Electronic Colloquium on Computational Complexity, Report No. 152 (2006)

Tight integrality gaps for Vertex Cover SDPs in the Lovász-Schrijver hierarchy

Konstantinos Georgiou* Avner Magen* Toniann Pitassi* Iannis Tourlakis*

Department of Computer Science
University of Toronto

Abstract

We prove that the integrality gap after tightening the standard LP relaxation for VERTEX COVER with $\Omega(\sqrt{\log n/\log\log n})$ rounds of the SDP LS_+ system is $2-o(1)$.

1 Introduction

A *vertex cover* in a graph $G=(V,E)$ is a set $S\subseteq V$ such that every edge $e\in E$ intersects S in at least one endpoint. The minimum VERTEX COVER problem asks what size the minimum vertex cover in G is. Determining how well we can approximate VERTEX COVER is one of the outstanding open problems in the complexity of approximation.

In a seminal paper, Goemans and Williamson [9] introduced semidefinite programming (SDP) as a tool for obtaining approximation algorithms. Since then semidefinite programming has been applied to various NP-hard optimization problems and has become an important technique. Indeed, for many problems the best approximation algorithms rely on semidefinite programming relaxations.

When semidefinite programming was introduced it was hoped that it could be used to yield a $2-\Omega(1)$-approximation algorithm for VERTEX COVER. Unfortunately, this has not proved the case: In '95 Kleinberg and Goemans [15] showed that the standard SDP for VERTEX COVER has an integrality gap of $2-o(1)$. Subsequently, Charikar [5] showed that the integrality gap remains $2-o(1)$ even if we add additional triangle inequality constraints. Later, Hatami et al. [11] strengthened this further, to show that this state of affairs remains even when we add the so-called pentagonal inequality constraints. Interestingly enough, all three of these papers use the same graph family about which we will say more below.

Indeed, the state of the art is such that SDP based algorithms for VERTEX COVER must settle for competing in "how big" the "little oh" term is in the $2-o(1)$ factor. Halperin [10] gives a $(2-\log\log\Delta/\log\Delta)$ approximation, where Δ is the maximal degree of the graph. Later, Karakostas [12] obtained a $(2-\Omega(1/\sqrt{\log n}))$-approximation algorithm by using a stronger SDP relaxation.

Nevertheless, it is consistent with the known hardness results for VERTEX COVER that there could exist some other SDP for VERTEX COVER with integrality gap, say, 1.4. In particular, the best PCP-based hardness results known only show that 1.36-approximation of VERTEX COVER is NP-hard ([6]). Only by assuming Khot's Unique Games Conjecture [14] do we get a tight $2-\Omega(1)$ inapproximability result [13]. However, determining the validity of the Unique Games Conjecture (or directly improving Dinur and Safra's hardness result) remains a difficult open problem.

*Funded by NSERC

ISSN 1433-8092

To get a better picture of the approximability of VERTEX COVER (especially in light of the inability to resolve the issue with PCP-based methods), Arora et al. [2] suggested the following approach: rule out good approximations for VERTEX COVER by large families of algorithms. One such family is the class of relaxations for VERTEX COVER in the Lovász-Schrijver hierarchies. Lovász and Schrijver [16] define procedures LS and LS_+ for systematically tightening linear and semidefinite relaxations, respectively, over many rounds. The key algorithmic properties LS and LS_+ enjoy are that (a) n rounds of even the weaker LS procedure suffice to derive the integral hull (and hence obtain exact solutions) and that (b) we can optimize a linear function over the rth round LS and LS_+ relaxations in $n^{O(r)}$ time.

Many celebrated SDP-based algorithms, including the seminal MAX-CUT algorithm of Goemans-Williamson [9] for MAX-CUT and the Arora-Rao-Vazirani algorithm [3] for SPARSEST-CUT, can be derived using a constant number of rounds of LS_+. Thus proving inapproximability results for LS_+ based algorithms rules out the most promising class of algorithms that we currently have for obtaining $2-\Omega(1)$ approximations for VERTEX COVER. Furthermore, unlike PCP-based results we emphasize that such results do not rely on any complexity theoretic assumptions.

Arora et al. [2] obtained the first result along these lines for VERTEX COVER showing that $\Omega(\log n)$ rounds of the weaker LS procedure has an integrality gap of $2-o(1)$. Tourlakis [20] subsequently proved an integrality gap of $1.5-o(1)$ for VERTEX COVER, for $\Omega(\log^2 n)$ rounds of LS. Very recently, a beautiful result by Schoenebeck et al. [19] showed that the integrality gap is $2-o(1)$ even after $\Omega(n)$ rounds of LS. Unfortunately, the hard examples used in all three of these papers cannot be used to prove a $2-o(1)$ integrality gap for even one round of LS_+.

As aluded above, one round of LS_+ suffices to derive the Goemans-Williamson [9] algorithm for MAX CUT and hence give a 0.878-approximation. However, Schoenebeck et al. [19] show that $\Omega(n)$ rounds of LS for MAX CUT still do not suffice to get better than a 0.5-approximation. It would be reasonable then to wonder if a similar gap exists for VERTEX COVER.

The only known integrality gaps for semidefinite relaxations for VERTEX COVER in the LS_+ hierarchy prior to the current paper were proved by Schoenebeck et al. in [18]. They show that an integrality gap of 7/6 remains after $\Omega(n)$ rounds of LS_+. Their result built upon LS_+ lower bounds for MAX-3AT by Alekhnovich et al. [1] and MAX-kSAT by Buresh-Oppenheim et al. [4], as well as using ideas from Feige and Ofek [17]. At root of their result is a graph family obtained using the standard FGLSS [7] reduction from MAX-3XOR to VERTEX COVER. It is not hard to show that this result is tight for this graph family since the integrality gap for it is *at most* 7/6 after one round of LS_+. Thus it remained a challenging open problem to prove a $2-o(1)$ integrality gap for even two rounds of LS_+. (Note that Charikar's construction [5] does imply a one round integrality gap of $2-o(1)$ for VERTEX COVER.)

To prove integrality gaps of $2-o(1)$ for SDP relaxations in the LS_+ hierarchy, the obvious place to start would be the graph families used by [15, 5, 11]. We briefly describe these graphs now. The vertex set is $\{-1,1\}^m$ and two vertices are adjacent if their Hamming distance is exactly $(1-\gamma)m$. Here γ is a sufficently small real number, and m is an integer such that γm is even. A result of Frankl and Rödl [8] then implies that the largest independent set of these graphs is of size at most $(2-\eta(\gamma))^m$ where $\eta(\gamma)>0$ and does not depend on m. This immediately says that the vertex cover of these graphs must have size $(1-o(1))|V|$ for any fixed γ. Interestingly enough, no other family of graphs is known that allows for $2-o(1)$ integrality gap for any SDP based algorithm for VERTEX COVER.

In this work we use this family to prove that $\Omega(\sqrt{\log n/\log\log n})$ rounds of LS_+ has an integrality gap of $2-o(1)$ for VERTEX COVER. Our main technical tool is the construction of a sequence of tensoring operations on vectors. This operation has the property that inner products on the set of tensored vectors are a polynomial function of the the inner products of the original vectors. A similar tensoring operation was used in [5]. However our application calls for more complicated polynomials, and moreover the polynomials (and hence the tensored vectors) will change as the induction unwinds in our lower bound argument. (More details are given in Section 3.)

