Smallest Critical Sets of Latin Squares

Yingjie Qian

Master of Science

Department of Mathematics and Statistics

McGill University, Montreal

Montreal, Quebec

2018-08

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Science

ACKNOWLEDGEMENTS

My past six years at McGill have been fruitful and enjoyable. I am indebted to the professors, classmates and friends from whom I have learned a great deal of mathematics, and who have always supported me in academics and in life.

In particular, I would like to express the deepest appreciation to my supervisor and mentor Hamed Hatami. I know I am far from being the best student but he is the best supervisor I would have ever hoped for. His knowledge and hard work always inspire me. He patiently guided me through every step during my master's. I owe him everything.

I would also like to thank Sergey Norin who is the reason I am in discrete mathematics. He has been a great mentor and motivator for me to improve. He has been a big help in my academic career and I cannot thank him enough for his support.

As always and forever, I am grateful to my parents and family for their unconditional love and support. I couldn't have achieved any of this without them in my corner.

For this thesis, other than Hamed's meticulous scrutiny, timely and scholarly advice, I would also like to thank Louigi Addario-Berry for his time and helpful comments as the examiner, and Katherine Edwards for the French translation of the abstract.

Finally I am grateful to Hamed Hatami and the Department of Mathematics and Statistics for their generous financial support.

ABSTRACT

A Latin square L of order n is an $n \times n$ array filled with elements of $\{1, 2, \ldots, n\}$ such that each value appears exactly once in each column and each row. A critical set in a Latin square is a minimal set of entries that uniquely identifies it among all Latin squares of the same size. It is conjectured by Nelder in 1979, and later independently by Mahmoodian, and Bate and van Rees that the size of the smallest critical set is $\lfloor n^2/4 \rfloor$.

We confirm the quadratic order predicted by this conjecture by establishing a lower-bound of $n^2/10^4$ for sufficiently large n. Previously the best known lower-bound was of order $\Omega(n^{3/2})$. Our proof uses a recent graph decomposition theorem due to Barber, Kühn, Lo, Osthus and Taylor. To be more self-contained, we will present two major steps in the proof of this graph decomposition theorem.

From the point of view of computational learning theory, the size of the smallest critical set corresponds to the minimum teaching dimension of the set of Latin squares. We study two related notions of dimension from learning theory. We also prove a lower-bound of $n^2 - (e + o(1))n^{5/3}$ for both of the VC-dimension and the recursive teaching dimension of class of Latin squares in this thesis.

ABRÉGÉ

Un carré Latin L d'ordre n est un tableau $n \times n$ rempli d'éléments parmi $\{1, 2, \ldots, n\}$ tel que chaque élément apparaisse exactement une fois dans chaque colonne et dans chaque rangée. Un ensemble critique dans un carré Latin est un ensemble minimal d'entrées qui l'identifie de manière unique parmi tous les carrés Latins de la même taille. Il a été conjecturé par Nelder en 1979, et plus tard indépendamment par Mahmoodian, et Bate et van Rees que la taille du plus petit ensemble critique est $\lfloor n^2/4 \rfloor$.

Nous confirmons l'ordre quadratique prédit par cette conjecture en établissant une borne inférieure de $n^2/10^4$ pour un n suffisamment grand. Auparavant, la meilleure limite inférieure connue était d'ordre $\Omega(n^{3/2})$. Notre preuve utilise un théorème récent de décomposition de graphe dûà Barber, Kühn, Lo, Osthus et Taylor. Afin que notre preuve soit autonome, nous présenterons deux étapes majeures dans la démonstration de ce théorème de décomposition de graphe.

Du point de vue de la théorie de l'apprentissage machine, la taille du plus petit ensemble critique correspond à la dimension d'enseignement minimale de l'ensemble des carrés Latins. Nous étudions deux notions connexes de la dimension de la théorie de l'apprentissage. Nous démontrons aussi une limite inférieure de $n^2 - (e + o(1))n^{5/3}$ pour la dimension VC et la dimension d'enseignement récursive de la classe des carrés Latins dans cette thèse.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
Introduction

Consider a set consisting of a finite number of k-dimensional vectors. Here, we think of each one of the k coordinates as a *feature* of the corresponding vector. Given a particular vector in the list, we are interested in the minimum number of features that identifies the vector uniquely. This parameter arises naturally in combinatorics, complexity theory, and machine learning. For example in the setting of computational machine learning, one can think of those features as the information that a *teacher* has to give to allow the *learners* to identify a target object.

Table 1–1: People with Features

Name	Sex	Eye Color	Height	Hair Length
Hypatia	F	Brown	Tall	Short
Paul	M	Blue	Tall	Long
Sofia	F	Brown	Short	Short
Maria	F	Brown	Short	Long
Euclid	M	Brown	Short	Short

Consider the example in Table 1. One needs 2 features, e.g. "Height" and "Hair Length", to identify Hypatia, but only 1 feature, e.g. "Eye Color", to identify Paul. It is an interesting question to find the vectors that require the smallest and the largest number of features to be identified. Here, the minimum is 1 feature (for Paul) and the maximum is 3 features (for Sofia).

In the language of computational machine learning, the set of the people in Table 1 is called a concept class, and the smallest number of features needed to identify a specific person is called the teaching dimension of that person (with respect to that concept class). The largest teaching dimension among all the elements in a concept class is called the *teaching dimension* of the concept class. The notion of *teaching dimension* was independently introduced by Goldman and Kearns [21], Shinohara and Miyano [39] and Anthony et al. [1]. It has also been studied under the names *witness set* by Kushilevitz et al. in [31], *discriminant* in [34], and *specifying set* in [1].

In combinatorics, similar notations of identifying an object inside a class of combinatorial objects have been defined and studied independently under various names in different contexts. For example, one can consider the concept class of all of the proper 3-vertex colourings of a given graph, where each colouring is represented as a vector whose coordinates represent the colours of the vertices. Then one could ask questions about the minimum number of features to identify a particular colouring among all the colourings. Indeed there is an extensive literature investigating such problems. The term *defining set* is used for block designs and graph colourings, and the term *forcing set*, coined by Harary [23], is used for other concepts such as perfect matchings, dominating sets, and geodetics (see the survey [14]), and finally the term *critical set* is used in the context of Latin squares, which is the main focus of this thesis.

1.1 Latin Squares

A *Latin square* L of order n is an $n \times n$ array filled with elements of $\{1, 2, \ldots, n\}$ such that each value appears exactly once in each column and each row. Note that we can use a set of triples to represent L:

$$\{(i, j, k)| \text{ the } (i, j)\text{-th entry is filled with value } k \}.$$

The name “Latin square” was inspired by mathematician Leonhard Euler [43] who used Latin characters as symbols instead of integer values filled in the entries. An example of a 3×3 Latin square filled with Latin characters L or integer values L' is the following:

Figure 1–1: Latin Square Filled with Latin Characters or Integer Values

$$L = \begin{array}{|c|c|c|} \hline A & B & C \\ \hline B & C & A \\ \hline C & A & B \\ \hline \end{array} \qquad L' = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

A *partial Latin square* P of order n is an $n \times n$ array that is partially filled with elements of $\{1, 2, \ldots, n\}$ and no element appears more than once in any column or row. We adopt the set notion $|P|$ to denote the number of entries filled, and we write $P \subseteq L$ if the filled entires of P match that of L. In the latter case, we say P can be completed to L. Note that not all partial Latin squares can be completed to Latin squares, and some partial Latin squares can be completed to many different Latin squares.

1.2 Defining Sets and Critical Sets

In 1977, the statistician John Nelder [35] asked a seemingly simple question regarding partial Latin squares: What is the size of the smallest partial Latin square P that can be completed to a *unique* Latin square L? We refer to a partial Latin square that can be completed to a unique Latin square L as a *defining set* for L. Nelder used the term *critical set* to refer to minimal defining set. Here, minimality means that no proper subset of them is a defining set. Since in this thesis, we are interested in the smallest defining sets for each Latin square, this minimality condition is automatically satisfied and need not be imposed. In other words, being a smallest defining set is equivalent to being a smallest critical set. However, for historical reasons, we will use the term “smallest critical set” rather than “smallest defining set”.

Consider the following examples given by Keedwell [30] which illustrate two facts regarding sizes of critical sets:

Figure 1–2: Examples of Critical Sets

$P_1 =$

1	2	*	*
2	*	*	*
*	*	*	*
*	*	*	3

$P_2 =$

1	2	3	*
2	3	*	*
3	*	*	*
*	*	*	*

$P_3 =$

*	2	*	*
2	*	*	3
*	*	1	*
4	*	*	*

$L_1 =$

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

$L_2 =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

In the above example, all P_1, P_2, P_3 are critical sets. Moreover, both P_1, P_2 can be completed to L_1, and P_1, P_3 are the smallest critical sets of L_1, L_2 respectively. The former says that there exist critical sets of different sizes for the same Latin square, and the latter says that different Latin squares of the same order could have smallest critical sets of different sizes.

In this thesis, we are mainly interested in the size of the smallest defining sets, or equivalently the size of the smallest critical sets.

1.3 Maximum Smallest Critical Sets

Let us denote by $\mathrm{scs}(L)$ the size of smallest critical set for a specific Latin square L. For the example in Figure 1.2, $\mathrm{scs}(L_1) = 4$ and $\mathrm{scs}(L_2) = 5$. The problem of determining the maximum and minimum sizes of smallest critical sets among all Latin squares of a fixed order n, i.e. $\max_L \mathrm{scs}(L)$ and $\min_L \mathrm{scs}(L)$ respectively, has been studied extensively. We refer the readers to the two surveys [29] and [9] for more on this topic.

The best known bounds on the maximum size of the smallest critical sets for Latin squares of order n are given by Ghandehari, Hatami and Mahmoodian [20]:

$$n^2 - (e + o(1))n^{10/6} \leq \max_L \operatorname{scs}(L) \leq n^2 - \frac{\sqrt{2}}{2} n^{9/6}$$

They proved the above inequalities by showing that every Latin square of order n has a critical set of size no larger than $n^2 - \frac{\sqrt{2}}{2} n^{3/2}$ and there exist Latin squares of order n with no critical sets of size smaller than $n^2 - (e + o(1))n^{5/3}$. Note that the latter also gives a lower-bound of $n^2 - (e + o(1))n^{5/3}$ on the size of the largest critical sets for Latin squares of order n.

1.4 Minimum Smallest Critical Sets

Now, let us turn our attention to the main topic of the thesis: $\min_L \operatorname{scs}(L)$ over all Latin squares L of order n, denoted by $\operatorname{scs}(n)$ for simplicity.

