Revisiting Block-Diagonal SDP Relaxations for the Clique Number of the Paley Graphs

Vladimir A. Kobzar
Department of Applied Physics and
Applied Mathematics, Columbia University
vak2116@columbia.edu

Krishnan Mody
Courant Institute of Mathematical Sciences
New York University, New York, NY
km2718@nyu.edu

***Abstract*—This work addresses the block-diagonal semidefinite program (SDP) relaxations for the clique number of the Paley graphs. The size of the maximal clique (clique number) of a graph is a classic NP-complete problem; a Paley graph is a deterministic graph where two vertices are connected if their difference is a quadratic residue (square) in a finite field with the number of elements given by certain primes and prime powers. Improving the upper bound for the Paley graph clique number for prime powers that are non-squares is an open problem in combinatorics. Moreover, since quadratic residues exhibit pseudorandom properties, Paley graphs are related to the construction of deterministic restricted isometries, an open problem in compressed sensing. Recent work provides numerical evidence that the current upper bounds can be improved by the sum-of-squares (SOS) relaxations. In particular, the bounds given by the SOS relaxations of degree 4 (SOS-4) have been empirically observed to be growing at an order smaller than square root of the prime. However, computations of SOS-4 appear to be intractable with respect to large graphs. Gvozdenovic et al. introduced a more computationally efficient block-diagonal hierarchy of SDPs and computed the values of these SDPs of degrees 2 (L2) for the Paley graph clique numbers associated with primes p less or equal to 809, which bound from above the corresponding SOS-4 relaxations. We compute the values of the L2 relaxations for p's between 821 and 997. Our results provide some numerical evidence that these relaxations, and therefore also the SOS-4 relaxations, may be scaling at an order smaller than the square root of p. However, due to the size of the SDPs, we have not been able to compute L2 relaxations for p's greater than 997. Therefore, our scaling estimate is not conclusive and presents an interesting open problem for further study.**

I. The clique number of the Paley graphs

A *Paley graph* G_q is a graph with q vertices, where q is a prime power such that $q = 1 \mod 4$;[1] two vertices are connected by an edge $\{i, j\}$ whenever $i-j$ is a quadratic residue in $\mathbb{F}_q$. (We may sometimes refer to quadratic residues as *squares*, and to nonresidues as *nonsquares*.)[2]

The *clique number* $\omega(G)$ of a graph G is the number of vertices in its largest complete subgraph or *clique*. For any Paley graph G_q, this number is bounded above by $\sqrt{q}$ [33].

For a Paley graph with $q = p^{2k}$ where k is a positive integer, the foregoing bound is tight [11]. However, less is known about $\omega(G_q)$ when q is a prime power that is a non-square. In particular, if $q = p$, the state-of-the-art lower bounds are scaling as $\log p \cdot \log\log\log p$; the $\log\log\log p$ term can be improved to $\log\log p$ conditional on the Generalized Riemann Hypothesis (see [15] and Theorem 13.5 in [28]). On the other hand, the existing state-of-the-art upper bounds in references [7], [18] improve on $\sqrt{p}$ only by a constant prefactor. We will refer to the upper bound $(\sqrt{2p-1}+1)/2$ in those references as $HP(G_p)$. Numerical experiments appear to suggest that the Paley graph clique number is polylogarithmic in p (see discussion of [13], [31] in [2]). However, proving even a $p^{\frac{1}{2}-\epsilon}$ bound for some $\epsilon > 0$ is regarded as a difficult open problem in additive combinatorics [20], sometimes referred to as the *square root bottleneck* (see also [23]).

II. Connections to deterministic restricted isometries

Paley graphs are connected to the construction of deterministic $M \times N$ matrices with the restricted isometry property (RIP), an important problem in compressed sensing and sparse recovery [32]. Random matrix constructions achieve RIP when sparsity is on the order of $M/\text{polylog}(N)$. However, most deterministic constructions, such as equiangular frames (*ETFs*), are based on controlling a certain *coherence* value, which achieves RIP only when sparsity is on the order of $\sqrt{M}$;

[1] By the law of quadratic reciprocity, this condition ensures that -1 is a quadratic residue in $\mathbb{F}_q$. Therefore, if $i-j$ is a quadratic residue then so is $j-i$, and the graph is undirected.