2 Definitions and Notation

2.1 Standard SDPs for VERTEX COVER

The standard way to formulate VERTEX COVER as a quadratic integer program is as follows:

$$\begin{array}{lll} \min & \sum_{i \in V}(1 - x_0 x_i)/2 & \\ \text{s.t.} & (x_0 - x_i)(x_0 - x_j) = 0 & \forall ij \in E \\ & x_i \in \{-1, 1\} & \forall i \in \{0\} \cup V \end{array}$$

The set of vertices i for which $x_i = x_0$ correspond to the minimal vertex cover. Relaxing this to a semidefinite program we obtain the following:

$$\begin{array}{lll} \min & \sum_{i \in V}(1 - \mathbf{v_0} \cdot \mathbf{v_i})/2 & \\ \text{s.t.} & (\mathbf{v_0} - \mathbf{v_i}) \cdot (\mathbf{v_0} - \mathbf{v_j}) = 0 & \forall ij \in E \\ & \|\mathbf{v}_i\| = 1 & \forall i \in \{0\} \cup V \end{array} \tag{1}$$

We can strengthen this relaxation by adding all constraints valid in the integral case. One such set of constraints commonly considered are the triangle inequalities:

$$(\mathbf{v_i} - \mathbf{v_j}) \cdot (\mathbf{v_i} - \mathbf{v_k}) \geq 0 \quad \forall i, j, k \in \{0\} \cup V. \tag{2}$$

2.2 Lovász-Schrijver Lift-and-Project Systems

A convex cone is a set $K \subseteq \mathcal{R}^{d+1}$ such that for every $\mathbf{y}, \mathbf{z} \in K$, and for every $\alpha, \beta \geq 0$, $\alpha\mathbf{y} + \beta\mathbf{z} \in K$. For a matrix Y, we denote by Ye_i the ith column of Y.

If $K \subseteq \mathbb{R}^{d+1}$ is a convex cone, we define $M_+(K) \subseteq \mathbb{R}^{(d+1)\times(d+1)}$ to consist of all $(d+1) \times (d+1)$ matrices Y such that,

1. Y is symmetric and positive semidefinite (PSD).

2. For all $i = 0, 1, \ldots, d$, $Y_{0i} = Y_{ii}$.

3. For all $i = 0, 1, \ldots, d$, Ye_i and $Ye_0 - Ye_i$ are in K.

We then define $N_+(K) = \{Ye_0 : Y \in M_+(K)\} \subseteq \mathbb{R}^{d+1}$. That is, a vector $\mathbf{y} = (y_0, \ldots, y_d)$ is in $N_+(K)$ if there exists $Y \in M_+(K)$ such that $Ye_0 = \mathbf{y}$ in which case Y is called a *protection matrix for* $\mathbf{y}$.

We define the notation $N_+^k(K)$ inductively by setting $N_+^0(K) = K$ and $N_+^k(K) = N_+(N_+^{k-1}(K))$.

Let $G = (V, E)$ be a graph and assume that $V = \{1, \ldots, n\}$. The VERTEX COVER polytype for G, $VC(G)$, is the set of vectors $\mathbf{y} \in \mathbb{R}^{n+1}$ such that:

$$y_i + y_j \geq y_0 \quad \text{for all } ij \in E \tag{3}$$

$$y_0 \geq y_i \geq 0 \quad \text{for all } i \in V \tag{4}$$

$$y_0 \geq 0 \tag{5}$$

We call the constraints given by (3) the *edge constraints* and the constraints given by (4) the *box constraints.*

The relaxation of the VERTEX COVER problem arising from k rounds of LS_+ is the solution of

- $\min \sum_{i=1}^n y_i$
- subject to $(y_0, \ldots, y_n) \in N_+^k(VC(G))$, and $y_0 = 1$

The *integrality gap* of this relaxation (for graphs over n vertices) is the largest ratio between the minimum vertex cover size of G and the optimum in the above program, over all graphs G with n vertices.

We note that the relaxation $N_+(VC(G))$ is at least as strong as the the standard SDP relaxation (1) for VERTEX COVER in the sense that the Choleski decomposition of any matrix $Y \in M_+(VC(G))$ satisfies (under an affine transformation) the SDP (1). In fact, it even satisfies the triangle inequalities (2) for the case $i = 0$.

2.3 Vectors and Tensoring

We will use $\mathbf{0}$ to denote the all-0 vector. Given two vectors $\mathbf{x}, \mathbf{y} \in \{-1, 1\}^n$ their *Hamming distance* $d_H(x, \mathbf{y})$ is $|\{i \in [n] : x_i \neq y_i\}|$. For two vectors $\mathbf{u} \in \mathbb{R}^n$ and $\mathbf{v} \in \mathbb{R}^m$ denote by $(\mathbf{u}, \mathbf{v}) \in \mathbb{R}^{n+m}$ the vector whose projection on the first n coordinates is $\mathbf{u}$ and on the last m coordinates is $\mathbf{v}$.

Recall that the tensor product $\mathbf{u} \otimes \mathbf{v}$ of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ is the vector in $\mathbb{R}^{n^2}$ indexed by ordered pairs from $n \times n$ and that assumes the value $\mathbf{u}_i \mathbf{v}_j$ at coordinate (i, j). Define $\mathbf{u}^{\otimes d}$ to be the vector in $\mathbb{R}^{n^d}$ obtained by tensoring $\mathbf{u}$ with itself d times.

Definition 1 *Let $P(x) = c_1 x^{t_1} + \ldots + c_q x^{t_q}$ be a polynomial with nonnegative coefficients. Then we define T_P to be the function that maps a vector $\mathbf{u}$ to the vector $T_P(\mathbf{u}) = (\sqrt{c_1} u^{\otimes t_1}, \ldots, \sqrt{c_q} u^{\otimes t_q})$.*

Fact 1 *For all vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$, $T_P(\mathbf{u}) \cdot T_P(\mathbf{v}) = P(\mathbf{u} \cdot \mathbf{v})$.*

2.4 Frankl-Rödl Graphs

Definition 2 *Fix γ, $0 \leq \gamma \leq 1$ and an integer $m \geq 1$. The* Frankl-Rödl graph *G_m^γ is the graph with vertices $\{-1, 1\}^m$ and where two vertices $i, j \in \{-1, 1\}^m$ are adjacent if $d_H(i, j) = (1 - \gamma)m$.*

Relatives of the following lemma appear in [8] in various guises, but it seems as if the exact statement that we will use requires a further small step which we sketch in Appendix A. The key difference with variants in [8] is that we explicitly allow γ to be a function of m.

Lemma 1 *Let m be an integer, and let $\gamma = \gamma(m) > 0$ be a sufficiently small number so that γm is an even integer. Then there are no independent sets in G_m^γ of size larger than $m 2^m (1 - \gamma^2/64)^m$.*

For technical reasons that we will make clear later, we will in fact use a variant of G_m^γ which we denote by $\frac{1}{2} G_{m+1}^\gamma$. This graph $\frac{1}{2} G_{m+1}^\gamma$ is the subgraph of G_{m+1}^γ spanned by all vertices of the form $\{1\} \times \{-1, 1\}^m$. The critical point to notice here is that $\frac{1}{2} G_{m+1}^\gamma$ has no independent set of size larger than $(m + 1) 2^{m+1} (1 - \gamma^2/64)^{m+1}$ which is still $o(|V|)$ when $\gamma \in \Omega(\sqrt{\log m / m})$.

2.5 Saturated Vectors and their Properties

In general, our lower bounds will be proved by arguing about vectors whose coordinates are either 0/1 or take on at most one other fixed value. The following definition formalizes this.

Definition 3 *A vector* $\mathbf{y} \in [0,1]^{n+1}$ *is an* ϵ-vector *if* $y_0 = 1$ *and* $y_i \in \left\{0, \frac{1}{2}+\epsilon, 1\right\}$ *for all* $1 \leq i \leq n$.

