Fourier Analysis in Additive Problems

Dissertation submitted to
The Hungarian Academy of Sciences
for the degree "Doctor of the HAS"

Máté Matolcsi

Alfréd Rényi Institute of Mathematics
Budapest

2014

dc_823_13

Contents

dc_823_13

1 Introduction

This dissertation focuses on my research results of additive nature, most of them using Fourier analysis in the proofs. This has been the central theme of my research activity in the past 10 years. The dissertation is based on the results of the papers [4, 40, 52, 53, 72, 74, 91, 92, 94–97], which are put into context by recalling the relevant preceding results and follow-ups from the literature.

Fourier analysis is a standard tool in additive combinatorics and additive number theory. Problems in these branches of mathematics typically concern the structure or size (cardinality or measure) of a subset A of a locally compact Abelian group $\mathcal{G}$, given some additive properties of A. The most famous example, where Fourier analysis is the central tool, is the estimation of the maximal cardinality of a set $A \subset [1, N]$, such that A does not contain a 3-term arithmetic progression (cf. [120] and references therein for the latest developments). Another example of similar flavour is the estimation of the maximal cardinality of a set A in a cyclic group $\mathbb{Z}_p$ such that $A - A$ does not contain quadratic residues. This latter problem, among many-many others, will be considered in this work in detail.

The dissertation is organized as follows. After the Introduction the results are presented in three chapters according to thematic concepts. Chapter 2 is devoted to results concerning translational tilings of locally compact Abelian groups. Chapter 3 describes a very general scheme, the Fourier analytic version of Delsarte's method, which is then applied to several problems from different parts of mathematics. Finally, Chapter 4 contains some interesting bounds on the cardinality of k-fold sumsets. I will now briefly highlight the most important results of each chapter below.

Chapter 2 contains selected results about translational tiles in Abelian groups. A subset A of a locally compact Abelian group $\mathcal{G}$ is called a translational tile (or simply tile) if one can cover $\mathcal{G}$ by the union of some disjoint translates of A. In this work we are only able to describe a small and biased fraction of the vast literature available on translational tiling.

In Section 2.1 we will review some well-known theorems and notoriously difficult open problems about translational tiles. We will restrict our attention to results needed in later sections and some of the most interesting results directly related to those. In this preliminary section my own contributions are only Example 2.1.11 and 2.1.13 which answer questions of M. N. Kolountzakis and M. Szegedy, respectively.

The main results of Chapter 2 are contained in Section 2.2, where we investigate Fuglede's Conjecture 2.2.2. This conjecture stated that a bounded measurable set Ω is a translational tile in $\mathbb{R}^d$ if and only if it is *spectral* (a notion to be defined rigorously later). The conjecture has also been investigated in finite Abelian groups and $\mathbb{Z}^d$. In Section 2.2.1 we prove several positive results which tentatively support the validity of the conjecture (at least in special cases). We prove a general transition scheme from $\mathbb{Z}^d$ to $\mathbb{R}^d$ in Proposition 2.2.9, and from finite groups to $\mathbb{Z}^d$ in Proposition 2.2.12. These results are summarized in Corollary 2.2.13 which states that a counterexample in any finite group can automatically be transferred to $\mathbb{Z}^d$ and $\mathbb{R}^d$. In finite groups

we prove that the natural tiling construction of Proposition 2.2.16 works analogously for spectral sets in Proposition 2.2.17. Also, in Propositions 2.2.18 and 2.2.20 we prove the 'spectral $\to$ tile' direction of the conjecture for sets of small cardinality in finite groups or $\mathbb{Z}^d$. Then, in Section 2.2.2 we turn to the main results of the section: counterexamples. Based on an example by T. Tao [132] and some observations of the author [73, 91] we will construct a set in $\mathbb{R}^3$ which is spectral but does not tile, in Theorem 2.2.21. For the converse direction, in Theorem 2.2.23 [40] we will make a precise connection between the Universal Spectrum Conjecture of Lagarias and Wang [82] and the 'tile $\to$ spectral' direction Fuglede's conjecture. Then we will exhibit a non-spectral tile in $\mathbb{R}^3$ in Theorem 2.2.27.

In Section 2.3 we will use the existing connections between tiles and spectral sets to produce new families of complex Hadamard matrices. Namely, some natural tiling constructions work analogously for spectral sets, and such sets correspond directly to complex Hadamard matrices. In this manner, some peculiar tiling constructions of Szabó [126] lead to new families of complex Hadamard matrices, one of which is described in detail in Example 2.3.2. In Proposition 2.3.5 we prove that the arising family is indeed new (i.e. it has not been considered in the literature).

In Chapter 3 we describe a Fourier analytic version of Delsarte's method. The linear programming bound of Delsarte was first applied in [34] in coding theory to the following problem: determine the maximal cardinality $A(n, d)$ of binary codewords of length n such that each two of them differ in at least d coordinates. The original version of the method, as described by Delsarte, was not phrased in Fourier analytic language. Here we will concentrate on a version which is general enough to encompass most of the applications but simple enough to require only elementary Fourier analysis.

Let $\mathcal{G}$ be a compact Abelian group, and let a symmetric subset $A = -A \subset \mathcal{G}$, $0 \in A$ be given. We will call A the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \dots b_m\} \subset \mathcal{G}$ such that all differences $b_j - b_k \in A^c \cup \{0\}$ (in other words, all differences avoid the forbidden set A). In Section 3.1 we will describe the Fourier analytic version of Delsarte's bound. The maximal cardinality of the set B will be bounded above by constructing certain positive exponential sums using frequencies from the forbidden set A. After introducing the necessary notations Delsarte's linear programming bound will be given as $\delta(A) \leq \lambda^-(A)$ in Theorem 3.1.4. We will then study the general properties of the method. In particular, we prove several propositions describing the behaviour of the δ and λ quantities under the set theoretical operations of union, intersection and direct product. Maybe the most important general property is the duality relation given in Theorem 3.1.13. We then study the limitations of the method by considering the λ and δ quantities for random sets in Theorems 3.1.28 and 3.1.29. Finally, the important consequence of Theorems 3.1.35 and 3.1.36 is that allowing only nonnegative coefficients in the character sums can lead to drastically worsened estimates in the Delsarte bound.

In Section 3.2 we will apply Delsarte's method to give an improved upper bound on the independence number s of the Paley-graph $\mathcal{P}_p$, for a prime $p \equiv 1 \pmod 4$. In fact, the Delsarte bound, in itself, gives the trivial bound $s \leq \sqrt{p}$, only. However,

a 'subgraph-trick', introduced in [106] in connection with the unit-distance graph of $\mathbb{R}^d$, will come to our help to achieve a slightly improved upper bound in Theorem 3.2.2.

Section 3.3 gives a surprising application of Delsarte's method to the problem of mutually unbiased bases (MUBs). It is known that the existence of a complete system of MUBs is equivalent to the existence of certain complex matrices (MUHs). In this section we will view complex Hadamard matrices as finite sets in the compact group $\mathbb{T}^d$, and apply Delsarte's method in this group. In Theorem 3.3.6 we will obtain a generalization of the fact that the maximal number of MUBs in dimension d cannot exceed $d+1$. We also discuss the question whether a real Hadamard matrix can be part of a complete system of MUHs. While it is known to be possible for $d = 2^k$, we show that the presence of a real Hadamard matrix puts heavy constraints on the columns of the other matrices. In particular, Theorem 3.3.12 implies that it is impossible to have two real Hadamards in a complete system of MUHs. We will also prove in Theorem 3.3.15 that in dimension 6 the matrices of the Fourier family $F_(a, b)$ cannot be extended to a complete system of MUBs.

In Section 3.4 we give a brief outlook on possible future applications of Delsarte's method in the following problems. What is the maximal density of a set of integers $B \subset [1, \dots, N]$ such that $B - B$ does not contain squares (or, in general, kth powers for some fixed k)? What is the maximal upper density of a measurable set $B \subset \mathbb{R}^d$ such that $B - B$ does not contain vectors of unit length? Maybe the most surprising possible application is given in Section 3.4.3: Littlewood's conjecture on simultaneous approximation. Finally in Theorem 3.4.1 we give a possible improvement of the Delsarte bound, under the assumption that some further information on the subset $B \subset \mathcal{G}$ is available.

In Chapter 4 we describe some selected results concerning the cardinality of sumsets. The structure and cardinality of sumsets are central objects of study in additive combinatorics. In this chapter the methods are purely combinatorial and do not use Fourier analysis, and therefore I will keep this chapter shorter.

In Section 4.1 we consider finite sets of integers $A_1, \dots, A_k$ and study the cardinality of the k-fold sumset $A_1 + \dots + A_k$ compared to those of $(k-1)$-fold sumsets $A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_k$. We prove interesting superadditivity and submultiplicativity properties for these quantities in Theorems 4.1.1 and 4.1.2. A possible generalization of the submultiplicativity property is then obtained in Theorem 4.1.6.

In Section 4.2, Theorem 4.2.3 extends Freiman's inequality on the cardinality of the sumset of a proper d dimensional set A. We also consider the case of different sets A, B related by an inclusion of their convex hull, and one of them added possibly several times, in Theorem 4.2.5.

Convention. All the theorems and propositions in this work are referenced. In order to make it easier for the reader to distinguish my own results from those of others, I will use the following convention throughout this work: references to my papers will be marked with an asterisk, e.g. [72]*. For the sake of readability, I will use this convention only for marking the theorems and propositions and not in the textflow.

2 Translational tiling

This chapter focuses on some selected results about translational tiles in Abelian groups. A subset A of a locally compact Abelian group $\mathcal{G}$ is called a *translational tile* if one can cover $\mathcal{G}$ by the union of some disjoint translates of A (this somewhat intuitive definition will be made more rigorous later). We emphasize that in this work we are only able to describe a small and biased fraction of the vast literature available on translational tiling.

In Section 2.1 we will review some well-known theorems and notoriously difficult open problems about translational tiles. We will restrict our attention to results needed in later sections and some of the most interesting results directly related to these.

In Section 2.2 we will be concerned Fuglede's conjecture, which stated that a bounded measurable set Ω is a translational tile in $\mathbb{R}^d$ if and only if it is *spectral* (a notion to be defined later). The conjecture has also been investigated in finite groups and $\mathbb{Z}^d$. We will first show some special classes of sets for which the conjecture holds true in Theorem 2.2.3, 2.2.5 and Proposition 2.2.18, as well as proving several common properties of spectral sets and tiles. We will also prove a general transition scheme from finite groups to $\mathbb{Z}^d$ and $\mathbb{R}^d$ in Corollary 2.2.13. Then, based on an example by T. Tao [132] and some observations of the author [73,91] we will construct a set in $\mathbb{R}^3$ which is spectral but does not tile, in Theorem 2.2.21. For the converse direction, in Theorem 2.2.23 [40] we will make a precise connection between the Universal Spectrum Conjecture of Lagarias and Wang [82] and the 'tile $\rightarrow$ spectral' direction Fuglede's conjecture. Then we will exhibit a non-spectral tile in $\mathbb{R}^3$ in Theorem 2.2.27. This section is based on the papers [40, 72, 73, 91]

In Section 2.3 we will use the existing connections between tiles and spectral sets to produce new families of complex Hadamard matrices. Namely, some natural tiling constructions work analogously for spectral sets, and such sets correspond directly to complex Hadamard matrices. In this manner, some peculiar tiling constructions of Szabó [126] lead to new families of complex Hadamard matrices, one of which is described in detail in Example 2.3.2. This section is based on the paper [94].

2.1 Preliminary results on tiling

This introductory section reviews several well-known results concerning translational tiling.

2.1.1 Combinatorial and Fourier analytic conditions

In full generality, tiling can be discussed in any locally compact Abelian group, but throughout this work we will restrict our attention to the following standard cases: finite groups, $\mathbb{Z}^d$, and $\mathbb{R}^d$. Also, we will make the discussion technically easier by considering only bounded, open sets T as tiles (rather than allowing any measurable sets). In notation, the indicator function of the set T will be denoted by χ_T.

Definition 2.1.1. *Let $\mathcal{G}$ be a locally compact Abelian group of the following type: finite group, $\mathbb{Z}^d$, or $\mathbb{R}^d$. Let $T \subset \mathcal{G}$ be a bounded open set, and $\Lambda \subset \mathcal{G}$ be a discrete set. We say that T tiles $\mathcal{G}$ with translation set Λ if $\sum_{\lambda\in\Lambda} \chi_T(x-\lambda) = 1$ for almost all $x \in \mathcal{G}$. More generally, if Λ is a multiset (i.e. any element $\lambda \in \Lambda$ can appear with multiplicity more than one), and $0 \leq f \in L^1(\mathcal{G})$ is a nonnegative integrable function then we say that f tiles $\mathcal{G}$ with Λ at level s if $\sum_{\lambda\in\Lambda} f(x-\lambda) = s$ for almost all $x \in \mathcal{G}$. In notation we write $T + \Lambda = \mathcal{G}$ and $f + \Lambda = s\mathcal{G}$, respectively.*

The set Λ is also said to be a *tiling complement* of T. The assumption of T being open ensures that the translated copies $\lambda + T$ are pairwise disjoint, and the non-covered points of $\mathcal{G}$ have measure zero (the measure is always meant to be the appropriately normalized Haar measure on $\mathcal{G}$, i.e. the counting measure if $\mathcal{G}$ is discrete, and the Lebesgue measure if $\mathcal{G} = \mathbb{R}^d$).

The group of multiplicative characters of $\mathcal{G}$ will be denoted by $\hat{\mathcal{G}}$. In this chapter we will use the additive notation for both $\mathcal{G}$ and $\hat{\mathcal{G}}$. That is, for $\gamma_1, \gamma_2 \in \hat{\mathcal{G}}$ we define $(\gamma_1 + \gamma_2)(x) = \gamma_1(x)\gamma_2(x)$. This is motivated by the fact that in Section 2.2 we want to treat tiles and spectral sets in an analogous manner.

We use the following definition for the Fourier transform of a function $f : \mathcal{G} \to \mathbb{C}$:

$$\hat{f}(\gamma) = \int_{x\in\mathcal{G}} f(x)\gamma(x)dx, \quad \gamma \in \hat{\mathcal{G}}. \tag{2.1}$$

For a good textbook on Fourier analysis on locally compact Abelian groups we refer to [113].

Tiling implies some trivial but important combinatorial and Fourier analytic restrictions on T and Λ.

Lemma 2.1.2. *Let $\mathcal{G}$ be finite. The following are equivalent:*
(i) $T + \Lambda = \mathcal{G}$ is a tiling
(ii) $(T - T) \cap (\Lambda - \Lambda) = \{0\}$, and $|T||\Lambda| = |\mathcal{G}|$
(iii) $\mathrm{supp}\hat{\chi}_T \cap \mathrm{supp}\hat{\chi}_\Lambda = \{0\}$, and $|T||\Lambda| = |\mathcal{G}|$.

Proof. The equivalence of (i) and (ii) is trivial: the translates $\lambda + T$ are disjoint and cover $\mathcal{G}$ if and only if (ii) holds. For the equivalence of (i) and (iii) notice that $T + \Lambda = \mathcal{G}$ can be written as $\chi_T * \chi_\Lambda = \chi_\mathcal{G}$, and therefore $\hat{\chi}_T\hat{\chi}_\Lambda = |\mathcal{G}|\delta_0$, which is equivalent to (iii). □

The advantage of the Fourier characterization is that it remains valid for general tilings $f + \Lambda = \mathcal{G}$, even if $\mathcal{G}$ is infinite. Strictly speaking, we will not need this result but let me quote a convenient formulation of it for completeness (this formulation is a combination of Theorem 1.1 and 1.2 in [69]).

Lemma 2.1.3. ([69]) *Let $0 \leq f \in L^1(\mathbb{R}^d)$ be a nonnegative function with integral 1, such that $\hat{f} \in C^\infty(\mathbb{R}^d)$. Let $\Lambda \subset \mathbb{R}^d$ be a discrete multiset of density 1, and let δ_Λ denote the measure $\delta_\Lambda = \sum_{\lambda\in\Lambda} \delta_\lambda$, and assume that $\hat{\delta}_\Lambda$ is locally a measure. Then the following conditions are equivalent:*
(i) $f + \Lambda = \mathbb{R}^d$ is a tiling
(ii) $\mathrm{supp}\hat{\delta}_\Lambda \subset \{0\} \cup \{\hat{f} = 0\}$.

The characterization of lattice tilings is particularly elegant. We recall that the dual lattice Λ^* of a lattice $\Lambda \subset \mathbb{R}^d$ is defined as $\Lambda^* = \{\xi \in \mathbb{R}^d : \langle \xi, \lambda \rangle \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\}$.

Lemma 2.1.4. ([69]) *Let $0 \leq f \in L^1(\mathbb{R}^d)$ be a nonnegative function with integral 1, and let $\Lambda \subset \mathbb{R}^d$ be a lattice of density 1. Let Λ^* denote the dual lattice. The following are equivalent:*
(i) $f + \Lambda = \mathbb{R}^d$ is a tiling
(ii) $\Lambda^* \subset \{0\} \cup \{\hat{f} = 0\}$.

2.1.2 Tilings of $\mathbb{Z}$ and periodicity properties

Definition 2.1.5. *A subset $\Lambda \subset \mathcal{G}$ is periodic with period $0 \neq r \in \mathcal{G}$ if $x \in \Lambda$ implies $x + r \in \Lambda$. If $\mathcal{G} = \mathbb{Z}^d$ or $\mathbb{R}^d$ then we call Λ fully-periodic if there exist periods $r_1, \ldots, r_d$ which are $\mathbb{R}$-linearly independent.*

Let $A \subset \mathbb{Z}$ be a finite set with diameter n (the diameter is the difference between the largest element and the smallest element). It is well-known that in every tiling $A + B = \mathbb{Z}$ the translation set B must be periodic. For the minimal period r of B, Newman [105] proved that $r \leq 2^n$, which was improved later by Kolountzakis [70], Ruzsa [117], and finally Biró [15] who proves $r \leq e^{n^{1/3+\varepsilon}}$.

In the other direction, tilings with long periods ($r \geq cn^2$) were first constructed by Kolountzakis [70]. Then Steinberger [125] showed that r can be superpolynomial in n (the first step of the construction in [125] is basically the same as Proposition 2.2.16 below).

Theorem 2.1.6. [15, 125] *Let $A \subset \mathbb{Z}$ be a finite set of integers with diameter n, and let $A + B = \mathbb{Z}$ be a tiling. Then B is periodic, and the smallest period r of B satisfies $r \leq e^{n^{1/3+\varepsilon}}$. On the other hand, there exist tilings $A + B = \mathbb{Z}$ such that diameter of A is n and the least period r of B satisfies $r \geq e^{\frac{1}{4}\log^2 n/\log\log n}$.*

These upper and lower bounds refer to the *largest* possible period of a tiling of a set A of diameter n. What about the shortest period? A famous conjecture of Coven and Meyerowitz [30] implies that it can always be as small as $2n$ (as explained in the remark following Lemma 2.1 in [30]). That is, the tiling complement B of A can always be chosen so that the smallest period of B is at most $2n$. For the discussion of the Coven-Meyerowitz conjecture suppose that A is a finite set of nonnegative integers and $0 \in A$ (one can always shift any $A \subset \mathbb{Z}$ to achieve this). Write, as is customary, $A(X) = \sum_{a \in A} X^a$.

Let $\Phi_d(X)$ denote the dth cyclotomic polynomial, and let S_A be the set of prime powers p^α such that $\Phi_{p^\alpha}(X) \mid A(X)$. In [30] Coven and Meyerowitz wrote down the following two conditions on a such a polynomial $A(X)$.

(T_1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$,

(T_2) If $s_1, \ldots, s_m \in S_A$ are powers of distinct primes then $\Phi_{s_1 \cdots s_m}(X) \mid A(X)$.

They proved the following important theorem in [30].

Theorem 2.1.7. ([30]) *Let $A \subset \mathbb{Z}$ be a finite set of nonnegative integers such that $0 \in A$. If (T_1) and (T_2) hold then A tiles $\mathbb{Z}$ by translation. If A tiles $\mathbb{Z}$ by translation then (T_1) necessarily holds. If A tiles $\mathbb{Z}$ and $|A|$ has at most two different prime factors then (T_2) also holds.*

It was explicitly conjectured by Konyagin and Laba [77] that A is a tile of the integers if and only if both (T_1) and (T_2) hold. Nevertheless we call it the Coven-Meyerowitz conjecture.

Conjecture 2.1.8. (Coven-Meyerowitz conjecture, [30,77].) *A finite set of nonnegative integers A (such that $0 \in A$) tiles the integers by translation if and only if the conditions (T_1) and (T_2) are satisfied.*

This is probably the most important conjecture concerning the tilings of $\mathbb{Z}$. It is also easy to formulate 'local versions' (T_1^N) and (T_2^N) of conditions (T_1) and (T_2) for a set $A \subset \mathbb{Z}_N$ to tile $\mathbb{Z}_N$. Using these, we described an algorithm in [74] to list all non-periodic tilings $A + B = \mathbb{Z}_N$, if N has at most two different prime factors. Interestingly, the same algorithm can be used to *test* the validity of the conditions (T_1^N) and (T_2^N) if N has at least 3 prime factors. We have investigated many tilings for fairly large values of N, and the conditions (T_1^N) and (T_2^N) were always satisfied.

Periodicity in dimension 1 remains valid also for tilings of the real line. Also, the structure of translation sets can be described when we consider tilings of $\mathbb{R}$ with nonnegative functions of compact support (although periodicity is not true anymore for such general tilings).

Theorem 2.1.9. [71,81,84] *Let $T \subset \mathbb{R}$ be a bounded open set, and $T + \Lambda = \mathbb{R}$ be a tiling. Then Λ is periodic, i.e. $\Lambda = \cup_{j=1}^{N}(\alpha\mathbb{Z} + \beta_j)$. Moreover, all the differences $\beta_j - \beta_k$ are rational multiples of α. More generally, if $f + \Lambda = s\mathbb{R}$ is a multiple tiling for some nonnegative function $f \in L^1(\mathbb{R})$ with compact support, then Λ is a finite union of lattices, $\Lambda = \cup_{j=1}^{N}(\alpha_j\mathbb{Z} + \beta_j)$.*

One important consequence of periodicity is that tiling is an algorithmically decidable property in $\mathbb{Z}$: given a finite set $T \subset \mathbb{Z}$ one can decide by a finite algorithm whether T tiles $\mathbb{Z}$ or not. Surprisingly this is not known in higher dimensions:

Problem 2.1.10. *Given a finite set $T \subset \mathbb{Z}^d$, is there an algorithm to decide whether T tiles $\mathbb{Z}^d$ by translation?*

Already in $\mathbb{Z}^2$ this question is wide open, apart from the result of Szegedy [127] who gave an algorithm for the special cases of $|A|$ being a prime or 4. There are also algorithms for other special cases but these all have topological conditions [45, 143] on the tile (e.g. to be simply connected).

In a more general form of the problem, that of asking whether a given *set of tiles* can be moved around (by a group of motions) to tile $\mathbb{R}^d$, tiling has long been shown to be undecidable. Berger [13] first showed this (it is undecidable to determine if a given finite set of polygons can tile $\mathbb{R}^2$ using rigid motions). Many other models of tiling have been shown to undecidable (cf. [112]).

In dimensions $d \geq 3$ it is fairly easy to construct examples $T + \Lambda = \mathbb{Z}^d$ such that Λ does not have any periods. For $d = 2$ this was posed as an open problem in [69], but it is not hard to find such an example, and we sketch the idea here.

Example 2.1.11. Let $T = \{(0,0),(0,2),(2,0),(2,2)\} \subset \mathbb{Z}^2$. Then T tiles the subgroup $\mathcal{G}_0 = 2\mathbb{Z} \times 2\mathbb{Z}$ (the elements with even coordinates), and one can arrange a tiling $T + \Lambda_1 = \mathcal{G}_0$ so that Λ_1 has only vertical periods, $r = (0,2)$. But one can also tile the coset of $\mathcal{G}_0$ with odd coordinates, $T + \Lambda_2 = \mathcal{G}_0 + (1,1)$, in such a way that Λ_2 has only horizontal periods, $r = (2,0)$. Then the choice $\Lambda = \Lambda_1 \cup (\Lambda_1 + (0,1)) \cup (\Lambda_1 + (1,0)) \cup \Lambda_2$ shows that $T + \Lambda = \mathbb{Z}^2$ but Λ does not have any periods.

Although non-periodic tilings exist, it is still possible that whenever T tiles, it can also tile periodically (after modification of the translation set, if necessary).

Problem 2.1.12. (Periodic Tiling Conjecture [50,81]) *If a finite set $T \subset \mathbb{Z}^d$ (resp. a bounded measurable set T) tiles $\mathbb{Z}^d$ (resp. $\mathbb{R}^d$) by translation, then the translation set can be chosen to be fully-periodic.*

Again, a positive answer to the Periodic Tiling Conjecture would provide a positive answer to Problem 2.1.10. These questions are discussed in detail by M. Szegedy in [127]. He proves that if $\mathbb{Z}^d$ (or any finitely generated Abelian group) is generated by T, $|T|$ is a prime, and $T + T' = \mathbb{Z}^d$ then T' must be fully periodic. This is stronger than the Periodic Tiling Conjecture, for the case of $|T|$ being a prime. He also conjectures that if $|T|$ is a prime-power and T generates $\mathbb{Z}^d$ then in every tiling $T + T'$ the translation set T' must have a period vector. However, this conjecture fails, as a construction similar to Example 2.1.11 shows.

Example 2.1.13. Let $2T = \{(0,0),(0,4),(4,0),(4,4)\}$ be the dilated copy of the set defined in Example 2.1.11, and consider the following union of its translated copies: $T_0 = 2T \cup (2T + (0,1)) \cup (2T + (1,0)) \cup (2T + (1,1))$. Then $|T_0| = 16$ and it is clear that T_0 generates $\mathbb{Z}^2$ since $(0,1),(1,0) \in T_0$. Also, if $T + T' = \mathbb{Z}^2$ is a tiling such that T' is non-periodic, then $T_0 + 2T' = \mathbb{Z}^2$ is also such a tiling.

Example 2.1.11 and 2.1.13 are some simple observations of the author, and they have not been published.

What about periodicity in finite groups? Let $\mathcal{G}$ be finite, and $A + B = \mathcal{G}$. Hajós [55] called the group $\mathcal{G}$ 'good' if in any tiling $A + B = \mathcal{G}$ at least one of the sets A, B is necessarily periodic with a period $r < |\mathcal{G}|$. Good groups have been fully classified by Sands [122, 123], but we restrict our attention here to the cyclic case. Classifying non-periodic tilings of cyclic groups $\mathbb{Z}_N$ has been motivated by modern compositions of music [2, 136]. We have given such a classification algorithmically in [74].

We recall the classification of Sands for the cyclic case.

Theorem 2.1.14. [123] *The cyclic groups $\mathbb{Z}_N$ which are good are exactly those N that divide one of $pqrs$, p^2qr, p^2q^2 or p^nq, where p, q, r, s are any distinct primes and $n \geq 1$.*

The weaker property of quasi-periodicity was also introduced by Hajós: a tiling $A + B = \mathcal{G}$ is called quasi-periodic if either A or B, say B, can be partitioned into disjoint subsets $B_1, \ldots, B_m$ with $m > 1$ such that there is a subgroup $\mathcal{H} = \{h_1, \ldots, h_m\}$ of $\mathcal{G}$ with $A + B_i = A + B_1 + h_i$. Hajós conjectured that all tilings of finite Abelian groups are quasi-periodic, but this was disproved by an example of Sands [121] in $\mathbb{Z}_5 \times \mathbb{Z}_{25}$. However, the conjecture remains open in cyclic groups.

Conjecture 2.1.15. (Hajós quasi-periodicity conjecture [55].) *All tilings $A + B = \mathbb{Z}_N$ of a cycling group $\mathbb{Z}_N$ are quasi-periodic.*

2.1.3 Geometric results on tiling

Let us now turn to classical geometric results of tiling $\mathbb{R}^d$. There is a vast literature on translational tilings and multi-tilings of $\mathbb{R}^d$ by geometric objects (cube tilings alone have a very rich theory). We purposefully restrict our attention to some famous results that we will need in connection with Fuglede's conjecture.

Theorem 2.1.16. (Minkowski, [102]) *If a convex body P tiles $\mathbb{R}^d$ by a lattice, then P must be a centrally symmetric polytope whose $d-1$-dimensional facets are centrally symmetric.*

A precise characterization of the polytopes which tile $\mathbb{R}^d$ by translation was later given by Venkov [135] (and re-discovered by McMullen [101]). We will not recall this characterization here, only the fact that the translation set can always be chosen to be a lattice.

Theorem 2.1.17. ([101, 135]) *If a convex body P tiles $\mathbb{R}^d$, $P + \Lambda = \mathbb{R}^d$, then P is a polytope and the translation set Λ can be chosen to be a lattice.*

We remark that a generalization of Minkowski's theorem to multiple tilings was recently given in [49].