[2] See [21] for general background on Paley graphs.

this limitation is known as the *square root bottleneck*.[3] The only unconditional construction that overcomes this bottleneck was provided in [9], [10], which leveraged additive combinatorics techniques to achieve RIP for $\Omega(M^{\frac{1}{2}+\epsilon})$ sparsity for small $\epsilon > 0$ (see also [27]).

Reference [4] constructed a family of deterministic ETF matrices using the quadratic residues modulo a prime number p (the *Paley matrices*) which provably achieve RIP when sparsity is on the order of $\sqrt{p}$ by the aforementioned coherence analysis but are *conjectured* to achieve it when sparsity on the order of $p/\text{polylog}(p)$ (which would match the random construction if p is proportional to M). Reference [3] used a matrix construction based on the Legendre symbol (which is closely connected to Paley graphs) to reduce the number of random bits in a random RIP matrix.

Finally, conditioned on a conjecture about the number of edges in any subgraph of a Paley graph, the Paley matrices overcome the square root bottleneck [5].[4] In this conditional construction, a lower bound on $\omega(G_p)$ would lead to a lower bound on the distortion in the sparse recovery (Theorem 2.3 in [5]).

III. SDP relaxations of the clique number

The clique number $\omega(G)$ of a graph G is a classical NP-complete problem. It can be formulated as a polynomial optimization over $x \in \mathbb{R}^n$ where n is the number of vertices of $G = (V, E)$:

$$\omega(G) = \left\{ \begin{array}{ll} \max & \sum_{i \in V} x_i \\ \text{s.t.} & x \in \mathbb{R}^n,\ x_i^2 = x_i \text{ for all } i \in V, \\ & x_i x_j = 0 \text{ for all } \{i,j\} \notin E \end{array} \right\}.$$

An extensive body of literature considered upper bounds produced by convex relaxations, which are more computationally efficient. One particular question in this literature is whether semidefinite program (SDP) relaxations would lead to an $O(n^{\frac{1}{2}-\epsilon})$ upper bound on the clique number for some $\epsilon > 0$.

Erdos-Renyi graphs $G \sim \mathcal{G}(\frac{1}{2}, n)$ are random graphs where each edge is present independently with probability $\frac{1}{2}$. In this setting, reference [14] showed that the *Lovasz-Schrijver hierarchy* of SDPs attains an $\Omega(\sqrt{n})$ lower bound for clique number relaxations of any constant degree.

Another line of work considered the *sum of squares (SOS)* hierarchy of SDPs, also known as the *Lasserre-Parrilo hierarchy*. In the context of the clique number problem, these relaxations, denoted by $SOS_{2t}(G)$ where t is the degree of the hierarchy, are defined as follows. Let $\mathcal{P}(V)$ be the collection of all subsets (power set) of V, and let $\mathcal{P}_t = \{I \in \mathcal{P}(V) \,|\, |I| \le t\}$ and $\mathcal{P}_{=t} = \{I \in \mathcal{P}(V) \,|\, |I| = t\}$ denote the subsets of V with at most t and exactly t elements, respectively. For $y \in \mathbb{R}^{\mathcal{P}_{2t}}$, we define the *moment matrix* of y $M_t(y) \in \mathbb{R}^{\mathcal{P}_t \times \mathcal{P}_t}$ by $M_t(y)_{IJ} = y_{I \cup J}$ where $I, J \in \mathcal{P}_t(V)$. We also denote by $\mathcal{K}$ the set of all cliques of G. Then the SOS hierarchy is given by

$$SOS_{2t}(G) = \left\{ \begin{array}{ll} \max & \sum_{i \in V} y_{i,\emptyset} \\ \text{s.t.} & y \in \mathbb{R}^{\mathcal{P}_{2t}},\ y_\emptyset = 1 \\ & y_{S,T} = 0 \ \forall\ S \cup T \notin \mathcal{K} \\ & M_t(y) \succeq 0 \end{array} \right\}$$

In the average-case setting of $\mathcal{G}(\frac{1}{2}, n)$, reference [6] established an $\Omega(\sqrt{n})$ lower bound for the SOS relaxation of any constant degree for the clique number problem (see also earlier work [12], [19], [30] focusing on the SOS_4 relaxation).