Note that ϵ-vectors have the property that the sum of any two non-0/1 coordinates is $1+2\epsilon$. A weaker condition on vectors in $[0,1]^{n+1}$ would be to only require that the sum of any two non-0/1 coordinates is at least $1+2\epsilon$. Such vectors were used in Schoenebeck et al. [19], and the following definition is adapted from their paper:

Definition 4 ([19]) *Let* $G = (V, E)$ *be a graph. A vector* $\mathbf{y} \in VC(G)$ *is* ϵ-saturated *if for every edge* $ij \in E$ *such that* y_j *and* y_k *are both not integral,* $y_i + y_j \geq 1 + 2\epsilon$.

Saturated vectors have the important following property proved in Schoenebeck et al. [19] (for completeness we include the proof of their lemma in the Appendix):

Lemma 2 ([19]) *Let* $G = (V, E)$ *be any graph and suppose* $\mathbf{x} \in VC(G)$ *is* ϵ*-saturated. Then* $\mathbf{x}$ *is a convex combination of* ϵ*-vectors in* $VC(G)$.

The lemma essentially says that even though being ϵ-saturated is a weaker condition than being an ϵ-vector, proving lower bounds for ϵ-saturated vectors is no harder than proving lower bounds for ϵ-vectors. This will be crucial for our arguments.

3 Overview of the Proof

We start with the Frankl-Rödl graph family, $G = G_m^\gamma$, and denote by $n = 2^m$ the size of G. We will show that the point $\mathbf{x} = (1, 1/2+\epsilon, \ldots, 1/2+\epsilon)$ is contained in the polytope defined after $\Omega(\sqrt{\log n / \log\log n})$ rounds of LS_+. This clearly gives us our desired $2 - o(1)$-inapproximability result.

The standard way to prove that a certain point $\mathbf{x}$ is in the polytope resulting from r rounds of LS_+ (hereafter, the "rth polytope") is as follows: (1) Exhibit a symmetric PSD "protection" matrix Y for $\mathbf{x}$ such that its diagonal and first column of Y equal $\mathbf{x}$. (2) Show inductively that the vectors Ye_i and $Y(e_0 - e_i)$ are in the $(r-1)$st polytope. By definition of LS_+ it will then follow that $\mathbf{x}$ is in the rth polytope.

To define the protection matrix for a a point $\mathbf{x}$ we will start with the canonical set of vectors associated with the vertices of G, namely the normalized versions of the vectors $\{-1, 1\}^m$ (these vectors were also the starting point for [15, 5, 11]). These vectors have the appealing property that the inner product of vectors associated with vertices i and j is solely a function of the Hamming distance $d_H(i, j)$ between i and j. Observe that this property will not be compromised by applying the T_P tensoring transformation to the vectors. Indeed, we will use this tensoring transformation with a specific polynomial P to obtain a new set of tensored vectors and then define our candidate protection matrix to be essentially the Gram matrix of these vectors. (Note that Charikar [5] also uses a tensor transformation to prove his integrality gap for the SDP with triangle inequalities.)

A consequence of the observation above is that the values on the diagonal of the Gram matrix are all identical. So using this recipe to come up with a protection matrix will only work for vectors like $\mathbf{x}$ where all fractional values are the same. In fact, for technical reasons which we do not get into in this outline, this recipe produces valid protection matrices only when $\mathbf{x}$ is a ρ-vector for some $0 < \rho < 1/2$.

To continue our inductive argument we would in turn like to use the same recipe to find candidate protection matrices for each of the $2n$ vectors Ye_i and $Y(e_0 - e_i)$ (or, more accurately, for the projections of these vectors on to the hyperplane $x_0 = 1$). The problem is that while these $2n$ vectors may indeed be in the $(r-1)$st polytope, they may not be ρ-vectors. (This is because the entries Y_{ij} of Ye_i are a polynomial function of $d_H(i,j)$ and the latter is distributed like a binomial distribution when i is fixed.) So the recipe cannot be used without extra work.

To remedy the situation, we will apply a "correction" phase as follows. (Note that "correction" phases of some sort or another can be found in many previous works [2, 1, 4, 20, 18, 19].) We will construct the tensored vectors so that the vectors Ye_i, $Y(e_0 - e_i)$ have high saturation. We will then use Lemma 2 to express these vectors as convex combinations of ρ'-vectors from $VC(G)$ for some $\rho' > 0$ (this is the "correction" part). We then carry on the induction with these ρ'-vectors to show that they lie in the $(r-1)$st polytope. Convexity then implies that the vectors Ye_i, $Y(e_0 - e_i)$ are also in the $(r-1)$st polytope.

To summarize, we start with a vector $\mathbf{x} = (1, 1/2+\epsilon_0, \ldots, 1/2+\epsilon_0)$, $\epsilon_0 = \epsilon$, and after one round we wish to show that the $2n$ vectors Ye_i, $Y(e_0 - e_i)$ corresponding to $\mathbf{x}$'s protection matrix Y have large saturation ϵ_1; and then we continue with vectors with fractional values $1/2 + \epsilon_1$, and so on. In this process, the obvious objective is to make the sequence $\epsilon_0, \epsilon_1, \epsilon_2, \ldots$ as slowly decreasing as possible, thereby making it last for many rounds before it becomes negative (which amounts to negative saturation, and hence that the corresponding vectors are not in $VC(G)$ at all). We will show that for each round i, we can maintain that $\epsilon_i = \epsilon_{i-1} - O(\gamma)$. Thus for arbitrarily small initial ϵ_0, we get an induction chain of length $\Omega(1/\gamma)$.

The engine of this process and our main technical tool are the tensor-inducing polynomials. Along with the sequence of decreasing saturation values we shall have a sequence of polynomials with positive coefficients, $P_0, P_1, P_2, \ldots$ where P_i depends on ϵ_i and determines ϵ_{i+1}. The choice of this sequence is at the heart of the matter. The nonnegativity requirement on the coefficients makes this a challenging task as otherwise we could approximate any continuous function that fits our needs. In [5], Charikar uses a polynomial designed to produce vectors that satisfy the triangle inequality. This polynomial is the sum of a linear term and a degree $O(1/\gamma)$ monomial that unfortunately produces a poor saturation, and hence cannot be used to proceed beyond one round of LS_+. In particular, the saturation it provides is about $1/m \ll \gamma$. The problem is intrinsic: let's suppose that we are dealing with $Y(e_0 - e_i)$ for some fixed i. It's easy to see that whatever polynomial we may use, edges ij will have no slack at all in $Y(e_0 - e_i)$. This edge itself does not affect the saturation as one of its values is integral. However, the continuous nature of the construction means that nearby edges $i'j'$ correspond to fractional values that are attained by the polynomial at nearby points. The only way to deal with this state of affairs is to make sure that the polynomial we use varies a lot between such points. This calls for a polynomial with a very large derivative, and hence one with very high degree $d \gg m$; in contrast, the polynomial that Charikar uses has degree independent of m.

There is one more complication which is the "shadow" of the above problem. Consider $Y(e_0 - e_i)$ for some fixed i. Our problem occurs in this vector for edges $\hat{i}j$ where $\hat{i}$ is the antipodal vertex to i in $\{-1,1\}^m$. When we start with the normalized versions of the vectors $\{-1,1\}^m$ this leads (again, regardless of the polynomial) to an undesirable multiplicative (as opposed to additive) drop in the saturation after each round. Consequently, this leads to an inferior lower bound, namely the integrality gap we get will be guaranteed for only $\Theta(\log m) = \Theta(\log\log n)$ rounds. The problem disappears if we disallow inner products of the normalized cube which are -1 or extremely close to it. This can be achieved by starting with the graph $\frac{1}{2}G^\gamma_{m+1}$ instead of G^γ_m and proceeding as before.