Note that a partially filled Latin square can determine the values of certain empty entries (i, j) in a straightforward manner: if all the values $\{1, \ldots, n\} \setminus \{k\}$ already appear in the i-th row and j-th column, then the (i, j)-th entry is determined to be k. One can start from a partially filled Latin square P and iteratively set the values of the entries that are determined in this manner. If this finally leads to a full Latin square L, then P is obviously a defining set for L. Such defining sets are called *strong defining sets*. In Figure 1.2, all P_1, P_2, P_3 are strong defining sets.

Bate and van Rees [4] proved that $\operatorname{scs}(6) = 9$. In the same paper, they showed that the size of the smallest *strong* defining set among all Latin squares of order n is $\lfloor n^2/4 \rfloor$. They conjectured that the same bound holds for general defining sets that are not necessarily strong. This was also independently conjectured earlier by Nelder[1] , and Mahmoodian [32].

Conjecture 1. *Every critical set for a Latin square of order n is of size at least $\lfloor n^2/4 \rfloor$.*

The existence of critical sets of size $\lfloor n^2/4 \rfloor$ was shown by Curran and van Rees [12] and Cooper, Donovan and Seberry [11], so the above conjecture is equivalent to $\mathrm{scs}(n) = \lfloor n^2/4 \rfloor$. The first nontrivial linear lower-bound of $\lfloor (7n-3)/6 \rfloor$ for $n \geq 20$ was showed by Fu, Fu, and Rodger [19] in 1997, which was improved by Horak, Aldred, and Fleischner [26] to $\lfloor (4n-8)/3 \rfloor$ for $n \geq 8$. In 2007, Cavenagh [8] gave the first superlinear lower-bound of $n\lfloor (\log n)^{1/3}/2 \rfloor$. After another decade, Cavenagh and Ramadurai [7] improved it to $\Omega(n^{3/2})$. Most recently, Hatami and the author [24] finally confirmed the quadratic order predicated by this conjecture with the following theorem.

Theorem 2 (Main Theorem [24])**.** *For sufficiently large n, every critical set for a Latin square of order n is of size at least $10^{-4}n^2$.*

The proof uses an approach that is very different from the previously used methods. It relies on a recent graph decomposition theorem, which will be introduced along with some notations in Chapter 2. Roughly speaking, this decomposition theorem says that under some natural divisibility conditions every graph with large minimum degree can be decomposed into triangles. In Chapter 3, we use this graph decomposition theorem to prove Theorem 2.

We will not present the full proof of the graph decomposition theorem in this thesis. However in Chapters 4 and 5, we will present two of the main steps that guarantee the existence of an approximate decomposition. The proof for obtaining a precise decomposition from an approximate one is

[1] John Nelder: Private communication to Jennifer Seberry (1979).

technical, long and complicated. We refer the interested readers the original paper [3]. Finally, in Chapter 6, we give some concluding remarks.

CHAPTER 2
Background

In this chapter, we recall some basic notations and facts in computational learning theory (in Section 2.1) and in graph theory (in Section 2.2). Then, we present more details regarding the graph decomposition theorem that we will use to prove Theorem 2.

2.1 VC, Teaching, and Recursive Teaching Dimensions

As mentioned earlier, the general concept of identifying an object by a small set of its attributes arises naturally in the area of computational learning theory. Consider a finite set Ω, and let $\mathcal{F}(\Omega)$ denote the power set of Ω. In computational learning theory, a subset $\mathcal{C} \subseteq \mathcal{F}(\Omega)$ is refered to as a *concept class*, and the elements $c \in \mathcal{C}$ are called *concepts*. A set $S \subseteq \Omega$ is called a *teaching set* for a concept $c \in \mathcal{C}$ if $c \cap S$ uniquely identifies c among all other concepts. In other words, $(c \cap S) \neq (c' \cap S)$ for every concept $c' \neq c$.

The notion of a teaching set naturally gives rise to various notions of dimension associated to concept classes. Let $\mathrm{TD}(c;\mathcal{C})$ denote the smallest size of a teaching set for a concept $c \in \mathcal{C}$. The *teaching dimension* and the *minimum teaching dimension* of a concept class $\mathcal{C}$ are respectively defined as $\mathrm{TD}(\mathcal{C}) = \max_{c\in\mathcal{C}} \mathrm{TD}(c;\mathcal{C})$ and $\mathrm{TD}_{\min}(\mathcal{C}) = \min_{c\in\mathcal{C}} \mathrm{TD}(c;\mathcal{C})$. It turns out that for some purposes, due to its local nature, the teaching dimension and minimum teaching dimension do not capture the characteristics of teaching and learning, and thus the related notion of *recursive teaching dimension* is often considered:

$$\mathrm{RTD}(\mathcal{C}) = \max_{\mathcal{C}' \subseteq \mathcal{C}} \mathrm{TD}_{\min}(\mathcal{C}').$$

Note that $\mathrm{TD}_{\min}(\mathcal{C}) \leq \mathrm{RTD}(\mathcal{C}) \leq \mathrm{TD}(\mathcal{C})$ for every concept class $\mathcal{C}$.

Finally let us recall one of the most celebrated notions of dimension associated to a concept class, i.e. its VC dimension (for Vapnik-Chervonenkis dimension). A subset $S \subseteq \Omega$ is said to be *shattered* by $\mathcal{C}$ if for every $T \subseteq S$ there exists a concept c with $c \cap S = T$. The size of the largest set shattered by $\mathcal{C}$ is called the *VC-dimension* of $\mathcal{C}$. Recently in [10], using a surprisingly short argument, Chen, Cheng and Tang showed that $\mathrm{RTD}(\mathcal{C}) \leq 2^{d+1}(d-2)+d+4$, where $d = \mathrm{VC}(\mathcal{C})$. This was subsequently improved to $O(d^2)$ by Hu, Wu, Li and Wang in [28].

2.2 Graph Basics

We recall the following basic graph definitions. A *graph* G is a pair of sets (V, E), where the vertex set V is a finite set of vertices and the edge set E is a set of 2-element subsets of V. Two graphs G, H are *isomorphic* if there exists a bijection $\phi : V(G) \mapsto V(H)$ such that $\{u, v\} \in E(G)$ if and only if $\{\phi(u), \phi(v)\} \in E(H)$. Two vertices $u, v \in V$ are called *adjacent* if $\{u, v\} \in E(G)$;

A graph $H = (V', E')$ is a *subgraph* of G if $V' \subseteq V$ and $E' \subseteq E$. The *complete graph* on n vertices, denoted by K_n, is the graph whose edge set contains all 2-element subsets of V. A *path* in G is a sequence of distinct vertices $v_1, v_2, \ldots, v_k \in V(G)$ such that for all $i \in \{1, 2, \ldots, k-1\}$, v_i and v_{i+1} are adjacent. A graph is called *connected* if there is a path between every pair of vertices.

For an integer $r > 1$, a graph G is called an *r-partite* graph if one can partition the vertex set into r sets such that there is no edge with both ends in the same partite set.

We will use the following notations. Consider a graph $G = (V, E)$.

(a) The number of edges is $e(G) = \left|E(G)\right|$;

(b) The neighbourhood of $v \in G$ in $S \subset V$: $N_S(v) = \{u \in S : \{u, v\} \in G\}$;

(c) The degree of vertex $v \in G$ in $S \subset V$: $\deg_S(v) = \left|\{N_S(v)\}\right|$;

(d) The minimum degree of G: $\delta(G) = \min_{v \in V} \deg(v)$.

2.3 Graph Decomposition

Let us formally define graph decompositions.

Definition 3. *A graph G has an F-decomposition if $E(G)$ can be partitioned into subgraphs, each isomorphic to F.*

Graph decompositions are linked to many combinatorial problems, such as hypergraph matchings and graph labelings. It is easy to see that two necessary conditions for G to have an F-decomposition are the followings: $e(F)$ must divide $e(G)$; and the greatest common divisor of the degrees of F must divide the greatest common divisor of the degrees of G. On the other hand, the sufficient conditions are wildly open in general.

In this thesis, we are in particular interested in the special case of K_3-decompositions in 3-partite graphs.

2.4 Exact K_3-decompositions

Consider a 3-partite graph G with partite sets V_1, V_2, V_3. One specific necessary condition for such a graph G to have a K_3-decomposition is that every vertex has the same number of neighbours in the other two partite sets. Two special properties of a 3-partite graph including the above mentioned are defined as follows.

Definition 4. *Let G be a 3-partite graph with partite sets V_1, V_2, V_3. Then,* *(a) G is balanced if* $|V_1| = |V_2| = |V_3|$;

(b) G is locally balanced if for all $v \in V_i$, $\deg_{V_j}(v) = \deg_{V_k}(v)$ *with* $i \neq j \neq k$.

When searching for conditions which force the existence of a certain structure that covers *all* vertices, one usually needs a large minimum degree condition to prevent the existence of local obstacles (e.g. isolated vertices). A similar intuition applies in searching for sufficient conditions for the existence of graph decompositions. Large minimum degree increases the chance of having the decomposition as there are more choices for decomposing the edges incident to every vertex.

Indeed, the series of works Barber, Kühn, Lo and Osthus [2], Haxell and Rödl [25], and Dross [15] showed that the aforementioned divisibility necessary conditions together with the minimum degree condition of $9n/10 + o(n)$ guarantee that a large n-vertex graph G has a K_3-decomposition. Moreover, together with the works of Barber, Kühn, Lo, Osthus and Taylor [3], Bowditch and Dukes [5], and Montgomery [33], they were able to prove better minimum degree conditions for balanced and locally balanced large 3-partite graphs.

We formulate some of the above works into the following theorem that will be used in Chapter 3 in the proof of our main theorem.

Theorem 5 ([3],[25],[5]). *For sufficiently large n, every balanced and locally balanced 3-partite graph G on 3n vertices satisfying* $\delta(G) \geq 1.94n$ *admits a* K_3*-decomposition.*

As mentioned earlier, it was a series of works that lead to the above theorem. These works reduce the problem of finding a decomposition into finding weaker notions of graph decompositions: approximate decomposition and fractional decomposition. In details, Theorem 5 is proved with the following three steps:

Step 1 Existence of a fraction decomposition due to Bowditch and Dukes [5]. Presented in Chapter 4;

Step 2 Existence of an approximate decomposition follows from a fraction decomposition, due to Haxell and Rödl [25]. Yuster [44] used a simpler proof to generalize the result to family of graphs. Presented in Chapter 5 (based on [44]);

Step 3 Existence of an exact decomposition follows from an approximate decomposition, due to Barber, Kühn, Lo, Osthus and Taylor [3] (which was an improvement on a previous result of Barber, Kühn, Lo and Osthus [2] on K_3-decompositions in a not necessarily 3-partite graph). (Not presented in this thesis).