A *stable set* of a graph $G = (V, E)$ is a subset $S \subset V$ such that no two nodes in S have an edge between them. The size $\alpha(G)$ of the largest stable set of G is called the independence or stability number of G. The *Lovász* ϑ *function*, which can be also formulated as an SDP, is a convex relaxation of $\alpha(G)$. Note that for a complement graph $\bar{G}$, $\alpha(G) = \omega(\bar{G})$, and Lovász ϑ represents the first and weakest degree of the SOS hierarchy, i.e., $\vartheta(G) = SOS_2(\bar{G})$ (see, e.g., Section 4.1.3 in [16]).

Since the Paley graphs are self-complementary, $\omega(G_p) = \alpha(G_p)$. The classic upper bound $\alpha(G_p) \le \sqrt{p}$ is realized by the $SOS_2(G_p)$ relaxation of the Paley graph clique problem (Theorem 13.14 in [8] and Theorem 8 in [25]), but the current state-of-the-art upper bound $HP(G_p)$ in [7], [18] has a tighter constant prefactor. Numerical experiments in [26] show that the Lovasz ϑ relaxation with respect to appropriately chosen local subgraphs of G_p with additional Schrijver's nonnegativity constraints often improves on $HP(G_p)$; see also [23].

Recent work revisited the higher-degree SOS relaxations in the deterministic context of the Paley graphs. Specifically, for $q = p$ prime, reference [24] presented numerical experiments suggesting that $SOS_4(G_p)$ may scale as $O(p^{\frac{1}{2}-\epsilon})$ for some $\epsilon > 0$ and proved that these values are at least $\Omega(p^{\frac{1}{3}})$.

For large graphs, the SOS relaxations appear to be computationally intractable, especially for higher degree

[3] Reference [1] designed deterministic RIP matrices that support the same sparsity $\sqrt{M}$ based on the coherence analysis; however, they are constructed using the adjacency matrix of a Paley graph rather than an ETF.

[4] Using a similar analysis, reference [22] showed an improvement on the *square root bottleneck* by $\epsilon = \frac{9}{40} + \kappa$ for small κ; while this result is not conditioned on any conjectures, it only holds for signals with a certain sparse structure.

t of the hierarchy, which entail optimization over $\mathbb{R}^{\mathcal{P}_t \times \mathcal{P}_t}$ matrices. For example, the SOS_4 relaxations do not appear to be currently computationally feasible for $p > 250$ (Section 6 and Figure 1 in [24]).

IV. Block-diagonal SDP hierarchy

References [16], [17] introduced a new hierarchy of SDPs, denoted by L^t, which is nested between the Lovasz-Schrijver and SOS hierarchies, and in particular the optimal values of this new hierarchy L^t bound from above the corresponding SOS-$2t$ values. This new hierarchy is more computationally tractable that the SOS hierarchy because it is based on the block-diagonal submatrices of the moment matrix. In the context of the Paley graph clique number, the size of the block-diagonal relaxations can be reduced further by leveraging graph symmetries. This section provides an exposition of the L^2 relaxations in [16], [17].

For $y \in \mathbb{R}^{\mathcal{P}_{t+1}}$ and a subset of vertices $T \subset V$ of size $|T| = t-1$, let $M(T;y) \in \mathbb{R}^{\mathcal{P}_{t-1} \times (n+1)}$ be a principal submatrix of $M_t(y)$ whose rows and columns are indexed by $\mathcal{A}(T) = \bigcup_{S \subseteq T} \mathcal{A}_S$ where $\mathcal{A}_S = \{S\} \cup \{S \cup \{i\} \,|\, i \in V\}$. Following [17], we consider $\mathcal{A}_S$ as a multiset, i.e., we keep possible repeated occurrences, e.g., S and $S \cup \{i\}$ if $i \in S$.[5] Let $A_S(y)$ denote the principal submatrix of $M(T;y)$ indexed by the set $\mathcal{A}_S$: it is a symmetric $(n+1) \times (n+1)$ matrix with entries

$$A_S(y)_{00} = y_S, A_S(y)_{0i} = y_{S \cup \{i\}}, \;\; A_S(y)_{ij} = y_{S \cup \{i,j\}}$$

for $i, j \in V$. We will index matrix and vector entries by $[0, \ldots, n-1]$, the elements of a finite field $\mathbb{F}_n$ to simplify our subsequent discussion of the Paley graph relaxations. By Lemma 2.2 in [17] $M(T;y)$ is positive semidefinite (PSD) if and only if for all $S \subseteq T$ the matrix

$$A(S,T)(y) := \sum_{S' : S \subseteq S' \subseteq T} (-1)^{|S' \setminus S|} A_{S'}(y)$$

is PSD.