4 Main Theorem

Lemma 3 *Let m be a sufficiently large integer and $\gamma > 0$. Let $n = 2^m$ and let ϵ be such that $5\gamma \le \epsilon < 1/4$. Suppose in addition that $\mathbf{y} \in \mathbb{R}^{n+1}$ is an ϵ-vector in $VC(\frac{1}{2}G^\gamma_{m+1})$. Then there exists a protection matrix Y for $\mathbf{y}$ such that for all i with $0 < y_i < 1$, Ye_i/y_i and $Y(e_0 - e_i)/(1 - y_i)$ are convex combinations of $(\epsilon - 5\gamma)$-vectors. In particular, $y \in N_+(VC(\frac{1}{2}G^\gamma_{m+1}))$.*

Given Lemma 3, we can prove our main theorem:

Theorem 5 *Let m be sufficiently large, and fix $\gamma \ge 12\sqrt{\frac{\log m}{m}}$ such that γm are all even. Let ϵ be such that $5\gamma \le \epsilon < 1/4$. Let $n = 2^m$ and let $r = \lfloor \frac{\epsilon}{5\gamma} \rfloor - 1$. Then the integrality gap of $N^r_+(VC(\frac{1}{2}G^\gamma_{m+1}))$ is at least $2 - 4\epsilon - 4/m$.*

Proof: Let $\mathbf{y} = (1, \frac{1}{2}+\epsilon, \ldots, \frac{1}{2}+\epsilon) \in \mathbb{R}^{n+1}$. Clearly $\mathbf{y} \in VC(\frac{1}{2}G^\gamma_{m+1})$. A simple inductive argument using Lemma 3 then implies that $\mathbf{y} \in N^r_+(VC(\frac{1}{2}G^\gamma_{m+1}))$.

On the other hand, Lemma 1 implies that the largest independent set in $\frac{1}{2}G^\gamma_{m+1}$ has size at most

$$2^{m+1}[(m+1)(1-\gamma^2/64)^{m+1}] \le (m+1)2^{m+1}e^{-\frac{\gamma^2 m}{64}} \le (m+1)2^{m+1}e^{-\frac{144}{64}\log m} \le 2 \cdot 2^m/m.$$

Hence, the integrality gap for $N^r_+(VC(G^\gamma_m))$ is at least,

$$\frac{2^m - 2\cdot 2^m/m}{n(\frac{1}{2}+\epsilon)} = \frac{2(1-2/m)}{1+2\epsilon} \ge 2 - 4\epsilon - \frac{4}{m}.$$

□

The remainder of this section is dedicated to proving Lemma 3.

Proof:[Lemma 3] Fix m and γ and consider $G = \frac{1}{2}G^\gamma_{m+1}$. Denote the vertices V of G as vectors $\mathbf{w}_i \in \{1\} \times \{-1,1\}^m$, $1 \le i \le 2^m$, and for each vector $\mathbf{w}_i \in V$ we define $\mathbf{u}_i = \frac{1}{\sqrt{m+1}}\mathbf{w}_i$. Note that $\|\mathbf{u}_i\| = 1$ and $\mathbf{u}_i \cdot \mathbf{u}_j = 2\gamma - 1$ for all $ij \in E$. Moreover, $|\mathbf{u}_i \cdot \mathbf{u}_j| \le 1 - \frac{2}{m+1}$ for all $1 \le i < j \le 2^m$.

Given a polynomial P with nonnegative coefficients we will now define a procedure that takes the vectors $\{\mathbf{u}_i\}$, applies the tensoring operation T_P defined in Proposition 1 to obtain a new set of vectors, and then applies a linear transformation to the resulting vectors. The Gram matrix of the vectors resulting from this procedure will be called $Y(P, \mathbf{y})$. Our goal will be to pick P so that $Y(P, \mathbf{y})$ is a protection matrix for $\mathbf{y}$.

First, define $\mathbf{v}_0 = (1, 0, \ldots, 0)$. For each vertex $1 \le i \le 2^m$ define,

$$\mathbf{v}_i = \begin{cases} \mathbf{v}_0, & \text{if } y_i = 1 \\ \mathbf{0}, & \text{if } y_i = 0 \\ (\frac{1}{2}+\epsilon, \frac{\sqrt{1-4\epsilon^2}}{2} \cdot T_P(\mathbf{u}_i)), & \text{if } y_i = \frac{1}{2}+\epsilon \end{cases}$$

Let $Y(P, \mathbf{y}) \in \mathbb{R}^{(n+1)\times(n+1)}$ be the positive semi-definite matrix $Y(P, \mathbf{y})_{ij} = \mathbf{v}_i \cdot \mathbf{v}_j$.

We now define a class of polynomials and show that for any polynomial P in this class, $Y(P, \mathbf{y})$ is a protection matrix for $\mathbf{y}$.

Definition 6 *A polynomial $P(x)$ is called (γ,ϵ,m)-*useful *if it satisfies the following four conditions:*

1. *P has only nonnegative coefficients.*
2. *$P(1) = 1$,*
3. *$P(x) \geq P(2\gamma-1) = -\frac{1-2\epsilon}{1+2\epsilon}$ for all $x \in [-1,1]$.*
4. *For all $i \in \{1,\ldots,2^m\}$ and all $jk \in E$,*

$$-\frac{4\epsilon}{1-2\epsilon} \leq P(\mathbf{u}_i\cdot\mathbf{u}_j) + P(\mathbf{u}_i\cdot\mathbf{u}_k) \leq \frac{4\epsilon}{1+2\epsilon}, \tag{6}$$

Claim 1 *If P is (γ,ϵ,m)-useful, then $Y = Y(P,\mathbf{y}) \in M_+(VC(G))$. In particular, $\mathbf{y} \in N_+(VC(G))$.*

Proof: Since Y is PSD by definition, to show that Y is a protection matrix for $\mathbf{y}$ it suffices to show that:

A. For all $0 \leq i \leq n$, $Y_{i0} = Y_{ii} = y_i$,

B. For all $1 \leq i \leq n$, $Ye_i, Y(e_0 - e_i) \in VC(G)$.

Consider constraints A first. Clearly $Y_{i0} = Y_{ii} = y_i$ whenever $y_i \in \{0,1\}$. In particular, note that $Y_{00} = 1$. So assume that $y_i = 1/2+\epsilon$. Clearly $Y_{i0} = \frac{1}{2}+\epsilon$, so consider Y_{ii}. It follows that

$$Y_{ii} = \mathbf{v}_i\cdot\mathbf{v}_i = \left(\frac{1}{2}+\epsilon\right)^2 + \frac{1-4\epsilon^2}{4}T_P(\mathbf{u}_i)\cdot T_P(\mathbf{u}_i) = \frac{1}{4}+\epsilon+\epsilon^2+\frac{1-4\epsilon^2}{4}P(\mathbf{u}_i\cdot\mathbf{u}_i) = \frac{1}{2}+\epsilon,$$

where the last equality follows from the fact that the $\mathbf{u}_i$ are unit vectors and $P(1) = 1$.

Now consider constraints B. We must show that for all $1 \leq i \leq n$, Ye_i and $Y(e_0 - e_i)$ both satisfy the edge constraints (3) and the box constraints (4). Note that if $y_i \in \{0,1\}$, then $\{Ye_i, Y(e_0-e_i)\} = \{\mathbf{0}, Ye_0\} \subseteq VC(G)$ and the constraints are of course satisfied. So assume $y_i = \frac{1}{2}+\epsilon$.