Theorem 2.1.18. ([49]) *If a convex polytope tiles $\mathbb{R}^d$ at any level k by translations, then it is centrally symmetric and its facets are centrally symmetric.*

2.2 Fuglede's conjecture

Let Ω be a bounded open domain in $\mathbb{R}^d$ (again, one could consider any measurable set with finite measure, but we do not want to enter the arising technical difficulties). In connection with commutation properties of the partial differential operators ∂_j on $L^2(\Omega)$ Fuglede [44] introduced the notion of *spectral sets*. He also remarks that this notion makes sense in any locally compact Abelian group, but as in the case of translational tiling we will restrict our attention to finite groups, $\mathbb{Z}^d$, and $\mathbb{R}^d$.

Definition 2.2.1. *Let $\mathcal{G}$ be a locally compact Abelian group of the following type: finite group, $\mathbb{Z}^d$, or $\mathbb{R}^d$. A bounded open set Ω in $\mathcal{G}$ is called spectral if $L^2(\Omega)$ has an orthogonal basis consisting of restrictions of characters of $\mathcal{G}$ to Ω, i.e. there exists a set $S \subset \hat{\mathcal{G}}$ such that $(S|_\Omega)_{s\in S}$ is an orthogonal basis of $L^2(\Omega)$. In such a case S is called a spectrum of Ω and (Ω, S) is called a spectral pair.*

Fuglede conjectured that the class of spectral sets in $\mathbb{R}^d$ is the same as the class of translational tiles. He originally stated the conjecture for any measurable set of finite measure but we restrict our attention to bounded open sets here. It will turn out that counterexamples already exist in this setting.

Conjecture 2.2.2. (Fuglede's conjecture, [44].) *A bounded open set $\Omega \in \mathbb{R}^d$ is spectral if and only if it tiles $\mathbb{R}^d$.*

There has been a tremendous amount of research in connection with this conjecture over the past decades. To keep the discussion at a reasonable length we will mostly restrict our attention to results related to our own research. In the next sections we will first discuss some positive results which prove or indicate the validity of the conjecture in some special cases, and then we will proceed to give counterexamples in the general case.

2.2.1 Positive results

We start by giving some useful equivalent characterizations of spectral sets.

The inner product and norm on $L^2(\Omega)$ are

$$\langle f, g\rangle_\Omega = \int_\Omega f\overline{g}, \quad \text{and} \quad \|f\|_\Omega^2 = \int_\Omega |f|^2,$$

and therefore for any $\lambda, \nu \in \widehat{\mathcal{G}}$ we have

$$\langle \lambda, \nu\rangle_\Omega = \widehat{\chi_\Omega}(\nu - \lambda).$$

This gives

$$\Lambda \text{ is an orthogonal set} \Leftrightarrow \forall \lambda, \mu \in \Lambda, \lambda \neq \mu : \ \widehat{\chi_\Omega}(\lambda - \mu) = 0$$

For Λ to be complete as well we must in addition have (Parseval)

$$\forall f \in L^2(\Omega) : \quad \|f\|_2^2 = \frac{1}{|\Omega|} \sum_{\lambda \in \Lambda} |\langle f, \lambda\rangle|^2. \tag{2.2}$$

For the groups we care about (finite groups, $\mathbb{Z}^d$, and $\mathbb{R}^d$) in order for Λ to be complete it is sufficient to have (2.2) for any character $\gamma \in \widehat{\mathcal{G}}$, since then we have it in the closed linear span of these functions, which is all of $L^2(\Omega)$. An equivalent reformulation for Λ to be a spectrum of Ω is therefore that

$$\sum_{\lambda \in \Lambda} |\widehat{\chi_\Omega}|^2(\gamma - \lambda) = |\Omega|^2, \tag{2.3}$$

for every $\gamma \in \widehat{\mathcal{G}}$. Therefore, Fuglede's conjecture is equivalent to the following: χ_Ω tiles $\mathcal{G}$ at level 1 if and only if $|\widehat{\chi_\Omega}|^2$ tiles $\hat{\mathcal{G}}$ at level $|\Omega|^2$.

For finite sets Ω (the group is finite or $\mathbb{Z}^d$) the characterization is even simpler: for a set $\Lambda \subseteq \widehat{\mathcal{G}}$ to be a spectrum it is necessary and sufficient that Λ satisfy the two conditions:

$$\Lambda - \Lambda \subseteq \{\widehat{\chi_\Omega} = 0\} \cup \{0\} \text{ (orthogonality)}, \ \ \#\Lambda = \#\Omega \text{ (maximal dimension)} \tag{2.4}$$

Another useful characterization of finite spectral sets is given in terms of *complex Hadamard* matrices. Recall that a $k \times k$ complex matrix H is called a (complex) Hadamard matrix if all entries of H have absolute value 1, and $HH^* = kI$ (where I

denotes the identity matrix). This means that the rows (and also the columns) of H form an orthogonal basis of $\mathbb{C}^k$. A *log-Hadamard matrix* is any real square matrix $(h_{i,j})_{i,j=1}^k$ such that the matrix $(e^{2\pi i h_{i,j}})_{i,j=1}^k$ is Hadamard. It is clear that a finite set $\Omega = \{t_1, \dots, t_k\}$ in a discrete group $\mathcal{G}$ is spectral with spectrum $\Gamma = \{\gamma_1, \dots, \gamma_k\} \subset \hat{\mathcal{G}}$ if and only if the $k \times k$ matrix $[H]_{j,m} = \gamma_j(t_m)$ is complex Hadamard.

For subsets $\Omega \subseteq \mathbb{R}^d$, when the spectra are infinite, we fall back on (2.3).

We now turn to results which show that spectral sets and tiles share many common properties. Most of the results will be quoted from the literature without proof. The ones with proof are taken from [40, 72, 73, 91]. All the results in this section support Fuglede's conjecture (at least, in special cases). However, in the next section it will turn out that counterexamples can still be constructed.

The first positive result is that of lattice tilings, or lattice spectra. This special case was already proved by Fuglede.

Theorem 2.2.3. ([44]) *Let $\Omega \subset \mathbb{R}^d$ be a bounded open domain of measure 1, and let $\Lambda \subset \mathbb{R}^d$ be a lattice of density 1. Then $\Omega + \Lambda = \mathbb{R}^d$ if and only if Λ^* (the dual lattice) is a spectrum of Ω.*

Proof (sketch, [69]). By (2.3) Λ^* is a spectrum of Ω if and only if $|\widehat{\chi_\Omega}|^2(\gamma - \lambda) = 1$ for almost all $\gamma \in \mathbb{R}^d$. By Lemma 2.1.4 this is equivalent to the Fourier transform of $|\widehat{\chi_\Omega}|^2$ vanishing on the dual lattice of Λ^* (except at 0), i.e. $\chi_\Omega * \chi_{-\Omega}$ vanishing on Λ except at 0. The latter condition is equivalent to $\Omega - \Omega \cap \Lambda = \{0\}$, which means that the translates $\Omega + \lambda$, $\lambda \in \Lambda$ do not intersect each other. By the assumptions on the volume of Ω and the density of Λ this is equivalent to $\Omega + \Lambda = \mathbb{R}^d$. □

Together with Theorem 2.1.17 this means that the "tile → spectral" direction of Fuglede's conjecture is true for convex bodies:

Corollary 2.2.4. ([44]) *If $\Omega \subset \mathbb{R}^d$ is a convex body which tiles $\mathbb{R}^d$ then it is also spectral in $\mathbb{R}^d$.*

Quite remarkably, the converse implication was also proven in dimension 2 by Iosevich, Katz and Tao:

Theorem 2.2.5. ([59]) *Fuglede's conjecture is true in $\mathbb{R}^2$ for convex domains. That is, the tiles and spectral sets are the parallelograms and centrally symmetric hexagons.*

The counterpart of Minkowski's Theorem 2.1.16 for spectral sets was proved by Kolountzakis:

Theorem 2.2.6. ([68]) *If a convex domain $\Omega \subset \mathbb{R}^d$ is spectral then it is centrally symmetric.*

If a convex body has smooth boundary then it cannot be a tile in any dimension d. The same is true for spectral sets:

Theorem 2.2.7. ([58]) *If $\Omega \subset \mathbb{R}^d$ is a convex body with smooth boundary then Ω cannot be spectral.*

We will now turn away from convex bodies and lattice tilings, but let us remark that Fuglede's conjecture may be true in any dimension $d \geq 1$ for *convex bodies*, counterexamples are not known. In the rest of the section we will consider sets of the type

$$\Omega = A + (0,1)^d, \quad A \subset \mathbb{Z}^d, \tag{2.5}$$

that is, unions of unit cubes situated at points with integer coordinates. Fuglede's conjecture for such sets has a rich theory invoking ideas from combinatorics, number theory (for $d = 1$), and Fourier analysis.

As the zero-sets of Fourier transforms play a central role in our investigations, it will be convenient to introduce the following notation.

Notation 2.2.8. *For any function $f : \mathcal{G} \to \mathbb{C}$ the set of zeros of f is denoted by $Z(f) = \{x \in \mathcal{G} : f(x) = 0\}$.*

Our first result is that considering sets of type (2.5) is equivalent to investigating Fuglede's conjecture in $\mathbb{Z}^d$. The 'spectral' part of the following lemma is taken from [72] while the 'tile' part is basically trivial.

Proposition 2.2.9. ([72]*) *A set Ω of the form (2.5) is spectral (respectively, a tile) in $\mathbb{R}^d$ if and only if the set A is spectral (resp. a tile) in $\mathbb{Z}^d$.*

Proof. We first prove the spectral part of the lemma. Write $Q = (0,1)^d$, $\Omega = A + Q$. Then $\widehat{\chi_\Omega} = \widehat{\chi_A}\widehat{\chi_Q}$ and $Z(\widehat{\chi_\Omega}) = Z(\widehat{\chi_A}) \cup Z(\widehat{\chi_Q})$. By calculation we have

$$Z(\widehat{\chi_Q}) = \left\{\boldsymbol{\xi} \in \mathbb{R}^d : \ \exists j \text{ such that } \xi_j \in \mathbb{Z} \setminus \{\mathbf{0}\}\right\}.$$

Now suppose $\Lambda \subset \mathbb{T}^d$ is a spectrum of A as a subset of $\mathbb{Z}^d$. Viewing $\mathbb{T}^d$ as Q we observe that the set $Z(\widehat{\chi_A})$ is periodic with $\mathbb{Z}^d$ as a period lattice. Define now $S = \Lambda + \mathbb{Z}^d$. The differences of S are either points which are on $Z(\widehat{\chi_A})$ (mod $\mathbb{Z}^d$) or points with all integer coordinates. In any case these differences fall in $Z(\widehat{\chi_\Omega})$, hence $\sum_{s\in S} |\widehat{\chi_\Omega}(x-s)|^2 \leq (\#A)^2$. Furthermore, the density of S is $\#A$ which, along with the periodicity of S, implies that $|\widehat{\chi_\Omega}|^2 + S$ is a tiling of $\mathbb{R}^d$ at level $(\#A)^2$. That is, S is a spectrum for Ω.

Conversely, assume S is a spectrum for Ω as a subset of $\mathbb{R}^d$. It follows that the density of S is equal to $|\Omega| = \#A$, hence there exists $\boldsymbol{k} \in \mathbb{Z}^d$ such that $\boldsymbol{k} + Q$ contains at least $\#A$ points of S. Call the set of these points S_1, and observe that the differences of points of S_1 are contained in $Q - Q = (-1,1)^d$, and that $Q - Q$ does not intersect $Z(\widehat{\chi_Q})$. It follows that the differences of the points of S_1 are all in $Z(\widehat{\chi_A})$, and, since their number is $\#A$, they form a spectrum of A as a subset of $\mathbb{Z}^d$.

Let us now turn to the 'tile' part of the lemma. If A tiles $\mathbb{Z}^d$ then it is trivial that Ω tiles $\mathbb{R}^d$. In the converse direction the simplest proof I know of was given by G. Kós, as follows. Assume $\Omega + \Lambda$ is a tiling of $\mathbb{R}^d$. Due to $\mathbb{Z}^d$ being countable and the boundary of Ω being measure zero we can find a vector $\mathbf{x} \in \mathbb{R}^d$ such that for all $\lambda \in \Lambda$ the set $\lambda + \mathbf{x} + \Omega$ does not contain any points of $\mathbb{Z}^d$ on its boundary. That is, in the tiling $\Omega + (\Lambda + \mathbf{x}) = \mathbb{R}^d$ in each translated copy of Ω the integer points

correspond to a translated copy of A. Therefore, we get a tiling of $\mathbb{Z}^d$ by translated copies of A as required. □

The situation is particulary interesting in dimension 1. Due to the rational periodicity result of Lagarias and Wang [81] (cf. Theorem 2.1.9 above), all bounded open sets that tile $\mathbb{Z}$ are essentially equivalent to sets of the type (2.5). Therefore, the 'tile $\rightarrow$ spectral' direction of Fuglede's conjecture holds in $\mathbb{R}$ if and only if it holds in $\mathbb{Z}$. Intriguingly, an observation of Laba shows that the validity of the Coven-Meyerowitz conjecture would be sufficient for this.

Theorem 2.2.10. ([79]) *If $A \subset \mathbb{Z}$ is a finite set of nonnegative integers (such that $0 \in A$), and the corresponding polynomial $A(X) = \sum_{a \in A} X^a$ satisfies the conditions (T_1) and (T_2) of Conjecture 2.1.8, then A is spectral in $\mathbb{Z}$.*

It is less clear whether the 'spectral $\rightarrow$ tile' direction of Fuglede's conjecture in $\mathbb{R}$ is also equivalent to its validity in $\mathbb{Z}$. A recent breakthrough by Bose and Madan [19], followed by that of Kolountzakis and Iosevich [60] shows that the spectrum of a bounded measurable set must be periodic.

Theorem 2.2.11. ([60]) *Let $\Omega \subset \mathbb{R}$ be a bounded measurable set with measure 1, and let S be a spectrum of Ω. Then S is periodic and any period is an integer.*

However, this in itself does not mean that it is enough to consider the 'spectral $\rightarrow$ tile' implication in $\mathbb{Z}$ instead of $\mathbb{R}$. A very good account of the known implications concerning Fuglede's conjecture in $\mathbb{Z}_n, \mathbb{Z}$ and $\mathbb{R}$ is given in [37].

The following 'amplification' property is also shared by spectral sets and tiles.

Proposition 2.2.12. ([72, 91]*) *Let $\boldsymbol{n} = (n_1, \dots, n_d) \in \mathbb{Z}^d$, consider a set $A \subset [0, n_1 - 1) \times \cdots \times [0, n_d - 1) \subset \mathbb{Z}^d$ and let $\tilde{A} \subset \mathcal{G} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ denote the reduction of A modulo $\boldsymbol{n}$. Write*

$$T = T(\boldsymbol{n}, k) = \{0, n_1, 2n_1, \dots, (k-1)n_1\} \times \cdots \times \{0, n_d, 2n_d, \dots, (k-1)n_d\}, \quad (2.6)$$

and define $A_k = A + T$. Then, for large enough values of k, the set $A_k \subset \mathbb{Z}^d$ is spectral (resp. a tile) in $\mathbb{Z}^d$ if and only if $\tilde{A}$ is spectral (resp. a tile) in $\mathcal{G}$.

Proof. The 'if' part for tiles follows from the fact that the reduction $\tilde{A}_k$ of A_k modulo $(kn_1 \times, \cdots \times kn_d)$ tiles the group $\mathcal{G}_k = \mathbb{Z}_{kn_1} \times \cdots \times \mathbb{Z}_{kn_d}$ in an obvious way. The 'if' part for spectral sets follows in a similar manner: it will be shown in Proposition 2.2.17 (in a more general form) that $\tilde{A}_k$ is spectral in the group $\mathcal{G}_k$.

We now prove the 'only if' part of the lemma for spectral sets. Observe first that $\chi_{A_k} = \chi_A * \chi_T$, hence we obtain

$$Z(\widehat{\chi_{A_k}}) = Z(\widehat{\chi_A}) \cup Z(\widehat{\chi_T}).$$

Elementary calculation of $\widehat{\chi_T}$ (it is a cartesian product) shows that it is a union of "hyperplanes"

$$Z(\widehat{\chi_T}) = \left\{ \boldsymbol{\xi} \in \mathbb{T}^d : \ \exists j \ \exists \nu \in \mathbb{Z}, \ k \text{ does not divide } \nu, \text{ such that } \xi_j = \frac{\nu}{kn_j} \right\}. \quad (2.7)$$

Define the group

$$\mathcal{H} = \left\{ \boldsymbol{\xi} \in \mathbb{T}^d : \ \forall j \ \exists \nu \in \mathbb{Z} \text{ such that } \xi_j = \frac{\nu}{n_j} \right\}.$$

which is the group of characters of the group $\mathcal{G}$ and does not depend on k. Observe that $\mathcal{H} + (Q - Q)$ does not intersect $Z(\widehat{\chi_T})$, where

$$Q = \left[0, \frac{1}{kn_1}\right) \times \cdots \times \left[0, \frac{1}{kn_d}\right).$$

Assume now that $S \subseteq \mathbb{T}^d$ is a spectrum of A_k, so that $\#S = \#A_k = rk^d$, if $r = \#A$. Define, for $\boldsymbol{\nu} \in \{0, \ldots, k-1\}^d$, the sets

$$S_{\boldsymbol{\nu}} = \left\{ \boldsymbol{\xi} \in S : \ \boldsymbol{\xi} \in (\frac{\nu_1}{kn_1}, \ldots, \frac{\nu_d}{kn_d}) + Q + (\frac{m_1}{n_1}, \ldots, \frac{m_d}{n_d}), \text{ for some } \boldsymbol{m} \in \mathbb{Z}^d \right\}.$$

Since the number of the $S_{\boldsymbol{\nu}}$ is k^d and they partition S, it follows that there exists some $\boldsymbol{\mu}$ for which $\#S_{\boldsymbol{\mu}} \geq r$.

We also note that, if k is sufficiently large, then any translate of Q may contain at most one point of the spectrum. The reason is that $Q - Q$ contains no point of $Z(\widehat{\chi_T})$ (for any k) and no point of $Z(\widehat{\chi_A})$ for all large k (as $\widehat{\chi_A}(\mathbf{0}) > 0$).

Observe next that if $\boldsymbol{x}, \boldsymbol{y} \in S_{\boldsymbol{\mu}}$ then

$$\begin{aligned} \boldsymbol{x} - \boldsymbol{y} &\in \mathcal{H} + (Q - Q) \\ &= \mathcal{H} + \left(-\frac{1}{kn_1}, \frac{1}{kn_1}\right) \times \cdots \times \left(-\frac{1}{kn_d}, \frac{1}{kn_d}\right) \end{aligned}$$

and that this set does not intersect $Z(\widehat{\chi_T})$ (from (2.7)). It follows that for all $\boldsymbol{x}, \boldsymbol{y} \in S_{\boldsymbol{\mu}}$ we have $\boldsymbol{x} - \boldsymbol{y} \in Z(\widehat{\chi_A})$.

Let k be sufficiently large so that for all points $\boldsymbol{h} \in \mathcal{H}$ for which $\widehat{\chi_A}(\boldsymbol{h}) \neq 0$ the rectangle $\boldsymbol{h} + Q - Q$ does not intersect $Z(\widehat{\chi_A})$. It follows that if $\boldsymbol{x}, \boldsymbol{y} \in S_{\boldsymbol{\mu}}$ then $\boldsymbol{x} - \boldsymbol{y} \in \boldsymbol{h} + (Q - Q)$, where $\boldsymbol{h} \in Z(\widehat{\chi_A})$.

For each $\boldsymbol{x} \in \mathbb{T}^d$ define $\lambda(\boldsymbol{x})$ to be the unique point $\boldsymbol{z}$ whose j-th coordinate is an integer multiple of $\frac{1}{kn_j}$ for which $\boldsymbol{x} \in \boldsymbol{z} + Q$. If $\boldsymbol{x}, \boldsymbol{y} \in S_{\boldsymbol{\mu}}$ it follows that $\lambda(\boldsymbol{x}) - \lambda(\boldsymbol{y}) \in \mathcal{H} \cap Z(\widehat{\chi_A})$. Define now $\Lambda = \left\{ \lambda(\boldsymbol{x}) : \ \boldsymbol{x} \in S_{\boldsymbol{\mu}} \right\}$ (and shift Λ to contain 0, so that $\Lambda \subset \mathcal{H}$). It is obvious that $\#\Lambda \geq r$ and $\Lambda - \Lambda \subseteq Z(\widehat{\chi_{\tilde{A}}}) \cup \{\mathbf{0}\}$, therefore Λ is a spectrum of $\tilde{A}$.

We now prove the 'only if' part of the lemma for tiles. For the sake of technical simplicity we assume $n_1 = n_2 = \cdots = n_d =: m$, which will be the case in applications later. The proof remains valid for general $n_1, \ldots, n_d$ after obvious modifications. The proof proceeds along the same lines as in [91, 132].

Assume, for contradiction, that A_k tiles $\mathbb{Z}^d$ with some translation set Σ. Take a cube $C_l = [0, l)^d$, where l is much larger than k. Let $\Sigma_l := \{\sigma \in \Sigma \ : (\sigma + A_k) \cap C_l \neq$

$\emptyset\}$. Note that $\#A_k = rk^d$. We have $\#\Sigma_l \leq \frac{(l+2mk)^d}{rk^d}$, because all Σ_l-translates of A_k are contained in the cube $(-mk, l+mk)^d$.

Let $\mathcal{A}$ denote the annulus $\mathcal{A} := [-m, mk+m)^d - [m, mk-m)^d$. Then $\#\mathcal{A}$ $(\approx 4dm(mk)^{d-1}) \leq 5dm(mk)^{d-1}$, if k is large enough compared to m. Hence, $\Sigma_l + \mathcal{A}$ cannot cover the cube $C_{l-m} := [0, l-m)^d$ because $(\#\Sigma_l)(\#\mathcal{A}) \leq (l+2mk)^d \left(\frac{5dm(mk)^{d-1}}{rk^d}\right) < (l-m)^d$, if the numbers k, l are chosen so that k is sufficiently large compared to m, and l is sufficiently large compared to k.

Take a point $x \in C_{l-m}$ not covered by $\Sigma_l + \mathcal{A}$. Consider the cube $C_m^x := x + [0,m)^d$. This cube is fully inside C_l, therefore if any translate $\sigma + A_k$ intersects C_m^x then σ necessarily belongs to Σ_l. The point x is not covered by the annulus $\sigma + \mathcal{A}$, therefore C_m^x is contained in the cube $\sigma + [0,mk)^d$. Let S denote the set $A + m \cdot \mathbb{Z}^d$. In view of what has been said, we have $(\sigma + A_k) \cap C_m^x = (\sigma + S) \cap C_m^x = (x + [0,m)^d) \cap (\sigma + A + m\mathbb{Z}^d)$. The mod m reduction of this set is exactly the translate $\sigma + A$ mod m. Hence, the tiling of the cube C_m^x by Σ-translates of A_k contradicts the assumption that $\tilde{A}$ does not tile $\mathbb{Z}_m^d$. □

While Proposition 2.2.9 and 2.2.12 prove that certain properties are shared by spectral sets and tiles, they have the important implication that it is enough to find a counterexample in any finite Abelian group, and the transition to $\mathbb{Z}^d$ and $\mathbb{R}^d$ will be automatic. We summarize this important fact in the following corollary.

Corollary 2.2.13. ([72]*) *Let $\mathcal{G} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ be a finite Abelian group, and assume $\tilde{A} \subset \mathcal{G}$ is a spectral set which is not a tile (resp. a tile which is not a spectral set). Consider a set $A \subset [0, n_1 - 1) \times \cdots \times [0, n_d - 1) \subset \mathbb{Z}^d$ such that the reduction of A modulo $(n_1, \ldots, n_d)$ is $\tilde{A}$. Then, for large enough k, the set $A_k = A + T(\boldsymbol{n}, k)$ defined in Proposition 2.2.12 is spectral (resp a tile) in $\mathbb{Z}^d$ but it is not a tile (resp. not spectral) in $\mathbb{Z}^d$. Furthermore, the union of unit cubes $A_k + (0,1)^d \subset \mathbb{R}^d$ is spectral (resp. a tile) in $\mathbb{R}^d$ but it is not a tile (resp. not spectral).*

We now turn to properties in finite Abelian groups. First we show that tiles and spectral sets behave in the same way in subgroups and under homomorphic images. The tiling part of Lemma 2.2.15 was given by Szegedy in [127].

Lemma 2.2.14. *Let $\mathcal{G}$ be a finite Abelian group, and let $\mathcal{G}_0$ be a subgroup. A set $T \subset \mathcal{G}_0$ is spectral (resp. a tile) in $\mathcal{G}_0$ if and only if it is spectral (resp. a tile) in $\mathcal{G}$.*

Proof. The statement is trivial for tiles. For spectral sets the 'if' part is trivial because the restriction of any character $\gamma \in \hat{\mathcal{G}}$ to $\mathcal{G}_0$ is a character of $\mathcal{G}_0$. Conversely, for any character $\gamma_0 \in \hat{\mathcal{G}}_0$ there exists a character $\gamma \in \hat{\mathcal{G}}$ (typically not uniquely), such that $\gamma|_{\mathcal{G}_0} = \gamma_0$, and therefore any spectrum $S_0 \subset \hat{\mathcal{G}}_0$ gives rise to a spectrum $S \subset \hat{\mathcal{G}}$. □

Lemma 2.2.15. *Let $\mathcal{G}, \mathcal{H}$ be finite Abelian groups, $T \subset \mathcal{G}$ and suppose that there exists a homomorphism $\phi : \mathcal{G} \to \mathcal{H}$ such that ϕ is injective on T and $\phi(T)$ is spectral (resp. a tile) in $\mathcal{H}$. Then T is spectral (resp. a tile) also in $\mathcal{G}$.*

Proof. If $\gamma \in \hat{\mathcal{H}}$ then one can define $\gamma' \in \hat{\mathcal{G}}$ by $\gamma'(g) = \gamma(\phi(g))$, and therefore any spectrum $S_{\mathcal{H}}$ of T gives rise to a spectrum $S_{\mathcal{G}}$ of T. For the tiling property, it is easy to check that if $\phi(T) + L = \mathcal{H}$ then $T + \phi^{-1}(L) = \mathcal{G}$. □

Next, we consider a 'natural' tiling construction (which is a generalization of the amplification procedure of Proposition 2.2.12), and show that the same construction works for spectral sets, too.