These reductions lead to the following relaxation of the independence set problem of an arbitrary graph with n vertices:[6] $L^t(G) =$

$$\left\{ \begin{array}{l} \max \sum_{i \in V} y_{\{i\}} \\ \quad \text{s.t.} y \in \mathbb{R}^{\mathcal{P}_{t+1}}, \;\; y_\emptyset = 1 \\ \qquad y_{\{i,j\}} = 0 \;\forall\; (i,j) \in E \\ \qquad A(S,T)(y) \succeq 0 \text{ for all } S \subset T \text{ and } T \in \mathcal{P}_{=t-1} \end{array} \right\}$$

This optimization problem has $\binom{n}{t-1} 2^{t-1}$ PSD constraints with respect to $n+1 \times n+1$ matrices $A(S,T)(y)$.

In the remainder of this section, for consistency with [16], [17], we will consider the independent set problem rather than the equivalent maximal clique problem.

In the context of a Paley graph G_p, references [16], [17] exploit its symmetries to reduce the number of the PSD constraints. Using the vertex-transitivity of the graph and Lemma 2.4.5 in [16], the PSD constraints in $L^2(G_p)$ is reformulated in terms of two $(p+1) \times (p+1)$ matrices using just one arbitrary vertex $h \in V$, e.g., $\{0\}$; the resulting matrices $A_\emptyset(y)$ and $A_{\{0\}}(y)$ used in the constraints are given below. Furthermore, a Paley graph is edge-transitive - this symmetry allows to reduce the number of optimization variables corresponding to non-edges to one variable, $y_{\{0,k\}}$ for some $\{0,k\} \notin E$.

The cliques and independent sets of size 3 (triangles) form orbits under the graph automorphism group of affine mappings $\phi_{ab} : \mathbb{F}_p \to \mathbb{F}_p$ given by $\phi_{ab}(u) = au + b$ where $u \in \mathbb{F}_p$, $a, b \in \mathbb{F}_p$ and $a \neq 0$ is a square in $\mathbb{F}_p$. Therefore, the number of optimization variables corresponding to triangles without edges can be reduced to the number of the orbits of ϕ_{ab} acting on such triangles.

Since a Paley graph is edge-transitive, the representatives of the orbits of fully connected triangles are given by $\{0, 1, \beta\}$ where both β and $\beta - 1$ are squares in $\mathbb{F}_p$. The representatives of the orbits of ϕ_{ab} acting on triangles without any edges, which can be represented as $\{0, \alpha, \beta\}$, can be expressly computed as well. Lemma 6.2.1 in [29] explicitly sets forth their orbits; there are approximately $(p-5)/24$ orbits. Let Ω be the set of representatives of such orbits, and denote $m := |\Omega|$. Then

$$L_2(G_p) = \left\{ \begin{array}{ll} \max \; p \cdot y_{\{0\}} & \quad (2a) \\ \quad \text{s.t. } y_{\{0\}}, y_{\{0,k\}} \in \mathbb{R}, \;\; y \in \mathbb{R}^m & \quad (2b) \\ \qquad A_\emptyset(y) - A_{\{0\}}(y) \succeq 0 & \quad (2c) \\ \qquad A_{\{0\}}(y) \succeq 0 & \quad (2d) \end{array} \right\}$$

[5] Therefore, $|\mathcal{A}_S| = 2^{t-1}(n+1)$ and $M(T;y) \in \mathbb{R}^{2^{t-1}(n+1) \times 2^{t-1}(n+1)}$. Technically $M(T;y)$ is a submatrix of $M_t(y)$ after removing the repeating rows of the latter.