CHAPTER 3
Main Results

In this chapter, we will present our main results. In particular, we will establish a quadratic lower-bound on the size of the smallest critical sets, a major step towards resolving Conjecture 1. In Sections 3.1 and 3.2, we will prove new results on the VC-dimension and the recursive teaching dimension of the class of Latin squares.

Noting that a Latin square of order n is a K_3-decomposition of the complete 3-partite graph $K_{n,n,n}$, Barber, Kühn, Lo, Osthus and Taylor [3] obtained the following corollary to Theorem 5.

Corollary 6 ([3])**.** *Let P be a partial Latin square of order $n \geq n_0$ such that every row, column, and symbol is used at most $0.0288n$ times. Then P can be completed to a Latin square.*

We will take a similar approach to prove our main theorem.

Theorem 2 (Main Theorem [24])**.** *For sufficiently large n, every critical set for a Latin square of order n is of size at least $10^{-4}n^2$.*

Proof for Theorem 2. Set $\epsilon = 10^{-4}$. We need to show that provided that n is sufficiently large, if a partial Latin square P of size at most ϵn^2 can be completed to a Latin square L, then P can also be completed to a different Latin square L'.

For such a P, let R, C, S be respectively the set of all rows, columns and symbols in P that have at least δn filled entries, where $\delta = 0.012$. We extend P to a larger partial Latin square P_1 by completing all those rows, columns and symbols by filling the empty cells with the entries of L. Let $m = \max\{|R|, |C|, |S|\}$, and note $m \le \frac{\epsilon}{\delta} n \le 0.0084n$. We obtain P_2 by filling $m - |R|$ additional rows, $m - |C|$ additional columns, and $m - |S|$ additional symbols with entries of L. Consider any row r in P with less than δn filled entries and it is not selected to be filled as an additional row when building P_2. This row r is filled with at most $2m$ entries during the filling process of columns and symbols. Since $2m + \delta n < n$, r is not completed in P_2 and thus exactly m rows are fully filled in P_2. Similarly, exactly m columns and m symbols are fully filled in P_2.

Let $(x, y, z) \in L \setminus P_2$. Such an element exists because $|P_2| \le |P| + 3mn \le (\epsilon + \frac{3\epsilon}{\delta})n^2 < n^2$. Let z' be any symbol such that $(x, j, z'), (i, y, z') \notin P_2$ for all $i, j \in \{1, \ldots, n\}$. In other words, z' is a symbol which does not appear in either row x or column y in the partial Latin square P_2. Such a symbol z' exists because the number of symbols in the x-th row and the number of symbols in the y-th column of P_2 are each at most $\delta n + 2m$, and thus there are in total at most $2\delta n + 4m < 0.06n$ symbols appearing in the x-th row and the y-th column.

Let $P_3 = P_2 \cup \{(x, y, z')\}$. We claim that P_3 can be completed to a Latin square. Note that P_3 still has exactly m completed rows, columns and symbols as filling (x, y, z') in P_2 cannot create another complete row, column or symbol. Start from the complete 3-partite graph $K_{n,n,n}$ where the vertices of each part are labeled with $\{1, \ldots, n\}$, and for every entry $(i, j, k) \in P_3$ remove the three edges of the triangle (i, j, k) from the graph. Let G be the resulting graph. Note that G has $3m$ vertices of degree 0 corresponding to the completed rows, columns and symbols in P_3. Ignoring the 0-degree vertices, G is balanced and locally balanced, and it is of minimum degree at least $2n-2(\delta n+2m+1) > 1.9426n > 1.94(n-m)$. Hence by Theorem 5, it admits a K_3-decomposition, which in turn corresponds to a completion to a Latin square L'. Note that $L' \neq L$ as the two Latin squares disagree on the (x, y) entry. □

3.1 VC, Teaching, and Recursive Teaching Dimensions for Latin Squares

Recall that every Latin square of order n can be represented as a subset of $\{1, \ldots, n\}^3$. Hence the set $\mathcal{L}_n$ of all Latin squares of order n can be considered as a concept class. It is worth noting that our definition of a defining set for a Latin square coincides with the teaching dimension when $\mathcal{L}_n$ is considered as a concept class. We illustrate this in the following lemma.

Lemma 7. *Let L be any Latin square of order n, then* $\mathrm{scs}(L) = \mathrm{TD}(L; \mathcal{L}_n)$.

Proof. Consider Latin square $L \in \mathcal{L}_n$, then $\mathrm{TD}(L; \mathcal{L}_n)$ is the smallest size of any set $P \subseteq \{1, 2, \ldots, n\}^3$ with the property that $L \cap P \neq L' \cap P$ for all $L' \in \mathcal{L}_n$ and $L' \neq L$. We call such a property teaching property and let P' be any set with such property of smallest size. We claim that P' is a partial Latin square of smallest size which can be uniquely completed to L, which is the definition of a defining set.

Suppose P' is not a partial Latin square, then there exists $(i, j, k) \in P'$ such that at least one of $(i', j, k), (i, j', k), (i, j, k')$ is also in P' with $i \neq i', j \neq j', k \neq k'$. Without loss of generality, $(i, j', k) \in P'$. Since at most one of $(i, j, k), (i, j', k)$ is in L, there are two cases: (i) exactly one of them is in L, without loss of generality, $(i, j, k) \in L$ and $(i, j', k) \notin L$. Consider any Latin square $L' \in \mathcal{L}_n$ and $L' \neq L$ such that $L' \cap \{(i, j', k)\} \neq L \cap \{(i, j', k)\} = \emptyset$. Then, $(i, j', k) \in L'$. Since $(i, j, k), (i, j', k)$ cannot both be in L', $(i, j, k) \notin$

L'. So $L' \cap \{(i,j,k)\} = \emptyset \neq \{(i,j,k)\} = L \cap \{(i,j,k)\}$. It follows that $P' \setminus \{(i,j',k)\}$ has teaching property, which contradicts the minimality of P'; (ii), none of them is in L, i.e., $(i,j,k),(i,j',k) \notin L$. Let k'' be the symbol such that $(i,j,k'') \in L$. For any $L' \in \mathcal{L}_n$ and $L' \neq L$, with similar reasoning in the previous case, if $L' \cap \{(i,j,k),(i,j',k)\} \neq L \cap \{(i,j,k),(i,j',k)\} = \emptyset$, then $(i,j,k'') \notin L'$ and thus, $L' \cap \{(i,j,k'')\} \neq L \cap \{(i,j,k'')\}$. Then, $\Big(P' \setminus \{(i,j,k),(i,j',k)\}\Big) \cup \{(i,j,k'')\}$ has teaching property, which also contradicts the minimality of P'.

The lemmas follows as desired. $\square$

Our main result, Theorem 2, says that $\mathrm{TD}_{\min}(\mathcal{L}_n) \geq 10^{-4}n^2$ for sufficiently large n. Recall the result of Ghandehari, Hatami and Mahmoodian [20] on $\max_L \mathrm{scs}(L)$, which is equivalent to the following by Lemma 7, for sufficiently large n:

$$n^2 - (e + o(1))n^{5/3} \leq \mathrm{TD}(\mathcal{L}_n) \leq n^2 - \frac{\sqrt{\pi}}{2}n^{3/2}.$$

On the other hand, $\mathrm{RTD}(\mathcal{L}_n)$ does not seem to correspond to any of the previously studied parameters related to critical sets. In Theorem 9 below, we show that one can adapt the argument of [20] to obtain a stronger result that $\mathrm{RTD}(\mathcal{L}_n) \geq n^2 - (e+o(1))n^{5/3}$. Surprisingly, a similar argument combined with a lemma of Pajor (Lemma 12) implies the same bound for the VC-dimension. Both theorems are joint work with Hatami in [24].

Theorem 8. *The VC-dimension of the class of Latin squares of order n is at least $n^2 - (e + o(1))n^{5/3}$.*

Theorem 9. *The recursive teaching dimension of the class of Latin squares of order n is at least $n^2 - (e + o(1))n^{5/3}$.*

3.2 Proofs of Theorem 8 and Theorem 9

The van der Waerden conjecture, proved in [22, 16, 17], can be used to obtain a lower-bound for the number of Latin squares of order n.

Lemma 10 ([41, Theorem 17.2])**.** *Let $\mathcal{L}_n$ be the set of all Latin squares of order n. Then*

$$|\mathcal{L}_n| \geq \frac{(n!)^{2n}}{n^{n^2}}.$$

Ghandehari, Hatami and Mahmoodian [20, Theorem 3] used Bregman's theorem [6] to obtain an upper-bound for the number of partial Latin squares of a given size.

Lemma 11 ([20, Theorem 3])**.** *Let $\mathcal{T}_{n,k}$ be the set of all partial Latin squares of order n and of size k. Then*

$$|\mathcal{T}_{n,k}| \leq \binom{n^2}{k} \frac{n!^{2n-\frac{k}{n}} e^{n(3+\frac{\ln(2\pi n)^2}{4})}}{(n-\frac{k}{n})!^{2n} e^k}.$$

The most basic result concerning VC-dimension is the Sauer-Shelah lemma. This lemma, which has been independently proved several times (e.g. in [37] [38] [42]), provides an upper-bound on the size of a concept class $\mathcal{C} \subseteq \mathcal{F}(\Omega)$ in terms of $|\Omega|$ and $\mathrm{VC}(\mathcal{C})$. Formally it says $|\mathcal{C}| \leq \sum_{i=0}^{d} \binom{|\Omega|}{i}$ where $d = \mathrm{VC}(\mathcal{C})$. Note that for the set of $n \times n$ Latin squares $\mathcal{L}_n \subseteq \{1, \ldots, n\}^3$, we have $|\Omega| = n^3$. Then it is not difficult to see that the Sauer-Shelah lemma together with Lemma 10 implies $\mathrm{VC}(\mathcal{L}_n) \geq n^2 \left(\frac{1}{3} - o(1)\right)$. The $1/3$ factor in this bound is due to the cubic size of $|\Omega|$ in terms of n. To obtain the $n^2(1-o(1))$ bound of Theorem 8, rather than use the Sauer-Shelah lemma we will instead use the following result due to Pajor [36], which is easily seen to imply the Sauer-Shelah lemma.