The box constraints require for all $1 \leq j \leq n$ that $0 \leq Y_{ij} \leq Y_{i0}$ and $0 \leq Y_{0j} - Y_{ij} \leq Y_{00} - Y_{i0}$. Equivalently, for all $1 \leq j \leq n$,

$$Y_{i0} + Y_{j0-00} \leq Y_{ij} \leq Y_{i0}. \tag{7}$$

On the other hand, the edge constraints require for all $1 \leq i \leq n$ and all $jk \in E$ that

$$Y_{ij} + Y_{ik} \geq Y_{i0}, \tag{8}$$

$$(Y_{0j} - Y_{ij}) + (Y_{0k} - Y_{ik}) \geq Y_{00} - Y_{i0}. \tag{9}$$

Since (7) holds when $y_i \in \{0,1\}$, by symmetry it also holds if $y_j \in \{0,1\}$. So assume $y_j = \frac{1}{2}+\epsilon$. We first show that the right inequality in (7) holds. Fix $j \in \{1,\ldots,n\}$. Note first that since $P(1) = 1$, it follows that $\|\mathbf{v}_i\| = \|\mathbf{v}_j\|$. So, $Y_{ij} = \mathbf{v}_i\cdot\mathbf{v}_j \leq \|\mathbf{v}_i\|^2 = Y_{ii} = Y_{i0}$.

Now consider the left inequality in (7). We have that,

$$\begin{aligned}
Y_{ij} + Y_{00} - Y_{i0} - Y_{j0} = Y_{ij} - 2\epsilon &= \left[\frac{1}{4}+\epsilon+\epsilon^2+\frac{1-4\epsilon^2}{4}T_P(\mathbf{u}_i)\cdot T_P(\mathbf{u}_j)\right] - 2\epsilon \\
&= \frac{1}{4}-\epsilon+\epsilon^2+\frac{1-4\epsilon^2}{4}P(\mathbf{u}_i\cdot\mathbf{u}_j) \\
&\geq \frac{1}{4}-\epsilon+\epsilon^2+\frac{1-4\epsilon^2}{4}\cdot\frac{2\epsilon-1}{2\epsilon+1} = 0,
\end{aligned}$$

where the inequality follows by Property 3 of a (γ, ϵ, m)-useful polynomial and the fact that the $\mathbf{u}_i$ are unit vectors. So constraints (7) holds.

Now we move on to the remaining constraints. Fix $j, k \in \{0, 1, \dots, 2^m\}$. Using constraints (7), the fact that $Y_{ii} = Y_{i0}$ for all i, and the fact that $\mathbf{y}$ is an ϵ-vector in $VC(G)$, it is easy to verify that constraints (8) and (9) hold whenever one of y_j or y_k are integral. So assume that $y_j = y_k = \frac{1}{2} + \epsilon$.

In that case, note first that constraint (8) holds if the following is at least 1:

$$\begin{aligned}\frac{Y_{ij} + Y_{ik}}{Y_{i0}} &= 2\left(\frac{1}{2} + \epsilon\right) + \frac{1 - 2\epsilon}{2}(T_P(\mathbf{u}_i) \cdot T_P(\mathbf{u}_j) + T_P(\mathbf{u}_i) \cdot T_P(\mathbf{u}_k)) \\ &= 1 + 2\epsilon + \frac{1 - 2\epsilon}{2}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k)). \end{aligned} \tag{10}$$

Similarly, constraint (9) holds if the following is at least 1:

$$\frac{(Y_{0j} - Y_{ij}) + (Y_{0k} - Y_{ik})}{Y_{00} - Y_{i0}} = 1 + 2\epsilon - \frac{1 + 2\epsilon}{2}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k)). \tag{11}$$

But by Property 4 of a (γ, ϵ, m)-useful polynomial, for all $i \in \{1, \dots, 2^m\}$ and all $jk \in E$, equations (10) and (11) are indeed both at least 1 and the claim follows. □

By Lemma 2, to complete the proof of the lemma it suffices to show that there exists a (γ, ϵ, m)-useful polynomial P such that if $Y = Y(P, \mathbf{y})$, then for all i such that $y_i = \frac{1}{2} + \epsilon$ the vectors Ye_i/y_i and $Y(e_0 - e_i)/(1 - y_i)$ are $(\epsilon - 5\gamma)$-saturated. Note that the vectors Ye_i/y_i and $Y(e_0 - e_i)/(1 - y_i)$ are the "normalized" versions of vectors Ye_i and $Y(e_0 - e_i)$, i.e., their projections on to the hyperplane $x_0 = 1$.

To that end, let us first compute the saturation of these vectors for an arbitrary but fixed (γ, ϵ, m)-useful polynomial P. Fix i such that $y_i = \frac{1}{2} + \epsilon$ and consider Ye_i/y_i. Let $I = \{i\} \cup \{j : y_j \in \{0, 1\}\}$. Then the saturation of Ye_i/y_i is at least

$$\begin{aligned}\min_{j,k \notin I, jk \in E} \frac{1}{2}((Y_{ij} + Y_{ik})/y_i - 1) &= \min_{j,k \notin I, jk \in E} \left[\epsilon + \frac{1 - 2\epsilon}{4}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k))\right] \\ &\geq \min_{j,k \neq i, jk \in E} \left[\epsilon + \frac{1 - 2\epsilon}{4}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k))\right],\end{aligned}$$

where the equality follows by (10) and the fact that $y_j, y_k \notin \{0, 1\}$. The saturation of $Y(e_0 - e_i)/(1 - y_i)$ is at least

$$\begin{aligned}\min_{j,k \notin I, jk \in E} \frac{1}{2}\left(\frac{(Y_{0j} - Y_{ij}) + (Y_{0k} - Y_{ik})}{1 - y_i} - 1\right) &= \min_{j,k \notin I, jk \in E} \left[\epsilon - \frac{1 + 2\epsilon}{4}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k))\right] \\ &\geq \min_{j,k \neq i, jk \in E} \left[\epsilon - \frac{1 + 2\epsilon}{4}(P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k))\right],\end{aligned}$$

where the equality follows by (11) and the fact that $y_j, y_k \notin \{0, 1\}$.

Lemma 3 now follows from the following lemma proved in Section 5 which shows that (γ, ϵ, m)-useful polynomials of the type we require do in fact exist:

Lemma 4 *Let m be an integer and γ a sufficiently small positive real such that $\frac{m}{2\gamma}$ and $\frac{1}{2\gamma}$ are even integers and m is significantly larger than $\frac{1}{\gamma}$. Suppose $\epsilon > 5\gamma$. Then there exists a (γ, ϵ, m)-useful polynomial P such that for all $i, j, k \in \{-1, 1\}^m$ where $j, k \neq i$ and $jk \in E$,*

$$-2\gamma \leq P(\mathbf{u}_i \cdot \mathbf{u}_j) + P(\mathbf{u}_i \cdot \mathbf{u}_k) \leq 13\gamma. \tag{12}$$

□

5 Proof of Lemma 4: Constructing (γ, ϵ, m)-useful polynomials

In this section we prove Lemma 4. Fix ϵ and γ as in the statement of the lemma.