[6] The independence set formulation leads more naturally than the equivalent clique number formulation to further simplifications of the L^t program discussed here in the context of Paley graphs.

where

$$A_{\emptyset}(y) = \left(\begin{array}{c|c} 1 & y_{\{0\}}\mathbb{1}^{\intercal} \\ \hline y_{\{0\}}\mathbb{1} & y_{\{0\}}I + y_{\{0,k\}}A_{\bar{G}_p} \end{array}\right)$$

encodes the vertices by $y_{\{0\}}$ and nonedges by $y_{\{0,k\}}$, both scalars, and $A_{\bar{G}_p}$ is the adjacency matrix of the complement graph $\bar{G}_p$. Also we have

$$A_{\{0\}}(y) = \left(\begin{array}{c|c|c} y_{\{0\}} & y_{\{0\}} & y_{\{0,k\}}q^{\intercal} \\ \hline y_{\{0\}} & y_{\{0\}} & y_{\{0,k\}}q^{\intercal} \\ \hline y_{\{0,k\}}q & y_{\{0,k\}}q & M \end{array}\right)$$

where the leftmost column $q := (A_{\bar{G}_p})_{1:\text{end},0}$ of the adjacency matrix $A_{\bar{G}_p}$, and

$$M := y_{\{0,k\}}\operatorname{diag}(q) + \sum_{\{\alpha,\beta\}\in\Omega} y_{\{0,\alpha,\beta\}}X^{\alpha\beta}.$$

The matrix $X^{\alpha\beta} \in \mathbb{R}^{p-1\times p-1}$ encodes the orbit of ϕ_{ab} acting on each representative triangle $\{0,\alpha,\beta\}$: $X_{ij}^{\alpha\beta} = 1$ if $\{i,j\} \in \phi_{ab}(\{0,\alpha,\beta\})$ for any $a,b \in \mathbb{F}_p$ where $a \neq 0$ is a square in $\mathbb{F}_p$, and $X_{ij}^{\alpha\beta} = 0$ otherwise. (Note $X_{ii}^{\alpha\beta} = 0$ for all $\{\alpha,\beta\} \in \Omega$.)

Since the second row and columns of $A_{\{0\}}(y)$ will match those of $A_{\emptyset}(y)$, we can remove the first row and column in each matrix for purposes of the (2c) constraint. This leads to a $p\times p$ rather than $p+1\times p+1$ matrix in that constraint. Lastly for purposes of the other constraint (2d), we can remove from $A_{\{0\}}(y)$ the rows and columns with edges (which are indexed by the nonresidues) leading to a $(p+1)/2\times(p+1)/2$ matrix.

V. New Computations

We replicated the $L^2(G_p)$ computations reported in [16], [17] using Matlab/CVX for primes $p \leq 809$ as well as extended them for all $p < 1000$.[7] These resulting new values are shown in Table I. Figure 1 shows that $L^2(G_p) \sim p^{0.456}$ which is tighter than $HP(G_p) = (\sqrt{2p-1}+1)/2$, the upper bound on $\omega(G_p)$ established in [7], [18].[8] Moreover, since $SOS_4(G_p) \leq L^2(G_p)$, our results provide some numerical evidence that the SOS_4 relaxations of the Paley graph clique number may be asymptotically growing at an order smaller than square root of p. However, due to the size of the SDPs, we have not been able to compute the $L^2(G_p)$ values for $p > 997$. Therefore, our scaling estimate is not conclusive and presents an interesting open problem for further study.

p	$\vartheta(G_p)$	$L^2(G_p)$	$\omega(G_p)$
821	28.653	18.673	12
829	28.792	18.105	11
853	29.206	18.909	13
857	29.275	18.429	13
877	29.614	19.711	13
881	29.682	18.689	11
929	30.48	19.292	13
937	30.61	19.248	11
941	30.676	19.34	11
953	30.871	19.199	11
977	31.257	19.737	13
997	31.575	20.058	13

TABLE I: The $L^2(G_p)$ values for $809 < p < 1000$ determined in this paper, together with the values of $\omega(G_p)$ obtained from [31].