Proposition 2.2.16. ([72]*) *Let $\mathcal{G}$ be a finite Abelian group, and $\mathcal{H} \leq \mathcal{G}$ a subgroup. Let $T_1, T_2, \dots T_k \subset \mathcal{H}$ be subsets of $\mathcal{H}$ such that they share a common tiling complement in $\mathcal{H}$; i.e. there exists a set $T' \subset \mathcal{H}$ such that $T_j + T' = \mathcal{H}$ is a tiling for all $1 \leq j \leq k$. Consider any tiling decomposition $S + S' = \mathcal{G}/\mathcal{H}$ of the factor group $\mathcal{G}/\mathcal{H}$, with $\#S = k$, and take arbitrary representatives $s_1, s_2, \dots s_k$ from the cosets of $\mathcal{H}$ corresponding to the set S. Then the set $\Gamma := \cup_{j=1}^{k}(s_j + T_j)$ is a tile in the group $\mathcal{G}$.*

Proof. The proof is simply the observation that for any system of representatives $\tilde{S}' := \{s'_1, s'_2, \dots\}$ of S' the set $T' + \tilde{S}'$ is a tiling complement for Γ in $\mathcal{G}$. □

Proposition 2.2.17. ([72, 94]*) *Let $\mathcal{G}$ be a finite Abelian group, and $\mathcal{H} \leq \mathcal{G}$ a subgroup. Let $T_1, T_2, \dots T_k \subset \mathcal{H}$ be subsets of $\mathcal{H}$ such that they share a common spectrum in $\widehat{\mathcal{H}}$; i.e. there exists a set $L \subset \widehat{\mathcal{H}}$ such that L is a spectrum of T_m for all $1 \leq m \leq k$. Consider any spectral pair (Q, S) in the factor group $\mathcal{G}/\mathcal{H}$, with $|Q| = k$, and take arbitrary representatives $\mathbf{q}_1, \mathbf{q}_2, \dots \mathbf{q}_k$ from the cosets of $\mathcal{H}$ corresponding to the set Q. Then the set $\Gamma := \cup_{m=1}^{k}(\mathbf{q}_m + T_m)$ is spectral in the group $\mathcal{G}$.*

Proof. The proof is trivial, although the notations are somewhat cumbersome. We will simply construct a spectrum $\Sigma \subset \widehat{\mathcal{G}}$ for Γ. Let n denote the number of elements in each T_m (they necessarily have the same number of elements as there exists a common spectrum), and $\mathbf{t}_r^m$ ($r = 1, \dots n$ and $m = 1, \dots k$) the rth element of T_m. By assumption, there exist characters $\mathbf{l}_j \in \widehat{\mathcal{H}}$ ($j = 1, \dots n$) such that the matrices $[A_m]_{j,r} := [\mathbf{l}_j(\mathbf{t}_r^m)]$ are $n \times n$ complex Hadamard for each m. Let $\tilde{\mathbf{l}}_j$ denote any extension of $\mathbf{l}_j$ to a character of $\mathcal{G}$ (such extensions always exist, although not unique). Also, the elements $\mathbf{s}_1, \dots, \mathbf{s}_k$ of $S \subset \widehat{\mathcal{G}/\mathcal{H}}$ can be identified with characters $\tilde{\mathbf{s}}_i \in \widehat{\mathcal{G}}$ which are constant on cosets of $\mathcal{H}$. Then we consider the product characters $\tilde{\mathbf{s}}_i\tilde{\mathbf{l}}_j$ and let $\Sigma := \{\tilde{\mathbf{s}}_i\tilde{\mathbf{l}}_j\}_{i,j}$ where $i = 1, \dots, k$ and $j = 1, \dots, n$. We claim that Σ is a spectrum of Γ. For each $m = 1, \dots k$ let $D_{L\mathbf{q}_m}$ denote the $n \times n$ diagonal matrix with entries $[D_{L\mathbf{q}_m}]_{j,j} = \tilde{\mathbf{l}}_j(\mathbf{q}_m)$. Then, for fixed i and m the product characters $\tilde{\mathbf{s}}_i\tilde{\mathbf{l}}_j$ ($j = 1, \dots, n$) restricted to the set $\mathbf{q}_m + T_m = \{\mathbf{q}_m + \mathbf{t}_1^m, \dots, \mathbf{q}_m + \mathbf{t}_n^m\}$ simply give the $n \times n$ matrix

$$B^{i,m} := \tilde{\mathbf{s}}_i(\mathbf{q}_m) D_{Lq_m} A_m, \tag{2.8}$$

because the entries are given as $[B^{i,m}]_{j,r} = \tilde{\mathbf{s}}_i\tilde{\mathbf{l}}_j(\mathbf{q}_m + \mathbf{t}_r^m) = \tilde{\mathbf{s}}_i(\mathbf{q}_m)\tilde{\mathbf{l}}_j(\mathbf{q}_m)\tilde{\mathbf{l}}_j(\mathbf{t}_r^m)$. This means that the characters $\tilde{\mathbf{s}}_i\tilde{\mathbf{l}}_j \in \Sigma$ restricted to Γ will give the $nk \times nk$ block matrix

$$H := \begin{bmatrix} B^{1,1} & . & . & B^{1,k} \\ . & . & . & . \\ . & . & . & . \\ B^{k,1} & . & . & B^{k,k} \end{bmatrix}. \tag{2.9}$$

Now, observe that each block $B^{i,m}$ is given as a product $\tilde{\mathbf{s}}_i(\mathbf{q}_m)D_{Lq_m}A_m$ where $N_m := D_{Lq_m}A_m$ is a complex Hadamard matrix (because A_m is such and D_{Lq_m} is a unitary diagonal matrix), and $\tilde{\mathbf{s}}_i(\mathbf{q}_m)$ is the entry of a $k \times k$ complex Hadamard matrix by the assumption that S is a spectrum of Q. Therefore H is seen to be a complex Hadamard matrix arising directly with formula (2.10) (see Section 2.3.1), and hence Σ is indeed a spectrum of Γ. □

It turns out that the the construction of Proposition 2.2.16 is so general that it is not trivial to produce tilings which do not arise in such manner. In fact, it was once asked by Sands [124] whether *every* tiling of finite Abelian groups is such that one of the factors is contained in a subgroup (note that such tilings correspond to the special case $Q = \mathcal{G}/\mathcal{H}$ in Proposition 2.2.16). This question was then answered in the negative by *a construction of Szabó* [126]. Quite intriguingly, we will see in Section 2.3 that Szabó's construction also works analogously for spectral sets.

In the last part of this section we show that the 'spectral → tile' direction of Fuglede's conjecture holds for sets of size ≤ 5. This is best possible, as the counterexamples in Section 2.2.1 will show.

Proposition 2.2.18. ([73]*) *Let $\mathcal{G}$ be any finite Abelian group and $A \subset \mathcal{G}$ a spectral set in $\mathcal{G}$ with $|A| \leq 5$. Then A tiles $\mathcal{G}$.*

Proof. For any finite Abelian group $\mathcal{G}$ we may choose natural numbers N, d such that $\mathcal{G} \leq \mathbb{Z}_N^d$. Therefore, by Lemma 2.2.14, it is enough to prove the statement for groups of the type $\mathcal{G} = \mathbb{Z}_N^d$. This observation makes the proof technically simpler.

It will be convenient to regard any element $x \in \mathcal{G} = \mathbb{Z}_N^d$ as a column vector of length d with integer entries ranging from 0 to $N-1$. Also, an element $\gamma \in \hat{\mathcal{G}}$ will be regarded as a row vector of length d with entries ranging from 0 to $N-1$. The action of the character γ on x is then given by $\gamma(x) = e^{2i\pi\langle\gamma,x\rangle/N}$.

The essential part of the proof relies on the fact that we have a full characterization of complex Hadamard matrices up to order 5.

We identify the elements of $\mathcal{G}$ and $\hat{\mathcal{G}}$ with d-dimensional column- and row-vectors, respectively. Let $A \subset \mathcal{G} = \mathbb{Z}_N^d$, with $|A| = k \leq 5$. We regard A as a $d \times k$ matrix with integer coefficients. If $L \subset \hat{\mathcal{G}}$ is a spectrum of A (regarded as a $k \times d$ matrix), then $H := \frac{1}{N}L \cdot A$ is a log-Hadamard (where the matrix multiplication can be taken mod N). Multiplication by the matrix L defines a homomorphism from $\mathcal{G}$ to $\mathbb{Z}_N^k$, and the images of the elements of A are given by the columns c_j of $L \cdot A$ ($1 \leq j \leq k$). By Lemma 2.2.15 it is enough to prove that the vectors c_j tile $\mathbb{Z}_N^k$.

In the cases $k = 1, 2, 3, 5$ this follows immediately from the uniqueness (up to natural equivalence) of complex Hadamard matrices of order k. This uniqueness is trivial for $k = 1, 2, 3$, while the case $k = 5$ is settled in [54]. Indeed, we can assume without loss of generality that $0 \in A$ and $0 \in L$ (due to the trivial translation invariance of the notion of spectrality and spectrum), and this already implies that the matrix $H = h_{m,j}$ is (after a permutation of columns) given by $h_{m,j} = \frac{1}{k}mj$ ($0 \leq m, j \leq k-1$). It follows that N is a multiple of k, say $N = Mk$, and the column vectors c_j are given as $c_j = (0, jM, 2jM, \ldots, (k-1)jM)^T$. In order to see that these vectors tile $\mathbb{Z}_N^d$ we invoke Lemma 2.2.15 once again. Let $V := (0, 1, 0, \ldots, 0)$, and

consider the mod N product $V \cdot L \cdot A = (0, M, 2M, \dots (k-1)M)$. It is obvious that the set $\{0, M, 2M, \dots (k-1)M\}$ tiles $\mathbb{Z}_N$, and therefore the columns c_j tile $\mathbb{Z}_N^k$.

The case $k = 4$ is settled in a similar manner, although we have no uniqueness of Hadamard matrices in this case. The general form of a 4×4 complex Hadamard matrix is given (see e.g. [54], Proposition 2.1) by the parametrization

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{2\pi i\phi} & -e^{2\pi i\phi} \\ 1 & -1 & -e^{2\pi i\phi} & e^{2\pi i\phi} \end{pmatrix}.$$

Due to the presence of -1's it follows that N must be a multiple of 2, say $N = 2M$. Also, $t := N\phi$ must be an integer. The matrix LA is then given by

$$LA = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & M & M \\ 0 & M & t & M+t \\ 0 & M & M+t & t \end{pmatrix}.$$

To see that the columns of this matrix tile $\mathbb{Z}_N^4$, consider the matrix

$$V_2 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Then

$$V_2 LA = \begin{pmatrix} 0 & 0 & M & M \\ 0 & M & t & M+t \end{pmatrix}.$$

It is easy to check that the columns of this matrix tile $\mathbb{Z}_N^2$, and by Lemma 2.2.15 this implies that the columns of LA tile $\mathbb{Z}_N^4$. □

Next, we extend the previous result to the infinite grid $\mathbb{Z}^d$. First, we need to establish the rationality of the spectra in the cases considered.

Proposition 2.2.19. ([73]*) *Let $A \subset Z^d$ be a spectral set with $|A| \leq 5$. Then A admits a rational spectrum.*

Proof. Note that we do not claim that *all* spectra of A must be rational, but only that the spectrum can be chosen rational.

The proof is an easy argument from linear algebra. Let us first consider the case $|A| = 5$ (the cases $|A| = 1, 2, 3$ are settled the same way, while $|A| = 4$ will require some extra considerations). Let $L \subset \mathbb{T}^d$ denote a spectrum of A. We may assume that $0 \in A$ and $0 \in L$. Then, after a permutation of elements of A, we have

$$LA = \frac{1}{5} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix} \pmod 1.$$

Let $l_{m,j}$ denote the elements of L. Considering, for example, the second row of L we see that there exist integers $z_{2,1}, \dots, z_{2,5}$ such that

$$(l_{2,1}, \dots, l_{2,d}) \cdot A = \left(z_{2,1}, z_{2,2} + \frac{1}{5}, \dots z_{2,5} + \frac{4}{5} \right).$$

Regarding this equation as a set of linear equations with variables $l_{2,1}, \dots, l_{2,d}$ we see that if there exists a solution, then the solution can be chosen rational. The same argument holds for the other rows of L.

We now turn to the case $|A| = 4$. Then, for some $q \in [0, 1]$ we have

$$LA = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} + q & q \\ 0 & \frac{1}{2} & q & \frac{1}{2} + q \end{pmatrix} \pmod 1.$$

If q is rational then the previous argument applies. If q is irrational we need some additional considerations. Applying the previous argument we see that the first two rows of L can be chosen rational even in this case (they do not depend on q). It is also clear that the fourth row of L can be chosen as the sum of the second and third rows. Consider therefore the third row only. For some integers $z_{3,1}, \dots, z_{3,4}$ we have

$$(l_{3,1}, \dots, l_{3,d}) \cdot A = \left(z_{3,1}, z_{3,2} + \frac{1}{2}, z_{3,3} + \frac{1}{2} + q, z_{3,4} + q \right)$$

Regard this equation as a set of linear equations with variables $x_1, \dots, x_d, y$ in place of $l_{3,1}, \dots, l_{3,d}, q$. By assumption, a solution $x_1 = l_{3,1}, \dots, x_d = l_{3,d}, y = q$ of this set of equations exists. By the coefficients being rational this means that a solution consisting of rational numbers also exists, i.e. we can replace $l_{3,1}, \dots, l_{3,d}, q$ by rational numbers. Finally, we can choose the fourth row of L as the sum of the second and third rows, which automatically becomes rational. □

Now, we are in position to prove the analogue of Proposition 2.2.18 in $\mathbb{Z}^d$.

Proposition 2.2.20. ([73]*) *Let $A \subset \mathbb{Z}^d$ be a spectral set in $\mathbb{Z}^d$ with $|A| \leq 5$. Then A tiles $\mathbb{Z}^d$.*

Proof. By Proposition 2.2.19 we can choose the spectrum of A rational. This means that A is already spectral in some finite group $\mathcal{G} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$. By Theorem 2.2.18 we conclude that A tiles $\mathcal{G}$, and therefore it tiles $\mathbb{Z}^d$. □

2.2.2 Counterexamples

In the previous section we have seen many properties that are common for spectral sets and tiles. On the other hand, we have also seen in Corollary 2.2.13 that any counterexample in a finite group will automatically lead to counterexamples in $\mathbb{Z}^d$ and $\mathbb{R}^d$. This section will be devoted to constructing such counterexamples.

Let us first consider the 'spectral → tile' direction of the conjecture. We have seen in Proposition 2.2.18 that no counterexamples exist with $|A| \leq 5$. However,

the abundance of complex Hadamard matrices of order 6 allows us to construct counterexamples already with $|A| = 6$. This was first done by T. Tao in [132], by first constructing a non-tile spectral set in $\mathbb{Z}_3^5$ and then transferring the example to $\mathbb{Z}^5$ and $\mathbb{R}^5$. The credit to refuting this direction of Fuglede's conjecture therefore goes to T. Tao. Subsequently, a minor observation in [91] allowed me to decrease the dimension to 4, and finally to 3 in [73] in a joint work with M. N. Kolountzakis. We will only include the 3-dimensional example here. All the known examples are based on particular complex Hadamard matrices of order 6. At present, we do not have a full characterization of complex Hadamard matrices of order 6 or greater. On the other hand we do possess particular examples and even descriptions of some parametric families of 6×6 Hadamard matrices. The family described in [35] contains a matrix which leads to a 3-dimensional counterexample.

Theorem 2.2.21. ([73]*) *There exists a spectral set $A \subset \mathbb{Z}_8^3$ which is not a tile. As a consequence, there exist sets in $\mathbb{Z}^3$ and $\mathbb{R}^3$ which are spectral but do not tile $\mathbb{Z}^3$ and $\mathbb{R}^3$, respectively.*

Proof. Consider the following 6×6 log-Hadamard matrix:

$$H := \frac{1}{8}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 6 & 6 & 2 \\ 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \\ 0 & 6 & 7 & 2 & 4 & 3 \\ 0 & 2 & 6 & 5 & 1 & 4 \end{pmatrix}.$$

It is easy to check that H is log-Hadamard (i.e. the entry-wise exponential $[e^{2i\pi h_{j,k}}]_{j,k}$ is complex-Hadamard).

Next, we observe that there exist integer matrices A and L of size 3×6 and 6×3, respectively, such that $8H = LA \pmod 8$. A possible example of such a decomposition is the following:

$$A := \begin{pmatrix} 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \\ 0 & 6 & 7 & 2 & 4 & 3 \end{pmatrix} \quad \text{and} \quad L := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 7 & 1 & 1 \end{pmatrix}.$$

This means that the set (of the columns of) A is spectral in the group $\mathcal{G} = \mathbb{Z}_8^3$. However, $|A| = 6$, therefore A cannot tile $\mathcal{G}$ due to obvious divisibility reasons. □

We now turn to the 'tile → spectral' direction of Fuglede's conjecture. Constructing counterexamples in finite groups causes considerably greater difficulties in this case. The reason for this is that the 'natural' properties and constructions of tiles are also shared by spectral sets, as described in Section 2.2.1. The breakthrough observation in [72] was that Propositions 2.2.16 and 2.2.17 are not *entirely* analogous. This observation led the authors to consider the following Universal Spectrum Conjecture of Lagarias and Wang.

Conjecture 2.2.22. (Universal Spectrum Conjecture [82]) *Assume $T \subset \mathcal{G}$ is a tile in a finite Abelian group. Then T possesses a "universal spectrum" $S \subset \hat{\mathcal{G}}$, i.e. a set S which is a common spectrum for all the tiling complements $T_1, \ldots, T_n$ of T.*

In [72] we first refuted the Universal Spectrum Conjecture in a particular finite group by a duality argument, and then proceeded to construct a non-spectral tile in an appropriate finite group. The transition to $\mathbb{Z}^5$ and $\mathbb{R}^5$ was achieved by using Corollary 2.2.13. Subsequently, the connection of Fuglede's conjecture and the Universal Spectrum conjecture was clarified in [40], and the dimension of the counterexample was lowered to 3. Here we will restrict our attention to the latter (stronger) results, but we emphasize that the credit for the first counterexample goes to [72].

Theorem 2.2.23. ([40]*) *For any dimension d, the Universal Spectrum Conjecture is valid for all finite groups $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ if and only if the 'tile $\rightarrow$ spectral' direction of Fugelede's conjecture is valid for all such groups.*

Proof. One direction of this statement is trivial. Namely, if T is a non-spectral tile in a group $\mathcal{G}$ then any tiling complement T' does not possess a universal spectrum in $\hat{\mathcal{G}}$.

Conversely, assume that we find a d-dimensional group $\mathcal{G} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d}$ and a tile $T \subset \mathcal{G}$ which does not have a universal spectrum. Let $k := |T|$ and $n := |\mathcal{G}|$. We will exhibit a non-spectral tile R in a larger group $\mathcal{G}_1 := \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_d} \times \mathbb{Z}_p$, where p is a large integer, relatively prime to $n_1, \ldots, n_d$. ($\mathcal{G}_1$ is isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{pn_d}$, so the dimension does not increase.) Note that $S \subset \hat{\mathcal{G}}$ is a universal spectrum of T if and only if $|S| = n/k$ and $S - S \subset \cap_{j=1}^{m} Z_{T_j'} \cup \{0\}$, where T_j' run through all possible tiling complements of T. By assumption T does not have a universal spectrum, which implies that for any set $S \subset \hat{\mathcal{G}}$, $|S| = n/k$ we have a "witness" $\mathbf{v}_S \in S - S$ such that $\mathbf{v}_S \notin \cap_j Z_{T_j'} \cup \{0\}$. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ denote the finite set of all such witnesses. Consider now the matrix

$$A = \begin{pmatrix} \hat{\chi}_{T_1'}(\mathbf{v}_1) & \hat{\chi}_{T_2'}(\mathbf{v}_1) & \cdots & \hat{\chi}_{T_m'}(\mathbf{v}_1) \\ \hat{\chi}_{T_1'}(\mathbf{v}_2) & \hat{\chi}_{T_2'}(\mathbf{v}_2) & \cdots & \hat{\chi}_{T_m'}(\mathbf{v}_2) \\ \vdots & & \ddots & \vdots \\ \hat{\chi}_{T_1'}(\mathbf{v}_r) & \hat{\chi}_{T_2'}(\mathbf{v}_r) & \cdots & \hat{\chi}_{T_m'}(\mathbf{v}_r) \end{pmatrix}.$$

We know that each row contains a non-zero entry. We now choose an integer vector $\mathbf{k} := (k_1, k_2, \ldots, k_m)^\top$ such that $A\mathbf{k} \neq 0$ and $k_1 + k_2 + \cdots + k_m = p$ is relatively prime to $n_1, n_2, \ldots, n_d$. (It is easy to see that such choice is possible, as the $A\mathbf{k} \neq 0$ condition means only an exclusion of r hyperplanes, and the relative prime condition means only an exclusion of a set of density strictly less than 1.)

We will now glue together the desired non-spectral tile $R \subset \mathcal{G}_1$ from several copies of the sets $T_1', \ldots, T_m'$. The idea is that we can consider $\mathcal{G}_1$ as p "layers" of $\mathcal{G}$ and we will copy the sets T_j' on different layers.

We can regard the elements of $\mathcal{G}_1$ as column vectors of length $d + 1$. (Note, however, that the dimension of $\mathcal{G}_1$ is still d as p was chosen relatively prime to

$n_1, \ldots, n_d$; in fact it would suffice that p is relatively prime to one them.) Also, the elements of $\hat{\mathcal{G}}$ can be regarded as row vectors, the action of a character $\gamma \in \hat{\mathcal{G}}$ on an element $\mathbf{x} \in \mathcal{G}$ being defined as $\gamma(\mathbf{x}) := e^{\sum_{j=1}^{d+1} \gamma_j x_j / n_j}$ (where $n_{d+1} := p$). Let $\mathbf{z}_j = (0, 0, \ldots, j)^\top$. For any set $A \subset \mathcal{G}$ the notation $\tilde{A}$ will stand for the set A extended by zero in the last coordinate. Let also $1 = \sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_p = m$ be a sequence of integers, the number i occurring exactly k_i times among σ_j (recall that $k_1 + k_2 + \cdots + k_m = p$). Consider the set

$$R = \bigcup_{j=1}^{p} \left(\mathbf{z}_j + \tilde{T'_{\sigma_j}} \right)$$

We claim that R is a tile in $\mathcal{G}_1$ and it is not spectral. It is clear that R tiles $\mathcal{G}_1$ because a tiling complement can be given as $\tilde{T}$.

Consider any set $L \subset \hat{\mathcal{G}}_1$, $|L| = |R|$ as a candidate for being a spectrum of R. By the pigeonhole principle there exist an $L_1 \subset L$, $|L_1| = n/k$ such that the last coordinates of the elements of L_1 are equal. Consider the set $\tilde{S}_1$ whose elements have the same coordinates as those of L_1 except for the last coordinate which is set to 0 in $\tilde{S}_1$. Then $\tilde{S}_1 - \tilde{S}_1 = L_1 - L_1 \subset L - L$. Consider now the witness $\mathbf{v}_{S_1}$ corresponding to S_1, and the extended vector $\tilde{\mathbf{v}_{S_1}}$. We have

$$\hat{\chi}_R(\tilde{\mathbf{v}_{S_1}}) = k_1 \cdot \hat{\chi}_{T'_1}(\mathbf{v}_{S_1}) + k_2 \cdot \hat{\chi}_{T'_2}(\mathbf{v}_{S_1}) + \cdots + k_m \cdot \hat{\chi}_{T'_m}(\mathbf{v}_{S_1}) \neq 0$$

by construction. This shows that R is not spectral in $\mathcal{G}_1$ and the proof is complete. □

Remark 2.2.24. One can also introduce the notion of *universal tiling complement*. A set $U \subset \hat{\mathcal{G}}$ is a universal tiling complement of $T \subset \mathcal{G}$ if U is a tiling complement in $\hat{\mathcal{G}}$ of all spectra of T.

Then one can prove the "dual" of the statement above, i.e., that all spectral sets are tiles in all d-dimensional finite groups if and only if all spectral sets possess universal tiling complements in all d-dimensional finite groups. In fact, one can use an analogous construction as above, building up layer by layer a spectral set which is not a tile in a larger group $\mathcal{G}_1 = \mathcal{G} \times \mathbb{Z}_p$ (to see that the constructed set does not tile $\mathcal{G}_1$ one needs to recall the Fourier condition $Z_T \cup Z_{T'} = \mathcal{G} \setminus \{0\}$ of tiling pairs). We do not give a detailed proof here as we will not need this result. However, we remark that the 1-dimensional case was studied recently in detail in [38], and it is very well possible that these considerations will be useful in producing 1 or 2 dimensional examples in the future. Let us also remark that the recent paper [37] clarifies all the existing implications among the two directions of the Fuglede conjecture, the Universal Spectrum Conjecture and the Universal Tiling Conjecture in the groups $\mathbb{Z}_n, \mathbb{Z}$ and $\mathbb{R}$. □

The result of the previous theorem shows that our task is reduced to finding a tile T of a 3-dimensional finite group $\mathcal{G}$ which does not have a universal spectrum. We will exhibit such a set in $\mathbb{Z}_{24}^3$. Unfortunately, it is not at all straightforward to check whether a set T possesses universal spectra or not. There is an elegant

sufficient condition for this by Lagarias and Szabó [80], which also turns out to be sufficient for the existence of a universal tiling complement:

Proposition 2.2.25. ([80], [40]*) *For a given set T in a finite group $\mathcal{G}$, if a set $S \subset \hat{\mathcal{G}}$ satisfies the conditions $|S| = |\mathcal{G}|/|T|$ and $S - S \subset Z_T^c$ then S is a universal spectrum of T, and also S is a universal tiling complement of T.*

Proof. Assume T' is a tiling complement of T. Then $Z_T^c \subset Z_{T'} \cup \{0\}$, and $|T'| = |\mathcal{G}|/|T| = |S|$. Therefore S is a spectrum of T' by condition (2.4).

Conversely, assume that L is any spectrum of T. Then $|L| \cdot |S| = \hat{\mathcal{G}}$ and $L - L \cap S - S = \{0\}$, because $L - L \subset Z_T \cup \{0\}$ and $S - S \subset Z_T^c$. It follows that $L + S = \hat{\mathcal{G}}$. □

In fact, in [80] it is tentatively conjectured that the existence of such set S is also a necessary condition for the existence of universal spectrum. If it were so, we could simply use the duality argument of [72] to produce a set without universal spectrum in $\mathcal{G} = \mathbb{Z}_{24}^3$. The idea is to use the *mod 8* log-Hadamard matrix H given in the proof of Theorem 2.2.21. Then, one can define a spectral set T_1 in $\mathbb{Z}_{24}^3$ with spectrum L as follows (again the columns are the elements of $\mathcal{G}$, while the rows correspond to elements of the dual group $\hat{\mathcal{G}}$)

$$T_1 := \begin{pmatrix} 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \\ 0 & 6 & 7 & 2 & 4 & 3 \end{pmatrix} \quad \text{and} \quad L := 3 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 7 & 1 & 1 \end{pmatrix}.$$

Note that $24H = LT_1$ *mod 24*, therefore L is indeed a spectrum of T_1 in $\mathcal{G}$. Note also, that L is contained in the subgroup of elements whose coordinates are all divisible by 3. This subgroup has 8^3 elements, hence L cannot tile this subgroup due to obvious divisibility reasons, and therefore L cannot tile $\hat{\mathcal{G}}$ either, by Lemma 2.2.14.

On the other hand, it is not hard to see that T_1 tiles $\mathcal{G}$ (this can be seen e.g. via the homomorphism $\varphi : \mathcal{G} \to \mathbb{Z}_{24}$ induced by the row vector $(2, 9, 3)$), but the existence of a set $S \subset \hat{\mathcal{G}}$, $|S| = 24^3/6$ and $S - S \subset Z_{T_1}^c$ is impossible due to the following reason: such an S would be a tiling complement of L by Proposition 2.2.25, which is impossible as L does not tile $\hat{\mathcal{G}}$.

If the sufficient condition of Proposition 2.2.25 were also necessary then we could conclude that T_1 does not have a universal spectrum in $\mathcal{G}$. However, it was shown in the Appendix of [40], by means of a particular example, that the condition of Proposition 2.2.25 is not necessary. Of course it still might happen that the set T_1 above does not have a universal spectrum but, in any case, we are unable to check it at the time of writing. (In general, even the elegant sufficient condition of Proposition 2.2.25 seems to be hard to check algorithmically in large groups, let alone finding all tiling complements of a given set.) The failure of the necessity of the Lagarias–Szabó condition poses some difficulty in checking whether a set possesses universal spectra, and therefore presents an obstacle to finding a 3-dimensional counterexample to

Fuglede's conjecture. We will use ideas of Farkas and Révész [41] to overcome this difficulty. The observation is that we are free to add $+8$ or $+16$ to the entries of T_1 without ruining the decomposition $24H = LT_1$ *mod 24*. We must find an alteration T of T_1 such that the existence of a universal spectrum of T can be excluded.

Proposition 2.2.26. ([40]*) *The set*

$$T := \begin{pmatrix} 0 & 10 & 20 & 1 & 21 & 14 \\ 0 & 22 & 3 & 20 & 2 & 7 \\ 0 & 22 & 23 & 18 & 4 & 11 \end{pmatrix}$$

is a tile in $\mathcal{G} = \mathbb{Z}_{24}^3$ which does not have a universal spectrum.

Proof. As observed before, the decomposition $24H = LT$ still holds, therefore L is a spectrum of T.

Consider all the *mod 24* vectors $\mathbf{v}_{ij} := \mathbf{l}_i - \mathbf{l}_j \in \hat{\mathcal{G}}$ where $\mathbf{l}_i, \mathbf{l}_j$ are arbitrary rows of the matrix L. For each such vector $\mathbf{v}_{ij}$ we will exhibit a tiling complement T'_{ij} of T in $\mathcal{G}$ in such a way that $\mathbf{v}_{ij} \notin Z_{T'_{ij}}$. Accepting the existence of such T'_{ij} for the moment, we can easily show that T does not have a universal spectrum. Indeed, if S were a universal spectrum, then $|S| = |\mathcal{G}|/|T|$ and $S - S \subset \cap_{ij} Z_{T'_{ij}} \cup \{0\}$ would hold, and therefore $S - S \cap L - L = \{0\}$ would follow. That is, $S + L$ would be a tiling of $\hat{\mathcal{G}}$, which is a contradiction because L is not a tile, as observed in the paragraph after the definition of L. It remains to show the existence of T'_{ij}.

Consider all possible *mod 8* differences $\mathbf{h}_i - \mathbf{h}_j$ of the rows of the integer matrix $8H$. Let $H - H$ denote the matrix containing these differences as row vectors. Now, regard $H - H$ as a *mod 24* matrix and modify the entries by $+8$ or $+16$ in such a way that each row becomes a tile in $\mathbb{Z}_{24}$, and also the *mod 3* rank of the resulting matrix P is 3. It will soon be apparent why these modifications are helpful in finding the sets T'_{ij}. We remark that the existence of such modifications appears to be pure luck. We give a possible example below:

$$H - H = \begin{pmatrix} 0&0&2&4&4&6\\ 0&0&4&2&6&4\\ 0&0&4&6&2&4\\ 0&0&6&4&4&2\\ 0&2&1&6&4&5\\ 0&2&4&1&5&6\\ 0&2&5&4&6&1\\ 0&2&6&5&1&4\\ 0&4&1&5&3&7\\ 0&4&2&6&6&2\\ 0&4&3&1&7&5\\ 0&4&5&7&1&3\\ 0&4&6&2&2&6\\ 0&4&7&3&5&1\\ 0&6&2&3&7&4\\ 0&6&3&4&2&7\\ 0&6&4&7&3&2\\ 0&6&7&2&4&3 \end{pmatrix} \longrightarrow \begin{pmatrix} 0&16&2&4&12&14\\ 0&16&12&2&14&4\\ 0&16&12&14&2&4\\ 0&16&14&12&4&2\\ 0&2&1&14&12&13\\ 0&2&12&1&13&14\\ 0&2&13&12&14&1\\ 0&2&14&13&1&12\\ 0&12&1&13&11&23\\ 0&12&2&22&14&10\\ 0&12&11&1&23&13\\ 0&12&13&23&1&11\\ 0&12&22&2&10&14\\ 0&12&23&11&13&1\\ 0&22&10&11&23&12\\ 0&22&11&12&10&23\\ 0&22&12&23&11&10\\ 0&22&23&10&12&11 \end{pmatrix} = P$$

It is easy to check that all required properties are fulfilled. In fact, each row of the modified matrix P has tiling complement $C_1 = \{0, 3, 6, 9\}$ or $C_2 = \{0, 1, 6, 7\}$ in $\mathbb{Z}_{24}$, and regarding P *mod 3* an easy Gaussian elimination shows that the 1^{st}, 2^{nd} and 4^{th} rows $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_4$ generate the others.