Let R be the following subset of $\mathbb{R}^2$:

$$R = \left\{ (x, y) \in [-1, 1]^2 : |x + y| \leq 2\gamma, |x - y| \leq 2(1 - \gamma), |x| < 1 - \frac{1}{m}, |y| < 1 - \frac{1}{m} \right\}.$$

Claim 2 *To prove the lemma it suffices to find a polynomial P with nonnegative coefficients such that $P(1) = 1$, $\forall x \in [0, 1]$ $P(x) \geq P(2\gamma - 1) = (2\epsilon - 1)/(2\epsilon + 1)$, and such that,*

$$-2\gamma \leq P(x) + P(y) \leq 13\gamma \quad \forall (x, y) \in R. \tag{13}$$

Proof: By definition, P satisfies the first three properties of a (γ, ϵ, m)-useful polynomial. Now, he vectors $\mathbf{u}_i$ satisfy the following properties: $|\mathbf{u}_i \cdot \mathbf{u}_j| \leq 1 - \frac{2}{m+1}$ for all $1 \leq i \neq j \leq 2^m$. Further, since $\mathbf{u}_j + \mathbf{u}_k$ is supported on $\gamma(m + 1)$ coordinates on which it assumes values $\pm 2/\sqrt{m+1}$ we get that

$$|\mathbf{u}_i \cdot \mathbf{u}_j + \mathbf{u}_i \cdot \mathbf{u}_k| = |\mathbf{u}_i \cdot (\mathbf{u}_j + \mathbf{u}_k)| \leq 2\gamma.$$

Similarly, $|\mathbf{u}_i \cdot \mathbf{u}_j - \mathbf{u}_i \cdot \mathbf{u}_k| \leq 2(1 - \gamma)$. Hence, $\{(\mathbf{u}_i \cdot \mathbf{u}_j, \mathbf{u}_i \cdot \mathbf{u}_k) : j, k \neq i \text{ and } jk \in E\} \subseteq R$. So (13) implies (12). Moreover, since $5\gamma < \epsilon$, it implies Property 4 of a (γ, ϵ, m)-useful polynomial in all cases except when $i = k$. However, in that case we have

$$P(\mathbf{u}_i \cdot \mathbf{u}_i) + P(\mathbf{u}_i \cdot \mathbf{u}_j) = P(1) + P(1 - 2\gamma) = 1 + \frac{2\epsilon - 1}{2\epsilon + 1} = \frac{4\epsilon}{1 + 2\epsilon},$$

and hence Property 4 holds in that case too. □

Given the claim, Lemma 4 will now follow from the following technical lemma:

Lemma 5 *Let m be an integer and γ a sufficiently small positive real such that $\frac{m}{2\gamma}$ and $\frac{1}{2\gamma}$ are even integers and m is significantly larger than $\frac{1}{\gamma}$. Let $\epsilon > 3\gamma$. Then there exists a polynomial P satisfying the properties:*

1. *P has only nonnegative coefficients,*
2. *$P(1) = 1$,*
3. *$P(x) \geq P(2\gamma - 1) = (2\epsilon - 1)/(2\epsilon + 1)$ for all $x \in \mathbb{R}$, and*
4. *Over the region R, the function $f(x, y) = P(x) + P(y)$ satisfies*

$$-2\gamma \leq f(x, y) \leq 13\gamma.$$

Proof: Let $\lambda = 1 - 2\gamma$ and let $T = \frac{m}{2\gamma}$ and $S = \frac{1}{2\gamma}$. Let $q(x)$ and $r(x)$ be the unique polynomials

$$q(x) = ax^T + bx$$
$$r(x) = cx^S + dx$$

satisfying $q(1) = r(1) = 1$ and $q'(-\lambda) = r'(-\lambda) = 0$. Note that

$$a = \frac{1}{1 + T\lambda^{T-1}}, \quad b = \frac{T\lambda^{T-1}}{1 + T\lambda^{T-1}}, \quad c = \frac{1}{1 + S\lambda^{S-1}}, \quad d = \frac{S\lambda^{S-1}}{1 + S\lambda^{S-1}}.$$

Our polynomial P will be the following weighted average of q and r

$$P(x) = \Delta q(x) + (1 - \Delta)r(x),$$

where $\Delta \in (0, 1/4)$ will be defined below. Note that $P(1) = 1$ and $P'(-\lambda) = 0$.

The polynomials q, r enjoy complementary properties that we will exploit to ensure P satisfies the properties of the lemma. The leading coefficient of q is close to 1, while the leading coefficient of r is close to 0. Moreover, the exponent of the leading term of q is significantly bigger than the corresponding exponent of r. Hence, even though $q(x), r(x)$ both tend to 1 as x tends to 1, $q(x)$ is significantly smaller than 1 even for $x = 1 - 1/m$; in fact, q remains extremely close to 0 when $x \in [-1 + 1/m, 1 - 1/m]$ (See Figure 1). We state the The particular properties enjoyed by q and r that we require are as follows:

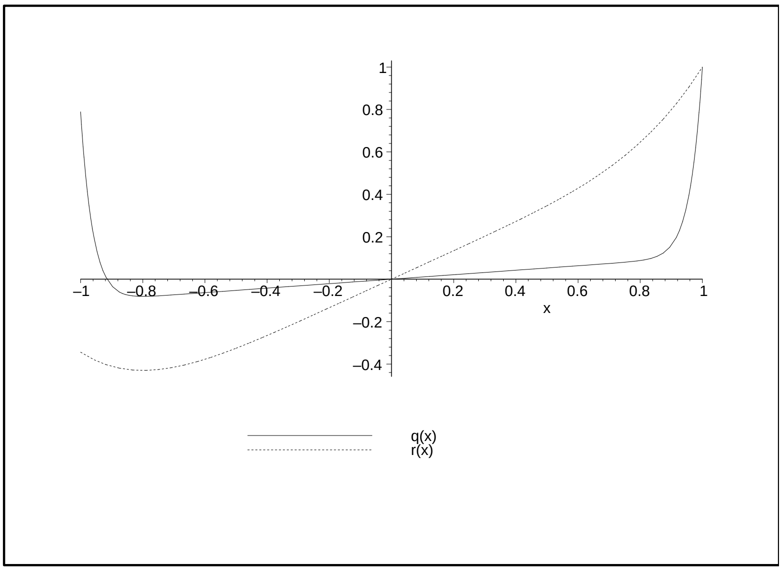

Figure 1: Example illustrating the different behaviours of q and r.

A. Since S and T are both even and $a, c > 0$, it follows that q, r are convex. So P is also convex, and consequently, $P'(x) = 0$ if and only if $x = -\lambda$. So P attains its minimum at $-\lambda$.

B. The coefficients a, b, c, d satisfy the following bounds: $a > 1 - 2^{-m}$, $b < 2^{-m}$, $c \in (5\gamma, 2e\gamma)$, $d \in (1 - 2e\gamma, 1 - 5\gamma)$. These estimates follows from the fact that since γ is sufficiently small, $\lambda^{1/(2\gamma)} \approx e^{-1}$.

C. Our bounds on a, b, c, d immediately imply that $r(-\gamma) > -\gamma$ and $q(-\gamma) > -\gamma 2^{-m}$. In addition, we have the following upper bounds, most of which are quite loose but still good enough for our purposes: (a) $|q(x)| < e^{-\frac{1}{2\gamma}}$ when $x \in [-1+1/m, 1-1/m]$, (b) $r(-1+1/m) < -1 + 11\gamma$, (c) $r(-\lambda - 1/m) < -1 + 12\gamma$, and (d) $r(\lambda + 1/m) < 1 - 3\gamma$.

Given our bounds for a and b and estimates for c and d in **B**, it is easy to see that there exists a constant C, $8 \le C \le 9$ and for which,

$$P(-\lambda) = \Delta 2^{O(-m)} + (1 - \Delta)(-1 + C\gamma - O(\gamma^2)).$$

A simple continuity argument now shows that there exists $\Delta \in (0, 1/4)$ such that $P(-\lambda) = (2\epsilon - 1)/(2\epsilon + 1)$, as desired. Fix Δ to this value for the remainder of the proof. Using the fact that $\epsilon > 3\gamma$ and $m > 1/\gamma$ it is not hard to show that $\Delta \approx 4\epsilon + O(\epsilon^2)$. However, perhaps somewhat surprisingly, the only fact about Δ that we will require to bound f on R is that $0 \le \Delta \le 1$.