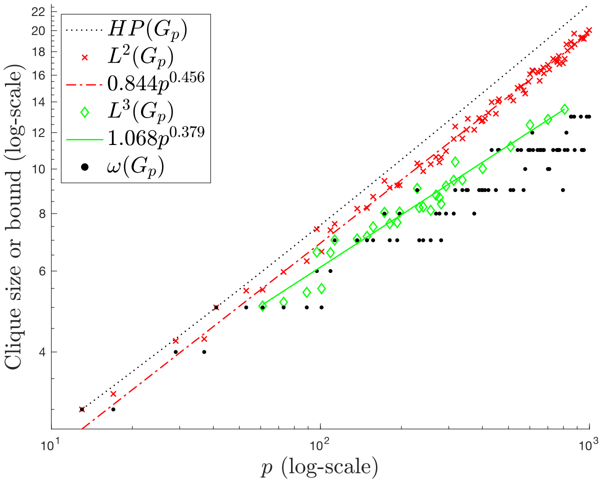

Fig. 1: The $L^2(G_p)$ values for $809 < p < 1000$ determined in this paper, and the $L^2(G_p)$ and $L^3(G_p)$ values for $p \leq 809$ determined in [16], [17] are fitted to power models of the form ap^b. The values of $\omega(G_p)$ were obtained from [31] and $HP(G_p) = (\sqrt{2p-1}+1)/2$ represents the upper bound on $\omega(G_p)$ established in [18].

VI. Potential Extensions

We hope that the $L^2(G_p)$ values can be either estimated analytically, or computed numerically for $p > 997$ leading to a new scaling estimate with a higher confidence level than that of the estimate obtained in this work. We also hope that the higher degree L^t relaxations can be computed and used to upper bound the corresponding SOS_{2t} values in the context of the Paley graph clique number and beyond. To achieve new numerical results, it may be advantageous to decompose the $A_S(y)$ matrices in the positive semidefinite constraints in terms of smaller matrices. A result of this

[7] The code is available at http://vkobzar.com/.

[8] For reference, we have also plotted and fitted to a power model the $L^3(G_p)$ values for $p \leq 809$ determined in [16], [17].

kind was obtained in [29] with respect to the Lovasz ϑ by decomposing the moment matrix in terms of the so-called "zonal" matrices. Another possible alternative would entail adapting the approach used in [26] by computing a block diagonal relaxation with respect to a suitable local subgraph of a Paley graph. We leave these potential extensions for future work.

VII. Acknowledgements

V.A.K. acknowledges support by NSF grant DMS-1937254. We thank Afonso Bandeira for suggesting the research direction that led to this paper; we are also very grateful to him, Nebosja Gvozdenovic, Tim Kunisky, Monique Laurent and Chi Hoi Yip for their helpful input.

References

[1] Hamed Bagh-Sheikhi Arash Amini and Farokh Marvasti. From Paley graphs to deterministic sensing matrices with real-valued Gramians. In *2015 International Conference on Sampling Theory and Applications (SampTA)*, 2015.

[2] C. Bachoc, M. Matolcsi, and I. Z. Ruzsa. Squares and difference sets in finite fields. *Integers: Electronic Journal of Combinatorial Number. Theory, Vol 13.*, 2014.

[3] Afonso S. Bandeira, Matthew Fickus, Dustin G. Mixon, and Joel Moreira. Derandomizing restricted isometries via the Legendre symbol. *Constr. Approx.*, 43:409–424, 2016.

[4] Afonso S. Bandeira, Matthew Fickus, Dustin G. Mixon, and Percy Wong. The road to deterministic matrices with the restricted isometry property. *J. Fourier Anal. Appl.*, 19:1123–1149, 2013.

[5] Afonso S. Bandeira, Dustin G. Mixon, and Joel Moreira. A conditional construction of restricted isometries. *International Mathematics Research Notices*, 2017:2:372–381, 2016.

[6] Boaz Barak, Samuel Hopkins, Jonathan Kelner, Pravesh K. Kothari, Ankur Moitra, and Aaron Potechin. A nearly tight sum-of-squares lower bound for the planted clique problem. *SIAM Journal on Computing*, 48(2):687–735, 2019.

[7] Daniel Di Benedetto, Jozsef Solymosi, and Ethan P White. On the directions determined by a Cartesian product in an affine Galois plane. *Combinatorica*, 41(6):755–763, 2021.

[8] Béla Bollobás. *Ramsey Theory*, page 319–347. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 2001.

[9] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova. Breaking the k^2 barrier for explicit RIP matrices. In *STOC*, pages 637–644, 2011.

[10] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova. Explicit constructions of RIP matrices and related problems. *Duke Math. J.*, 159:145 – 185, 2011.

[11] I. Broere, D. Doman, and J.N. Ridley. The clique numbers and chromatic numbers of certain Paley graphs. *Quaestiones Mathematicae*, 11(1):91–93, 1988.