Observe that the set T above is defined in such a way that the rows coincide *mod 3* with $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_4$ (and, of course, the entries of T coincide *mod 8* with those of T_1).

Consider now an arbitrary row vector $\mathbf{v}_{ij} = \mathbf{l}_i - \mathbf{l}_j$. We will exhibit the existence of the required tiling complement T'_{ij}. For the sake of clarity we follow the proof through a particular example: let $\mathbf{v}_{31} = \mathbf{l}_3 - \mathbf{l}_1 = (3, 0, 0) - (0, 0, 0) = (3, 0, 0)$. Take the corresponding row $\mathbf{k}_i - \mathbf{k}_j$ of $H - H$, i.e., $\mathbf{k}_3 - \mathbf{k}_1 = (0, 2, 4, 1, 5, 6)$ in our particular case. Consider the corresponding row $\mathbf{p}_{ij}$ of the matrix P, i.e., $(0, 2, 12, 1, 13, 14)$ in our case. We claim that there exists a *mod 24* row vector $\mathbf{y}_{ij}$ which is a solution of the equation $\mathbf{y}_{ij}T = \mathbf{p}_{ij}$ *mod 24*. Clearly, a solution of the same equation *mod 3* exists, as $\mathbf{p}_{ij}$ is in the linear span of the rows of T *mod 3* (recall that T was chosen in such a way that its rows generate *every* vector $\mathbf{p}_{ij}$ *mod 3*). In our case the *mod 3* solution is seen to be $(0, 2, 0)$. A solution of the same equation *mod 8* is simply obtained by dividing each entry of $\mathbf{v}_{ij}$ by 3, i.e., in our case a *mod 8* solution is $(3, 0, 0)/3 = (1, 0, 0)$. (This is because $\frac{1}{3}LT = 8H$ *mod 8*.) Then, a solution $\mathbf{y}_{ij}$ *mod 24* can easily be obtained from the *mod 3* and *mod 8* solutions; in our example it is $\mathbf{y}_{31} = (9, 8, 0)$.

Given such $\mathbf{y}_{ij}$ we can define a homomorphism $\varphi_{ij} : \mathbb{Z}_{24}^3 \to \mathbb{Z}_{24}$ by the formula $\varphi_{ij}(\mathbf{x}) := \langle \mathbf{y}_{ij}, \mathbf{x} \rangle$. This homomorphism takes the set T to the elements of the row $\mathbf{p}_{ij}$ by construction, and this resulting set tiles $\mathbb{Z}_{24}$ with complement $C_{ij} := C_1$ or $C_{ij} := C_2$ also by construction. In our example, $\varphi_{31}(T) = (0, 2, 12, 1, 13, 14)$, which tiles $\mathbb{Z}_{24}$ with complement $C_{31} := C_1 = \{0, 3, 6, 9\}$. Finally, the desired tiling complement T'_{ij} is defined as the pre-image of C_{ij} under φ_{ij}. Here we need to invoke

Lemma 2.2.15.

Thus, we define $T'_{ij} := \varphi^{-1}(C_{ij})$. It remains to check that $\mathbf{v}_{ij} \notin Z_{T'_{ij}}$. The point of the whole construction above is that we can now evaluate $\hat{\chi}_{T'_{ij}}(\mathbf{v}_{ij})$. Note that each homomorphism φ_{ij} is easily seen to be surjective (indeed, a homomorphism $\varphi(x,y,z) := \langle (a,b,c),(x,y,z)\rangle$ is *not* surjective if and only if a,b,c are all even or all are divisible by 3; whereas our vectors are not of this type). Therefore every element in $\mathbb{Z}_{24}$ has 24^2 pre-images in $\mathbb{Z}_{24}^3$. Observe that $3\mathbf{y}_{ij} = \mathbf{v}_{ij}$ *mod 24*, hence for any $\mathbf{x} \in T'_{ij}$ we have $\langle \mathbf{v}_{ij}, \mathbf{x}\rangle \in 3C_{ij}$. Let $\rho = (1+i)/\sqrt{2}$ denote the first 8^{th} root of unity. Then

$$\hat{\chi}_{T'_{ij}}(\mathbf{v}_{ij}) = \sum_{\mathbf{x}\in T'_{ij}} e^{2\pi i/24\langle \mathbf{v}_{ij},\mathbf{x}\rangle} = \sum_{\mathbf{x}\in T'_{ij}} e^{2\pi i/24\langle 3\mathbf{y}_{ij},\mathbf{x}\rangle} = \sum_{\mathbf{x}\in T'_{ij}} e^{2\pi i/8\langle \mathbf{y}_{ij},\mathbf{x}\rangle} = 24^2 \sum_{k\in C_{ij}} \rho^k \neq 0.$$

The last sum is non-zero as $\rho^0+\rho^3+\rho^6+\rho^9 \neq 0$ and $\rho^0+\rho^1+\rho^6+\rho^7 \neq 0$. □

Putting together Proposition 2.2.26, Theorem 2.2.23, and Corollary 2.2.13 we obtain a 3-dimensional counterexample to Fuglede's "tile → spectral" conjecture:

Theorem 2.2.27. ([40]*) *There exists an appropriate finite union of unit cubes in* $\mathbb{R}^3$ *which tiles the space but which is not spectral.*

Remark 2.2.28. At present, all known counterexamples to Fuglede's conjecture (in either direction, and in any dimensions) have their origins in the existence of complex Hadamard matrices with certain properties. It is conceivable that a tile having no universal spectrum (or a spectral set having no universal tiling complement) can be exhibited in a 1 or 2 dimensional finite group without any reference to Hadamard matrices. By the results of this section such an example would immediately lead to a counterexample to (the corresponding direction of) Fuglede's conjecture. The 1-dimensional case seems particularly interesting, as it is related to the conjecture of Coven and Meyerowitz. In search of a tile without universal spectrum we have conducted some numerical experiments in several cyclic groups. The main difficulty is the lack of quick algorithms for deciding whether a set is a tile, and whether it has universal spectrum. Given the lack of such algorithms we were unable to search large groups exhaustively, but our "sporadic" tests indicate that such examples, if they exist at all, are to be found in cyclic groups of fairly large order. □

2.3 Construction of complex Hadamard matrices via tiling

This section describes a beautiful example of how seemingly distant parts of mathematics are related to each other. In the previous sections we have seen that Fuglede's conjecture fails *in general*. However, there are several special cases in which the conjecture is true, and we can make use of this connection between tiles and spectral sets in an interesting manner. Namely, we have seen that spectral sets are directly related complex Hadamard matrices, and therefore there is some hope that peculiar tiling constructions will lead to the discovery of new complex Hadamard matrices. This is the content of this section.

Hadamard matrices, real or complex, appear in several branches of mathematics such as combinatorics, Fourier analysis and quantum information theory. Various applications in quantum information theory have raised recent interest in *complex* Hadamard matrices.

One example, taken from quantum tomography, is the problem of existence of *mutually unbiased bases*, which is known to be a question on the existence of certain complex Hadamard matrices. The existence of $d + 1$ such bases is known for any prime power dimension d, but the problem remains open for all non prime power dimensions, even for $d = 6$ (for a more detailed exposition of this example see the Introduction of [131]). We will return to this problem in detail in Section 3.2.

Other important questions in quantum information theory, such as construction of teleportation and dense coding schemes, are also based on complex Hadamard matrices. Werner in [141] proved that the construction of bases of maximally entangled states, orthonormal bases of unitary operators, and unitary depolarizers are all equivalent in the sense that a solution to any of them leads to a solution to any other, as well as to a corresponding scheme of teleportation and dense coding. A general construction procedure for orthonormal bases of unitaries, involving complex Hadamard matrices, is also presented in [141].

On the one hand, it seems to be impossible to give any complete, or satisfactory *characterization* of complex Hadamard matrices of high order. On the other hand, we can hope to give fairly *general constructions* producing large families of Hadamard matrices, and we can also hope to characterize Hadamard matrices of small order (currently a full characterization is available only up to order 5). A recent paper by Dita [35] describes a general construction which leads to parametric families of complex Hadamard matrices in composite dimensions. Another recent paper by Tadej and Życzkowski [131] gives an (admittedly incomplete) *catalogue* of complex Hadamard matrices of *small order* (up to order 16).

The aim of this section is to show how tiling constructions of Abelian groups can lead to constructions of complex Hadamard matrices, and in this way to complement the catalogue of [131] with new parametric families. In particular, we first show how Dita's construction can be arrived at via a natural tiling construction (this part does not lead to new results, but it is an instructive example of how tiling and Hadamard matrices are related). Second, we observe some regularities satisfied by all Dita-type matrices, and thus arrive at an effective method to decide whether a given complex Hadamard matrix is of Dita-type. Then we use a combinatorial tiling construction due to Szabó [126] to produce Hadamard matrices *not of Dita-type*, and complement the catalogue of [131] with *new parametric families* of order 8, 12 and 16.

2.3.1 Recovering Dita's construction via tiling

One approach to tackle Fuglede's conjecture was to look for 'canonical' constructions for tilings of Abelian groups, and see whether similar constructions work also for spectral sets. This, indeed, turned out to be the case for the very general construction of Proposition 2.2.16. The spectral counterpart of this construction is

given in Proposition 2.2.17, and it leads directly to Dita's construction of complex Hadamard matrices.

Let us recall the most general form of Dita's construction, formula (12) in [35] (his subsequent results on parametric families of complex Hadamard matrices with some free parameters follow easily from this formula, as described very well in Proposition 3 and Theorem 2 of [35]).

$$K := \begin{bmatrix} m_{11}N_1 & \cdot & \cdot & m_{1k}N_k \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ m_{k1}N_1 & \cdot & \cdot & m_{kk}N_k \end{bmatrix} \tag{2.10}$$

In this formula Dita assumes m_{ij} to be the entries of any $k \times k$ complex Hadamard matrix M, while N_j are any $n \times n$ complex Hadamard matrices (possibly different from each other). Then he shows that K is a complex Hadamard matrix of order kn. While this construction is fairly natural (a less general construction was given earlier in [54]), we remark that it is so powerful that it leads to most of the parametric families included in [131].

Definition 2.3.1. *A complex Hadamard matrix K is called Dita-type if it is equivalent to a matrix arising with formula* (2.10)*. Here we use the standard notion of equivalence of Hadamard matrices (see e.g. [131]), i.e. K_1 and K_2 are equivalent if $K_1 = D_1P_1K_2P_2D_2$ with unitary diagonal matrices D_1, D_2 and permutation matrices P_1, P_2.*

Recall now the set Γ of Proposition 2.2.17, and its spectrum Σ constructed in the proof. We see that the spectral pair (Σ, Γ) gives rise to a Dita-type complex Hadamard matrix in formula (2.9). We remark that the set Γ might well have many other spectra than Σ above (and other spectra might produce complex Hadamard matrices not of the Dita-type). There is no efficient algorithm known to list out all the spectra of a given set.

Proposition 2.2.17 remains in the finite group setting. This has the disadvantage that the entries of the arising complex Hadamard matrices are necessarily some Nth roots of unity. Therefore, in this way one cannot expect to obtain continuous parametric families of complex Hadamard matrices, such as the ones described in [35]. However, an obvious generalization of the construction of Proposition 2.2.17 works also in the infinite setting $\mathcal{G} = \mathbb{Z}^d$, $\hat{\mathcal{G}} = \mathbb{T}^d$, and it turns out that *every Dita-type matrix* arises in this manner (including the parametric families). The details are described in [94] but we do not include them here, as the basic idea is the same as in Proposition 2.2.17.

2.3.2 Other tiling constructions yield new families of complex Hadamard matrices

Once the connection between tilings and complex Hadamard matrices has been noticed, it is natural to look for tiling constructions other than that of Proposition 2.2.17 above, in the hope of producing new complex Hadamard matrices not of the

Dita-type. Furthermore, when a new complex Hadamard matrix M is discovered, the 'linear variation of phases' method of [131] gives hope to find new parametric affine families of complex Hadamard matrices stemming from M. This is exactly the route we are going to follow in this section. First, we show how a tiling method of Szabó [126] leads to complex Hadamard matrices not of the Dita-type. Then, stemming from these matrices, we produce new parametric families of order 8, 12, and 16 which complement the catalogue [131].

Let us now turn to the construction of Szabó [126]. Assume $\mathcal{G} = \mathbb{Z}_{p_1q_1} \times \mathbb{Z}_{p_2q_2} \times \mathbb{Z}_{p_3q_3}$ where $p_j, q_j \geq 2$. The idea of Szabó is to take the obvious tiling $\mathcal{G} = A + B$ where

$$A = \{0, 1, \dots p_1 - 1\} \times \{0, 1, \dots p_2 - 1\} \times \{0, 1, \dots p_3 - 1\} \tag{2.11}$$

and $B = \{0, p_1, \dots, (q_1 - 1)p_1\} \times \{0, p_2, \dots, (q_2 - 1)p_2\} \times \{0, p_3, \dots, (q_3 - 1)p_3\}$ and then modify the grid B by pushing three grid-lines in different directions (see [126] for details. Here we use the *analogous construction for spectral sets* which we now describe in detail (it may be easier to follow the general construction by looking at the specific Example 2.3.2 below).

Consider the set A above. By formula (2.4) a set $S \subset \widehat{\mathcal{G}}$ is a spectrum of A if and only if $|S| = |A|$ and $S - S \subset Z_A \cup \{0\} := \{\mathbf{r} \in \widehat{\mathcal{G}} : \widehat{\chi}_A(\mathbf{r}) = 0\} \cup \{0\}$ Recall that $\widehat{\mathcal{G}}$ is identified with 3-dimensional row vectors. It is clear that if $\mathbf{r} = (r_1, r_2, r_3) \in \widehat{\mathcal{G}}$ is such that q_1 divides r_1 and $r_1 \neq 0$ then $\widehat{\chi}_A(\mathbf{r}) = 0$. Similarly, if $q_2 | r_2 \neq 0$ or $q_3 | r_3 \neq 0$ then $\widehat{\chi}_A(\mathbf{r}) = 0$. Therefore the grid

$$S = \{0, q_1, \dots (p_1 - 1)q_1\} \times \{0, q_2, \dots (p_2 - 1)q_2\} \times \{0, q_3, \dots (p_3 - 1)q_3\} \tag{2.12}$$

is a spectrum of A. Using an analogous idea to that of Szabó we now modify this grid.

Consider the grid-line $L_1 := \{\{0, q_1, \dots (p_1 - 1)q_1\} \times \{q_2\} \times \{0\}$ and change it to $L_1' := \{1, q_1 + 1, \dots (p_1 - 1)q_1 + 1\} \times \{q_2\} \times \{0\}$ (adding $+1$ to the first coordinates). Similarly, change $L_2 := \{0\} \times \{0, q_2, \dots (p_2 - 1)q_2\} \times \{q_3\}$ to $L_2' := \{0\} \times \{1, q_2 + 1, \dots (p_2 - 1)q_2 + 1\} \times \{q_3\}$, and change $L_3 := \{q_1\} \times \{0\} \times \{0, q_3, \dots (p_3 - 1)q_3\}$ to $L_3' := \{q_1\} \times \{0\} \times \{1, q_3 + 1, \dots (p_3 - 1)q_3 + 1\}$. It is easy to see that

$$S' := S \cup (L_1' \cup L_2' \cup L_3') \setminus (L_1 \cup L_2 \cup L_3) \tag{2.13}$$

is still a spectrum of A. Indeed, for any $\mathbf{r} \in S' - S'$ it still holds that either the first coordinate is divisible by q_1 or the second by q_2 or the third by q_3. Then the spectral pair (A, S') gives rise to a complex Hadamard matrix of size $p_1p_2p_3$. Below we will apply this construction in the groups $\mathcal{G}_1 = \mathbb{Z}_{2\cdot2} \times \mathbb{Z}_{2\cdot2} \times \mathbb{Z}_{2\cdot2}$, $\mathcal{G}_2 = \mathbb{Z}_{2\cdot2} \times \mathbb{Z}_{2\cdot2} \times \mathbb{Z}_{3\cdot3}$ and $\mathcal{G}_3 = \mathbb{Z}_{2\cdot2} \times \mathbb{Z}_{4\cdot2} \times \mathbb{Z}_{2\cdot4}$ (it may be instructive to see the step-by-step numerical exposition of the construction in Example 2.3.2 in group $\mathcal{G}_1$ below).

We will then prove that these matrices are *not of the Dita-type*. (It would be very interesting to see a proof of a general statement that all matrices arising with the above construction are non-Dita-type.) As a result we will conclude that these matrices have not been included in the catalogue [131].

We can see from the construction above that the *size* of the arising matrix is $p_1p_2p_3$, while the numbers q_1, q_2, q_3 are chosen arbitrarily to determine the group we are working in. It is not clear whether different choices of q_1, q_2, q_3 lead to non-equivalent Hadamard matrices. Here we only list the three examples for which the dimension is not greater than 16 (as in [131]) and for which we can *prove* that the arising matrices are new, i.e. non-equivalent to any matrix listed in [131].

Example 2.3.2. Let us follow the construction above, step by step, in $\mathcal{G}_1 = \mathbb{Z}_{2\cdot 2} \times \mathbb{Z}_{2\cdot 2} \times \mathbb{Z}_{2\cdot 2} = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

By (2.11) we take $A = \{0,1\} \times \{0,1\} \times \{0,1\}$. This is a Cartesian product, each element of which is a 3-dimensional vector composed of 0's and 1's. We list out the elements in lexicographical order as

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \tag{2.14}$$

where the columns represent the elements of $A \subset \mathcal{G}_1$, in accordance with our notation introduced earlier. (The order of the elements is up to our choice, but a permutation of the elements only corresponds to a permutation of the columns of the matrix S_8 below.)

Then, by equation (2.12) we have $S = \{0,2\} \times \{0,2\} \times \{0,2\}$, which we list out (also in lexicographical order) as

$$S = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \\ 0 & 2 & 2 \\ 2 & 0 & 0 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \\ 2 & 2 & 2 \end{bmatrix} \tag{2.15}$$

Now, S is a spectrum of A, therefore the product $\frac{1}{4}SA$ already gives a log-Hadamard matrix but we do not take that matrix (which *is* Dita-type, as can be verified by the reader), but modify the set S first. The grid-line L_1 in S is given as $L_1 = \{0,2\} \times \{2\} \times \{0\} = \{(0,2,0);(2,2,0)\}$. This we replace by $L_1' = \{(1,2,0);(3,2,0)\}$. Similarly, the grid-line $L_2 = \{(0,0,2);(0,2,2)\}$ is replaced by $L_2' = \{(0,1,2);(0,3,2)\}$ and finally $L_3 = \{(2,0,0);(2,0,2)\}$ by $L_3' =$

$\{(2,0,1);(2,0,3)\}$. Therefore, by (2.13) we get

$$S' = S \cup (L_1' \cup L_2' \cup L_3') \setminus (L_1 \cup L_2 \cup L_3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 3 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 2 & 0 & 3 \\ 2 & 2 & 2 \\ 3 & 2 & 0 \end{bmatrix} \tag{2.16}$$

(Once again, the order of the elements of S' is arbitrary, and we take lexicographical order.) The point, as explained above in the general description of this construction, is that the set S' is still a spectrum of A. Therefore the matrix product $\frac{1}{4}S'A$ is a log-Hadamard matrix (we reduce the entries *mod* 1 because the integer part of an entry plays no role after exponentiation) given by:

$$\frac{1}{4}S'A = \log S_8 = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 0 & 2 & 1 & 3 \\ 0 & 2 & 3 & 1 & 0 & 2 & 3 & 1 \\ 0 & 0 & 2 & 2 & 1 & 1 & 3 & 3 \\ 0 & 1 & 0 & 1 & 2 & 3 & 2 & 3 \\ 0 & 3 & 0 & 3 & 2 & 1 & 2 & 1 \\ 0 & 2 & 2 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 & 3 & 1 & 1 \end{bmatrix} \tag{2.17}$$

with the corresponding complex Hadamard matrix given by

$$S_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathbf{i} & -\mathbf{i} & 1 & -1 & \mathbf{i} & -\mathbf{i} \\ 1 & -1 & -\mathbf{i} & \mathbf{i} & 1 & -1 & -\mathbf{i} & \mathbf{i} \\ 1 & 1 & -1 & -1 & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} \\ 1 & \mathbf{i} & 1 & \mathbf{i} & -1 & -\mathbf{i} & -1 & -\mathbf{i} \\ 1 & -\mathbf{i} & 1 & -\mathbf{i} & -1 & \mathbf{i} & -1 & \mathbf{i} \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} \end{bmatrix} \tag{2.18}$$

□

Having described how to produce the matrix S_8 the remaining questions are whether S_8 is new (i.e. not already included in the catalogue [131]), and whether any parametric family of complex Hadamard matrices stems from S_8.

We will first proceed to show that S_8 is *not Dita-type* (nor is it its transpose). This is a delicate matter, as not many criteria are known to decide inequivalence of Hadamard matrices. The Haagerup condition with the invariant set $\Lambda := \{h_{ij}\overline{h}_{kj}h_{kl}\overline{h}_{il}\}$ (see [54] and Lemma 2.5 in [131]) cannot be used here. Also, the elegant characterization of equivalence classes of Kronecker products of Fourier matrices [130] does not apply to S_8. The 'regular' structure of a Dita-type matrix must

be exploited in some way. The key observation relies on the following definition.

Definition 2.3.3. *Let L be an $N \times N$ real matrix. For an index set $I = \{i_1, i_2, \ldots, i_n\} \subset \{1, 2, \ldots, N\}$ two rows (or columns) $\mathbf{s}$ and $\mathbf{q}$ are called I-equivalent, in notation $\mathbf{s} \sim_I \mathbf{q}$, if the fractional part of the entry-wise differences $s_i - q_i$ are the same for every $i \in I$ (we need to consider fractional parts as the entries of a log-Hadamard matrix are defined only mod 1). Two rows (or columns) $\mathbf{s}$ and $\mathbf{q}$ are called (d)-n-equivalent if there exist n-element disjoint sets of indices $I_1, \ldots, I_d$ such that $\mathbf{s} \sim_{I_j} \mathbf{q}$ for all $j = 1, \ldots, d$.*

We have the following trivial observation.

Proposition 2.3.4. ([94]*) *Let L be an $N \times N$ complex Hadamard matrix. Assume that there exists an index set $I = \{i_1, i_2, \ldots, i_n\} \subset \{1, 2, \ldots, N\}$ and m different rows (resp. columns) $\mathbf{r}_{s_1}, \ldots \mathbf{r}_{s_m}$ in the log-Hadamard matrix $\log L$ such that each two of them are I-equivalent. Let M be any complex Hadamard matrix equivalent to L. Then the same property holds for $\log M$, i.e. there exists an index set $J = \{j_1, j_2, \ldots, j_n\} \subset \{1, 2, \ldots, N\}$ and m different rows (resp. columns) $\mathbf{r}_{k_1}, \ldots \mathbf{r}_{k_m}$ such that each two of them are J-equivalent. (Of course, the index sets I and $\{s_1, \ldots s_m\}$ might not be the same as J and $\{k_1, \ldots k_m\}$.)*

Proof. It follows from the definition of the equivalence of Hadamard matrices that $\log M$ is obtained from $\log L$ by permutation of rows and columns, and addition of constants to rows and columns. It is clear that such operations preserve the existing equivalences between rows and columns (with the index sets being altered according to the permutations used). □

The essence of the proposition is that *"existing equivalences between rows and columns are retained"*. The next main point is that there are many equivalences among the rows of a Dita-type matrix and we will see that such equivalences are not present in $\log S_8$.

By formula (2.10), the structure of an $N \times N$ Dita-type matrix D (where $N = nk$) implies for the log-Hadamard matrix $\log D$ that there exists a partition of indices to n-element sets $I_1 = \{1, 2, \ldots n\}, \ldots, I_k = \{(k-1)n + 1, \ldots kn\}$ and k-tuples of rows $R_j = \{\mathbf{r}_j, \mathbf{r}_{j+n} \ldots \mathbf{r}_{j+(k-1)n}\}$ $(j = 1, \ldots n)$ such that any two rows in a fixed k-tuple are equivalent with respect to any of the I_m's, i.e. $\mathbf{r}_{j+(i-1)n} \sim_{I_m} \mathbf{r}_{j+(s-1)n}$ for all $j = 1, \ldots n$, and $i, s, m = 1, \ldots k$. In other words, in any k-tuple R_j any two rows are (k)-n-equivalent with respect to the I_m's. We will use the terminology (k)-n-*Dita-type* for such matrices D. Naturally, the same property holds for the transposed of a (k)-n-Dita-type matrix, with the role of rows and columns interchanged.

This observation makes it possible to prove the following proposition.

Proposition 2.3.5. ([94]*) *S_8 and its transposed are not Dita-type.*

Proof. The matrix size being 8×8 the only possible values for n are 2 and 4 (with k being 4 and 2, respectively). Therefore we only need to check existing (2)-4-equivalences and (4)-2-equivalences in $\log S_8$ and its transposed.

First, let us assume that $n = 4, k = 2$ and look for (2)-4-equivalences among the rows of $\log S_8$. If S_8 were (2)-4-Dita type, there should be a partition of indices to

two 4-element sets I_1, I_2 such that in $\log S_8$ four pairs of rows are equivalent with respect to I_1, I_2. The first row $\mathbf{r}_1$ of $\log S_8$ consists of zeros only, therefore it must be paired with a row containing only two different values. There is only one such row $\mathbf{r}_7$ and then the index sets must correspond to the position of 0's and 2's in $\mathbf{r}_7$, i.e. $I_1 = \{1, 4, 6, 7\}$ and $I_2 = \{2, 3, 5, 8\}$. However, there should exist *three further pairs of rows* which are equivalent with respect to the same set of indices I_1, I_2. It is easy to check that such pairs do not exist (e.g. the second row $\mathbf{r}_2$ is not (2)-4-equivalent with respect to I_1, I_2 to any other row), and hence S_8 cannot be (2)-4-Dita type.

To check the transposed matrix we interchange the role of rows and columns and see that the first column $\mathbf{c}_1$ of $\log S_8$ (all zeros) should be paired with a column containing two values only. But such column does not exist, therefore $\mathbf{c}_1$ is not (2)-4-equivalent to any other column, and hence the transposed of S_8 cannot be (2)-4-Dita type.

Let us turn to the case $n = 2, k = 4$. If S_8 were (4)-2-Dita type, there should be a partition of indices to four 2-element sets I_1, I_2, I_3, I_4 such that in $\log S_8$ two 4-tuples of rows $R_1 = \{\mathbf{r}_{s_1}, \ldots, \mathbf{r}_{s_4}\}$ and $R_2 = \{\mathbf{r}_{s_5}, \ldots, \mathbf{r}_{s_8}\}$ are equivalent with respect to I_1, I_2, I_3, I_4. Assume, without loss of generality that $1 \in I_1$ (i.e. $I_1 = \{1, m\}$ for some m) and that $\mathbf{r}_{s_1} = \mathbf{r}_1$. Then $\mathbf{r}_{s_2}, \mathbf{r}_{s_3}, \mathbf{r}_{s_4}$ are I_1-equivalent to $\mathbf{r}_1$ which implies that there should be a 4×2 block of 0's in $\log S_8$ corresponding to R_1 and I_1, i.e. $[\log S_8]_{i,j} = 0$ for all $i \in R_1$ and $j \in I_1$. Such block of 0's does not exist, therefore S_8 is not (4)-2-Dita-type.

In the transposed case there exists such a 2×4 block of zeros, corresponding to the row indices $I_1 = \{1, 7\}$ and column indices $C_1 = \{1, 4, 6, 7\}$. This means that there should be further two-element index sets I_2, I_3, I_4 such that the columns $\{c_1, c_4, c_6, c_7\}$ are equivalent with respect to I_2, I_3, I_4. It is trivial to check that such indices do not exist. This concludes the proof that S_8 and its transposed are not Dita-type. □

The significance of this fact is that the *only known* 8×8 *parametric family of complex Hadamard matrices so far is the one constructed by Dita's method* (see [131]). It is an affine family $F_8^{(5)}(a, b, c, d, e)$ containing 5 free parameters. We have established that this family does not go through S_8, therefore S_8 is indeed *new*. In particular, the matrix S_8 cannot be equivalent to any of the well-known tensor products of Fourier-matrices $F_2 \otimes F_2 \otimes F_2$, $F_4 \otimes F_2$, F_8 which are all contained in the family $F_8^{(5)}(a, b, c, d, e)$.