It remains to bound f on R. By symmetry of both f and R we can restrict our attention to $x \ge y$. Moreover, by **A** above, ∇f is $(0,0)$ only at $(-\lambda, -\lambda) \notin R$, and hence, f attains extreme points on the boundary of R. The following sets define the boundary of R when $x \ge y$ (see Figure 2):

$$\begin{aligned}
R_1 &= \{(x,y) \in R : x \in (-\gamma, \lambda - 1/m), y = -x - 2\gamma\},\\
R_2 &= \{(x,y) \in R : x \in (\gamma, 1 - 1/m), y = -x + 2\gamma\},\\
R_3 &= \{(x,y) \in R : x \in (\lambda + 1/m, 1 - 1/m), y = x - 2(1-\gamma)\},\\
R_4 &= \{(x,y) \in R : y = -1 + 1/m, x \in (\lambda - 1/m, \lambda + 1/m)\},\\
R_5 &= \{(x,y) \in R : x = 1 - 1/m, y \in (-\lambda - 1/m, -\lambda + 1/m)\}.
\end{aligned}$$

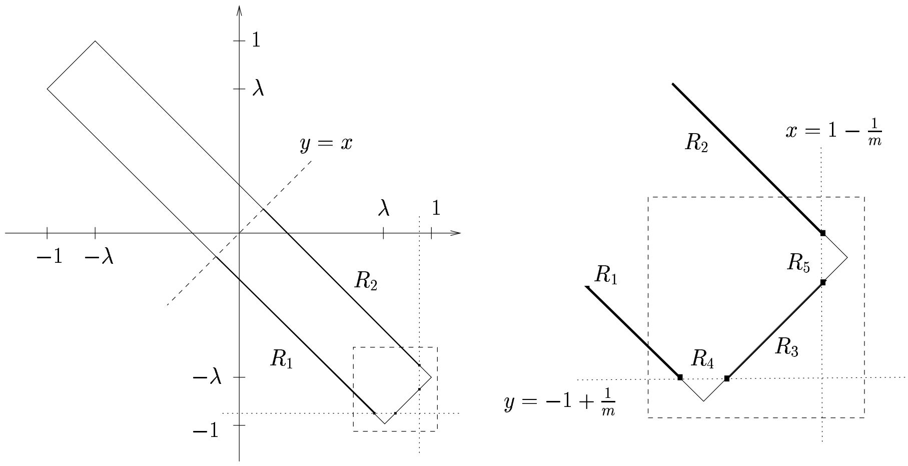

Figure 2: The domain R and the boundaries R_1 through R_5.

So we must find f's extreme points on $\cup R_i$. Consider ∇f when $x \ge y$. Note that $\nabla f \cdot (1, -1) \ge 0$ for all $(x, y) \in \cup R_i$. This follows from the fact that P is convex and hence, $P'(x) \ge P'(y)$ whenever $x \ge y$; in particular, $\nabla f \cdot (1, -1) = P'(x) - P'(y) \ge 0$. It follows that the minima of f on $\cup R_i$ are obtained at $(-\gamma, -\gamma)$ and (γ, γ), and that the maxima of f on $\cup R_i$ must lie on R_3.

We tackle the minima first. Using our estimates in **C** for $q(-\gamma)$ and $r(-\gamma)$ from above, we that

$$f(-\gamma, -\gamma) = 2P(-\gamma) = 2(\Delta q(-\gamma) + (1 - \Delta) r(-\gamma)) > -2\gamma.$$

On the other hand, $f(\gamma, \gamma) > 0$ since $P(x) > 0$ when $x > 0$. So $f \ge -2\gamma$ on R as desired.

Now we tackle the maxima. The convexity of P and the fact that R_3 has slope 1 implies that f restricted to R_3 is convex. Hence, the local maxima occur at $(\lambda + 1/m, -1)$ and $(1 - 1/m, -\lambda - 1/m)$.

Using our estimates in **B** and **C** and the fact that $0 \leq \Delta \leq 1$,

$$\begin{aligned} f(1-\tfrac{1}{m}, -\lambda-\tfrac{1}{m}) &= P(1-\tfrac{1}{m}) + P(-\lambda-\tfrac{1}{m}) \\ &= \Delta[q(1-\tfrac{1}{m}) + q(-\lambda-\tfrac{1}{m})] + (1-\Delta)[r(1-\tfrac{1}{m}) + r(-\lambda-\tfrac{1}{m})] \\ &\leq 2\Delta e^{-\frac{1}{2\gamma}} + (1-\Delta)[1 + (-1+12\gamma)] \\ &\leq \gamma + (1-\Delta)12\gamma < 13\gamma. \end{aligned}$$

Similarly we can show that $f(\lambda + 1/m, -1 + 1/m) < 9\gamma$. □

References

[1] Mikhail Alekhnovich, Sanjeev Arora, and Iannis Tourlakis. Towards strong nonapproximability results in the Lovász-Schrijver hierarchy. In *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, New York, NY, USA, 2005. ACM Press.

[2] S. Arora, B. Bollobas, L. Lovász, and I. Tourlakis. Proving integrality gaps without knowing the linear program. *Theory of Computing*, 2:19–51, 2006.

[3] Sanjeev Arora, Satish Rao, and Umesh Vazirani. Expander flows, geometric embeddings and graph partitioning. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 222–231 (electronic), New York, 2004. ACM.

[4] J. Buresh-Oppenheim, N. Galesi, S. Hoory, A. Magen, and T. Pitassi. Rank bounds and integrality gaps for cutting planes procedures. In *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science*, pages 318–327, 2003.

[5] Moses Charikar. On semidefinite programming relaxations for graph coloring and vertex cover. In *SODA '02: Proceedings of the thirteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 616–620, Philadelphia, PA, USA, 2002. Society for Industrial and Applied Mathematics.

[6] Irit Dinur and Shmuel Safra. On the hardness of approximating minimum vertex-cover. *Annals of Mathematics*, 162(1):439–486, 2005.

[7] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[8] P. Frankl and V. Rödl. Forbidden intersections. *Trans. Amer. Math. Soc.*, 300(1):259–286, 1987.

[9] M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. Assoc. Comput. Mach.*, 42(6):1115–1145, 1995.

[10] E. Halperin. Improved approximation algorithms for the vertex cover problem in graphs and hypergraphs. *SIAM J. Comput.*, 31(5):1608–1623 (electronic), 2002.

[11] H. Hatami, A. Magen, and E. Markakis. Integrality gaps of semidefinite programs for vertex cover and relations to l_1 embeddability of negative type metrics. In *Manuscript*, 2006.

[12] George Karakostas. A better approximation ratio for the vertex cover problem. In *Proceedings of the Thirty-Second International Colloquium on Automata, Languages and Programming*, 2005.

[13] S. Khot and O. Regev. Vertex cover might be hard to approximate to within $2 - \epsilon$. In *Proceedings of the 18th IEEE Conference on Computational Complexity*, pages 379–386, 2003.

[14] Subash Khot. On the power of unique 2-prover 1-round games. In *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing*, pages 767–775 (electronic), New York, 2002. ACM.

[15] Jon Kleinberg and Michel X. Goemans. The Lovász theta function and a semidefinite programming relaxation of vertex cover. *SIAM J. Discrete Math.*, 11(2):196–204 (electronic), 1998.