Lemma 12 ([36])**.** *Every finite set family $\mathcal{F}$ shatters at least $|\mathcal{F}|$ sets.*

Proof of Theorem 8. We will prove that $n^2 - e^{1+\frac{1}{\sqrt{n}}} n^{5/3} < \mathrm{VC}(\mathcal{L}_n)$ for sufficiently large n. Note that if a set $S \subseteq \{1, \ldots, n\}^3$ is shattered by $\mathcal{L}_n$, then in particular $S \cap L = S$ for some $L \in \mathcal{L}_n$, and thus $S \subseteq L$. Hence every shattered set S corresponds to a partial Latin square. By Lemma 12, the set of all Latin squares of order n shatters at least $|\mathcal{L}_n|$ sets. It follows that for $d = \mathrm{VC}(\mathcal{L}_n)$, we have

$$\sum_{k=0}^{d} |\mathcal{T}_{n,k}| \geq |\mathcal{L}_n|. \tag{3.1}$$

Hence to prove $n^2 - e^{1+\frac{1}{\sqrt{n}}} n^{5/3} < \mathrm{VC}(\mathcal{L}_n)$, it suffices to show that for every $k \leq n^2 - e^{1+\frac{1}{\sqrt{n}}} n^{5/3}$, we have $|\mathcal{T}_{n,k}| < \frac{|\mathcal{L}_n|}{n^2}$, or equivalently $|\mathcal{L}_n| \leq n^2 |\mathcal{T}_{n,k}|$ implies $k > n^2 - e^{1+\frac{1}{\sqrt{n}}} n^{5/3}$.

We can follow a similar calculation as in [20]: Assume $|\mathcal{L}_n| \leq n^2 |\mathcal{T}_{n,k}|$. Then by Lemma 10 and Lemma 11,

$$\frac{(n!)^{2n}}{n^{n^2}} \leq n^2 \binom{n^2}{k} \frac{n!^{2n-\frac{k}{n}} e^{n(3+\frac{\ln(2\pi n)^2}{4})}}{(n-\frac{k}{n})!^{2n} e^k}. \tag{3.2}$$

Setting $c = 1 - \frac{k}{n^2}$, and using $\binom{n^2}{k} = \binom{n^2}{n^2-k} \leq \left(\frac{e}{c}\right)^{cn^2}$, we obtain

$$\frac{n!^{n-cn}}{n^{n^2}} \leq \frac{n^2 e^{cn^2} e^{n \ln(2\pi n)^2}}{c^{cn^2} (cn)!^{2n} e^{n^2-cn^2}}.$$

Using $n! \geq (\frac{n}{e})^n$, we obtain

$$\frac{n^{n^2-cn^2}}{e^{n^2-cn^2} n^{n^2}} \leq \frac{n^2 e^{3cn^2} e^{n \ln(2\pi n)^2}}{c^{cn^2} (cn)^{2cn^2} e^{n^2-cn^2}},$$

and thus

$$c^{3c} n^c \leq e^{3c} e^{\frac{\ln(2\pi n)^2}{n}} n^{\frac{2}{n^2}}. \tag{3.3}$$

Fix a sufficiently large n. If $c = \frac{e^{1+\frac{1}{\sqrt{n}}}}{n^{1/3}}$, then $c^{3c} n^c > e^{3c} e^{\frac{\ln(2\pi n)^2}{n}} n^{\frac{2}{n^2}}$, and moreover $c^{3c} n^c e^{-3c}$ is an increasing function of c in $[n^{-1/3}, \infty)$. So inequality (3.3) implies $c < \frac{e^{1+\frac{1}{\sqrt{n}}}}{n^{1/3}}$, which in turn shows $k > n^2 - e^{1+\frac{1}{\sqrt{n}}} n^{5/3}$ as desired. $\square$

The proof of Theorem 9 will use a counting argument similar to that used in the proof of Theorem 8.

Proof of Theorem 9. Recall that $\mathcal{L}_n$ denotes the set of all Latin squares of order n, and $\mathcal{T}_{n,k}$ denotes the set of all partial Latin squares of order n and of size k. We create a series of bipartite graphs in the following way: Set a bipartite graph D_0 with vertex sets $A_0 = \mathcal{T}_{n,k}$ and $B_0 = \mathcal{L}_n$, with edges $\{(T, L) \in (A_0, B_0) : T \subseteq L\}$. Recursively define D_{i+1} from D_i by letting $A_{i+1} = A_i \setminus \{T \in A_i : \deg_{D_i}(T) = 1\}$, and letting $B_{i+1} = \{L \in B_i : \left|N_{A_{i+1}}(L)\right| \geq 1\}$. This process eventually terminates at a graph $D = (A, B)$. Then, $|\mathcal{L}_n - B| \leq \left|\mathcal{T}_{n,k}\right|$ as in each step, we only remove partial Latin squares in $\mathcal{T}_{n,k}$ that can be completed to a unique Latin square in the remaining set of Latin squares. Now, we claim that if B is not empty, then $\mathrm{TD}_{\min}(B) \geq k+1$. Consider any $L \in B$, then every partial Latin square $P \subseteq L$ with $|P| = k$ must be in A, otherwise this partial Latin square must have had a unique completion at the moment it was deleted, which contradicts the existence of L in B. So such an L cannot be uniquely completed from a partial Latin square of size k. We know from the proof of Theorem 8 that $|\mathcal{L}_n| > |\mathcal{T}_{n,k}|$ if $k \leq n^2 - (e + o(1))n^{5/3}$, and thus $\mathrm{RTD}(\mathcal{L}_n) \geq \mathrm{TD}_{\min}(B) \geq n^2 - (e + o(1))n^{5/3}$ as desired. □

CHAPTER 4
Fractional K_3-decomposition

As promised, in this chapter, we will present the first step towards the exact graph decomposition theorem (Theorem 5), which is to show the existence of a fractional decomposition under certain natural conditions (Theorem 14 below based on [5]).

Let us first formally define a fractional K_3-decomposition as the following.

Definition 13. *G has a fractional K_3-decomposition if there is a list of ordered pairs (F_i, w_i) such that F_i is a copy of K_3 in G and w_i is a nonnegative real weight such that for all $e \in E(G)$,*

$$\sum_{i:e\in E(F_i)} w_i = 1.$$

4.1 Existence of Fractional Decompositions

We use main ideas in [5] to show that a lower-bound on the minimum degree guarantees the existence of fractional K_3-decomposition for large balanced and locally balanced 3-partite graphs. The main theorem of this chapter states as following:

Theorem 14 ([5])**.** *For sufficiently large n, every balanced and locally balanced 3-partite graph G on $3n$ vertices satisfying $\delta(G) \geq 1.94n$ admits a fractional K_3-decomposition.*

Bowditch and Dukes [5] obtained a slightly better constant in their original paper. It requires more complicated computations but it does not improve much on our constant on size of the smallest critical set in Latin squares. So we will refer the readers to their paper if interested.

4.2 Proof of Theorem 14

Let n be a sufficiently large integer. We will show that every locally balanced spanning subgraph G of $K_{n,n,n}$ with $\delta(G) \geq 1.94n$ admits a fractional K_3-decomposition. The proof is organized as follows: In Section 4.2.1, we will build matrices for G to record the relationship between edges and K_3's that contain those edges, and set up the equations such that the existence of satisfying solutions would guarantee a fractional K_3-decomposition in G; we will then use certain techniques based on matrix norms in Section 4.2.2 to show that establishing a certain upper-bound on those matrix norms is sufficient to obtain the desired decompositions; finally in Section 4.2.3, we complete the proof by proving those bounds for graphs G that satisfy the minimum degree condition.

We work primarily in the vector space $\Omega(G) := \mathbb{R}^{E(G)}$ or $\Omega(K_{n,n,n}) := \mathbb{R}^{E(K_{n,n,n})}$. We use the notations α, β, γ to denote vertices in different partite sets of $K_{n,n,n}$ and α', β', γ' to denote the vertices in the corresponding same partite set but different from α, β, γ.

4.2.1 Fractional Decomposition as a Matrix Equation

Let W_G be a $\{0,1\}$-matrix whose rows are indexed by $E(G)$ and columns by $T(G)$, the set of all triangles in G. For $e \in E(G), t \in T(G)$, we define $W_G(e,t)$ to be

$$W_G(e,t) = \begin{cases} 1 \text{ if } s \in t, \\ 0 \text{ otherwise.} \end{cases}$$

Then, a fractional K_3-decomposition of G is equivalent to an entrywise non-negative solution $\mathbf{z}$ to the equation

$$W_G\mathbf{z} = \mathbf{1}, \tag{4.1}$$

where $\mathbf{1}$ is the vector of all 1's.

Let $M_G = W_G W_G^T$. Then, an entrywise nonnegative solution $\mathbf{x}$ to the following equation would imply a desired solution to Equation (4.1):

$$M_G\mathbf{x} = \mathbf{1}. \tag{4.2}$$

Combinatorially, M_G has rows and columns both indexed by $E(G)$ and the (e, f)-entry counts the number of triangles in G that contain both e and f.

For convenience, we denote $W_{K_{n,n,n}}$ as W and $M_{K_{n,n,n}}$ as M. It is not hard to calculate the ranks of W and M, and find a basis for their kernels.

Lemma 15. $\mathrm{rank(W) = rank(M) = n^3 - (n-1)^3}$.

Proof. For any matrix A, let $N(A)$ be its null space. Clearly, $N(W) \subseteq N(W^TW)$. For every $v \in N(W^TW)$, we have $v^TW^TWv = 0$, or equivalently $(Wv)^T(Wv) = 0$, which implies $Wv = 0$. Thus, $N(W) = N(W^TW) = N(M)$ and the first equality follows.

For the second equality, we give an explicit construction. Fix any triangle $\alpha\beta\gamma \in K_{n,n,n}$, and let $\mathcal{I}$ be the set of all triangles containing at least one of α, β, γ. We claim such a set $\mathcal{I}$ forms a linear basis for the columns of W, i.e., the vectors in $\mathcal{I}$ are independent and they span all of $T(K_{n,n,n})$.

For independence, consider $\beta'\gamma' \in E(K_{n,n,n})$, and it belongs only to the triangle $\alpha\beta'\gamma' \in \mathcal{I}$. For edges in the form of $\beta'\gamma$, it belongs to a unique triangle in $\mathcal{I}$ which intersects $\alpha\beta\gamma$ in two points.