Now, applying to S_8 the linear variation of phases method of [131] one can hope to obtain new parametric families of complex Hadamard matrices. Indeed, we have been able to obtain (with the help of some computational contribution from W. Tadej) the following maximal affine 4-parameter family (the notation is used as in [131], i.e. the symbol $\circ$ denotes the Hadamard product of two matrices $[H_1 \circ H_2]_{i,j} = [H_1]_{i,j} \cdot [H_2]_{i,j}$, and the symbol EXP denotes the entrywise exponential operation $[EXP\ H]_{i,j} = exp([H]_{i,j})$): $S_8^{(4)}(a, b, c, d) = S_8 \circ EXP(\mathbf{i}R_8^{(4)}(a, b, c, d)$,

where

$$R_8^{(4)}(a,b,c,d) = \left[\begin{array}{cccccccc} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & d & a & a-d & d & \bullet & a-d & a \\ \bullet & d & a & a-d & d & \bullet & a-d & a \\ \bullet & d & d & \bullet & b & b-d & b-d & b \\ \bullet & c & d & c-d & d & c-d & \bullet & c \\ \bullet & c & d & c-d & d & c-d & \bullet & c \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & d & d & \bullet & b & b-d & b-d & b \end{array}\right] \tag{2.19}$$

We do not claim that each matrix in $S_8^{(4)}(a,b,c,d)$ is non-Dita-type (in fact, it is not hard to see that the orbit $S_8^{(4)}(a,b,c,d)$ contains the only real 8×8 Hadamard matrix H_8, which *is* Dita-type, so the families $F_8^{(5)}(a,b,c,d,e)$ and $S_8^{(4)}(a,b,c,d)$ *intersect* each other at H_8). However, this is certainly true in a small neighbourhood of S_8 as the set of Dita-matrices is closed.

In [94] the construction above was also carried out in the groups $\mathcal{G}_2 = \mathbb{Z}_{2\cdot 2}\times\mathbb{Z}_{2\cdot 2}\times \mathbb{Z}_{3\cdot 3}$ and $\mathcal{G}_3 = \mathbb{Z}_{2\cdot 2}\times\mathbb{Z}_{4\cdot 2}\times\mathbb{Z}_{2\cdot 4}$, to produce the 5-parameter family $R_{12}^{(5)}(a,b,c,d,e)$, and the 11-parameter family $R_{16}^{(11)}(a,b,c,d,e,f,g,h,i,j,k)$ of complex Hadamard matrices of order 12 and 16, respectively. We do not include the details here.

In principle, the method of [126] works in any finite Abelian group $\mathcal{G} = \mathbb{Z}_{p_1q_1}\times \mathbb{Z}_{p_2q_2}\times\mathbb{Z}_{p_3q_3}$ and the corresponding spectral sets yield complex Hadamard matrices of size $p_1p_2p_3$ for any $p_1,p_2,p_3 \geq 2$. It is not clear whether different choices of q_1,q_2,q_3 lead to non-equivalent matrices. In the paper [94] we only included the cases where $p_1p_2p_3 \leq 16$, and for which we could prove that the arising matrices are new and thus complement the catalogue [131]. It would be interesting to see a *conceptual* proof that the Hadamard matrices constructed with this method are *never Dita-type* (for the matrices S_8, S_{12}, S_{16} in [94] we proved this with the help of Proposition 2.3.4 by a case-by-case analysis of the rows and columns).

The correspondence between tilings and complex Hadamard matrices is interesting in its own right and may well lead to new families of Hadamard matrices in the future. To achieve this, one would need any new tiling construction (different from that of [72] and [126] which have been used in this section), and use the spectral set analogue of the construction to produce new Hadamard matrices.

3 The Fourier analytic version of Delsarte's method

The linear programming bound of Delsarte was first applied (to the best of my knowledge in [34]) in coding theory to the following problem: determine the maximal cardinality $A(n, d)$ of binary codewords of length n such that each two of them differ in at least d coordinates. In the past decades the method of Delsarte has been applied to several other problems, most notably to sphere packings [29], and the unit-distance graph of $\mathbb{R}^n$ [106].

In this work I will not describe Delsarte's method in its most general form (as far as i know, the most general form is given by commutative association schemes), but rather concentrate on a version which is general enough to encompass most of the applications but simple enough to require only elementary Fourier analysis.

Let $\mathcal{G}$ be a compact Abelian group (actually, it is best to think of a finite group, for simplicity), and let a symmetric subset $A = -A \subset \mathcal{G}$, $0 \in A$ be given. We will call A the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \dots b_m\} \subset \mathcal{G}$ such that all differences $b_j - b_k \in A^c \cup \{0\}$ (in other words, all differences avoid the forbidden set A).

In Section 3.1 we will describe the Fourier analytic version of Delsarte's bound. The maximal cardinality (or density, in non-compact cases) of the set B will be bounded above by constructing certain positive exponential sums using frequencies from the forbidden set A. After introducing the necessary notations Delsarte's linear programming bound will be given below as $\delta(A) \leq \lambda^-(A)$ in Theorem 3.1.4. We will then study the general properties and some theoretical limitations of the method. This section is based on [96].

In Section 3.2 we will apply Delsarte's method to give an improved upper bound on the independence number s of the Paley-graph $\mathcal{P}_p$, for a prime $p \equiv 1 \pmod 4$. In fact, the Delsarte bound, in itself, gives the trivial bound $s \leq \sqrt{p}$, only. However, a 'subgraph-trick', introduced in [106] in connection with the unit-distance graph of $\mathbb{R}^d$, will come to our help to achieve a slightly improved upper bound in Theorem 3.2.2. This section is based on [4]. However, the published version of [4] contains a simplification by I. Ruzsa which makes no reference to Delsarte's method. Here we include the original proof.

In Section 3.3 we give a surprising application of Delsarte's method to the problem of mutually unbiased bases (MUBs). Complex Hadamard matrices were already discussed in Section 2.3 in connection with spectral sets. It is also known that the existence of a complete system of MUBs is equivalent to the existence of certain complex matrices. In this section we will view complex Hadamard matrices as finite sets in the compact group $\mathbb{T}^d$, and apply Delsarte's method in this group. In Theorem 3.3.6 we will obtain a generalization of the fact that the maximal number of MUBs in dimension d cannot exceed $d + 1$. We also discuss the question whether a real Hadamard matrix can be part of a complete system of MUHs. While it is known to be possible for $d = 2^k$, we show that the presence of a real Hadamard matrix puts heavy constraints on the columns of the other matrices. In particular, Theorem 3.3.12 implies that it is impossible to have two real Hadamards in a complete system of MUHs. We will also prove in Theorem 3.3.15 that in dimension 6

the matrices of the Fourier family $F_(a, b)$ cannot be extended to a complete system of MUBs. This section is based on [92, 97].

In Section 3.4 we give a brief outlook on possible future applications of Delsarte's method.

3.1 General properties

In this section we give an overview of the Fourier analytic version of Delsarte's method. We establish general properties of the method for sets in finite Abelian groups.

Difference sets are always symmetric and contain 0; similarly, the spectrum of a positive exponential sum is symmetric and contains 0. This motivates the following definitions.

Definition 3.1.1. *Let $\mathcal{G}$ be a finite commutative group. We call a set $A \subset \mathcal{G}$ a* standard set*, if $A = -A$ and $0 \in A$ (i.e. we require that A be both symmetric and contain 0).*

Definition 3.1.2. *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A \subset \mathcal{G}$ be a standard set. Write*

$$\Delta(A) = \max\big\{|B| : B \subset \mathcal{G}, (B - B) \cap A = \{0\}\big\},$$
$$\overline{\Delta}(A) = \max\big\{|B| : B \subset \mathcal{G}, B - B \subset A\big\},$$

$$\delta(A) = \Delta(A)/q,$$
$$\overline{\delta}(A) = 1/\overline{\Delta}(A).$$

We call $\delta(A)$ the measure of intersectivity *of the set A.*

Next we list the quantities related to positive character sums. We fix our notation as follows. A *character* is a homomorphism into

$$\mathbb{C}_1 = \{z \in \mathbb{C} : |z| = 1\}.$$

The set of all characters is the *dual group* of $\mathcal{G}$, denoted by $\hat{\mathcal{G}}$. In this chapter we will use additive notation for $\mathcal{G}$ and multiplicative notation for $\hat{\mathcal{G}}$, and accordingly $\mathbf{1} \in \hat{\mathcal{G}}$ denotes the identity element of $\hat{\mathcal{G}}$, the principal character. This is different from the additive notation of $\hat{\mathcal{G}}$ used in Chapter 2, but our emphasis here is to make a clear distinction between elements of $\mathcal{G}$ and those of $\hat{\mathcal{G}}$.

The *Fourier transform* of a function f on $\mathcal{G}$ is defined as

$$\hat{f}(\gamma) = \sum_{x \in \mathcal{G}} \gamma(x) f(x).$$

We define certain classes of functions, whose behaviour on A and $\mathcal{G} \setminus A$ is prescribed in various senses. The notation $f \not\equiv 0$ means that f is not identically zero. Put

$$\begin{aligned}
\mathcal{S}(A) &= \left\{ f : \mathcal{G} \to \mathbb{R}, f \not\equiv 0, f|_{\mathcal{G}\setminus A} = 0 \right\}, \\
\mathcal{S}^-(A) &= \left\{ f : \mathcal{G} \to \mathbb{R}, f \not\equiv 0, f|_{\mathcal{G}\setminus A} \leq 0 \right\}, \\
\mathcal{S}^+(A) &= \left\{ f : \mathcal{G} \to \mathbb{R}, f \not\equiv 0, f|_{\mathcal{G}\setminus A} = 0, f|_A \geq 0 \right\}, \\
\mathcal{S}^\pm(A) &= \left\{ f : \mathcal{G} \to \mathbb{R}, f \not\equiv 0, f|_{\mathcal{G}\setminus A} \leq 0, f|_A \geq 0 \right\}.
\end{aligned}$$

These classes of functions are used to define the relevant quantities in relation with positive exponential sums.

Definition 3.1.3. *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A \subset \mathcal{G}$ be a standard set. Write*

$$\lambda(A) = \min \left\{ \frac{f(0)}{\hat{f}(\mathbf{1})} : f \in \mathcal{S}(A), \hat{f}(\gamma) \geq 0 \text{ for all } \gamma \right\},$$

$$\lambda^-(A) = \min \left\{ \frac{f(0)}{\hat{f}(\mathbf{1})} : f \in \mathcal{S}^-(A), \hat{f}(\gamma) \geq 0 \text{ for all } \gamma \right\},$$

$$\lambda^+(A) = \min \left\{ \frac{f(0)}{\hat{f}(\mathbf{1})} : f \in \mathcal{S}^+(A), \hat{f}(\gamma) \geq 0 \text{ for all } \gamma \right\},$$

$$\lambda^\pm(A) = \min \left\{ \frac{f(0)}{\hat{f}(\mathbf{1})} : f \in \mathcal{S}^\pm(A), \hat{f}(\gamma) \geq 0 \text{ for all } \gamma \right\}.$$

Sometimes $\lambda(A)$ is called the Turán constant*, $\lambda^-(A)$ the* Delsarte constant *of the set A (for the history of these names and some related problems see [111]).*

Of these quantities $\lambda^\pm$ seems to be the least interesting, as it has not yet come up in any applications to the best of our knowledge. We include it to exhaust all possible combinations of restrictions on A and $\mathcal{G} \setminus A$. Seemingly these definitions depend on the ambient group $\mathcal{G}$; in the next section we will show that this is not the case, so the notations are justified.

We shall study inequalities between these numbers; how they change under set-theoretical operations (union, intersection, complement, direct product); and how they behave for a random set.

The main inequality connecting the various δ and λ quantities is the following.

Theorem 3.1.4. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A \subset \mathcal{G}$ be a standard set. We have*

$$1/q \leq \delta(A) \leq \lambda^-(A) \leq \left\{ \begin{matrix} \lambda(A) \\ \lambda^\pm(A) \end{matrix} \right\} \leq \lambda^+(A) \leq \overline{\delta}(A) \leq 1. \tag{3.1}$$

All the inequalities can hold with equality, as well as with strict inequality. There is no inequality between $\lambda(A)$ and $\lambda^\pm(A)$; each can be greater than the other, and they can also be equal.

The inequality $\delta(A) \le \lambda^-(A)$ above is usually referred to as *Delsarte's bound*. We will prove this theorem in Section 3.1.2. The main unsolved problem is whether there is any connection between these quantities in the other direction.

Problem 3.1.5. ([96]) *Is there a function $f : [0,1] \to [0,1]$ such that $f(x) \to 0$ as $x \to 0$ and we have always $\lambda^-(A) \le f\big(\delta(A)\big)$? Is there such a function for which we have always $\lambda(A) \le f\big(\lambda^-(A)\big)$?*

This question can be asked for any other pair of the quantities defined above. We have the following partial answer.

Theorem 3.1.6. ([96]*)

(a) Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and assume that $3 \nmid q$. There is a standard set $A \subset \mathcal{G}$ such that $\overline{\delta}(A) = 1/2$ and

$$\lambda^+(A) \le cq^{-1/6}(\log q)^{1/2},$$

with an absolute constant c.

(b) Let $\varepsilon > 0$. For every sufficiently large n there is a standard set $A \subset \mathbb{Z}_2^n$ such that

$$\lambda(A) < \varepsilon,\ \lambda^{\pm}(A) > 1/2 - \varepsilon.$$

(c) Let $\varepsilon > 0$. For infinitely many values of q there is a standard set $A \subset \mathbb{Z}_q$ such that

$$\delta(A) < \varepsilon,\ \lambda^+(A) > 1/2 - \varepsilon.$$

We will prove part (a) of this theorem in Section 3.1.8 and part (b) in Section 3.1.9. Part (c) is essentially a theorem of Bourgain [20] Bourgain's setting and terminology is quite different from ours. We do not give an account of his method in the hope that the stronger result in part (b) can also be extended to cyclic groups. We also remark here that the most difficult part in the proof of part (b) is a result of Samorodnitsky [118]; more details are given in Section 3.1.9.

Most of the defined quantities make sense also in infinite groups; the exception is δ, whose definition involves division by q. Here the proper generalization involves a concept of density; a very general formulation in locally Abelian groups can be found in a paper of Révész [111]. Here we restrict our attention to the finite case.

It seems to be difficult to say anything nontrivial about the cases of equality in Theorem 3.1.4. However, the extremal values are easily described.

Proposition 3.1.7. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A \subset \mathcal{G}$ be a standard set.*

(a) If $A = \mathcal{G}$, then

$$\delta(A) = \lambda^-(A) = \lambda(A) = \lambda^{\pm}(A) = \lambda^+(A) = \overline{\delta}(A) = 1/q. \tag{3.2}$$

In any other case $\delta(A) \ge 2/q$.

(b) If $A = \{0\}$, then

$$\delta(A) = \lambda^-(A) = \lambda(A) = \lambda^{\pm}(A) = \lambda^+(A) = \overline{\delta}(A) = 1. \tag{3.3}$$

In any other case $\overline{\delta}(A) \leq 1/2$.

Both statements are immediate consequences of the definitions.

3.1.1 Invariance properties

In Definition 3.1.2 and 3.1.3 the ambient group $\mathcal{G}$ occurs. A set A may be a subset of several groups (they being subgroups of a common group), and the definitions could, in principle, return different values. We show here that this is not the case, hence our notations $\delta(A)$, $\lambda(A)$, etc. are justified.

To formulate the results rigorously we temporarily extend the notation and write $\delta(A, \mathcal{G})$, $\lambda(A, \mathcal{G}), \ldots$, instead. Also, it will be convenient to introduce the following general notation.

Definition 3.1.8. *If X is a subset of Y, and $f : Y \to \mathbb{R}$ is a function on Y then f_X denotes the restriction of f to X. Conversely, if $g : X \to \mathbb{R}$ is a function on X then g^Y denotes the extension of g to Y with value 0 outside X.*

Proposition 3.1.9. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $\mathcal{G}_1, \mathcal{G}_2$ finite subgroups of $\mathcal{G}$, and $A \subset \mathcal{G}_1 \cap \mathcal{G}_2$ a standard set. Let φ be any of the functionals $\delta, \overline{\delta}, \lambda, \lambda^-, \lambda^+, \lambda^\pm$. We have*

$$\varphi(A, \mathcal{G}_1) = \varphi(A, \mathcal{G}_2).$$

Proof. The claim is obvious for $\overline{\delta}$: in the definition of $\overline{\Delta(A)}$ one can assume that $0 \in B$ (by shift-invariance), and then $B \subset A$ follows, making the ambient group $\mathcal{G}$ irrelevant.

For the rest of the quantities we first consider the particular case when $\mathcal{G}_2 = \mathcal{G}$. Write $|\mathcal{G}_1| = q_1$, $|\mathcal{G}| = q$.

Consider the case of δ. Let B, B_1 be the maximal sets in $\mathcal{G}$ and $\mathcal{G}_1$, resp., with the property that

$$(B - B) \cap A = (B_1 - B_1) \cap A = \{0\}.$$

Consider a coset $t + \mathcal{G}_1$ of $\mathcal{G}_1$. Since the set $B_t = (t + \mathcal{G}_1) \cap B$ satisfies $B'_t = B_t - t \subset \mathcal{G}_1$ and $(B'_t - B'_t) \cap A \subset \{0\}$, we conclude $|B_t| \leq |B_1|$. Applying this for each coset and summing we obtain $|B| \leq (q/q_1)|B_1|$. On the other hand, take a representative from each coset, say $t_1, \ldots, t_{q/q_1}$. The set $\bigcup (t_i + B_1)$ demonstrates $|B| \geq (q/q_1)|B_1|$.

Consider now the case when φ is any of the functionals $\lambda, \lambda^-, \lambda^+, \lambda^\pm$. First, if $f : \mathcal{G}_1 \to \mathbb{R}$ is an appropriate function with $f(0)/\hat{f}(\mathbf{1}) = \varphi(A, \mathcal{G}_1)$ then it is straightforward to see that $f^{\mathcal{G}}$ has all the required properties to testify that $\varphi(A, \mathcal{G}) \leq \varphi(A, \mathcal{G}_1)$.

To see the reverse inequality assume that $g : \mathcal{G} \to \mathbb{R}$ is an appropriate function with $g(0)/\hat{g}(\mathbf{1}) = \varphi(A, \mathcal{G})$, and consider the restricted function $h = g_{\mathcal{G}_1}$. If $\varphi = \lambda$ or λ^+ then h obviously testifies that $\varphi(A, \mathcal{G}_1) \leq \varphi(A, \mathcal{G})$. In the case $\varphi = \lambda^-$ or $\lambda^\pm$ we still have $h(0) = g(0)$ and $\hat{h}(\mathbf{1}) \leq \hat{g}(\mathbf{1})$, and therefore $h(0)/\hat{h}(\mathbf{1}) \leq \varphi(A, \mathcal{G})$. Also, h falls into the class $\mathcal{S}^-(A, \mathcal{G}_1)$ or $\mathcal{S}^\pm(A, \mathcal{G}_1)$. It remains to show that the Fourier

coefficients of h are nonnegative. To see this, let $\gamma \in \hat{\mathcal{G}}_1$ and consider all $\psi \in \hat{\mathcal{G}}$ such that $\psi_{\mathcal{G}_1} = \gamma$. There exist q/q_1 such characters ψ. Then

$$\begin{aligned} 0 \leq \sum_{\psi:\psi_{\mathcal{G}_1}=\gamma} \hat{g}(\psi) &= \sum_{\psi}\sum_{x\in\mathcal{G}} \psi(x)g(x) = \sum_{\psi}\sum_{x\in\mathcal{G}_1} \psi(x)g(x) + \sum_{\psi}\sum_{x\notin\mathcal{G}_1} \psi(x)g(x) \\ &= \frac{q}{q_1}\hat{h}(\gamma) + \sum_{x\notin\mathcal{G}_1}\left(g(x)\sum_{\psi}\psi(x)\right) = \frac{q}{q_1}\hat{h}(\gamma) \end{aligned} \tag{3.4}$$

where we have used that the inner summation in the last sum always returns 0. This shows that $\hat{h}(\gamma) \geq 0$.

Finally, in the general case, $\mathcal{G}_1, \mathcal{G}_2 \leq \mathcal{G}$, let $\mathcal{H} \leq \mathcal{G}$ be the subgroup generated by $\mathcal{G}_1$ and $\mathcal{G}_2$. Then $\mathcal{H}$ is also finite, and by the argument above $\varphi(A, \mathcal{G}_1) = \varphi(A, \mathcal{H}) = \varphi(A, \mathcal{G}_2)$. □

3.1.2 The basic inequality

In this section we prove Theorem 3.1.4. We will only prove $\delta(A) \leq \lambda^-(A)$ and $\lambda^+(A) \leq \overline{\delta}(A)$, the other inequalities are trivial.

To see $\delta(A) \leq \lambda^-(A)$, assume $f \in \mathcal{S}^-(A)$ is any function such that $\hat{f} \geq 0$, and $B \subset \mathcal{G}$ is such that $(B - B) \cap A = \{0\}$. We usually call such a function f a "witness" function. Introduce the function $\hat{B}(\gamma) = \sum_{b\in B}\gamma(b)$, and notice that $|\hat{B}(\gamma)|^2 = \sum_{b_1,b_2\in B}\gamma(b_1 - b_2)$. We now evaluate the sum $S = \sum_{\gamma\in\hat{\mathcal{G}}}\hat{f}(\gamma)|\hat{B}(\gamma)|^2$. On the one hand, all terms are nonnegative, hence by considering the term $\gamma = \mathbf{1}$ only we get a lower bound $S \geq \hat{f}(\mathbf{1})|B|^2$. On the other hand, by exchanging the order of summation and using the Fourier inversion formula we obtain

$$S = \sum_{\gamma}\sum_{b_1,b_2}\hat{f}(\gamma)\gamma(b_1 - b_2) = \sum_{b_1,b_2}\sum_{\gamma}\hat{f}(\gamma)\gamma(b_1 - b_2) = q\sum_{b_1,b_2} f(b_1 - b_2).$$

In the last summation all the terms are non-positive by assumption, except when $b_1 = b_2$. Hence, $S \leq qf(0)|B|$, and comparing the lower and upper bounds $\frac{|B|}{q} \leq \frac{f(0)}{\hat{f}(\mathbf{1})}$ follows.

To see $\lambda^+(A) \leq \overline{\delta}(A)$, assume $B \subset \mathcal{G}$ is such that $B - B \subset A$. Define the function $f : \mathcal{G} \to \mathbb{R}$ by setting $f(x)$ to be the number of ways x can be written in the form $x = b_1 - b_2$ where $b_1, b_2 \in B$. In other words, $f = 1_B * 1_{-B}$. Clearly, $f \in \mathcal{S}^+(A)$ and

$$\frac{f(0)}{\hat{f}(\mathbf{1})} = \frac{|B|}{|B|^2} = \frac{1}{|B|}.$$

Furthermore, $\hat{f} = |\widehat{1_B}|^2 \geq 0$, so f satisfies each criterion in the definition of $\lambda^+(A)$, and we conclude that $\lambda^+(A) \leq 1/|B|$. □

Example 3.1.10. The cases when all our quantities are equal are connected with

tilings. Indeed, assume that $\delta(A) = \overline{\delta}(A) = \delta$, say. Take sets $B, \overline{B}$ such that

$$|B| = \delta q, \quad (B-B) \cap A = \{0\},$$
$$|\overline{B}| = 1/\delta, \quad (\overline{B}-\overline{B}) \subset A.$$

The conditions on difference sets imply that all the sums $x + y : x \in B, y \in \overline{B}$ are distinct and their number is $|B||\overline{B}| = q$, so $(B, \overline{B})$ is a tiling of $\mathcal{G}$. Conversely, any tiling $(B, \overline{B})$ induces examples of equality as follows. Take any set $E \subset \mathcal{G} \setminus \big((B-B) \cup (\overline{B}-\overline{B})\big)$. The set $A = (\overline{B}-\overline{B}) \cup E$ satisfies $\overline{\delta}(A) \le 1/|\overline{B}|$ and $\delta(A) \ge |B-B|/q = 1/|\overline{B}|$, hence $\delta(A) = \overline{\delta}(A) = 1/|\overline{B}|$. □

Example 3.1.11. Let q be a prime, $q \equiv 1 \pmod 4$, $\mathcal{G} = \mathbb{Z}_q$ and let A be the set of quadratic residues. By the familiar properties of Gaussian sums one easily shows that $\lambda^-(A) = \lambda^+(A) = 1/\sqrt{q}$ (the case of composite q is more difficult). On the other hand $\delta(A) < 1/\sqrt{q} < \overline{\delta}(A)$, since the δ's must be rational. It is natural to conjecture that δ is much smaller, perhaps of size $O\big((\log q)^c\big)$, like for a random set (for random sets see Section 3.1.8), but nothing much stronger than $1/\sqrt{q}$ is known. We will return to this example in Section 3.2 in detail. □

Examples where the λ's are different, as well as examples where the δ's are very different from the λ's, will be given in Sections 3.1.8 and 3.1.9.

3.1.3 Complements and linear duality

Definition 3.1.12. *Two standard sets in a group $\mathcal{G}$ are* standard complements*, if $A \cup A' = \mathcal{G}$ and $A \cap A' = \{0\}$.*

The various quantities δ and λ of standard complements are nicely related to each other by the following theorem.

Theorem 3.1.13. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A, A' \subset \mathcal{G}$ be standard complements. We have*

$$\delta(A)\overline{\delta}(A') = \lambda(A)\lambda(A') = \lambda^-(A)\lambda^+(A') = \lambda^\pm(A)\lambda^\pm(A') = 1/q. \tag{3.5}$$

We express this by saying that δ and $\overline{\delta}$ are dual quantities, and so are λ^- and λ^+, while λ and $\lambda^\pm$ are self-dual.

Proof. The relation $\delta(A)\overline{\delta}(A') = 1/q$ is clear from $\overline{\Delta}(A') = \Delta(A)$. We prove the other three equalities. Let φ denote one of the functionals $\lambda, \lambda^-, \lambda^\pm$ and φ' its dual, i.e. $\lambda, \lambda^+, \lambda^\pm$, respectively.

First we show the easy inequality $1/q \le \varphi(A)\varphi'(A')$. To this end take any two functions f_1 and f_2 satisfying the requirements in the definition of $\varphi(A)$ and $\varphi'(A')$. Consider the function $h = f_1 f_2$. Then $h(0) = f_1(0)f_2(0)$ and

$$\hat{h}(\mathbf{1}) = \frac{1}{q}(\hat{f}_1 * \hat{f}_2)(\mathbf{1}) \ge \frac{1}{q}(\hat{f}_1(\mathbf{1})\hat{f}_2(\mathbf{1})).$$

Also, by the signs of f_1 and f_2 we see that h is non-positive everywhere except at 0. Therefore $h(0) \geq \hat{h}(\mathbf{1})$ which implies

$$f_1(0)f_2(0) \geq \frac{1}{q}(\hat{f}_1(\mathbf{1})\hat{f}_2(\mathbf{1})).$$

To prove the converse inequality we will apply linear duality. Let f be any real function on $\mathcal{G}$ and consider the values $f(x)$ as variables (as x ranges through $\mathcal{G}$). Consider the following systems of inequalities:
For $\varphi = \lambda$:

$$f(x) = 0 \text{ if } x \notin A, \ \sum_{x\in\mathcal{G}} f(x) \geq 1, \ \sum_{x\in\mathcal{G}} f(x)\gamma(x) \geq 0 \quad \text{if } \mathbf{1} \neq \gamma \in \hat{\mathcal{G}} \tag{3.6}$$

For $\varphi = \lambda^-$:

$$f(x) \leq 0 \text{ if } x \notin A, \ \sum_{x\in\mathcal{G}} f(x) \geq 1, \ \sum_{x\in\mathcal{G}} f(x)\gamma(x) \geq 0 \quad \text{if } \mathbf{1} \neq \gamma \in \hat{\mathcal{G}} \tag{3.7}$$

For $\varphi = \lambda^\pm$:

$$f(x) \leq 0 \text{ if } x \notin A, \ f(x) \geq 0 \text{ if } x \in A, \ \sum_{x\in\mathcal{G}} f(x) \geq 1, \ \sum_{x\in\mathcal{G}} f(x)\gamma(x) \geq 0 \text{ if } \mathbf{1} \neq \gamma \in \hat{\mathcal{G}} \tag{3.8}$$

In each case we know that the inequalities imply $f(0) \geq \varphi(A)$. Therefore, by the principle of linear duality (see e.g. [134] Theorem 5.2 for a convenient formulation), the inequality $f(0) \geq \varphi(A)$ is the weighted linear combination of the inequalities above, i.e. there exist coefficients $h_1(\mathbf{1}) \geq 0$, $h_1(\gamma) \geq 0$ (for $\gamma \neq \mathbf{1}$), and $h_2(x)$ (with appropriate signs for $x \in A$ and $x \notin A$; see the restrictions below), such that

$$f(0) = h_1(\mathbf{1}) \left(\sum_{x\in\mathcal{G}} f(x) \right) + \sum_{\gamma\neq 0} h_1(\gamma) \left(\sum_{x\in\mathcal{G}} f(x)\gamma(x) \right) + \sum_{x\in\mathcal{G}} h_2(x)f(x) \geq \tag{3.9}$$

$$\geq h_1(\mathbf{1}) = \varphi(A).$$

The restrictions for $h_2(x)$ are as follows:

For $\varphi = \lambda$:

$$h_2(x) = 0 \text{ if } x \in A \tag{3.10}$$

For $\varphi = \lambda^-$:

$$h_2(x) = 0 \text{ if } x \in A, \ h_2(x) \leq 0 \text{ if } x \notin A \tag{3.11}$$

For $\varphi = \lambda^\pm$:

$$h_2(x) \geq 0 \text{ if } x \in A, \ h_2(x) \leq 0 \text{ if } x \notin A \tag{3.12}$$

From (3.9) we conclude that $h_1(\mathbf{1}) = \varphi(A)$. Let $g : \mathcal{G} \to \mathbb{R}$ be the function such that $\hat{g} = h_1$. Then $\hat{g} \geq 0$ by definition. Also, $\hat{g}(\mathbf{1}) = \varphi(A)$, and $qg(0) = \sum_{\gamma\in\hat{\mathcal{G}}} h_1(\gamma) = 1 - h_2(0)$, as it is the coefficient of $f(0)$ in (3.9). For any $x \neq 0$,

comparing the coefficients of $f(x)$ in (3.9) we get

$$0 = \sum_{\gamma \in \hat{\mathcal{G}}} h_1(\gamma)\gamma(x) + h_2(x) = qg(x) + h_2(x),$$

which implies the following inequalities:
For $\varphi = \lambda$:

$$g(x) = 0 \text{ if } x \in A \ (x \neq 0) \Rightarrow g \in \mathcal{S}(A'). \tag{3.13}$$

For $\varphi = \lambda^-$:

$$g(x) = 0 \text{ if } x \in A \ (x \neq 0),\ g(x) \geq 0 \text{ if } x \notin A \Rightarrow g \in \mathcal{S}^+(A'). \tag{3.14}$$

For $\varphi = \lambda^\pm$:

$$g(x) \leq 0 \text{ if } x \in A \ (x \neq 0),\ g(x) \geq 0 \text{ if } x \notin A \Rightarrow g \in \mathcal{S}^\pm(A'). \tag{3.15}$$

Therefore, the function g testifies that

$$\varphi'(A') \leq \frac{1 - h_2(0)}{q\varphi(A)} \leq \frac{1}{q\varphi(A)}.$$

□

Remark 3.1.14. Perhaps the first application of linear duality to this sort of problem is in a paper by Ruzsa [115]; a good account can be found in Montgomery's book [103].

