suppose by contradiction that the intersection size is no more than $(1+\beta^{1/2})\log n$ vertices. Define $S_1' = S_1 \setminus C$ and similarly $S_2' = S_2 \setminus C$. Clearly, S_1', S_2' still contain at least $(2+12\beta^{1/2})\log n$ vertices, and all edges between S_1' and S_2' are random edges of $G_{n,1/2}$. Finally let us compute the density $\rho(S_1', S_2')$. Recall Equation (9) which guarantees that in $A[S_1 \times S_2]$ there are at most $(\beta/2)S_1 S_2$ zeros. As for $A[S_1' \times S_2']$, the fraction of zeros is at most

$$\frac{(\beta/2)|S_1||S_2|}{|S_1'||S_2'|} \leq \frac{(\beta/2)|S_1||S_2|}{(2/3)^2|S_1||S_2|} = \frac{9\beta}{8}.$$

In the inequality we use $|S_1'| \geq 2|S_1|/3$, $|S_2'| \geq 2|S_2|/3$. Now the same arguments that follow Equation (9) give $\rho(S_1', S_2') \geq 1 - 2 \cdot \frac{9\beta}{8} \geq 1 - 3\beta$. To conclude, we found two sets of size at least $(2+12\beta^{1/2})\log n$ each, and density $1-3\beta$, involving only edges of $G_{n,1/2}$. This however contradicts Proposition 7 (when plugging $\alpha^2 = 3\beta$ in that proposition).

Let us now assume that $S_1 \cup S_2$ contains at least $(1+\beta^{1/2})\log n$ vertices from the planted clique, call this set I. Further assume w.l.o.g. that $|S_1 \cup S_2| = O(\log n)$ (we can always do this since in Equations (6) and (8), which define S_1, S_2, we can limit the set size). Thus one can find I in polynomial time (using exhaustive search). Finally, let us compute the probability that a vertex $x \notin C$ has full degree in I. Since the planted clique was chosen independently of the random graph, this probability is at most

$$2^{-|I|} = 2^{-(1+\beta^{1/2})\log n} = n^{-(1+\beta^{1/2})}.$$

Using the union bound, *whp* no such vertex exists. Now apply the following greedy procedure on I: go over the vertices of G and add each vertex if its degree in I is full. By the latter argument, this algorithm succeeds *whp* in reconstructing the planted clique.

5 Discussion

In this work we explored the technique of [12] in the regime where the planted clique is close to the smallest possible, that is of size $(2+\delta)\log n$ for small $\delta > 0$. We showed that for the problem of distinguishing $G_{n,1/2}$ from $G_{n,1/2,k}$, where $k = (2+\delta)\log n$, the reduction works for arbitrarily small $\delta > 0$, provided that ε-best ε-approximate Nash equilibria can be found for a corresponding small $\varepsilon(\delta) > 0$.

We also showed that the problem of *finding* a planted clique of size $(3+\delta)\log n$ for small $\delta > 0$ can be reduced to finding an ε-best ε-approximate Nash equilibrium for a sufficiently small $\varepsilon > 0$. But since the maximal clique in $G_{n,1/2}$ is only of size $(2-o(1))\log n$, this is possibly not optimal, and the question whether one could achieve the optimal $2\log n$ clique size barrier for finding the clique is still open.

References

1. Alon, N., Kahale, N.: A spectral technique for coloring random 3-colorable graphs. SIAM Journal on Computation 26(6), 1733–1748 (1997)
2. Alon, N., Krivelevich, M., Sudakov, B.: Finding a large hidden clique in a random graph. Random Structures and Algorithms 13(3-4), 457–466 (1998)
3. Alon, N., Spencer, J.: The Probabilistic Method. Wiley, Chichester (1992)
4. Chen, X., Deng, X., Teng, S.-H.: Computing Nash equilibria: Approximation and smoothed complexity. In: FOCS 2006: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, USA, pp. 604–612 (2006)
5. Conitzer, V., Sandholm, T.: Complexity Results about Nash Equilibria. In: 18th International Joint Conference on Artificial Intelligence, pp. 765–771 (2003)
6. Daskalakis, C., Goldberg, P.W., Papadimitriou, C.H.: The complexity of computing a Nash equilibrium. In: STOC 2006: Proceedings of the 38th annual ACM Symposium on Theory of computing, USA, pp. 71–78 (2006)
7. Feige, U.: Relations between average case complexity and approximation complexity. In: STOC 2002: Proceedings of the 34th annual ACM Symposium on Theory of Computing, pp. 534–543 (2002)
8. Feige, U., Ofek, E.: Easily refutable subformulas of large random 3CNF formulas. Theory of Computing 3(1), 25–43 (2007)
9. Gilboa, I., Zemel, E.: Nash and correlated equilibria: Some complexity considerations. Games and Economic Behavior 1(1), 80–93 (1989)
10. Jerrum, M.: Large Cliques Elude the Metropolis Process. Random Structures and Algorithms 3(4), 347–359 (1992)
11. Juels, A., Peinado, M.: Hiding Cliques for Cryptographic Security. Designs, Codes and Cryptography 20(3), 269–280 (2000)
12. Hazan, E., Krauthgamer, R.: How hard is it to approximate the best Nash equilibrium? In: ACM-SIAM Symposium on Discrete Algorithms, USA, pp. 720–727 (2009)
13. Kučera, L.: Expected Complexity of Graph Partitioning Problems. Discrete Applied Mathematics 57(2-3), 193–212 (1995)
14. Lipton, R.J., Markakis, E., Mehta, A.: Playing large games using simple strategies. In: 4th ACM conference on Electronic commerce, USA, pp. 36–41 (2003)
15. Tsaknakis, H., Spirakis, P.G.: An Optimization Approach for Approximate Nash Equilibria. In: Deng, X., Graham, F.C. (eds.) WINE 2007. LNCS, vol. 4858, pp. 42–56. Springer, Heidelberg (2007)