[16] László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal on Optimization*, 1(2):166–190, May 1991.

[17] Ofek and Feige. Random 3CNF formulas elude the lovasz theta function. In *ECCCTR: Electronic Colloquium on Computational Complexity, technical reports*, 2006.

[18] G. Schoenebeck, L. Trevisan, and M. Tulsiani. A linear round lower bound for Lovász-Schrijver SDP relaxations of vertex cover. In *Electronic Colloquium on Computational Complexity Report TR06-098*, 2006.

[19] G. Schoenebeck, L. Trevisan, and M. Tulsiani. Tight integrality gaps for Lovász-Schrijver LP relaxations of vertex cover and max cut. In *Electronic Colloquium on Computational Complexity*, 2006.

[20] I. Tourlakis. New lower bounds for vertex cover in the Lovász-Schrijver hierarchy. In *Proceedings of the 21st IEEE Conference on Computational Complexity*, 2006.

A Proof sketch of Lemma 1

In [8] we find the following similar-looking statement to Lemma 1 about sets avoiding intersections.

Lemma 6 *(Corollary 4.2 in [8]) Let γ be a sufficiently small number, and m an integer. Also, let $\mathcal{F}$ and $\mathcal{G}$ be two set families over the universe $[m]$ so that $|F \cap G| \neq \lfloor m\eta \rfloor$ for every $F \in \mathcal{F}, G \in \mathcal{G}$. Then $4^{-m}|\mathcal{F}||\mathcal{G}| \leq (1 - \eta^2/4)$.*

By taking $\mathcal{F} = \mathcal{G}$ and treating set families as points in $\{-1,1\}^m$ we get that the above lemma says that a subset of size $> 2^m(1 - \eta^2/4)$ must contain two points whuch share exactly $\lfloor m\eta \rfloor$ ones.

Let S be a set in $\{-1,1\}^m$ avoiding distance $(1-\gamma)m$. Instead of bounding the size of S we will bound the size of the biggest set of the form form $S_k = \{s \in S : |s| = k\}$, where $|\cdot|$ denotes Hamming weight (i.e., the number of coordinates set to 1). Clearly S_w satisfies $|S_w| \geq |S|/m$. We shall assume wlog that $w \leq m/2$.

Having reduced to the case where all points have the same Hamming weight w we can easiliy relate to Lemma 6: it is easy to see that no two points in S_w may share exactly $w - m(1-\gamma)/2$ ones. Assume, first, that $w > \frac{m}{2}(1 - \gamma/2)$. Then S_w is a subset that avoids intersection of ηm where $\gamma/4 \leq \eta \leq \gamma/2$. We now apply Lemma 6 (or its corollary rather) to get that

$$|S_w| \leq 2^m(1 - \eta^2/4) \geq 2^m(1 - \gamma^2/64)^m,$$

and so $|S| \leq m|S_w| \leq m2^m(1-\gamma^2/64)^m$.

For the case that $w \leq \frac{m}{2}(1-\gamma/2)$ we may simply say that S_w is small by virtue of the bound on the number of points in the cube having small Hamming weight:

$$|S_w| \leq \binom{m}{\frac{m}{2}(1-\gamma/2)} \sim 2^{mH(1/2-\gamma/4)} \sim 2^m(2^{-\gamma^2/16})^m \leq 2^m \exp\left(-\frac{\log 2}{16}\gamma^2\right) \leq 2^m(1-\gamma^2/64)^m$$

and again S is at most m times this bound.

The above estimate is nearly tight: Consider the (open) Hamming ball B of radius $(1-\gamma)/2$; clearly this ball is an independent set in $G_{\gamma,m}$. Now

$$|B| = \sum_{j<\frac{m}{2}(1-\gamma)} \binom{m}{j} \geq \frac{\gamma m}{2}\binom{m}{\frac{m}{2}(1-2\gamma)} \geq \frac{\gamma m}{2}2^{mH(1/2-\gamma)} \sim \frac{\gamma m}{2}2^{m(1-\gamma^2/4} = 2^m\frac{\gamma m}{2}2^{-\gamma^2 m/4}.$$

So for $|B|$ to be $o(2^m)$ we must have that $\gamma m 2^{-\gamma^2 m/4} = o(1)$ and so $\gamma = \Omega(\sqrt{\log m/m})$.

B Proof of Lemma 2

For completeness, we include in this section a proof of Schoenebeck et al.'s [19] Lemma 2 for expressing an ϵ-saturated vector as a convex combination of ϵ-vectors.

Proof: Partition V as follows: Let $V_- = \{i \in V : x_i < 1/2+\epsilon\}, V_+ = \{i \in V : x_i > 1/2+\epsilon\}, V_0 = \{i \in V : x_i = 1/2+\epsilon\}$. Let $r(0) = 0$, and for all $i \in V$ let

$$r(i) = \begin{cases} 1 - \frac{x_i}{1/2+\epsilon}, & i \in V_- \\ 1, & i \in V_0 \\ 1 - \frac{1-x_i}{1/2-\epsilon}, & i \in V_+ \end{cases}$$

Note that since $\mathbf{x}$ is feasible, whenever $ij \in E$ and $i \in V_-$, we must have $j \in V_+$. Moreover, for such a pair we must have that $r(j) \geq r(i)$ because

$$\begin{aligned} r(j) - r(i) &= 1 - \frac{1-x_j}{1/2-\epsilon} - \left(1 - \frac{x_i}{1/2+\epsilon}\right) \\ &= \frac{x_i}{1/2+\epsilon} - \frac{1-x_j}{1/2-\epsilon} \\ &= \frac{x_i(1/2-\epsilon) - (1-x_j)(1/2+\epsilon)}{(1/2+\epsilon)(1/2-\epsilon)} \\ &= \frac{x_i + x_j - (1+2\epsilon)}{2(1/4-\epsilon^2)} + \frac{\epsilon(x_j - x_i)}{1/4-\epsilon^2} > 0, \end{aligned}$$

where the last inequality follows from the fact that $\mathbf{x}$ is ϵ-saturated.

Reorder the $r(i)$'s so that $0 = r(i_0) \leq r(i_1) \leq \ldots \leq r(i_{|V|})$. For each $t = 1, \ldots, |V|$, let $\mathbf{x}^{(t)}$ be the ϵ-vector where

$$x_i^{(t)} = \begin{cases} 0, & i \in V_- \text{ and } r(i) \geq r(i_t) \\ 1, & i \in V_+ \text{ and } r(i) \geq r(i_t) \\ \frac{1}{2}+\epsilon, & \text{otherwise} \end{cases}$$

We claim these vectors are in $VC(G)$. To see why consider an edge ij. The constraint $x_i^{(t)} + x_j^{(t)} \geq 1$ is satisfied unless both $x_i^{(t)}$ and $x_j^{(t)}$ are 0. However, if $x_i^{(t)} = 0$, then $i \in V_-$ and $r(i) \geq r(i_t)$. So the feasibility of $\mathbf{x}$ implies $j \in V_+$ and hence $r(j) \geq r(i_t)$. So $x_j^{(t)} = 1$ and the constraint is satisfied.

It remains to argue that $\mathbf{x}$ is in the convex hull of the $\mathbf{x}^{(t)}$'s. To that end, we define a distribution $\mathcal{D}$ over the vectors $\mathbf{x}^{(t)}$ such that $\mathbf{x}^{(t)}$ is assigned the probability $r(i_t) - r(i_{t-1})$. It is easy to verify now that $\mathrm{E}_t[x_j^{(t)}] = x_j$ for all $j \in V$. $\square$

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/