Now, we want to show that every triangle in $T(K_{n,n,n})$ is a linear combination of those in $\mathcal{I}$. Indeed, if we use $\alpha\beta\gamma$ to denote the formal linear combination of $\alpha\beta + \alpha\gamma + \beta\gamma \in \Omega(K_{n,n,n})$, then

$$\alpha'\beta'\gamma' = \alpha\beta\gamma - \alpha'\beta\gamma - \alpha\beta'\gamma - \alpha\beta\gamma' + \alpha'\beta'\gamma + \alpha'\beta\gamma' + \alpha\beta'\gamma'.$$

It is easy to count the size of $\mathcal{I}$, $|\mathcal{I}| = n^3 - (n-1)^3$, and we are done. □

By the above lemma, we have

$$\dim\ker(W^T) = \dim\ker(M) = 3n^2 - (n^3 - (n-1)^3) = 3n - 1.$$

We give the following explicit construction of a basis for the kernel. Fix a cyclic order of the three different partite sets and define the vector $\mathbf{v}_\beta \in \Omega(K_{n,n,n})$ by

$$\mathbf{v}_\beta = \begin{cases} 1 \text{ if } e = \alpha\beta \text{ for some } \alpha, \\ -1 \text{ if } e = \beta\gamma \text{ for some } \gamma, \\ 0 \text{ otherwise.} \end{cases}$$

There are $3n$ such vectors in total and pick any $3n-1$ of them. It is easy to see that these $3n-1$ vectors are linearly independent. Next note that any vector in $\ker(W^T)$ is in the following form: entries corresponding to the same partite set have the same value, and these three possible values are $c, -c, 0$, where c is a constant. It follows that these $3n-1$ vectors span $\ker(W^T)$ and they form a basis.

Let K be the matrix of the orthogonal projection onto $\ker(M)$, and $K[G]$ be its restriction to the principal submatrix indexed by $\Omega(G)$. It is not hard to obtain the following lemma as the first assertion is true by the locally balanced property and its orthogonality to every vector in $\ker(M)$, and the second half can be shown by reorganizing the rows.

Lemma 16. *With $K[G]$ and M_G defined as above, $K[G]\mathbf{1} = \mathbf{0}$ and $K[G]M_G = \mathbf{0}$.*

The following fact roughly says that if the coefficient matrix undergoes an orthogonal shift, solutions to a symmetric linear system are unchanged.

Lemma 17. *Let C and B be Hermitian $N \times N$ matrices with $CB = \mathbf{0}$ and $C + B$ nonsingular. Suppose also that $B\mathbf{b} = \mathbf{0}$. Then, $C(C+B)^{-1}\mathbf{b} = \mathbf{b}$.*

Later on, we will show that $A_G := M_G + 2nK[G]$ is nonsingular under minimum degree assumption for G. Then, applying Lemma 17 with $C = M_G, B = 2nK[G]$ and $\mathbf{b} = \mathbf{1}$, and by Lemma 16, the solution of $A_G\mathbf{x} = \mathbf{1}$ provides the same solution to $M_G\mathbf{x} = \mathbf{1}$, which is sufficient to have a fractional K_3-decomposition.

A short summary of what we have left to show is that A_G is non-singular and $A_G\mathbf{x} = \mathbf{1}$ has an entrywise nonnegative solution $\mathbf{x}$. The next section provides tools to ensure the existence of such an entrywise nonnegative solution.

4.2.2 Obtaining x by upper-bounding Certain Matrix Norms

For $x \in \mathbb{C}^N$ and $A \in \mathbb{C}^{N\times N}$, we consider the special norms defined as

$$\|x\|_\infty = \max\{|x_i| : i = 1, \dots, N\},$$

and

$$\|A\|_\infty = \max_i \sum_j \left|A(i,j)\right|,$$

where the latter is the maximum absolute row sum of A.

The following two results are true for any standard vector/matrix p-norm but we only need them for $p = \infty$.

Lemma 18. *Let $A, B \in \mathbb{C}^{N\times N}$. Then, $\|AB\|_\infty \leq \|A\|_\infty \|B\|_\infty$.*

Lemma 19 (See [27] and [5])**.** *Let $A \in \mathbb{C}^{N\times N}$ be invertible and $\mathbf{x}$ be a non-negative constant vector that satisfies $A\mathbf{x} = \mathbf{b}$. Suppose $A + \delta(A)$ is a perturbation with $\left\|A^{-1}\right\|_\infty \left\|\delta(A)\right\|_\infty \leq \frac{1}{2}$. Then, there exists a unique solution $\mathbf{y}$ to $(A + \delta(A))\mathbf{y} = \mathbf{b}$. Moreover, $\mathbf{y}$ is entrywise nonegative.*

Proof. Denote $B = A + \delta(A)$, then $B = A(I + A^{-1}\delta(A))$. By Lemma 18, $\left\|A^{-1}\delta(A)\right\|_\infty \leq \left\|A^{-1}\right\|_\infty \left\|\delta(A)\right\|_\infty \leq \frac{1}{2}$. So all eigenvalues of $A^{-1}\delta(A)$ have absolute value no greater than $\frac{1}{2}$. In particular, -1 is not an eigenvalue and thus B is nonsingular. The solution $\mathbf{y}$ to $(A + \delta(A))\mathbf{y} = \mathbf{b}$ exists.

Now, we want to show $\mathbf{y}$ is entrywise nonnegative. Let us first bound the norm of B^{-1} which will be used later. Note that

$$A^{-1}\delta(A)B^{-1} = A^{-1}(B - A)B^{-1} = A^{-1} - B^{-1},$$

then

$$B^{-1} = A^{-1} - A^{-1}\delta(A)B^{-1},$$

and thus,

$$\left\|B^{-1}\right\|_\infty \leq \left\|A^{-1}\right\|_\infty + \left\|A^{-1}\delta(A)B^{-1}\right\|_\infty \leq \left\|A^{-1}\right\|_\infty + \left\|A^{-1}\delta(A)\right\|_\infty \left\|B^{-1}\right\|_\infty .$$

From the above, we can obtain

$$\left\|B^{-1}\right\|_\infty \leq \frac{\left\|A^{-1}\right\|_\infty}{1 - \left\|A^{-1}\delta(A)\right\|_\infty}. \tag{4.3}$$

Let $\delta\mathbf{x} = \mathbf{y} - \mathbf{x}$. Since $\mathbf{b} = (A + \delta(A))(\mathbf{x} + \delta(\mathbf{x})) = \mathbf{b} + \delta(A)\mathbf{x} + B\delta(\mathbf{x})$,

$$\delta(\mathbf{x}) = -B^{-1}\delta(A)\mathbf{x}. \tag{4.4}$$

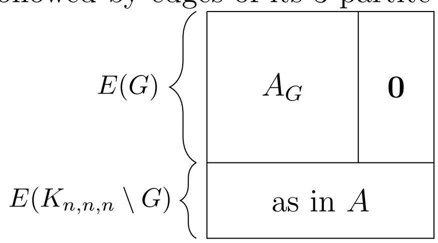
Without loss of generality, we may assume $\mathbf{x} = \mathbf{1}$ and so $\|\mathbf{x}\|_\infty = 1$. Then, by equations (4.3) and (4.4),

$$\left\|\delta(\mathbf{x})\right\|_\infty \leq \left\|B^{-1}\right\|_\infty \left\|\delta(A)\right\|_\infty \|\mathbf{x}\|_\infty \leq \frac{\left\|A^{-1}\right\|_\infty \left\|\delta(A)\right\|_\infty}{1 - \left\|A^{-1}\delta(A)\right\|_\infty} \leq 1$$

as $\left\|A^{-1}\delta(A)\right\|_\infty \leq \left\|A^{-1}\right\|_\infty \left\|\delta(A)\right\|_\infty \leq \frac{1}{2}$. It follows that all entries of $\mathbf{y} = \mathbf{x} + \delta(\mathbf{x})$ are between 0 and 2.

□

Recall that we use the notation $A_G := M_G + 2nK[G]$ to denote the $e(G) \times e(G)$ matrix. Similarly, we define the $n^3 \times n^3$ matrix $A = M + 2nK$. Moreover, we construct the perturbation $A + \delta(A)$ as below by rearranging the edges of A to have edges of G followed by edges of its 3-partite complement:



Suppose we can upper bound $\left\|A^{-1}\right\|_\infty \cdot \left\|\delta(A)\right\|_\infty \leq \frac{1}{2}$. Then by Lemma 19, $(A+\delta(A))\mathbf{x} = \mathbf{1}$ has an entrywise nonnegative solution as $\mathbf{x} = \frac{1}{3n}\mathbf{1}$ is a constant solution to $A\mathbf{x} = \mathbf{1}$. Note that we can restrict the solution of $(A+\delta(A))\mathbf{x} = \mathbf{1}$ to give a solution of $A_G\mathbf{x} = \mathbf{1}$. So we are left to show $\left\|A^{-1}\right\|_\infty \cdot \left\|\delta(A)\right\|_\infty \leq \frac{1}{2}$ to complete our proof.

4.2.3 Upper bounding $\left\|A^{-1}\right\|_\infty \cdot \left\|\delta(A)\right\|_\infty$

The minimum degree condition is used to upper bound $\left\|\delta(A)\right\|_\infty$. By observation, the (e,f)-entry of $A[G] - A_G = M[G] - M_G$ counts the number of triangles in $T(K_{n,n,n})$ which are missing in $T(G)$ and contain both e and f. For a given edge $e \in E(G)$, at most $0.06n$ edges of $K_{n,n,n}$ touching e are missing as $\delta(G) \geq 1.94n$ and every triangle missing from $T(G)$ is counted three times. So $\left\|\delta(A)\right\|_\infty \leq 0.18n$.

Now, we will compute A^{-1} explicitly by investigating the eigenspaces of M, which gives $\left\|A^{-1}\right\|_\infty \leq \frac{2.6}{n} + O(n^{-2})$ and completes our proof.

In $K_{n,n,n}$, there are essentially five different relationships between any two edges. For any fixed edge $\alpha\beta$, the five different representatives are $\alpha\beta, \alpha\beta', \alpha'\beta', \beta\gamma, \beta'\gamma$, and we use $R_0, \ldots, R_4$ to denote such relationships, correspondingly. We use the notation $(\alpha\beta, \alpha'\beta), (\alpha\beta, \alpha\beta') \in R_1$. Note that for any $(e,f) \in R_h$, the number of $g \in E(K_{n,n,n})$ such that $(e,g) \in R_i, (g,f) \in R_j$, a^h_{ij}, only depends on i, j, h. This *structure constant*, a_{ij}^h, together with the identity relation R_0, is called a *symmetric* 4-*class association scheme* on set $E(K_{n,n,n})$. It is very easy to compute all the a_{ij}^h's in this case simply by counting. In particular, the following values are used later:

Lemma 20. $a_{00}^0 = 1, a_{11}^0 = 2(n-1), a_{22}^0 = (n-1)^2, a_{33}^0 = 2n, a_{44}^0 = 2n(n-1)$.