[12] Yash Deshpande and Andrea Montanari. Improved sum-of-squares lower bounds for hidden clique and hidden submatrix problems. In *28th Annual Conference on Learning Theory (COLT 2015)*, pages 523–562, 2015.

[13] G. Exoo. Independence numbers for Paley graphs, accessed January 11, 2023. http://isu.indstate.edu/ge/PALEY/index.html.

[14] Uriel Feige and Robert Krauthgamer. The probable value of the Lovasz-Schrijver relaxations for maximum independent set. *SIAM Journal on Computing*, 32(2):345–370, 2003.

[15] S.W. Graham and CJ Ringrose. Lower bounds for least quadratic non-residues. In *Analytic number theory*, pages 269–309. Springer, 1990.

[16] N. Gvozdenovic. Approximating the stability number and the chromatic number of a graph via semidefinite programming, 2008. Ph.D. Thesis, University of Amsterdam.

[17] N. Gvozdenovic, M. Laurent, and F. Vallentin. Block-diagonal semidefinite programming hierarchies for 0/1 programming. *Operations Research Letters 37:27-31*, 2009.

[18] Brandon Hanson and Giorgis Petridis. Refined estimates concerning sumsets contained in the roots of unity. In *Proceedings of the London Mathematical Society*, volume 122(3), pages 353–358, 2021.

[19] Samuel B Hopkins, Pravesh K Kothari, and Aaron Potechin. SOS and planted clique: Tight analysis of MPW moments at all degrees and an optimal lower bound at degree four, 2015. https://arxiv.org/abs/1507.05230.

[20] E. S. Croot III and V. F. Lev. Open problems in additive combinatorics. In *Additive Combinatorics, CRM Proc. Lecture Notes*, volume 43, page 207–233, Providence, RI, 2007. Amer. Math. Soc.

[21] Gareth A. Jones. Paley and the Paley graphs. In Gareth A. Jones, Ilia Ponomarenko, and Jozef Širáň, editors, *Isomorphisms, Symmetry and Computations in Algebraic Graph Theory*. Springer, 2020.

[22] Alihan Kaplan, Volker Pohl, and Holger Boche. Deterministic matrices with a restricted isometry property for partially structured sparse signals. In *13th International conference on Sampling Theory and Applications (SampTA)*, 2019.

[23] Dmitriy Kunisky. Spectral pseudorandomness and the road to improved clique number bounds for Paley graphs, 2023. https://arxiv.org/abs/2211.02713.

[24] Dmitriy Kunisky and Xifan Yu. A degree 4 sum-of-squares lower bound for the clique number of the Paley graph, 2022. https://arxiv.org/abs/2211.02713.

[25] L. Lovasz. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[26] Mark Magsino, Dustin G. Mixon, and Hans Parshall. Linear programming bounds for cliques in Paley graphs. In *Proc. SPIE 11138, Wavelets and Sparsity XVIII*, 2019.

[27] Dustin G. Mixon. Explicit matrices with the restricted isometry property: Breaking the square-root bottleneck. In Holger Boche, Robert Calderbank, Gitta Kutyniok, and Jan Vybíral, editors, *Compressed Sensing and its Applications: MATHEON Workshop 2013*, pages 389–417, Cham, 2015. Springer International Publishing.

[28] Hugh L Montgomery. *Topics in multiplicative number theory*, volume 227. Springer, 1971.

[29] N. Passuello. Semidefinite programming in combinatorial optimization with applications to coding theory and geometry, 2013. Ph.D. Thesis, Université Sciences et Technologies – Bordeaux I.

[30] Prasad Raghavendra and Tselil Schramm. Tight lower bounds for planted clique in the degree-4 SOS program, 2015. https://arxiv.org/abs/1507.05136.

[31] J. B. Shearer. Independence numbers for Paley graphs, accessed January 11, 2023. https://web.archive.org/web/20000815214259/http://www.research.ibm.com/people/s/shearer/indpal.html.

[32] T. Tao. *Structure and Randomness: pages from year one of a mathematical blog*. Amer. Math. Soc., 2008.

[33] Chi Hoi Yip. On the clique number of Paley graphs of prime power order. *Finite Fields and Their Applications*, 77:101930, 2022.