3.1.4 Automorphisms

In this section we state some simple but useful properties of the behaviour of our quantities under automorphisms.

Proposition 3.1.15. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, π an automorphism of $\mathcal{G}$ and let φ be any of the functionals $\delta, \overline{\delta}, \lambda, \lambda^-, \lambda^+, \lambda^\pm$. For every $A \subset \mathcal{G}$ we have*

$$\varphi(A) = \varphi(\pi(A)).$$

We omit the simple proof. As an application, let q be a prime, $q \equiv 1 \pmod 4$, $\mathcal{G} = \mathbb{Z}_q$, and let A be the set of quadratic residues. The standard complement of A is A', the set of nonresidues. Since the multiplication by a nonresidue is an automorphism that transforms A into A', we have $\varphi(A) = \varphi(A')$ for any of the above functionals. On the other hand, from Theorem 3.1.13 we know that $\lambda(A)\lambda(A') = \lambda^\pm(A)\lambda^\pm(A') = 1/q$, so we immediately get that $\lambda(A) = \lambda^\pm(A) = 1/\sqrt{q}$. While this fact, and also the values of $\lambda^+(A)$ and $\lambda^-(A)$ are easily found directly using Gaussian sums, it is somewhat surprising that we can find them without resorting to any real number theory. We will return to this example in Section 3.2. Unfortunately this argument does not work for composite moduli or higher powers.

Proposition 3.1.16. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $A \subset \mathcal{G}$, and let Π be the set of those automorphisms that leave A fixed (as a set, not necessarily pointwise). Let φ be any of the functionals $\lambda, \lambda^-, \lambda^+, \lambda^\pm$, and let $\mathcal{T}$ be the corresponding class of functions (one of $\mathcal{S}(A), \mathcal{S}^-(A), \mathcal{S}^+(A)$ or $\mathcal{S}^\pm(A)$, restricted to functions with nonnegative Fourier transform). There is an $f \in \mathcal{T}$ such that $\varphi(A) = f(0)/\hat{f}(\mathbf{1})$ which is invariant under Π, that is, $f = f \circ \pi$ for all $\pi \in \Pi$.*

Proof. Indeed, take any $f_0 \in \mathcal{T}$ for which $\varphi(A) = f_0(0)/\hat{f}_0(\mathbf{1})$ and form

$$f(x) = \sum_{\pi \in \Pi} f(\pi(x)).$$

□

For sets that have lots of automorphisms, like power residues, this restricts the class of functions to be considered for finding the value of $\lambda, \lambda^-, \lambda^+, \lambda^\pm$.

3.1.5 Union and intersection

In this section we consider the behaviour of the various δ and λ quantities under intersection and union of standard sets.

Proposition 3.1.17. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A_1, A_2 \subset \mathcal{G}$ be standard sets. We have*

$$\overline{\delta}(A_1 \cap A_2) \leq q\overline{\delta}(A_1)\overline{\delta}(A_2). \tag{3.16}$$

Proof. Take sets B_i such that $B_i - B_i \subset A_i$, $i = 1, 2$. Any set of the form $B = B_1 \cap (t - B_2)$ satisfies $B - B \subset A_1 \cap A_2$, and an obvious averaging argument shows that there exists a t such that $|B| \geq |B_1||B_2|/q$. □

Proposition 3.1.18. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A_1, A_2 \subset \mathcal{G}$ be standard sets. We have*

$$\delta(A_1 \cup A_2) \geq \delta(A_1)\delta(A_2), \tag{3.17}$$

Proof. Using the duality $\delta(A)\overline{\delta}(A') = 1/q$ the statement follows from the previous result applied to the standard complements of A_1 and A_2. □

Proposition 3.1.19. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A_1, A_2 \subset \mathcal{G}$ be standard sets. We have*

$$\lambda(A_1 \cap A_2) \leq q\lambda(A_1)\lambda(A_2), \tag{3.18}$$

$$\lambda^+(A_1 \cap A_2) \leq q\lambda^+(A_1)\lambda^+(A_2), \tag{3.19}$$

$$\lambda^-(A_1 \cap A_2) \leq q\lambda^-(A_1)\lambda^+(A_2), \tag{3.20}$$

$$\lambda^\pm(A_1 \cap A_2) \leq q\lambda^\pm(A_1)\lambda^+(A_2). \tag{3.21}$$

Proof. Let f_1, f_2 be functions, belonging to some of the $\mathcal{S}$-classes of the sets A_1, A_2. Their product $h = f_1 f_2$ belongs to an $\mathcal{S}$-class of the intersection as follows:

$$\begin{aligned}
&f_1 \in \mathcal{S}(A_1), \quad && f_2 \in \mathcal{S}(A_2) && \Rightarrow h \in \mathcal{S}(A_1 \cap A_2),\\
&f_1 \in \mathcal{S}^+(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^+(A_1 \cap A_2),\\
&f_1 \in \mathcal{S}^-(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^-(A_1 \cap A_2),\\
&f_1 \in \mathcal{S}^\pm(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^\pm(A_1 \cap A_2).
\end{aligned}$$

Clearly $h(0) = f_1(0)f_2(0)$. Furthermore we have $\hat{h} = (\hat{f}_1 * \hat{f}_2)/q$, which shows that $\hat{h} \geq 0$ and $\hat{h}(\mathbf{1}) \geq \hat{f}_1(\mathbf{1})\hat{f}_2(\mathbf{1})/q$, and we conclude

$$\frac{h(0)}{\hat{h}(\mathbf{1})} \leq q \frac{f_1(0)}{\hat{f}_1(\mathbf{1})} \frac{f_2(0)}{\hat{f}_2(\mathbf{1})}.$$

By taking the minimum over all admissible f_1, f_2 we get the inequalities of the theorem. □

Proposition 3.1.20. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and let $A_1, A_2 \subset \mathcal{G}$ be standard sets. We have*

$$\lambda(A_1 \cup A_2) \geq \lambda(A_1)\lambda(A_2), \tag{3.22}$$

$$\lambda^+(A_1 \cup A_2) \geq \lambda^+(A_1)\lambda^-(A_2), \tag{3.23}$$

$$\lambda^-(A_1 \cup A_2) \geq \lambda^-(A_1)\lambda^-(A_2), \tag{3.24}$$

$$\lambda^\pm(A_1 \cup A_2) \geq \lambda^\pm(A_1)\lambda^-(A_2). \tag{3.25}$$

Proof. Using the duality relations these statements are easily seen to be equivalent to the statements of the previous theorem applied to the standard complements of A_1 and A_2. For example, in the case of (3.23) the calculation runs as follows:

$$\frac{1/q}{\lambda^+(A_1 \cup A_2)} = \lambda^-(A_1' \cap A_2') \leq q\lambda^-(A_1')\lambda^+(A_2') = q \frac{1/q}{\lambda^+(A_1)} \frac{1/q}{\lambda^-(A_2)}$$

□

Most of the above functionals satisfy a trivial monotonicity property. Let φ be any of the functionals $\delta, \overline{\delta}, \lambda, \lambda^-, \lambda^+$.

$$\text{If } \mathrm{A}_1 \subset \mathrm{A}_2 \text{ then } \varphi(\mathrm{A}_2) \leq \varphi(\mathrm{A}_1). \tag{3.26}$$

This observation can be applied to complement the upper estimates for intersection by the lower estimate

$$\varphi(A_1 \cap A_2) \geq \max\big(\varphi(A_1), \varphi(A_2)\big),$$

and the lower estimates for union by the upper estimate

$$\varphi(A_1 \cup A_2) \leq \min\big(\varphi(A_1), \varphi(A_2)\big).$$

Equality holds when $A_1 = A_2$, so in general nothing stronger can be asserted.

We will see in Example 3.1.37 that inequality (3.26) may fail for $\lambda^{\pm}$.

Problem 3.1.21. ([96]) *Find a nontrivial lower estimate for $\lambda^{\pm}(A_1 \cap A_2)$ and a nontrivial upper estimate for $\lambda^{\pm}(A_1 \cup A_2)$.*

3.1.6 Subgroups and factor groups

Let $\mathcal{G}$ be a commutative group and $\mathcal{H}$ a subgroup. We use $\mathcal{G}/\mathcal{H}$ to denote the factor group, and we use the cosets of $\mathcal{H}$ to represent its elements. We also introduce the following natural notions.

Definition 3.1.22. *For any set $A \subset \mathcal{G}$ we write $A/\mathcal{H} = \{\mathcal{H} + a : a \in A\}$ to denote the collection of cosets that intersect A (= the image of A under the canonical homomorphism from $\mathcal{G}$ to $\mathcal{G}/\mathcal{H}$). For any function $f : \mathcal{G} \to \mathbb{R}$ we introduce the factorization of f by $\mathcal{H}$ as the function $f_{/\mathcal{H}}$ on $\mathcal{G}/\mathcal{H}$ defined by $f_{/\mathcal{H}}(x+\mathcal{H}) = \sum_{t\in\mathcal{H}} f(x+t)$. Conversely, for a function $g : \mathcal{G}/\mathcal{H} \to \mathbb{R}$ we introduce the lifting $g^{\times\mathcal{H}}$ of g to the group $\mathcal{G}$ as $g^{\times\mathcal{H}}(x) = g(x+\mathcal{H})$.*

The following is essentially a result of Kolountzakis and Révész [75].

Proposition 3.1.23. ([75], [96]*) *Let $\mathcal{G}$ be a finite commutative group, $\mathcal{H}$ a subgroup, $\mathcal{G}_1 = \mathcal{G}/\mathcal{H}$. Let $A \subset \mathcal{G}$ be a standard set, and put $A_{\mathcal{H}} = A \cap \mathcal{H} \subset \mathcal{H}$, $A_1 = A/\mathcal{H} \subset \mathcal{G}_1$. We have*

$$\delta(A) \geq \delta(A_{\mathcal{H}})\delta(A_1), \tag{3.27}$$

$$\overline{\delta}(A) \geq \overline{\delta}(A_{\mathcal{H}})\overline{\delta}(A_1), \tag{3.28}$$

$$\lambda(A) \geq \lambda(A_{\mathcal{H}})\lambda(A_1), \tag{3.29}$$

$$\lambda^{+}(A) \geq \lambda^{+}(A_{\mathcal{H}})\lambda^{+}(A_1), \tag{3.30}$$

$$\lambda^{-}(A) \geq \lambda^{-}(A_{\mathcal{H}})\lambda^{-}(A_1), \tag{3.31}$$

$$\lambda^{\pm}(A) \geq \lambda^{\pm}(A_{\mathcal{H}})\lambda^{-}(A_1). \tag{3.32}$$

Proof. To see (3.27) let $B_{\mathcal{H}}$ be a set such that $B_{\mathcal{H}} \subset \mathcal{H}$ and $(B_{\mathcal{H}} - B_{\mathcal{H}}) \cap A_{\mathcal{H}} = \{0\}$, and let $B_1 \subset \mathcal{G}_1$ be a set such that $(B_1 - B_1) \cap A_1 = \{0\}$. The elements of B_1 are cosets of $\mathcal{H}$. Take a representative $x_i \in \mathcal{G}$ from each such coset, and consider the set $B = \cup_i (x_i + B_{\mathcal{H}}) \subset \mathcal{G}$. It is clear that $|B| = |B_{\mathcal{H}}||B_1|$ and $(B - B) \cap A = \{0\}$.

Inequality (3.28) is equivalent to $\overline{\Delta}(A) \leq \overline{\Delta}(A_{\mathcal{H}})\overline{\Delta}(A_1)$. Take a set $B \in \mathcal{G}$ such that $B - B \subset A$. In each coset $x + \mathcal{H}$ there can be at most $\overline{\Delta}(A_{\mathcal{H}})$ elements of B. Also, the number of cosets that contain some elements of B is at most $\overline{\Delta}(A_1)$. Therefore, $|B| \leq \overline{\Delta}(A_{\mathcal{H}})\overline{\Delta}(A_1)$.

We will prove the remaining four inequalities. Let $f : \mathcal{G} \to \mathbb{R}$ be any function and consider the functions $f_{\mathcal{H}} : \mathcal{H} \to \mathbb{R}$ and $f_{/\mathcal{H}} : \mathcal{G}_1 \to \mathbb{R}$. The following implications are straightforward:

$$\begin{aligned} f \in \mathcal{S}_{\mathcal{G}}(A) \quad &\Rightarrow f_{\mathcal{H}} \in \mathcal{S}_{\mathcal{H}}(A_{\mathcal{H}}), \quad f_{/\mathcal{H}} \in \mathcal{S}_{\mathcal{G}_1}(A/\mathcal{H}), \\ f \in \mathcal{S}^+(A) \quad &\Rightarrow f_{\mathcal{H}} \in \mathcal{S}^+_{\mathcal{H}}(A_{\mathcal{H}}), \quad f_{/\mathcal{H}} \in \mathcal{S}^+_{\mathcal{G}_1}(A/\mathcal{H}), \\ f \in \mathcal{S}^-(A) \quad &\Rightarrow f_{\mathcal{H}} \in \mathcal{S}^-_{\mathcal{H}}(A_{\mathcal{H}}), \quad f_{/\mathcal{H}} \in \mathcal{S}^-_{\mathcal{G}_1}(A/\mathcal{H}), \\ f \in \mathcal{S}^{\pm}(A) \quad &\Rightarrow f_{\mathcal{H}} \in \mathcal{S}^{\pm}_{\mathcal{H}}(A_{\mathcal{H}}), \quad f_{/\mathcal{H}} \in \mathcal{S}^-_{\mathcal{G}_1}(A/\mathcal{H}),. \end{aligned} \tag{3.33}$$

Assuming that $\hat{f} \geq 0$ the relation $\hat{f}_{\mathcal{H}} \geq 0$ can be seen in the same manner as in (3.4) in the proof of Proposition 3.1.9. Note also that

$$\frac{f_{\mathcal{H}}(0)}{\hat{f}_{\mathcal{H}}(\mathbf{1})} = \frac{f(0)}{\sum_{x\in\mathcal{H}} f(x)}. \tag{3.34}$$

Furthermore, $\hat{f}_{/\mathcal{H}} \geq 0$ also holds, because for each $\gamma \in \hat{\mathcal{G}}_1$ we have $\hat{f}_{/\mathcal{H}}(\gamma) = \sum_{x+\mathcal{H}\in\mathcal{G}_1} f_{/\mathcal{H}}(x+\mathcal{H})\gamma(x+\mathcal{H}) = \sum_{x+\mathcal{H}\in\mathcal{G}_1}(\sum_{y\in(x+\mathcal{H})} f(y))\gamma(x+\mathcal{H}) = \sum_{x+\mathcal{H}\in\mathcal{G}_1}(\sum_{y\in(x+\mathcal{H})} f(y)\gamma^{\times\mathcal{H}}(y)) = \hat{f}(\gamma^{\times\mathcal{H}}) \geq 0$. Observing that

$$\frac{f_{/\mathcal{H}}(0)}{\hat{f}_{/\mathcal{H}}(\mathbf{1})} = \frac{\sum_{x\in\mathcal{H}} f(x)}{\hat{f}(\mathbf{1})} \tag{3.35}$$

and using (3.34) we obtain the required inequalities (3.29), (3.30), (3.31), (3.32). □

We note here that the last inequality is less symmetric than the others. We do not know whether the stronger inequality

$$\lambda^{\pm}(A) \geq \lambda^{\pm}(A_{\mathcal{H}})\lambda^{\pm}(A_1)$$

holds or not.

3.1.7 Direct products

In this section we consider the behaviour of the various δ and λ quantities under the direct product operation.

Proposition 3.1.24. ([96]*) *Let $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ be the direct product of two finite commutative groups, and let $A = A_1 \times A_2$, where $A_1 \subset \mathcal{G}_1$, $A_2 \subset \mathcal{G}_2$. We have*

$$\lambda(A) = \lambda(A_1)\lambda(A_2), \tag{3.36}$$

$$\lambda^+(A) = \lambda^+(A_1)\lambda^+(A_2), \tag{3.37}$$

$$\lambda^-(A_1)\lambda^-(A_2) \leq \lambda^-(A) \leq \lambda^-(A_1)\lambda^+(A_2), \tag{3.38}$$

$$\lambda^{\pm}(A_1)\lambda^-(A_2) \leq \lambda^{\pm}(A) \leq \lambda^{\pm}(A_1)\lambda^+(A_2). \tag{3.39}$$

Proof. The claimed lower bounds on $\lambda(A)$, $\lambda^+(A)$, $\lambda^-(A)$, $\lambda^{\pm}(A)$ follow from inequalities (3.29), (3.30), (3.31), (3.32), respectively.

To prove the upper bounds, let f_1 and f_2 be appropriate functions for the sets A_1, A_2, and consider the function $h(x,y) = f_1(x)f_2(y)$. The following implications are straightforward:

$$\begin{aligned}
&f_1 \in \mathcal{S}(A_1), \quad && f_2 \in \mathcal{S}(A_2) && \Rightarrow h \in \mathcal{S}(A_1 \times A_2),\\
&f_1 \in \mathcal{S}^+(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^+(A_1 \times A_2),\\
&f_1 \in \mathcal{S}^-(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^-(A_1 \times A_2),\\
&f_1 \in \mathcal{S}^\pm(A_1), \quad && f_2 \in \mathcal{S}^+(A_2) && \Rightarrow h \in \mathcal{S}^\pm(A_1 \times A_2).
\end{aligned}$$

Also, $\hat{h} \geq 0$ follows from $\hat{f_1} \geq 0$ and $\hat{f_2} \geq 0$, and $h(0) = f_1(0)f_2(0)$ and $\hat{h}(\mathbf{1}) = \hat{f_1}(\mathbf{1})\hat{f_2}(\mathbf{1})$. Therefore, the function h testifies the upper bounds in (3.36), (3.37), (3.38) and (3.39), □

Proposition 3.1.25. ([96]*) *Let $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ be the direct product of two finite commutative groups, and let $A = A_1 \times A_2$, where $A_1 \subset \mathcal{G}_1$, $A_2 \subset \mathcal{G}_2$. We have*

$$\overline{\delta}(A) = \overline{\delta}(A_1)\overline{\delta}(A_2), \tag{3.40}$$

$$\delta(A_1)\delta(A_2) \leq \delta(A) \leq \delta(A_1)\overline{\delta}(A_2). \tag{3.41}$$

Proof. Given sets B_1, B_2 with $B_1 - B_1 \subset A_1$, $B_2 - B_2 \subset A_2$, their product $B = B_1 \times B_2$ satisfies $B - B \subset A$. Conversely, if $B - B \subset A$, and B_1, B_2 are the projections of B, then we have $B_1 - B_1 \subset A_1$, $B_2 - B_2 \subset A_2$ and $B \subset B_1 \times B_2$. This shows (3.40).

Given sets $B_1 \subset \mathcal{G}_1, B_2 \subset \mathcal{G}_2$ with $(B_1 - B_1) \cap A_1 = \{0\}$, $(B_2 - B_2) \cap A_2 = \{0\}$ their product $B = B_1 \times B_2$ satisfies $(B - B) \cap A = \{0\}$. This shows the lower estimate in (3.41).

To prove the upper estimate we rewrite it in the form

$$\frac{\Delta(A)}{q} \leq \frac{\Delta(A_1)}{q_1}\frac{1}{\overline{\Delta}(A_2)},$$

where $q_i = |\mathcal{G}_i|$ and $q = |\mathcal{G}| = q_1 q_2$. This can be rearranged as

$$\overline{\Delta}(A_2)\Delta(A) \leq q_2\Delta(A_1) = \Delta(A_1 \times \{0\}). \tag{3.42}$$

Let $B_2 \subset \mathcal{G}_2$, $B \subset \mathcal{G}$ be maximal sets with the properties $B_2 - B_2 \subset A_2$, $(B-B)\cap A = \{0\}$. Then the left hand side of (3.42) is $|B_2||B|$. Notice that $(\{0\} \times B_2) + B$ is a packing in $\mathcal{G}$: if $(0, b_i) \in B_2$ and $(t_i, u_i) \in B$ (for $i = 1, 2$) then $(0, b_1) + (t_1, u_1) = (0, b_2) + (t_2, u_2)$ is equivalent to $(0, b_1 - b_2) = (t_2 - t_1, u_2 - u_1)$, which is possible only if both coordinates are 0. Let $C = (\{0\} \times B_2) + B$. Then $|C| = |B_2||B|$ due to the packing property. Also, we claim that $C - C \cap (A_1 \times \{0\}) = \{(0,0)\}$. Consider $(v_1, v_2) = (0, b_1 - b_2) + (t_1 - t_2, u_1 - u_2) \in C - C$. Here $b_1 - b_2 \in A_2$ so v_2 can only be zero if $u_2 - u_1 \in A_2$, which means that $u_1 - u_2 \in A_2$ (recall that A_2 is symmetric). Also, $v_1 \in A_1$ means that that $t_1 - t_2 \in A_1$. Therefore $(t_1 - t_2, u_1 - u_2) \in A_1 \times A_2$, which is only possible if $(t_1 - t_2, u_1 - u_2) = \{0, 0\}$, and $(v_1, v_2) = \{(0,0)\}$. □

Example 3.1.26. Let $\mathcal{G}_1 = \mathcal{G}_2$, $A_1 \subset \mathcal{G}_1$ arbitrary, A_2 its standard complement, $A = A_1 \times A_2 \subset \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$, $|\mathcal{G}| = q = q_1^2$. We have

$$\delta(A) = \lambda(A) = 1/q_1 = q^{-1/2}.$$

Indeed, $\delta(A) \le \lambda(A) = \lambda(A_1)\lambda(A_2) = |\mathcal{G}_1|^{-1} = 1/q_1$ by the previous theorem and duality. We also have $\delta(A) \ge 1/q_1$, since the diagonal $B = \{(x,x) : x \in \mathcal{G}_1\}$ satisfies $(B-B) \cap A = \{0\}$.

This is also an example when the upper estimate of (3.41) holds with equality, since $\delta(A_1)\overline{\delta}(A_2) = 1/q_1$ by duality.

In contrast, $\overline{\delta}(A) = \overline{\delta}(A_1)\overline{\delta}(A_2)$ can be quite near 1. A random set satisfies

$$\max(\overline{\Delta}(A_1), \overline{\Delta}(A_2) \lesssim (\log q)^2,$$

see the next section, and then we have $\overline{\delta}(A) \gtrsim (\log q)^{-4}$. □

3.1.8 Random sets

First we describe our notion of a random standard set. Given a finite group $\mathcal{G}$, write

$$\mathcal{G}_1 = \{x \in \mathcal{G} : 2x = 0\},$$

the set of elements of order 2 (and the unit). The set $\mathcal{G} \setminus \mathcal{G}_1$ is a disjoint union of pairs $\{x, -x\}$; let $\mathcal{G}_2$ be a set containing exactly one element of each pair. We have

$$\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2 \cup -\mathcal{G}_2,$$

a disjoint union. Write $|\mathcal{G}_i| = q_i$, so that $q = q_1 + 2q_2$.

Take a real number $\rho \in (0,1)$. Let $\{\xi_y, y \in \mathcal{G}_1 \cup \mathcal{G}_2\}$ be a collection of independent 0-1 valued random variable satisfying

$$\Pr(\xi_y = 1) = \rho.$$

Our random standard set corresponding to the prescribed probability ρ will be

$$R = \{0\} \cup \{y \in \mathcal{G}_1 : \xi_y = 1\} \cup \bigcup_{y \in \mathcal{G}_2, \xi_y = 1} \{y, -y\}.$$

Nothing depends on the value of ξ_0 as 0 must be in R deterministically, but some formulas will look nicer using it. Observe that

$$\mathbf{E}(|R|) = 1 + \rho(q-1).$$

The standard complement of a random set will be a random standard set corresponding to the probability $1-\rho$. In the case $\rho = 1/2$ this observation, together with the dualities of Section 3.1.3 shows that the medians of λ and $\lambda^{\pm}$ are both $q^{-1/2}$.

To control various quantities related to our random set we need a large deviation estimate. Many forms of Bernstein's (or Chernov's) inequality will work; we quote one from Tao and Vu's book [133, Theorem 1.8] which is comfortable for us.

Lemma 3.1.27. ([133]) *Let $X_1, \dots, X_n$ be independent random variables satisfying $|X_i - \mathbf{E}(X_i)| \le 1$ for all i. Put $X = X_1 + \ldots + X_n$ and let σ^2 be the variance of X. For any $t > 0$ we have*

$$\Pr(|X - \mathbf{E}(X)| \ge t\sigma) \le 2\max\left(e^{-t^2/4}, e^{-t\sigma/2}\right).$$

Theorem 3.1.28. ([96]*) *Assume*

$$1 < c < \frac{q}{32\log q}$$

(hence implicitely $q \ge 164$) and

$$16c\frac{\log q}{q} < \rho < 1 - 16c\frac{\log q}{q}.$$

With probability exceeding $1 - 2q^{1-c}$ the random set R corresponding to probability ρ satisfies

$$\big||R| - \rho q\big| < 3\sqrt{c\rho(1-\rho)q\log q},$$

$$\frac{1}{3\sqrt{c\log q}}\sqrt{\frac{1-\rho}{\rho q}} < \lambda^-(R) \le \lambda^+(R) < 3\sqrt{c\log q}\sqrt{\frac{1-\rho}{\rho q}}.$$

Proof. Put $f_0(x) = \xi_x$ if $x \in \mathcal{G}_1 \cup \mathcal{G}_2$, $f_0(x) = \xi_{-x}$ if $x \in -\mathcal{G}_2$. The function testifying the upper estimate will be this with a modified value at 0.