Let A_i be the adjacency matrix indexed by $E(K_{n,n,n})$ to have (e, f)-entry equal to 1 if $(e, f) \in R_i$ and 0 otherwise. Then,

$$\sum_{i=0}^{4} A_I = J,$$

and

$$A_i A_j = \sum_{i=0}^{4} a_{ij}^h A_h.$$

The adjacency matrices span a commutative algebra of symmetric matrices and it is called the *Bose-Mesner algebra* of $E(K_{n,n,n})$. We write $\mathcal{A} = \langle A_0, \ldots, A_4 \rangle$. It follows that $\mathcal{A}$ has a common set of eigenspaces, and thus a basis of orthogonal idempotents.

Now, let us first compute the eigenvalues and eigenvectors of M.

Lemma 21. *The nonzero eigenvalues and their corresponding eigenvectors of M are:*

- $\theta_0 = 3n$, $\mathbf{e}_0 = \mathbf{1}$ *(unique up to multiples);*
- $\theta_1 = 2n$, $\mathbf{e}_1 = \sum_\alpha (\alpha\beta - \alpha\beta') + \sum_\gamma (\beta\gamma - \beta'\gamma)$ *(in total* $3(n-1)$ *independent vectors);*
- $\theta_2 = n$, $\mathbf{e}_2 = \alpha\beta - \alpha\beta' - \alpha'\beta + \alpha'\beta'$ *(in total* $3(n-1)^2$ *independent vectors).*

Proof Sketch. It is easy to verify those are indeed the eigenvectors with respect to their eigenvalues as we can apply them to each edge to see if it agrees.

For example, fix β, β' and consider the second given vector $\mathbf{u}_{\beta,\beta'} = \sum_\alpha(\alpha\beta - \alpha\beta') + \sum_\gamma(\beta\gamma - \beta'\gamma)$. Apply it to each edge and count the number of triangles. It is indeed $M\mathbf{u}_{\beta,\beta'}(\alpha\beta) = 2n$ since it gets n triangles in total for the $\alpha\beta$ entry of $\mathbf{u}_{\beta,\beta'}$ and one triangle each for that of $\beta\gamma$ with n different γ's. Similarly, $M\mathbf{u}_{\beta,\beta'}(\alpha\beta') = -2n$, $M\mathbf{u}_{\beta,\beta'}(\beta\gamma) = 2n$, $M\mathbf{u}_{\beta,\beta'}(\beta'\gamma) = -2n$ and $M\mathbf{u}_{\beta,\beta'}$ vanishes on any other edges as desired.

The number of each type vectors could be obtained by counting and the dimensions add up to the same value of $n^3 - (n-1)^3$ in Lemma 15.

□

Since we know the eigenspaces, we can compute the corresponding idempotents directly. As mentioned, the key thing to notice is that these idempotents live in $\mathcal{A}$, so they are linear combinations of the A_i's.

Lemma 22. *The orthogonal projections onto the eigenspaces of M for eigenvalues $\theta_0, \theta_1, \theta_2$ are, respectively,*

$$E_0 = \frac{1}{3n^2}A_0 + \frac{1}{3n^2}A_1 + \frac{1}{3n^2}A_2 + \frac{1}{3n^2}A_3 + \frac{1}{3n^2}A_4,$$
$$E_1 = \frac{n-1}{n^2}A_0 + \frac{n-2}{2n^2}A_1 - \frac{1}{n^2}A_2 + \frac{n-1}{2n^2}A_3 - \frac{1}{2n^2}A_4,$$
$$E_2 = \frac{(n-1)^2}{n^2}A_0 - \frac{n-1}{n^2}A_1 + \frac{1}{n^2}A_2.$$

Moreover, the orthogonal projection onto the kernel of M is given by $K = I - E_0 - E_1 - E_2$.

The above lemma can be easily verified by directly computating $E_i\mathbf{e}_j = \sigma_{ij}\mathbf{e}_j$, for $i, j = 0, 1, 2$.

Recall that $A = M + 2nK$, then

$$A^{-1} = \theta_0^{-1}E_0 + \theta_1^{-1}E_1 + \theta_2^{-1}E_2 + (2n)^{-1}K.$$

Substitute Lemma 21 and Lemma 22, and suppress some lower terms of n on each coefficient, we get

$$A^{-1} \approx \frac{1}{n}A_0 - \frac{1}{2n^2}A_1 - \frac{4}{9n^3}A_2 - \frac{1}{18n^3}A_4.$$

Apply triangle inequality and by Lemma 20,

$$\left\|A^{-1}\right\|_\infty \leq \frac{1}{n}a_{00}^0 + \frac{1}{2n^2}a_{11}^0 + \frac{4}{9n^2}a_{22}^0 + \frac{1}{18n^3}a_{44}^0 + \text{ lower terms} = \frac{23}{9n} + O(n^{-2}),$$

as desired.

We have completed the entire proof.

CHAPTER 5
Approximate K_3 Decomposition

We showed the existence of a fractional K_3-decomposition for large 3-partite graphs in Chapter 4. Here, we move forward to complete Step 2, which is to show the existence of an approximate decomposition under the same conditions.

Let us start with the necessary definitions, and then the main theorem of this chapter (Theorem 26 below based on [25] and [44]).

Definition 23. *An η-approximate K_3-decomposition of G is a set of edge-disjoint copies of K_3 covering all but at most ηn^2 edges of G.*

Definition 24. *For a graph G, the K_3-packing number, denoted as $\nu(G)$, is the maximum number of pairwise edge-disjoint copies of K_3's in G.*

Definition 25. *A function ψ assigning copies of K_3's in G to $[0,1]$ is a fractional K_3-packing of G if for each edge $e \in E(G)$, $\sum_{H:e\in H} \psi(H) \leq 1$. The fractional K_3-packing number, denoted $\nu^*(G)$, is defined to be the maximum value of $\sum_{H\in\binom{G}{K_3}} \psi(H)$ over all fractional K_3-packing ψ.*

The following theorem was first proved by Haxell and Rödl [25] (for any fixed graph including K_3), and Yuster [44] extended the result to families of graphs. Our proof for the special case is based on [44].

Theorem 26. *Let G be a graph with n vertices, then $\nu^*(G) - \nu(G) = o(n^2)$.*

Theorem 26 reduces the problem of finding an approximate decomposition to that of a fractional one. For any $\eta > 0$, suppose G has a fractional K_3-decomposition. Then, with the notations defined above, $\big|E(G)\big| \leq \nu^*(G) = \sum_i w_i$. Since there exists $\nu(G)$ edge-disjoint copies of K_3's in G and $\big|E(G)\big| - \nu(G) \leq \eta n^2$ for sufficiently large n, G has an η-approximate K_3-decomposition.

5.1 Tools

In this section, we introduce the necessary tools for proving our statement. Let us first start with the definitions and the famous Szemerédi's regularity lemma [40].

Definition 27. *Consider graph $G = (V, E)$. Let X, Y be disjoint subsets of V, and $E(X, Y)$ be the set of edges between them. Then, the density of the edges between X, Y is defined to be*

$$d(X,Y) = \frac{\big|E(X,Y)\big|}{|X||Y|}.$$

Definition 28. *For any $\epsilon > 0$, the vertex set pair (X, Y) is called ϵ-regular, if for all $A \subseteq X, B \subseteq Y$ such that $|A| > \epsilon|X|$,$|B| > \epsilon|Y|$, the following holds*

$$\big|d(X,Y) - d(A,B)\big| < \epsilon.$$

Lemma 29 (Regularity Lemma [40])**.** *For every $\gamma > 0$, there exists $M(\gamma) > 0$ such that the vertex set of any graph G on n vertices can be partitioned into k sets $V_1, \dots, V_k$ for some $1/\gamma < k \leq M(\gamma)$ so that*

- $\Big||V_i| - \big|V_j\big|\Big| \leq 1$, *for all i, j;*
- $|V_i| \leq \lceil \gamma n \rceil$, *for all i;*
- *All but at most $\gamma\binom{k}{2}$ of the pairs (V_i, V_j) are γ-regular.*

The following lemma is a special case of Lemma 2.2 in [44], which is almost identical to Lemma 15 in [25].

Lemma 30 ([44], [25]). *Given positive real numbers δ, ζ, there exists $\gamma = \gamma(\delta,\zeta), T = T(\delta,\zeta)$ such that the following holds: Let W be a 3-partite graph with vertex sets V_1, V_2, V_3 such that $|V_i| = t > T$, and (V_i, V_j) is a γ-regular pair with density $d(V_i, V_j) \geq \delta$, for all $i \neq j$. Then, there exists a spanning subgraph W' of W with at least $(1-\zeta)\big|E(W)\big|$ edges such that the following holds. For any edge $e \in E(W') \cap E(V_i, V_j)$, let $c(e)$ be the number of K_3's in W' that contain e. Then,*

$$\left| c(e) - t\frac{d(V_i,V_k)d(V_j,V_k)}{d(V_i,V_j)} \right| < \zeta t.$$

Again, the following is a special case of Lemma 2.3 in [44], which is a result of Frankl and Rödl [18] on near perfect coverings and matchings of uniform hypergraphs. In a hypergraph, the degree of a vertex is the number of edges that contain this vertex and the co-degree of two vertices is the number of edges that contain both of those vertices.

Lemma 31 ([44], [18]). *Given a real $\beta > 0$, there exists a real $\mu > 0$ such that: if the 3-uniform hypergraph L on q vertices has the following properties for some d:*

- $(1-\mu)d < \deg(v) < (1+\mu)d$ *for all vertices v;*
- $\deg(v,u) < \mu d$ *for all distinct vertices v, u,*

then L has a matching of size at least $\frac{q}{3}(1-\beta)$.

5.2 Proof of Theorem 26

Let $\epsilon > 0$ and we will show that there exists $N = N(\epsilon)$ such that for all $n > N$, if G is a graph on n vertices, then $\nu^*(G) - \nu(G) < \epsilon n^2$.

Take $\delta = \beta = \epsilon/4, \mu = \mu(\beta, 3)$ as in Lemma 31, $\zeta = \mu\delta^3/2, \gamma = \gamma(\delta,\zeta), T = T(\delta,\zeta)$ as in Lemma 30 and $M = M(\frac{\gamma\epsilon}{30})$ as in Lemma 29. We will define N to be sufficiently large and it will depend on all above parameters.

It will be clear as the proof proceeds that it indeed satisfies all the conditions and $N = N(\epsilon)$.