We calculate the expectation and variance of $\hat{f}_0$. Clearly

$$\hat{f}_0(\gamma) = \sum_{y\in\mathcal{G}_1} \xi_y\gamma(y) + 2\sum_{y\in\mathcal{G}_2} \xi_y \mathrm{Re}\,\gamma(y),$$

hence

$$\mathbf{E}(\hat{f}_0(\gamma)) = \rho\sum_{y\in\mathcal{G}_1}\gamma(y) + 2\rho\sum_{y\in\mathcal{G}_2}\mathrm{Re}\,\gamma(y) = \begin{cases}\rho q & \text{if } \gamma = \mathbf{1},\\ 0 & \text{otherwise.}\end{cases}$$

Similarly, the variance is

$$\mathbf{D}^2(\hat{f}_0(\gamma)) = \rho(1-\rho)\left(\sum_{y\in\mathcal{G}_1}\gamma(y)^2 + \sum_{y\in\mathcal{G}_2}\big(2\mathrm{Re}\,\gamma(y)\big)^2\right)$$

$$= \begin{cases}\rho(1-\rho)(2q_2+q) & \text{if } \gamma^2 = \mathbf{1},\\ 2\rho(1-\rho)q_2 & \text{otherwise,}\end{cases}$$

consequently

$$\mathbf{D}^2(\hat{f}_0(\gamma)) < 2\rho(1-\rho)q.$$

We apply Lemma 3.1.27 with an obvious rescaling (the variables $2\mathrm{Re}\,\gamma(y)\xi_y$ are bounded by 2 rather than 1) to obtain that in the range $t \le 2\sqrt{\rho(1-\rho)q}$

$$\Pr\bigl(|\hat{f}_0(\gamma)| \ge t\sqrt{\rho(1-\rho)q}\bigr) \le 2e^{-t^2/8} \quad (\gamma \ne \mathbf{1}),$$

$$\Pr\bigl(|\hat{f}_0(\mathbf{1}) - \rho q| \ge t\sqrt{\rho(1-\rho)q}\bigr) \le 2e^{-t^2/8}.$$

We put $t = \sqrt{8c\log q}$ (this is in accordance with $t \le 2\sqrt{\rho(1-\rho)q}$, as the assumptions of the theorem on ρ show), so that the right hand sides above become $2q^{-c}$. Since there are altogether q possible characters γ, with probability $1 - 2q^{1-c}$ none of the above events happens. In this favourable case we write

$$a = t\sqrt{\rho(1-\rho)q} = \sqrt{8c\rho(1-\rho)q\log q},$$

$$f(x) = \begin{cases} f_0(x) + a & \text{if } x = 0, \\ f_0(x) & \text{otherwise,} \end{cases}$$

$$\hat{f}(\gamma) = \hat{f}_0(\gamma) + a \ge \begin{cases} 0 & \text{always ,} \\ \rho q & \text{if } \gamma = \mathbf{1}. \end{cases}$$

This shows $f \in \mathcal{S}^+(R)$ and consequently

$$\lambda^+(R) \le \frac{f(0)}{\hat{f}(\mathbf{1})} < \frac{1+a}{\rho q} < 3\sqrt{c\log q}\sqrt{\frac{1-\rho}{\rho q}}.$$

To prove the lower estimate let R' be the standard complement of R, which is a random standard set for probability $1-\rho$, hence the above argument gives

$$\lambda^+(R') < 3\sqrt{c\log q}\sqrt{\frac{\rho}{(1-\rho)q}}$$

with the same probability. The lower estimate follows from the duality relation in Theorem 3.1.13.

The estimate of $|R|$ follows from $|R| = \hat{f}_0(\mathbf{1})$ or $\hat{f}_0(\mathbf{1}) + 1$. □

Our lower and upper estimates differ by a factor of $\log q$. We have no guess whether this is necessary, or the values of the λ's are more concentrated. The large deviation estimate used is quite sharp. If the values of $\hat{f}_0(\gamma)$ were independent for different characters γ, one could deduce that

$$\min \hat{f}_0(\gamma) < -c_1 a$$

with high probability, with some positive constant c_1. They are far from independent, but still it is likely that their dependence is not very strong, and the existence of large negative values can be proved. On the other hand there is no reason to think that the uniform weights used in the proof above are near optimal.

Now we turn to estimating the δ quantities. This problem drew some attention in the case $\rho = 1/2$, in the context of estimating the clique number of Cayley

graphs. Alon and Orilitsky [1] proved that typically $\Delta(R) \lesssim (\log q)^2$ in this case. Below we adapt their proof for general ρ. Green [48] improved this estimate to the optimal $O(\log q)$ for cyclic groups. (Green considers sumsets rather than difference sets, but an adaptation to differences is possible.) Prakash [108] improved Alon and Orilitsky's estimate for general commutative groups with cardinality composed of few primes. It is likely that Green's and Prakash' methods can also be extended to general ρ.

Theorem 3.1.29. ([96]*)

(a) Assume

$$q^{-1/2} < \rho < 1 - q^{-1/3}\log q.$$

With probability exceeding $1-\exp\left(-c_1 \log^2 q/\log\frac{1}{\rho}\right)$ *the random set* R *corresponding to probability* ρ *satisfies*

$$\overline{\Delta}(R) < c_2\left(\frac{\log q}{\log\frac{1}{\rho}}\right)^2,\ \overline{\delta}(R) > \frac{1}{c_2}\left(\frac{\log\frac{1}{\rho}}{\log q}\right)^2. \tag{3.43}$$

Here c_1, c_2 *are absolute constants. In the range*

$$1 - q^{-1/3}\log q < \rho < 1 - 16c\frac{\log q}{q},\ 1 < c < \frac{q}{32\log q}$$

with probability exceeding $1 - 2q^{1-c}$ *we have*

$$\overline{\Delta}(R) < 3\sqrt{c\log q}\sqrt{\frac{\rho q}{1-\rho}},\ \overline{\delta}(R) > \frac{1}{3\sqrt{c\log q}}\sqrt{\frac{1-\rho}{\rho q}}.$$

(b) Assume

$$q^{-1/3}\log q < \rho < 1 - q^{-1/2}.$$

With probability exceeding $1-\exp\left(-c_1 \log^2 q/\log\frac{1}{1-\rho}\right)$ *the random set* R *corresponding to probability* ρ *satisfies*

$$\Delta(R) < c_2\left(\frac{\log q}{\log\frac{1}{1-\rho}}\right)^2,\ \delta(R) < \frac{c_2}{q}\left(\frac{\log q}{\log\frac{1}{1-\rho}}\right)^2. \tag{3.44}$$

Here c_1, c_2 *are the same constants. In the range*

$$16c\frac{\log q}{q} < \rho < q^{-1/3}\log q,\ 1 < c < \frac{q}{32\log q}$$

with probability exceeding $1 - 2q^{1-c}$ *we have*

$$\Delta(R) < 3\sqrt{c\log q}\sqrt{\frac{(1-\rho)q}{\rho}},\ \delta(R) < 3\sqrt{c\log q}\sqrt{\frac{(1-\rho)}{\rho q}}.$$

For small values of ρ estimate (3.43) stops improving; we shall study later the

passage of $\overline{\Delta}$ from 2 to 3. For ρ very near 1 the estimate becomes trivial.

We need some preparation before turning to the proof of Theorem 3.1.29.

We define the *effective cardinality* of a standard set by the formula

$$|A|' = |A \cap (\mathcal{G}_1 \cup \mathcal{G}_2)| - 1.$$

This quantity is between $(|A| - 1)/2$ and $|A| - 1$. The probability that a difference set of a given set B is contained in a random standard set is

$$\Pr(B - B \subset R) = \rho^{|B-B|'}.$$

Consequently the expected number of difference sets of sets of cardinality k contained in R is

$$\sum_{B \subset \mathcal{G}, |B|=k} \rho^{|B-B|'}.$$

This quantity is difficult to control, because we do not know enough about the distribution of $|B - B|$. When k is small compared to q, we expect that for most sets $|B - B|$ will be of size $> ck^2$, but there is no applicable result of this kind. Instead we will select such subsets of an arbitrary set.

Lemma 3.1.30. ([96]*) *Let A be a finite set in a commutative group, $|A| = m$, and let k be an integer, $1 \le k \le \sqrt{m}$. There is a $B \subset A$, $|B| = k$ satisfying*

$$|B - B| \ge 1 + \frac{k(k-1)}{2}\left(1 - \frac{k(k-1)}{2m}\right). \tag{3.45}$$

This lemma is also in Alon and Orilitsky's paper; below we give a slightly simpler proof.

Proof. We use induction on k. Assume we found a k-element subset

$$B = \{b_1, \dots, b_k\}.$$

We try to add a further element $a \in A$. The elements $a - b_i$ will be in the difference set of the set $B' = B \cup \{a\}$; let z_a be the number of those that are already contained in $B - B$. This quantity does not exceed the number of solutions of

$$a - b_i = b_u - b_v,\ 1 \le i, u, v \le k$$

(it may be smaller, as several pairs u, v may exist for a given i). Hence

$$\sum_{a \in A} z_a \le k^3,$$

consequently there is an $a \in A$ with $z_a \le k^3/m$. This means that at least $k - k^3/m$ new differences occur, and this provides the inductive step. □

By a theorem of Komlós, Sulyok, Szemerédi [76], in $\mathbb{Z}_q$ we can find a set $B \subset A$ of size $|B| > c\sqrt{m}$ which is a Sidon set, that is, all differences are distinct. In

general groups we could only show the analogous result with $|B| > c\sqrt[3]{m}$; however, the weaker property given in Lemma 3.1.30 is equally applicable for our aims.

Proof of Theorem 3.1.29. We are going to estimate $\Pr\big(\overline{\Delta}(R) \geq m\big)$. Set $k = [\sqrt{m}]$. By the lemma above, the event $\overline{\Delta}(R) \geq m$ is contained in the event

$$\exists B : B - B \subset R,\ |B| = k,\ B \text{ satisfies (3.45)}.$$

Since (3.45) implies

$$|B - B|' \geq \frac{|B - B| - 1}{2} \geq c_4 m$$

with a suitable positive constant c_4, for a given B the probability is $\leq \rho^{c_4 m}$. Since the number of k-element sets is less than q^k, we obtain

$$\Pr\big(\overline{\Delta}(R) \geq m\big) < q^{\sqrt{m}} \rho^{c_4 m}.$$

This immediately gives the estimate in (3.43). The validity of this estimate is not restricted to the range given in Theorem 3.1.29; however, for ρ near to 1 we get a better result by applying Theorem 3.1.28 and the inequality $\overline{\delta}(R) \geq \lambda^+(R)$. This is presented in the next formula.

This proves part (a); part (b) is the dual formulation. □

Remark 3.1.31. One can give a lower estimate for $\overline{\Delta}(R)$ as follows. Select sets $B_1, \ldots, B_m$ satisfying $|B_i| = k$ and

$$(B_i - B_i) \cap (B_j - B_j) = \{0\}$$

whenever $i \neq j$. Then the events $B_i - B_i \subset R$ will be independent and we have

$$\begin{aligned} \Pr\big(\overline{\Delta}(R) \geq k\big) &\geq \Pr\big(B_i - B_i \subset R \text{ for some } i\big) \\ &= \prod_i \left(1 - \rho^{|B_i - B_i|'}\right). \end{aligned}$$

To make use of this one needs to find many such B_i with small difference set. This is comparably easy, if $\mathcal{G}$ has no element of order $< k$: we take arithmetic progressions $B_i = \{0, b_i, 2b_i, \ldots, (k-1)b_i\}$, and a simple greedy algorithm yields $m \geq q/k^2$ such sets. For $\rho = 1/2$ this shows that $\overline{\Delta}(R) \gtrsim \log q$ with high probability, so together with Green's bound this shows the proper order of magnitude for certain groups. For general groups a weaker form of this argument gives $\overline{\Delta}(R) \gtrsim \sqrt{\log q}$. □

We now study the threshold as $\overline{\Delta}$ passes from 2 to 3. Elements of order 3 play a special role here. Assume x is an element of order 3. The difference set of the 3-element set (subgroup) $\{0, x, -x\}$ is itself, hence $\overline{\Delta}(A) < 3$ is possible only if elements of order 3 are all absent from A. To avoid this we assume that $3 \nmid q$, that is, there are no elements of order 3. With some extra effort the next result can be extended (with a properly modified notion of a random set) to all groups, save those isomorphic to $\mathbb{Z}_3^k$.

Proposition 3.1.32. ([96]*) *Let $\mathcal{G}$ be a finite commutative group, $|\mathcal{G}| = q$, and assume that $3 \nmid q$. For $\frac{6}{5}q^{-1} < \rho < q^{-2/3}$ the random set R corresponding to probability ρ satisfies*

$$\Pr(\overline{\Delta}(R) \leq 2) > 1 - q^2\rho^3.$$

Proof. It is easy to see that the property $\overline{\Delta}(R) \geq 3$ is equivalent to the existence of $a, b, c \in R$, all different from 0, such that $a + b + c = 0$. For a given $a, b, c \in \mathcal{G}$ we have

$$\Pr(a, b, c \in R) = \begin{cases} \rho^3 & \text{if they are all distinct,} \\ \rho^2 & \text{if two coincide .} \end{cases}$$

(All three cannot coincide by the absence of elements of order 3, and one cannot coincide with the negative of another.) The number of such triples a, b, c containing distinct elements is $< q^2$, order counted, so without ordering it is $< q^2/6$; the number of triples containing two identical elements (that is, $a, a, -2a$) is exactly $q - 1$. We obtain

$$\Pr(\overline{\Delta}(R) \geq 3) < q^2\rho^3/6 + q\rho^2 < q^2\rho^3.$$

□

Remark 3.1.33. If $\overline{\Delta}(R) \leq 2$, its value can be 1 or 2. The probability that it is 1 is exactly $(1 - \rho)^{q_1+q_2-1}$; it becomes negligible around $\rho \sim (\log q)/q$.

With some effort the above proposition could be complemented by an upper estimate showing that $\Pr(\overline{\Delta}(R) \geq 3) \to 1$ if $\rho q^{2/3} \to \infty$. □

Part (a) of Theorem 3.1.6 follows from the results of this section. Indeed, if $\rho = q^{-2/3}/2$, then the corresponding random set satisfies $\overline{\delta}(R) = 1/2$ and $\lambda^+(R) < cq^{-1/6}(\log q)^{1/2}$ with positive probability, according to Proposition 3.1.32 and Theorem 3.1.28.

3.1.9 Balls in dyadic groups

In this section we will prove part (b) of Theorem 3.1.6 by studying some sets in the group $\mathcal{G} = \mathbb{Z}_2^n$ (so now $q = 2^n$). The elements will be written as 0-1 sequences. For an $x \in \mathcal{G}$ by its *norm* we mean the number of coordinates equal to 1, denoted by $\|x\|$. We consider the *ball*

$$B_k = \{x \in \mathcal{G} : \|x\| \leq k\},$$

and its standard complement, the *antiball*

$$A_k = \{x \in \mathcal{G} : \|x\| > k\} \cup \{0\}.$$

The size of maximal difference sets contained in B_k is known: for even $k < n$ we have

$$\overline{\Delta}(B_k) = \Delta(A_k) = |B_{k/2}| = \sum_{i \leq k/2} \binom{n}{i}, \tag{3.46}$$

see Kleitman [67]. Much less is known about $\Delta(B_k)$, in spite of much attention, due to its interpretation as the maximal size of a set of error-detecting codes. In

this context the inequality $\delta(B_k) \leq \overline{\delta}(B_k)$ is known as the Hamming bound, while Delsarte [34] introduced the improved bound $\delta(B_k) \leq \lambda^-(B_k)$. Asymptotically, as $k/n \to \gamma$ for some $0 < \gamma < 1$, the best current upper estimate for $\lambda^-(B_k)$ is by McEliece et al. [100], and numerical results in [8] suggest this estimate actually gives the correct value of $\lambda^-(B_k)$. The best lower bound for $\delta(B_k)$ is the Gilbert-Varshamov bound given by the usual covering argument (see [88]). Samorodnitsky [119] proved that the Delsarte bound cannot match the Gilbert-Varshamov bound.

In the sequel we apply Samorodnitsky's method from [118] to estimate certain λ's of the sets B_k and A_k. We focus on the case $k > n/2$, which is uninteresting from the point of view of coding theory. Samorodnitsky's aspect is rather different from ours, so we repeat a part of the argument in our words. The central ingredient is the following inequality, which is Lemma 3.3 in [118].

Lemma 3.1.34. ([118]) *Let F be a polynomial of degree at most k, satisfying $F(0) = 1$ and $F(i) \geq 0$ for integer values of i, $0 \leq i \leq n$. Assume $k \leq n$ and write $\alpha = k/(2n)$. We have*

$$\sum_{i=0}^{n} \binom{n}{i} F(i) \geq c_1 n^{-1/4} \binom{2n}{k}^{-1/2} 2^n \geq c_2 \alpha^{1/4} \left(2\alpha^{\alpha}(1-\alpha)^{1-\alpha}\right)^n \tag{3.47}$$

with positive absolute constants c_1, c_2.

Theorem 3.1.35. ([96]*) *Assume $k \leq n$ and write $\alpha = k/(2n)$,*

$$\beta = -(\alpha \log_2 \alpha + (1-\alpha)\log_2(1-\alpha)).$$

We have

$$\lambda(B_k) \geq c_2 \alpha^{1/4} \left(\alpha^{\alpha}(1-\alpha)^{1-\alpha}\right)^n = c_2 \alpha^{1/4} q^{-\beta}, \tag{3.48}$$

$$\lambda(A_k) \leq c_3 \alpha^{-1/4} q^{\beta - 1}, \tag{3.49}$$

with positive absolute constants c_2, c_3.

Proof. We want to estimate $f(0)/\hat{f}(\mathbf{1})$ for functions $f \in \mathcal{S}(B_k)$ such that $\hat{f} \geq 0$. By Proposition 3.1.16 we may assume that f is invariant under automorphisms that leave B_k fixed. Permutations of coordinates are such automorphisms, hence f depends only on the number of coordinates equal to 1. This means that there are real numbers $a_0, \ldots, a_k$ such that $f(x) = a_i$ if $\|x\| = i \leq k$, and $f(x) = 0$ if $\|x\| > k$. Consequently

$$\hat{f}(\gamma) = \sum_{i=0}^{k} a_i \sum_{\|x\|=i} \gamma(x). \tag{3.50}$$

The characters of $\mathcal{G}$ are easily described in the form

$$\gamma_y(x) = (-1)^{\langle x,y \rangle}, \ y \in \mathcal{G}$$

where $\langle x, y \rangle$ is the scalar product in the usual sense, so it is an integer between 0 and n. This defines a natural norm for characters; we write $\|\gamma\| = \|y\|$ if $\gamma = \gamma_y$.

It is easily seen, by grouping the elements $x \in \mathcal{G}$ according to the value of $j = \langle x, y\rangle$ that whenever $\|y\| = m$, we have

$$\sum_{\|x\|=i} \gamma_y(x) = \sum_{j=0}^{\min(i,m)} (-1)^j \binom{m}{j}\binom{n-m}{i-j}.$$

The important point is that this is a polynomial of degree i in m (these are called Krawchouk polynomials). By substituting this into (3.50) we obtain that

$$\hat{f}(\gamma) = F(\|\gamma\|),$$

where F is a polynomial of degree at most k. We have

$$\hat{f}(\mathbf{1}) = F(0)$$

and, by Fourier inversion,

$$f(0) = \frac{1}{q}\sum_{\gamma} \hat{f}(\gamma) = \frac{1}{q}\sum_{\gamma} F(\|\gamma\|) = \frac{1}{q}\sum_{m=0}^{n} \binom{n}{m} F(m).$$

Inequality (3.48) now follows by applying (3.47), and inequality (3.49) by duality (Theorem 3.1.13). □

So far we did not succeed in finding a function that would constructively demonstrate inequality (3.49).

We complement these inequalities by some easy bounds for $\lambda^{\pm}$.

Theorem 3.1.36. ([96]*) *Assume $n/2 - 1 < k \le n$.*

We have

$$\lambda^{\pm}(B_k) \le \frac{2k+2}{q(2k+2-n)}, \tag{3.51}$$

$$\lambda^{\pm}(A_k) \ge 1 - \frac{n}{2k+2}. \tag{3.52}$$

Proof. Consider the characters, corresponding to the basis vectors (with some abuse of notation):

$$\gamma_j(x_1, \ldots, x_n) = (-1)^{x_j} = 1 - 2x_j.$$

Clearly

$$\sum \gamma_j(x) = n - 2\|x\|,$$

hence the function

$$f(x) = 2k + 2 - n + \sum \gamma_j(x) = 2(k + 1 - \|x\|)$$

satisfies

$$f \in \mathcal{S}^{\pm}(B_k),\ f(0) = 2k+2,\ \hat{f}(\mathbf{1}) = q(2k+2-n).$$

This shows (3.51), and (3.52) follows by duality (Theorem 3.1.13). □

Let us summarize the results for the set A_k in the case when $\frac{1}{4} < \alpha = \frac{k}{2n} < \frac{1}{2}$. By equation (3.46) and standard approximations for the binomial coefficients we have $\delta(A_k) = q^{\beta-1+o(1)}$. Equation (3.49) shows that $\lambda(A_k)$ is in the same range $\lambda(A_k) = q^{\beta-1+o(1)}$. On the other hand, equation (3.52) shows that $\lambda^{\pm}(A_k) \geq 1 - \frac{1}{4\alpha}$. If $\alpha \approx 1/2$ this proves part (b) of Theorem 3.1.6.

Example 3.1.37. We show how examples of $\lambda^- < \lambda^{\pm}$ are related to monotonicity of $\lambda^{\pm}$. Let A be a set such that $\lambda^-(A) < \lambda^{\pm}(A)$, e.g. the antiball A_k above. Take an $f \in \mathcal{S}^-(A)$ which produces the value of $\lambda^-(A)$, and put

$$A^+ = \{x : f(x) > 0\}.$$

We have clearly $A^+ \subset A$ and $f \in \mathcal{S}^{\pm}(A^+)$, hence

$$\lambda^{\pm}(A^+) \leq f(0)/\hat{f}(\mathbf{1}) = \lambda^-(A) < \lambda^{\pm}(A).$$

□

3.2 Application to Paley graphs

For a prime $p \equiv 1 \pmod 4$, the Paley graph $\mathcal{P}_p$ is the graph with vertex set $\mathbb{Z}_p$ and an edge between x and y if and only if $x - y = a^2$ for some non-zero $a \in \mathbb{Z}_p$. More generally, Paley graphs can also be defined in the same manner for any finite field $\mathbb{F}_q$, $q \equiv 1 \pmod 4$, but we will only be concerned with the prime case.

Paley graphs are self-complementary, vertex and edge transitive, and $(p, (p-1)/2, (p-5)/4, (p-1)/4)$-strongly regular (see [16] for these and other basic properties of $\mathcal{P}_p$). Paley graphs have received considerable attention over the past decades because they exhibit many properties of random graphs $G(p, 1/2)$ where each edge is present with probability $1/2$. Indeed, $\mathcal{P}_p$ form a family of *quasi-random* graphs, as shown in [26].

In this note we will be concerned with the *independence number* of $\mathcal{P}_p$, i.e. the maximal cardinality $s(p)$ of a set $B \subset \mathbb{Z}_p$ such that the difference set $B - B$ contains only quadratic non-residues (and zero). It is clear by self-complementarity that the independence number of $\mathcal{P}_p$ is equal to its clique-number. The general lower bound $s(p) \geq (\frac{1}{2} + o(1)) \log_2 p$ is established in [28], while it is proved in [47] that $s(p) \geq c \log p \log\log\log p$ for infinitely many primes p. The "trivial" upper bound $s(p) \leq \sqrt{p}$ has been re-discovered several times (see [34, Theorem 3.9], [87, Problem 13.13], [25, Proposition 4.7], [16, Chapter XIII, Theorem 14], [86, Theorem 31.3], [78, Proposition 4.5], [33, Section 2.8] for various proofs). This bound is notoriously difficult to improve, and it is mentioned explicitly in the selected list of problems [33]. The only improvement we are aware of concerns the special case $p = n^2 + 1$ for which it is proved in [90] that $s(p) \leq n - 1$ (the same result was proved independently by T. Sanders – unpublished, personal communication). It is more likely, heuristically, that the lower bound is closer to the truth than the upper bound. Numerical data [137,138] up to $p < 10000$ suggest (very tentatively) that the correct order of magnitude for the clique number of $\mathcal{P}_p$ is $c \log^2 p$ (see the discussion and the plot of the function $s(p)$ at [139]).

In this note we prove the slightly improved upper bound $s(p) \leq \sqrt{p} - 1$ for the *majority* of the primes $p = 4k + 1$ (we will often suppress the dependence on p, and just write s instead of $s(p)$). The proof has two cornerstones. The first is Delsarte's bound as described in Theorem 3.1.4. The second is a "subclique trick" introduced in [106], which can be incorporated to the linear programming bound to yield an improvement. This will be described in Lemma 3.2.1 below.

We will denote the set of nonzero quadratic residues by Q, and that of nonzero non-residues by NQ. Note that $0 \notin Q$ and $0 \notin NQ$.

3.2.1 The improved upper bound

We will first formulate the "subclique trick" introduced in [106], in the general setting. We will describe it in finite groups for simplicity.

Lemma 3.2.1. ([106]) *Assume $B = \{b_1, \dots b_m\} \subset \mathcal{G}$ is such that $b_j - b_k \in A^c \cup \{0\}$. Let $h(x) = \frac{1}{|B|} \sum_{y \in \mathcal{G}} \mathbf{1}_B(y)\mathbf{1}_B(x+y)$. Assume $D \subset \mathcal{G}$ is such that any selection of k distinct elements of D contains two such that their difference falls in A. Then*

$$\sum_{x \in D} h(x) \leq k - 1. \tag{3.53}$$

Proof. Let us evaluate the sum in question:

$$\sum_{x \in D} h(x) = \frac{1}{|B|} \sum_{x,y \in \mathcal{G}} \mathbf{1}_D(x)\mathbf{1}_B(y)\mathbf{1}_B(x+y) = \tag{3.54}$$

$$\frac{1}{|B|} \sum_{y \in \mathcal{G}} \mathbf{1}_B(y) \sum_{x \in \mathcal{G}} \mathbf{1}_D(x)\mathbf{1}_B(x+y).$$

The point is that the inner sum is $\leq k - 1$ for each $y \in \mathcal{G}$. Indeed, if it were $\geq k$ for some y then there would exist distinct elements $d_1, \dots d_k \in D$ such that the elements $b_1 = d_1 + y, \dots, b_k = d_k + y$ are all in B. By assumption, however, there would exist two of them, say d_i and d_j such that $d_i - d_j \in A$ which contradicts that $b_i - b_j \in A^c$. □

In what way is this an improvement to Delsarte's bound? The function $h(x)$ trivially belongs to the set $\mathcal{S}^+(\mathcal{G} \setminus A)$, and satisfies $\hat{h} \geq 0$. The point is that inequality (3.53) might introduce *new linear constraints* on $h(x)$ if appropriate sets $D \subset \mathcal{G}$ exist.

After this preparation we are in position to state the slightly improved upper bound on the independence number of Paley-graphs.

Theorem 3.2.2. ([4]*) *Let $p = 4k + 1$ be a prime, and $B \subset \mathbb{Z}_p$, $|B| = s$, be a maximal set such that $B - B \subset NQ \cup \{0\}$. The following hold:*
(i) if $n = [\sqrt{p}]$ is even then $s^2 + s - 1 \leq p$
(ii) if $n = [\sqrt{p}]$ is odd then $s^2 + 2s - 2 \leq p$.

Proof. Consider the function $f(x) = \mathbf{1}_B * \mathbf{1}_{-B}(x) = \sum_{y\in\mathbb{Z}_p} \mathbf{1}_B(y)\mathbf{1}_B(x+y)$, which gives the number of representations $x = b - b'$ with $b, b' \in B$. This function has the following properties:

$$f(0) = s \tag{3.55}$$

$$\hat{f}(\mathbf{1}) = \sum_{x\in\mathbb{Z}_p} f(x) = s^2 \tag{3.56}$$

$$f(x) \geq 0 \text{ if } \ x \in NQ, \ f(x) = 0 \text{ if } x \in Q \tag{3.57}$$

$$\hat{f}(\gamma) = \sum_{x\in\mathbb{Z}_p} f(x)\gamma(x) \geq 0 \text{ for all } \gamma \in \hat{\mathbb{Z}}_p. \tag{3.58}$$

Using the notations of Section 3.1, properties (3.55), (3.56), (3.57) mean that $f \in \mathcal{S}^+(NQ)$, and $\hat{f} \geq 0$ by (3.58). It is quite easy to determine the quantities $\lambda^+(Q)$ and $\lambda^-(Q)$, both of which turn out to be $\frac{1}{\sqrt{p}}$. This implies the trivial bound $|B| \leq \sqrt{p}$, but we will impose further restrictions on f to get an improvement.

In order to use Lemma 3.2.1 we would need to identify a 'large' set $D \subset \mathbb{Z}_p$ such that $D - D \subset Q \cup \{0\}$. At first glance this seems to be impossible, as such sets D are cliques themselves, and hence are necessarily 'small'. However, we can circumvent this problem by considering the translated copies of the hypothetical set B. The details are as follows.