Let G be an n-vertex graph, where $n > N = N(\epsilon)$. Fix a fractional K_3-packing ψ such that $w(\psi) = \nu^*(G)$. We may assume $w(\psi) = \alpha n^2 \geq \epsilon n^2$, otherwise $\nu^*(G) < \epsilon n^2$ and we are done.

Take $\gamma' = \frac{\gamma\epsilon}{30}$. Apply Lemma 29 to G to obtain a γ'-regular partition with m' parts, where $1/\gamma' < m' < M(\gamma')$, and denote the partite sets as $U_1, U_2, \ldots, U_{m'}$. We may assume n/m', and later $n/(30m'/\epsilon)$, are integers as it does not change the asymptotic nature of our result. We randomly partition each U_i into $30/\epsilon$ equal parts, and have $m = 30m'/\epsilon$ refined partite sets in total. We denote them as $V_1, V_2, \ldots, V_m$ and each V_i has size of $n/(30m'/\epsilon)$.

We claim that for $V_i \subset U_s, V_j \subset U_t$ with $s \neq t$, if (U_s, U_t) is a γ'-regular pair, then (V_i, V_j) is a γ-regular pair. Consider $X \subset V_i, Y \subset V_j$ with $|X|, |Y| > \gamma n/m$, then $|X|, |Y| > \gamma n/(30m'/\epsilon) = \gamma' n/m'$ and thus $\left|d(X,Y) - d(U_s, U_t)\right| < \gamma'$. Since $\left|d(V_i, V_j) - d(U_s, U_t)\right| < \gamma'$, $\left|d(X,Y) - d(V_i, V_j)\right| < 2\gamma' < \gamma$ as desired.

Let H be a copy of K_3 in G and we call H good if all its 3 vertices belong to distinct partite sets of the refined partition. Then, the probability of H having two vertices in the same partite set is at most $\binom{3}{2}\epsilon/30 = \epsilon/10$. Now, let ψ^{**} be the restriction of ψ to the good copies with all bad copies H' being assigned $\psi^{**}(H') = 0$. Then, the expectation of $w(\psi^{**})$ is at least $(\alpha - \epsilon/10)n^2$ and thus, we fix a partition $V_1, \ldots, V_m$ for which $w(\psi^{**}) \geq (\alpha - 0.1\epsilon)n^2$ by ignoring the bad H's.

Now, let G^* be the spanning subgraph of G with only edges having endpoints in distinct vertex classes of the refined partition that form a γ-regular pair with density at least δ, and ψ^* be the restriction of ψ^{**} to copies of K_3's in G^*. It is sufficient for our calculations to count the number of discarded edges in the original partite sets U_i's. We lose at most $m'\binom{n/m'}{2}$ edges inside the partite sets, at most $\gamma'\binom{m'}{2}\frac{n^2}{m'^2}$ edges between non-regular pairs and at most $\binom{m'}{2}(\delta+\gamma')\frac{n^2}{m'^2}$ edges between sparse pairs. For n large enough,

$$\begin{aligned} w(\psi^{**}) - w(\psi^*) &\leq \big|E(G) - E(G^*)\big| \\ &< m'\binom{n/m'}{2} + \gamma'\binom{m'}{2}\frac{n^2}{m'^2} + \binom{m'}{2}(\delta+\gamma')\frac{n^2}{m'^2} \\ &< n^2\Big(\frac{1}{2m'} + \frac{\gamma'}{2} + \frac{\delta+\gamma'}{2}\Big) \\ &< 0.6\delta n^2 \quad \text{ since } 1/m' < \gamma' << \delta. \end{aligned}$$

Thus,

$$\nu^*(G^*) \geq w(\psi^*) > w(\psi^{**}) - 0.6\delta n^2 \geq (\alpha - 0.1\epsilon - 0.6\delta)n^2 = (\alpha-\delta)n^2.$$

Let R be the m-vertex graph with $V(R) = \{1, 2, \ldots, m\}$ and $(i,j) \in E(R)$ if and only if (V_i, V_j) is a γ-regular pair with density at least δ. We define a fractional K_3-packing ψ' on R in the following way: Let H be a copy of K_3 in R with vertices i, j, k, then we define $\psi'(H)$ to be the sum of the values of ψ^* taken over all K_3 subgraphs of $G^*[V_i, V_j, V_k]$ divided by n^2/m^2. By normalizing with n^2/m^2, ψ' is guaranteed to be a proper fractional K_3-packing of R and $\nu^*(R) \geq w(\psi') = w(\psi^*)m^2/n^2 \geq (\alpha-\delta)m^2$.

We use ψ' to "colour" edges of G^* with copies of K_3 in R in the following way: Let H be a copy of K_3 in R which contains the edge (i,j), then for each edge $e \in E(V_i, V_j)$, it chooses the "colour" H with probability $\psi'(H)/d(V_i, V_j)$. Note that such a random colouring is legal as the sum of $\psi'(H)$ taken over all copies of K_3 in R containing (i,j) is at most $d(V_i, V_j) \leq 1$, and some edges might not be coloured.

Let H be a copy of K_3 in R with vertices i, j, k and assume $\psi'(H) > 1/m^2$ (we will deal with the easy case for small values of $\psi'(H)$ later). Let

$W_H = G^*[V_i, V_j, V_k]$, then W_H is a subgraph of G^* which satisfies the conditions in Lemma 30 as we can make $N > 30MT/\epsilon$ to guarantee $t = n/m > N\epsilon/(30M) > T$. Let W'_H be the spanning subgraph of W_H which is obtained by Lemma 30 and X_H be the spanning subgraph of W'_H consisting only edges of W'_H with colour H. For an edge $e \in E(X_H)$, let $c_H(e)$ be the number of K_3's in X_H which contain edge e. We will bound the values of $c_H(e)$ and $\big|E(X_H)\big|$ with the following two crucial lemmas, and their proofs are followed respectively.

Lemma 32. *With probability at least* $1 - m^3/n$*, for all* $e \in E(X_H)$*,*

$$\left|c_H(e) - t\psi'(H)^2\right| < \mu t\psi'(H)^2.$$

Proof. Fix an edge $e \in E(X_H)$ belonging to $E(V_i, V_j)$, the probability of a copy of K_3 containing e in W'_H also belongs to that of X_H is

$$\rho = \psi'(H)^2 \frac{d(V_i, V_j)}{d(V_i, V_k)d(V_j, V_k)}. \tag{5.1}$$

Let $c(e)$ denote the number of K_3's in W'_H that contain edge e. Then, the expectation of $c_H(e)$ is $\rho c(e)$. If n is sufficiently large, hence t and $c(e) = \Theta(t)$ are also large enough. By Chernoff, for every $\eta > 0$, in particular $\eta = \mu/4$,

$$\Pr\left[\left|c_H(e) - \rho c(e)\right| > \eta\rho c(e)\right] < e^{-\frac{2(\eta\rho c(e))^2}{c(e)}} = e^{-2\eta^2\rho^2 c(e)} << t^{-3}.$$

So with probability at least $1 - t^{-3}$, $(1-\eta)\rho c(e) \le c_H(e) \le (1+\eta)\rho c(e)$. Then,

$$\begin{aligned} c_H(e) = \rho c(e) &\le \rho(1+\eta)c(e) \\ &< \rho(1+\eta)t(\zeta + \frac{d(V_i,V_k)d(V_j,V_k)}{d(V_i,V_j)}) \quad \text{by Lemma 30} \\ &= (1+\eta)t(\zeta\rho + \psi'(H)^2) \quad \text{by (5.1)} \\ &\le t\psi'(H)^2(1+\eta)(1+\zeta\delta^{-3}) \quad \text{since } \rho < \psi'(H)^2\delta^{-3} \\ &= t\psi'(H)^2(1+\mu/4)(1+\mu/2) \quad \text{since } \zeta = \mu\delta^3/2 \\ &\le t\psi'(H)^2(1+\mu). \end{aligned}$$

Similarly,

$$c_H(e) \le t\psi'(H)^2(1-\mu).$$

Thus, for a fixed edge $e \in E(X_H)$, the inequality in our lemma holds with probability at least $1 - t^{-3}$. Since $|E(X_H)| < n^2$, it holds for all edges with probability at least $1 - n^2/t^3 = 1 - m^3/n$ as required.

□

Lemma 33. *With probability at least* $1 - 1/n$,

$$|E(X_H)| > 3(1-2\zeta)\frac{n^2}{m^2}\psi'(H).$$

Proof. We use the same notations from Lemma 32. For one edge $(i,j) \in E(H)$, the expected number of edges of $E(V_i,V_j)$ was coloured with H is $d(V_i,V_j)\frac{n^2}{m^2}\frac{\psi'(H)}{d(V_i,V_j)} = \frac{n^2}{m^2}\psi'(H)$, and there are 3 edges in H. By Lemma 30, there are at most $\zeta|E(W_H)|$ edges belong in $W_H - W'_H$. So the expectation of $|E(X_H)|$ is at least $3(1-\zeta)\frac{n^2}{m^2}\psi'(H)$. Since $\psi'(H) > m^{-2}$ and ζ, m are constants, by Chernoff, for n sufficiently large, the probability of $|E(X_H)|$ deviates from its mean by more than $3\zeta\frac{n^2}{m^2}\psi'(H)$ is exponentially small in n. Hence, the lemma is true. □

Since there are at most $O(m^3)$ copies of K_3 in R, with probability at least $1 - m^3/n - m^6/n > 0$ (for N large enough), all copies H of K_3 in R with $\psi'(H) > m^{-2}$ satisfy both Lemma 32 and Lemma 33. We fix such a coloring.

Again, let H be a copy of K_3 in R with $\psi'(H) > m^{-2}$. We construct a 3-uniform hypergraph L_H such that the vertices are the edges of the corresponding X_H and edges of L_H are the edge sets in X_H that form K_3. We claim that L_H satisfies all conditions in Lemma 31. Take $d = t\psi'(H)^2$. By Lemma 32 and our choice of colouring, all vertices of L_H have their degrees between $(1-\mu)d$ and $(1+\mu)d$. Also, the codegree of any two vertices of L_H is at most 1 as any edges belong to at most one K_3. So for sufficiently large N and hence t large enough, $\mu d > 1$. By Lemma 31, we have at least $(q/3)(1-\beta)$ edge-disjoint copies of K_3 in X_H, where $q = \left|V(L_H)\right| = \left|E(X_H)\right| > 3(1-2\zeta)\frac{n^2}{m^2}\psi'(H)$ by Lemma 33 and our choice of colouring. Recall that $\delta = \beta = \epsilon/4, \zeta = \mu\delta^3/2$, we obtain at least

$$(1-\beta)(1-2\zeta)\frac{n^2}{m^2}\psi'(H) > (1-2\beta)\psi'(H)\frac{n^2}{m^2}$$

edge-disjoint K_3 copies H with $\psi'(H) > m^{-2}$.

Since there are at most $O(m^3)$ copies of K_3 in R with $0 < \psi'(H) \leq m^{-2}$, their total contribution to $w(\psi')$ is at most $O(m)$.

Recall that $w(\psi') \geq (\alpha - \delta)m^2$. Then, summing over all H with $\psi'(H) > m^{-2}$, we obtain at least

$$(1-2\beta)\frac{n^2}{m^2}\big(m^2(\alpha-\delta) - O(m)\big) = (1-2\beta)\frac{n^2}{m^2}m^2\big(\alpha - \delta - O(\frac{1}{m})\big) > n^2(\alpha - \epsilon)$$

disjoint copies of K_3 in G. Hence, $\nu(G) > n^2(\alpha - \epsilon)$. Since $\nu^*(G) = \alpha n^2$, we obtain $\nu^*(G) - \nu(G) < \epsilon n^2$ as desired.

CHAPTER 6
Concluding Remarks

In Theorem 2 we proved that the size of the smallest critical set for Latin squares of order n is of quadratic order, however Conjecture 1 still remains unsolved.

A conjecture of Daykin and Häggkvist [13] (see [3, Conjecture 1.3]) suggests that Theorem 5 holds under the weaker condition that the minimum degree of G is at least $3n/2$. If this is true, the proof of Theorem 2 provides a better lower-bound of $2^{-7}n^2$ on the size of the smallest critical set. However, this is still far from the conjectured bound of $\lfloor n^2/4 \rfloor$.

In Theorems 8 and 9 we established a lower-bound of $n^2 - (e + o(1))n^{5/3}$ for both VC-dimension and the recursive teaching dimension of the set of Latin squares of order n. One can easily obtain an upper-bound of the form $n^2 - \Omega(n)$ for the VC-dimension, but obtaining a stronger upper-bound, and more ambitiously, determining the exact asymptotics of the VC-dimension seems highly nontrivial. For the teaching dimension and consequently recursive teaching dimension, a stronger upper-bound of $n^2 - \frac{\sqrt{\pi}}{2}n^{3/2}$ follows from the results of [20]. Hence for sufficiently large n,

$$n^2 - (e + o(1))n^{5/3} \leq \mathrm{RTD}(\mathcal{L}_n) \leq \mathrm{TD}(\mathcal{L}_n) \leq n^2 - \frac{\sqrt{\pi}}{2}n^{3/2}.$$

It would be interesting to improve either of the constants 5/3 and 3/2 appearing in the power of n in the above bounds.

REFERENCES

[1] Martin Anthony, Graham Brightwell, Dave Cohen, and John Shawe-Taylor. On exact specification by examples. *Proceedings of the 5th Workshop on Computational Learning Theory*, pages 311–318, 1992.

[2] Ben Barber, Daniela Kühn, Allan Lo, and Deryk Osthus. Edge-decompositions of graphs with high minimum degree. *Adv. Math.*, 288:337–385, 2016.

[3] Ben Barber, Daniela Kühn, Allan Lo, Deryk Osthus, and Amelia Taylor. Clique decompositions of multipartite graphs and completion of Latin squares. *J. Combin. Theory Ser. A*, 151:146–201, 2017.

[4] John A. Bate and G. H. John van Rees. The size of the smallest strong critical set in a Latin square. *Ars Combin.*, 53:73–83, 1999.

[5] Flora C. Bowditch and Peter J. Dukes. Fractional triangle decompositions of dense 3-partite graphs. *arXiv preprint arXiv:1510.08998v2*, 2016.

[6] Lev M. Bregman. Some properties of nonnegative matrices and their permanents. *Soviet Math. Dokl.*, pages 945–949, 1973.

[7] Nicholas Cavenagh and Reshma Ramadurai. On the distances between Latin squares and the smallest defining set size. *J. Combin. Des.*, 25(4):147–158, 2017.

[8] Nicholas J. Cavenagh. A superlinear lower bound for the size of a critical set in a Latin square. *J. Combin. Des.*, 15(4):269–282, 2007.

[9] Nicholas J. Cavenagh. The theory and application of Latin bitrades: a survey. *Math. Slovaca*, 58(6):691–718, 2008.

[10] Xi Chen, Yu Cheng, and Bo Tang. A note on teaching for VC classes. *Electronic Colloquium on Computational Complexity, Report No.65*, 2016.

[11] Joan Cooper, Diane Donovan, and Jennifer Seberry. Latin squares and critical sets of minimal size. *Australas. J. Combin.*, 4:113–120, 1991. Combinatorial mathematics and combinatorial computing (Palmerston North, 1990).

[12] Donald J. Curran and G. H. John Van Rees. Critical sets in Latin squares. In *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing (Univ. Manitoba, Winnipeg, Man., 1978)*,

Congress. Numer., XXII, pages 165–168. Utilitas Math., Winnipeg, Man., 1979.

[13] David E. Daykin and Roland Häggkvist. Completion of sparse partial Latin squares. In *Graph theory and combinatorics (Cambridge, 1983)*, pages 127–132. Academic Press, London, 1984.

[14] Diane Donovan, Ebadollah S. Mahmoodian, Colin Ramsay, and Anne Penfold Street. Defining sets in combinatorics: a survey. In *Surveys in combinatorics, 2003 (Bangor)*, volume 307 of *London Math. Soc. Lecture Note Ser.*, pages 115–174. Cambridge Univ. Press, Cambridge, 2003.

[15] François Dross. Fractional triangle decompositions in graphs with large minimum degree. *SIAM J. Discrete Math.*, 30(1):36–42, 2016.

[16] Georgy P. Egorychev. Proof of the van der Waerden conjecture for permanents. *Sibirsk. Mat. Zh.*, 22(6):65–71, 225, 1981.

[17] Dmitry I. Falikman. Proof of the van der Waerden conjecture on the permanent of a doubly stochastic matrix. *Mat. Zametki*, 29(6):931–938, 957, 1981.

[18] P. Frankl and V. Rödl. Near perfect coverings in graphs and hypergraphs. *European J. Combin.*, 6(4):317–326, 1985.

[19] Chin-Mei Fu, Hung-Lin Fu, and C. A. Rodger. The minimum size of critical sets in Latin squares. *J. Statist. Plann. Inference*, 62(2):333–337, 1997.

[20] Mahya Ghandehari, Hamed Hatami, and Ebadollah S. Mahmoodian. On the size of the minimum critical set of a Latin square. *Discrete Math.*, 293(1-3):121–127, 2005.

[21] Sally A. Goldman and Michael J. Kearns. On the complexity of teaching. *J. Comput. System Sci.*, 50(1):20–31, 1995.

[22] Béla Gyires. The common source of several inequalities concerning doubly stochastic matrices. *Publ. Math. Debrecen*, 27(3-4):291–304, 1980.

[23] Frank Harary. Three new directions in graph theory. In *Proceedings of the First Estonian Conference on Graphs and Applications (Tartu-Kääriku, 1991)*, pages 15–19. Tartu Univ., Tartu, 1993.

[24] Hamed Hatami and Yingjie Qian. Teaching dimension, VC dimension, and critical sets in Latin squares. *J. Comb.*, 9(1):9–20, 2018.

[25] P. E. Haxell and V. Rödl. Integer and fractional packings in dense graphs. *Combinatorica*, 21(1):13–38, 2001.

[26] Peter Horak, Robert E. L. Aldred, and Herbert J. Fleischner. Completing Latin squares: critical sets. *J. Combin. Des.*, 10(6):419–432, 2002.

[27] Roger A. Horn and Charles R. Johnson. Matrix analysis, 2nd ed. *Cambridge University Press, Cambridge*, 2013.

[28] Lunjia Hu, Ruihan Wu, Tianhong Li, and Liwei Wang. Quadratic upper bound for recursive teaching dimension of finite vc classes. In *Proceedings of Machine Learning Research*, volume 65, pages 1–10, 2017.

[29] Anthony D. Keedwell. Critical sets for Latin squares, graphs and block designs: a survey. *Congr. Numer.*, 113:231–245, 1996. Festschrift for C. St. J. A. Nash-Williams.

[30] Anthony D. Keedwell. Critical sets in Latin squares: An intriguing problem. 85(503):239–244, 2001.

[31] Eyal Kushilevitz, Nathan Linial, Yuri Rabinovich, and Michael Saks. Witness sets for families of binary vectors. *J. Combin. Theory Ser. A*, 73(2):376–380, 1996.

[32] Ebadollah S. Mahmoodian. Some problems in graph colorings. In *Proceedings of the 26th Annual Iranian Mathematics Conference, Vol. 2 (Kerman, 1995)*, pages 215–218. Shahid Bahonar Univ. Kerman, Kerman, 1995.

[33] Richard Montgomery. Fractional clique decompositions of dense partite graphs. *Combin. Probab. Comput.*, 26(6):911–943, 2017.

[34] Balas K. Natarajan. *Machine Learning: A Theoretical Approach.* Morgan Kaufmann, 1991.

[35] John Nelder. Critical sets in Latin squares. *CSIRO Division of Math. and Stats Newsletter 38*, 1977.

[36] Alain Pajor. *Sous-espaces l_1^n des espaces de Banach*, volume 16 of *Travaux en Cours [Works in Progress]*. Hermann, Paris, 1985. With an introduction by Gilles Pisier.

[37] Norbert Sauer. On the density of families of sets. *J. Combinatorial Theory Ser. A*, 13:145–147, 1972.

[38] Saharon Shelah. A combinatorial problem; stability and order for models and theories in infinitary languages. *Pacific J. Math.*, 41:247–261, 1972.

[39] Ayumi Shinohara and Satoru Miyano. Teachability in computational learning. *New Gen. Comput.*, 8(4):337–347, 1991.

[40] Endre Szemerédi. Regular partitions of graphs. In *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, volume 260 of *Colloq. Internat. CNRS*, pages 399–401. CNRS, Paris, 1978.

[41] Jacobus H. van Lint and Richard M. Wilson. *A course in combinatorics.* Cambridge University Press, Cambridge, 1992.

[42] V. N. Vapnik and A. Ja. Cervonenkis. The uniform convergence of frequencies of the appearance of events to their probabilities. *Teor. Verojatnost. i Primenen.*, 16:264–279, 1971.

[43] Walter D. Wallis and John C. George. *Introduction to combinatorics.* Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, second edition, 2017.

[44] Raphael Yuster. Integer and fractional packing of families of graphs. *Random Structures Algorithms*, 26(1-2):110–118, 2005.