Let χ denote the quadratic multiplicative character, i.e. $\chi(t) = \pm 1$ according to whether $t \in Q$ or $t \in NQ$ (and $\chi(0) = 0$). Let

$$\varphi(t) = \sum_{b\in B} \chi(t+b), \tag{3.59}$$

giving the number of quadratic residues minus the number of non-residues in the shifted set $t + B$. If $t \in -B$ then by assumption $\varphi(t) = -s + 1 < 0$ (for the last inequality note that $s \geq 2$ for every $p = 4k + 1$). Also, $\sum_{t\in\mathbb{Z}_p} \varphi(t) = \sum_{b\in B} \sum_{t\in\mathbb{Z}_p} \chi(t+b) = 0$. Therefore, $\varphi(t)$ must also assume some positive values. Let t_0 be the place where φ assumes its maximum, $\varphi(t_0) > 0$ (note that $t_0 \notin -B$). Let $B_{t_0} = (t_0 + B) \cap Q$ denote the set of quadratic residues contained in $t_0 + B$, and let $r = |B_{t_0}|$. Then $r > \frac{s}{2}$, and B_{t_0} is a set of quadratic residues such that $B_{t_0} - B_{t_0} \subset NQ \cup \{0\}$. We claim that

$$s \leq 1 + \frac{p-1}{2r}. \tag{3.60}$$

Let $z \in NQ$ be arbitrary, and consider the set $C_z = zB_{t_0}$. Then $C_z \subset NQ$ and $C_z - C_z \subset Q \cup \{0\}$. By Lemma 3.2.1 we have

$$\sum_{x\in C_z} f(x) \leq s. \tag{3.61}$$

Summing up (3.61) for all $z \in NQ$ we obtain

$$\sum_{x \in NQ} f(x) \leq \frac{p-1}{2}\frac{s}{r}. \tag{3.62}$$

Finally, putting together (3.55), (3.56), (3.57), (3.62) we conclude

$$s^2 = \sum_{x \in \mathbb{Z}_p} f(x) = f(0) + \sum_{x \in NQ} f(x) \leq s + \frac{p-1}{2}\frac{s}{r}, \tag{3.63}$$

and hence we obtain (3.60).

We have seen that $r > \frac{s}{2}$. So, if s is even, $r \geq \frac{s}{2} + 1$, and if s is odd, $r \geq \frac{s+1}{2}$. However, in the latter case we will need the stronger inequality $r \geq \frac{s+3}{2}$.

Lemma 3.2.3. ([4]*) *If s is odd, then $r \geq \frac{s+3}{2}$.*

Proof. Assume to the contrary that $r = \frac{s+1}{2}$. Consider the numbers $\varphi(t)$, $t \notin -B$, and denote them for simplicity by $a_1 \leq \cdots \leq a_{p-s}$. They are odd integers, and

$$\sum_{j=1}^{p-s} a_j = \sum_{t \in \mathbb{Z}_p} \varphi(t) - \sum_{t \in -B} \varphi(t) = s(s-1). \tag{3.64}$$

We also know the sum of the squares:

$$\begin{aligned}\sum_{j=1}^{p-s} a_j^2 &= \sum_{t \notin -B} \varphi(t)^2 = \sum_{t \in \mathbb{Z}_p} \varphi(t)^2 - \sum_{t \in -B} \varphi(t)^2 \\ &= \sum_{b_1, b_2 \in B} \sum_{t \in \mathbb{Z}_p} \chi(t+b_1)\chi(t+b_2) - s(s-1)^2.\end{aligned}$$

We have

$$\sum_{b_1 = b_2 \in B} \sum_{t \in \mathbb{Z}_p} \chi(t+b_1)\chi(t+b_2) = \sum_{b \in B} \sum_{t \in \mathbb{Z}_p} \chi(t+b)^2 = s(p-1).$$

For $b_1 \neq b_2 \in B$, $b_1 - b_2 \in NQ$; from the strong regularity of the Paley graph we obtain

$$\sum_{b_1 \neq b_2 \in B} \sum_{t \in \mathbb{Z}_p} \chi(t+b_1)\chi(t+b_2) = -s(s-1).$$

Putting everything together, we find

$$\sum_{j=1}^{p-s} a_j^2 = s(p - s^2 + s - 1). \tag{3.65}$$

By our assumption, all the positive values of $\varphi(t)$ are equal to 1. Also, by the definition of φ we have $\varphi(t) \geq -s$ for all t. Notice, however, that the less trivial

inequality

$$-s+2 \leq \varphi(t) \leq 1 \tag{3.66}$$

also holds. Indeed, $\varphi(t) = -s$ is impossible because in that case the set B could be further extended by the element $-t$. Also, $\varphi(t) = -s+1$ is impossible due to parity reasons.

The end of the argument is that the constraints (3.64), (3.65), (3.66) contradict each other. Indeed, from (3.64) and (3.65), we compute

$$\sum_{j=1}^{p-s} \left(a_j + \frac{s-3}{2} \right)^2 = \frac{9p - s - 2ps - 6s^2 + ps^2 - s^3}{4} \tag{3.67}$$

and from (3.66) we have

$$\sum_{j=1}^{p-s} \left(a_j + \frac{s-3}{2} \right)^2 \leq \left(\frac{s-1}{2} \right)^2 (p-s), \tag{3.68}$$

but (3.67) and (3.68) imply $p \leq s^2$, a contradiction.

Therefore, we conclude that there exists a t such that $\varphi(t) > 1$, and hence $\varphi(t) \geq 3$ and $r \geq \frac{s+3}{2}$. □

Now we can conclude the proof of the theorem. Indeed, if $s \leq n-1$, then both parts of the claim follow immediately. We assume therefore that $s = n$. If s is even we have seen that $r \geq \frac{s}{2}+1$, hence $s^2+s-1 \leq p$ follows directly from (3.60). If s is odd, the trivial estimate $r \geq \frac{s+1}{2}$ combined with (3.60) just leads to the well-known $s \leq \sqrt{p}$. But we have proved that $r \geq \frac{s+3}{2}$ and hence $s^2+2s-2 \leq p$ follows from (3.60). □

Remark 3.2.4. It is clear from (3.60) that any improved lower bound on r will lead to an improved upper bound on s. If one thinks of elements of $\mathbb{Z}_p$ as being quadratic residues randomly with probability $1/2$, then we expect that $r \geq \frac{s}{2} + c\sqrt{s}$. This would lead to an estimate $s \leq \sqrt{p} - cp^{1/4}$. This seems to be the limit of this method. In order to get an improved lower bound on r one can try to prove non-trivial upper bounds on the third moment $\sum_{t \in \mathbb{Z}_p} \varphi^3(t)$. To do this, we would need that the distribution of numbers $\frac{b_1-b_2}{b_1-b_3}$ is approximately uniform on Q as b_1, b_2, b_3 ranges over B. This is plausible because if $s \approx \sqrt{p}$ then the distribution of $B-B$ must be close to uniform on NQ. However, we could not prove anything rigorous in this direction.

Remark 3.2.5. An alternative proof of Lemma 3.2.3 is as follows. The multiplicative character χ is a polynomial of degree $\frac{p-1}{2}$, $\chi(x) = x^{\frac{p-1}{2}}$, and therefore so is the function $\varphi(t)$. The sum of the positive values of $\varphi(t)$ is $\geq s(s-1)$, by (3.64). However, the value $+1$ is assumed at most $\frac{p-1}{2} < s(s-1)$ times due to the degree of φ. Therefore, there must be other positive values, i.e. values where $\varphi(t) \geq 3$. It is instructive to see how both proofs break down in $\mathbb{F}_{p^2}$ where the example $C = \mathbb{F}_p$ shows that there exists a clique of size p. In that case the function $\varphi(t)$ assumes the values $-p+1$ and $+1$ only (it becomes a constant polynomial over $\mathbb{F}_p$).

Remark 3.2.6. Theorem 3.2.2 gives the bound $s \leq [\sqrt{p}]-1$ for about three quarters of the primes $p = 4k+1$. Indeed, part *(ii)* gives this bound for almost all p such that $n = [\sqrt{p}]$ is odd, with the only exception when $p = (n+1)^2 - 3$. Part *(i)* gives the improved bound $s \leq n-1$ if $n^2 + n - 1 > p$. This happens for about half of the primes p such that n is even. To make these statements rigorous we note that $\sqrt{p}/2$ is uniformly distributed modulo one, when p ranges over primes of the form $p = 4k+1$: this is a special case of a result of Balog, [6, Theorem 1].

3.3 Application to mutually unbiased bases (MUBs)

This section describes a surprising application of Delsarte's method to the problem of mutually unbiased bases (MUBs) in $\mathbb{C}^d$. The fact that it can be applied to a problem from a completely different part of mathematics also highlights the flexibility of the method.

The section is organized as follows. In Section 3.3.1 we give a standard summary of relevant notions and results concerning mutually unbiased bases (MUBs) and mutually unbiased Hadamard matrices (MUHs). Then we describe how the problem of the MUBs fits the Delsarte scheme of Section 3.1. In Section 3.3.2 we use discrete Fourier analysis to prove several structural results on MUHs in low dimensions. Finally, in Section 3.3.3 we prove non-existence results. We also give a new proof, without using computer algebra, of the fact the Fourier matrix F_6 cannot be part of a complete system of MUHs in dimension 6.

3.3.1 Mutually unbiased bases

Two orthonormal bases in $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \ldots, \mathbf{f}_d\}$ are called *unbiased* if for every $1 \leq j, k \leq d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \dfrac{1}{\sqrt{d}}$. In general, we will say that two unit vectors $\mathbf{u}$ and $\mathbf{v}$ are *unbiased* if $|\langle \mathbf{u}, \mathbf{v} \rangle| = \dfrac{1}{\sqrt{d}}$. A collection $\mathcal{B}_0, \ldots \mathcal{B}_m$ of orthonormal bases is said to be *(pairwise) mutually unbiased* if every two of them are unbiased. What is the maximal number of pairwise mutually unbiased bases (MUBs) in $\mathbb{C}^d$? This question originates from quantum information theory and has been investigated thoroughly over the past decades. The motivation behind studying MUBs is that if a physical system is prepared in a state of one of the bases, then all outcomes are equally probable when we conduct a measurement in any other basis, and this fact finds applications in dense coding, teleportation, entanglement swapping, covariant cloning, and state tomography (see [36] for a recent comprehensive survey on MUBs and its applications). The following result is well-known:

Theorem 3.3.1. ([7, 12, 144]) *The maximal number of mutually unbiased bases in $\mathbb{C}^d$ is at most $d+1$.*

Another important result concerns prime-power dimensions.

Theorem 3.3.2. ([7,61,66,144]) *A collection of $d+1$ mutually unbiased bases (called a complete set of MUBs) exists if the dimension d is a prime or a prime-power.*

However, if the dimension $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is composite then very little is known except for the fact that there are at least $p_j^{\alpha_j} + 1$ mutually unbiased bases in Γ^d where $p_j^{\alpha_j}$ is the smallest of the prime-power divisors. In some specific square dimensions there is a construction based on orthogonal Latin squares which yields more MUBs than $p_j^{\alpha_j} + 1$ (see [142]). It is also known [140] that the maximal number of MUBs cannot be exactly d (i.e. it is either $d + 1$ or strictly less than d).

The following basic problem remains open for all non-primepower dimensions:

Problem 3.3.3. *Does a complete set of $d + 1$ mutually unbiased bases exist in $\mathbb{C}^d$ if d is not a prime-power?*

The answer is not known even for $d = 6$, despite considerable efforts over the past few years ([12,21,22,62,110]). The case $d = 6$ is particularly tempting because it seems to be the simplest to handle with algebraic and numerical methods. As of now, numerical evidence suggests that the maximal number of MUBs for $d = 6$ is 3 (see [21, 22, 24, 145]).

It will also be important for us to recall that mutually unbiased bases are naturally related to mutually unbiased *complex Hadamard matrices*. Indeed, if the bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ are mutually unbiased we may identify each $\mathcal{B}_l = \{\mathbf{e}_1^{(l)}, \dots, \mathbf{e}_d^{(l)}\}$ with the *unitary* matrix

$$[U_l]_{j,k} = \left[\left\langle \mathbf{e}_j^{(0)}, \mathbf{e}_k^{(l)} \right\rangle_{1 \le k,j \le d} \right],$$

i.e. the k-th column of U_l consists of the coordinates of the k-th vector of $\mathcal{B}_l$ in the basis $\mathcal{B}_0$. (Throughout the section the scalar product $\langle ., . \rangle$ of Γ^d is conjugate-linear in the first variable and linear in the second.) With this convention, $U_0 = I$ the identity matrix, and all other matrices are unitary and have all entries of modulus $1/\sqrt{d}$. Therefore, for $1 \le l \le m$ the matrices $H_l = \sqrt{d} U_l$ have all entries of modulus 1 and complex orthogonal rows (and columns). Such matrices are called *complex Hadamard matrices*. It is thus clear that the existence of a family of $m + 1$ mutually unbiased bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ is equivalent to the existence of a family of m complex Hadamard matrices $H_1, \dots, H_m$ such that for all $1 \le j \ne k \le m$, $\frac{1}{\sqrt{d}} H_j^* H_k$ is again a complex Hadamard matrix. In such a case we will say that these complex Hadamard matrices are *mutually unbiased* (MUHs).

A system $H_1, \dots, H_m$ of MUHs is called *complete* if $m = d$ (cf. Theorem 3.3.1). We remark that there has been a recent interest in *real* unbiased Hadamard matrices [14,57,83], and one result of this section is that no pair of real unbiased Hadamard matrices can be part of a complete system of MUHs (see Corollary 3.3.13). The system $H_1, \dots H_m$ of MUHs will be called *normalized* if the first column of H_1 has all coordinates 1, and all the columns in all the matrices have first coordinate 1. It is clear that this can be achieved by appropriate multiplication of the rows and columns by umimodular complex numbers. We will also use the standard definition that two complex Hadamard matrices H_1 and H_2 are equivalent, $H_1 \cong H_2$, if $H_1 = D_1 P_1 H_2 P_2 D_2$ with unitary diagonal matrices D_1, D_2 and permutation matrices P_1, P_2.

One possible approach to the MUB problem in dimension 6 is to try to classify (up to equivalence) all complex Hadamard matrices of order 6. However, such a

full classification is still out of reach, despite some promising recent developments [9, 64, 65, 98, 129].

The crucial observation here is that the columns of $H_1, \ldots, H_m$ can be regarded as elements of the group $\mathcal{G} = \mathbb{T}^d$, where $\mathbb{T}$ stands for the complex unit circle ([92]). By doing so, we can use Fourier analysis on $\mathcal{G}$ to investigate the problem of MUHs. We will now collect some notations that will be used in later sections. In this setting it is natural to use reversed notations compared to Section 3.1: the group operation in $\mathcal{G}$ is complex *multiplication* in each coordinate, while the operation will be *addition* in the dual group. In particular, the unit element will be denoted by $\mathbf{1}$ in $\mathcal{G}$ and by 0 in $\hat{\mathcal{G}}$. The dual group is $\hat{\mathcal{G}} = \mathbb{Z}^d$, and the action of a character $\gamma = (r_1, r_2, \ldots, r_d) \in \mathbb{Z}^d$ on a group element $\mathbf{v} = (v_1, v_2, \ldots, v_d) \in \mathbb{T}^d$ is given by exponentiation in each coordinate $\gamma(\mathbf{v}) = \mathbf{v}^\gamma = v_1^{r_1} v_2^{r_2} \ldots v_d^{r_d}$. The Fourier transform of (the indicator function of) a set $S \subset \mathcal{G}$ is given as $\hat{S}(\gamma) = \sum_{\mathbf{s} \in S} \mathbf{s}^\gamma$.

The notion of orthogonality and unbiasedness makes it natural to introduce the following definitions.

Definition 3.3.4. *The orthogonality set ORT_d is defined as $ORT_d = \{\mathbf{v} = (z_1, \ldots, z_d) \in \mathbb{T}^d \ : \ z_1 + \cdots + z_d = 0\}$, and the unbiasedness set is $UB_d = \{\mathbf{v} = (z_1, \ldots, z_d) \in \mathbb{T}^d \ : \ |z_1 + \cdots + z_d|^2 - d = 0\}$.*

If $H_1, \ldots, H_m$ are MUHs then the (coordinate-wise) quotient $\mathbf{v}/\mathbf{u} = (v_1/u_1, v_2/u_2, \ldots, v_d/u_d)$ of any two distinct columns from the matrices will fall into either ORT_d (if $\mathbf{v}$ and $\mathbf{u}$ are in the same matrix) or into UB_d (if $\mathbf{v}$ and $\mathbf{u}$ are in different matrices). This enables us to invoke the general scheme of Section 3.1, Delsarte's method. As the group $\mathbb{T}^d$ is not finite (but still compact), we include here the analogue of Theorem 3.1.4.

Lemma 3.3.5. ([92]*) *Let $\mathcal{G} = \mathbb{T}^d$, and let a symmetric subset $A = 1/A \subset \mathcal{G}$, $\mathbf{1} \in A$ be given. Assume h is a nonzero function with the following properties: $h(x) = h(1/x)$, $h(x) \leq 0$ for all $x \in A^c$, $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{\mathcal{G}}$. Assume also that the Fourier inversion formula holds for h (in particular, h can be any finite linear combination of characters on $\mathcal{G}$). Then for any $B = \{b_1, \ldots b_m\} \subset \mathcal{G}$ such that $b_j/b_k \in A^c \cup \{\mathbf{1}\}$ the cardinality of B is bounded by $|B| \leq \frac{h(\mathbf{1})}{\hat{h}(0)}$.*

Proof. The proof is analogous to that of Theorem 3.1.4. For any $\gamma \in \hat{\mathcal{G}}$ define $\hat{B}(\gamma) = \sum_{j=1}^m \gamma(b_j)$. Now, evaluate

$$S = \sum_{\gamma \in \hat{\mathcal{G}}} |\hat{B}(\gamma)|^2 \hat{h}(\gamma). \tag{3.69}$$

All terms are nonnegative, and the term corresponding to $\gamma = 0$ (the trivial character) gives $|\hat{B}(0)|^2 \hat{h}(0)$. Therefore

$$S \geq |B|^2 \hat{h}(0). \tag{3.70}$$

On the other hand, $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j/b_k)$, and therefore $S = \sum_{\gamma,j,k} \gamma(b_j/b_k)\hat{h}(\gamma)$. Summing up for fixed j, k we get

$\sum_\gamma \gamma(b_j/b_k)\hat{h}(\gamma) = h(b_j/b_k)$ (the Fourier inversion formula), and therefore $S = \sum_{j,k} h(b_j/b_k)$. Notice that $j = k$ happens $|B|$-many times, and all the other terms (when $j \neq k$) are non-positive because $b_j/b_k \in A^c$, and h is required to be non-positive there. Therefore

$$S \leq h(\mathbf{1})|B|. \tag{3.71}$$

Comparing the two estimates (3.70), (3.71) we obtain $|B| \leq \frac{h(\mathbf{1})}{\hat{h}(0)}$. □

We are now in position to prove a generalization of Theorem 3.3.1.

Theorem 3.3.6. ([92]*) *Let $\mathcal{A}$ be an orthonormal basis in $\mathbb{C}^d$, and let $B = \{\mathbf{c}_1, \dots \mathbf{c}_r\}$ consist of unit vectors which are all unbiased to $\mathcal{A}$. Assume that for all $1 \leq j \neq k \leq r$ the vectors $\mathbf{c}_j$ and $\mathbf{c}_k$ are either orthogonal or unbiased to each other, i.e. either $\langle \mathbf{c}_j, \mathbf{c}_k \rangle = 0$ or $|\langle \mathbf{c}_j, \mathbf{c}_k \rangle| = 1/\sqrt{d}$. Then $r \leq d^2$.*

Proof. Let us define the 'forbidden' set $A_d = (ORT_d \cup UB_d)^c$. As we saw in the discussion above, the vectors $\mathbf{u}_1, \dots \mathbf{u}_r \in \mathbb{T}^d$ (associated to $\sqrt{d}\mathbf{c}_1, \dots \sqrt{d}\mathbf{c}_r$) satisfy $\mathbf{u}_j/\mathbf{u}_k \in A_d^c \cup \{\mathbf{1}\}$ for all $1 \leq j, k \leq r$. Therefore Lemma 3.3.5 can be applied.

Define the 'witness' function $h : \mathbb{T}^d \to \mathbb{R}$ as follows:

$$h(z_1, \dots z_d) = \frac{1}{(d-1)d} \left|z_1 + \dots + z_d\right|^2 \left(\left|z_1 + \dots + z_d\right|^2 - d\right). \tag{3.72}$$

It is straightforward to check that h satisfies all requirements. Indeed, h is an even function which vanishes on $ORT_d \cup UB_d$. The Fourier coefficients of h are simply the coefficients of the terms after expanding the brackets, and these are clearly nonnegative. Also $\hat{h}(0) = 1$ because $\hat{h}(0)$ is the integral of h, which is just the constant term. Also, $h(\mathbf{1}) = d^2$, so that we conclude from Lemma 3.3.5 that $|B| \leq d^2$. □

As shown by Theorem 3.3.2 the result of Theorem 3.3.6 is sharp if d is a prime-power. If d is not a prime-power then, in principle, it could be possible to find a better witness function than the h above. However, so far we have not been able to identify such an improved function in dimension 6, and I personally do not believe that such an improvement exists (although I cannot prove it). I believe that Delsarte's method alone, as presented in Lemma 3.3.5, is not sufficient to prove $|B| < d^2$ in any dimension d.

All known complete systems of MUHs, in prime-power dimensions, contain exclusively roots of unity as entries. This means that it makes sense to consider the MUB problem in discrete subgroups of $\mathbb{T}^d$, containing Nth roots of unity. We have done this for $d = 6$ and $N = 12, 16$, and Delsarte's bound shows that for those values complete sets of MUBs cannot exist.

Proposition 3.3.7. ([92]*) *For $N = 12, 16$ there exists no complete system of MUBs in dimension 6 such that the coordinates of all appearing vectors are Nth roots of unity.*

Another observation is that if $r = d^2$ in Theorem 3.3.6 then both estimates (3.70), (3.71) must hold with equality. On the one hand, it is trivial that (3.71)

automatically becomes an equality for the h above (because h is zero on ORT_d and UB_d). On the other hand, inequality (3.70) becomes an equality *if only if* $|\hat{B}(\gamma)|^2\hat{h}(\gamma) = 0$ for all $\gamma \neq 0$. These are non-trivial conditions and we obtain the following corollary, which is a generalization of Theorem 8 in [11].

Corollary 3.3.8. ([92]*) *Let $\mathcal{A}$ be an orthonormal basis in $\mathbb{C}^d$, and let $B = \{\mathbf{c}_1, \dots \mathbf{c}_{d^2}\}$ consist of unit vectors which are all unbiased to $\mathcal{A}$. Assume that for all $1 \leq j \neq k \leq d^2$ the vectors $\mathbf{c}_j$ and $\mathbf{c}_k$ are either orthogonal or unbiased to each other. Write B as a $d \times d^2$ matrix, the columns of which are the vectors $\mathbf{c}_j$, $j = 1, \dots d^2$. Let $\mathbf{r}_1, \dots \mathbf{r}_d$ denote the rows of the matrix B, and let $\mathbf{r}_{j/k} = \mathbf{r}_j/\mathbf{r}_k$ denote the coordinate-wise quotient of the rows. Then the vectors $\mathbf{r}_{j/k}$ $(1 \leq j \neq k \leq d)$ are orthogonal to each other in $\mathbb{C}^{d^2}$, and they are all orthogonal to the vector $(1, 1, \dots 1) \in \mathbb{C}^{d^2}$.*

3.3.2 Structural results on MUBs in low dimensions

In this section we extend the investigations of Section 3.3.1 with new ideas, and prove several non-existence results concerning complete systems of MUBs, as well as some structural results in low dimensions.

In what follows we will assume that a *complete* system of MUHs $H_1, \dots H_d$ is given. In fact, much of the discussion below remains valid for non-complete systems after appropriate modifications, but it will be technically easier to restrict ourselves to the complete case. The general aim is to establish structural properties of $H_1, \dots H_d$ which give restrictions on what a complete system may look like. If some of these properties were to contradict each other in a non-primepower dimension d, then we could conclude that a complete system of dimension d does not exist. This is one of the main tasks for future research, mainly for $d = 6$. We will give some non-existence results in this direction in Section 3.3.3.

Consider each appearing complex Hadamard matrix H_j as a d-element set in $\mathbb{T}^d$ (the elements are the columns $\mathbf{c}_1, \dots \mathbf{c}_d$ of the matrix; the dependence on j is suppressed for simplicity), and introduce its Fourier transform

$$g_j(\gamma) := \hat{H}_j(\gamma) = \sum_{k=1}^{d} \mathbf{c}_k^{\gamma} \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{3.73}$$

Notice that the orthogonality of the *rows* of H_j implies that if $\rho \in \mathbb{Z}^d$ is any permutation of the vector $(1, -1, 0, 0, \dots, 0)$ then

$$g_j(\rho) = 0. \tag{3.74}$$

Also, note that conjugation is the same as taking reciprocal for unimodular numbers, i.e. $\overline{g_j(\gamma)} = \sum_{k=1}^{d} \mathbf{c}_k^{-\gamma}$, and therefore the square of the modulus of $g_j(\gamma)$ can be written as

$$G_j(\gamma) := |g_j(\gamma)|^2 = \sum_{k,l=1}^{d} (\mathbf{c}_k/\mathbf{c}_l)^{\gamma} \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{3.75}$$

Also, introduce the notation

$$G(\gamma) := \sum_{j=1}^{d} G_j(\gamma) \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{3.76}$$

In similar fashion, introduce the Fourier transform of the whole system as

$$f(\gamma) := \sum_{j=1}^{d} g_j(\gamma) \qquad \text{for each } \gamma \in \mathbb{Z}^d, \quad \text{and} \tag{3.77}$$

$$F(\gamma) := |f(\gamma)|^2 = \sum_{\mathbf{u},\mathbf{v}}^{d} (\mathbf{u}/\mathbf{v})^{\gamma} \qquad \text{for each } \gamma \in \mathbb{Z}^d, \tag{3.78}$$

where the summation goes for all pairs of columns $\mathbf{u}, \mathbf{v}$ in the matrices $H_1, \ldots, H_d$.

The main advantage of taking Fourier transforms is that any polynomial relation (such as orthogonality or unbiasedness) among the entries of the matrices H_j will be turned into a *linear* relation on the Fourier side. We will collect here linear equalities and inequalities concerning the functions $F(\gamma)$ and $G(\gamma)$.

Let $\pi_r = (0, 0, \ldots 0, 1, 0, \ldots 0) \in \mathbb{Z}^d$ denote the vector with the rth coordinate equal to 1. Then for each $j = 1, \ldots d$ we have

$$\sum_{r=1}^{d} G_j(\gamma + \pi_r) = \sum_{r=1}^{d} \left(\sum_{k,l=1}^{d} (\mathbf{c}_k/\mathbf{c}_l)^{\gamma+\pi_r} \right) = \sum_{k,l=1}^{d} (\mathbf{c}_k/\mathbf{c}_l)^{\gamma} \left(\sum_{r=1}^{d} (\mathbf{c}_k/\mathbf{c}_l)^{\pi_r} \right),$$

and observe that the last sum is zero by orthogonality if $k \neq l$, while it is d if $k = l$. This means that for each $j = 1, \ldots d$,

$$\sum_{r=1}^{d} G_j(\gamma + \pi_r) = d^2 \qquad \text{for each } \gamma \in \mathbb{Z}^d, \tag{3.79}$$

which then implies

$$\sum_{r=1}^{d} G(\gamma + \pi_r) = d^3 \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{3.80}$$

In a similar fashion we can turn the unbiasedness relations also to linear constraints on the Fourier side. Let $\mathbf{u}/\mathbf{v} = (z_1, z_2 \ldots, z_d) \in \mathbb{T}^d$ be the coordinate-wise quotient of any two columns from two *different* matrices from $H_1, \ldots H_d$. Then $\mathbf{u}$ and $\mathbf{v}$ are unbiased, which means that

$$0 = |\sum_{r} z_r|^2 - d = \sum_{r \neq t} z_r/z_t. \tag{3.81}$$

Using this we can write

$$\sum_{r\neq t} F(\gamma+\pi_r-\pi_t) - \sum_{r\neq t} G(\gamma+\pi_r-\pi_t) = \sum_{\mathbf{u},\mathbf{v}} (\mathbf{u}/\mathbf{v})^{\gamma} \left(\sum_{r\neq t} (\mathbf{u}/\mathbf{v})^{\pi_r-\pi_t} \right) = 0, \quad (3.82)$$

where the summation on $\mathbf{u}, \mathbf{v}$ goes for all pairs of columns from *different* matrices, and the last equality is satisfied because each inner sum is zero by (3.81). Also, by (3.80) we have $dG(\gamma) + \sum_{r\neq t} G(\gamma+\pi_r-\pi_t) = d^4$, and we can use this to rewrite (3.82) as

$$dG(\gamma) + \sum_{r\neq t} F(\gamma+\pi_r-\pi_t) = d^4, \quad (3.83)$$

which is somewhat more convenient than (3.82).

We also have some further trivial constraints on F and G. Namely,

$$F(0) = d^4, \quad G(0) = d^3, \qquad \text{and} \quad (3.84)$$

$$0 \leq F(\gamma) \leq d^4, \quad 0 \leq G(\gamma) \leq d^3, \quad \text{for each } \gamma \in \mathbb{Z}^d. \quad (3.85)$$

Also, by the Cauchy-Schwartz inequality we have

$$F(\gamma) \leq dG(\gamma), \qquad \text{for each } \gamma \in \mathbb{Z}^d. \quad (3.86)$$

Note that the linear constraints (3.80), (3.83), (3.84), (3.85), (3.86) put severe restrictions on the functions F and G. In fact, it turns out that *all* the structural results on complete systems of MUHs in dimensions 2, 3, 4, 5 follow from these constraints. These structural results are not new (cf. [23]) but nevertheless we list here the two most important ones as an illustration of the power of this Fourier approach. The first one is a celebrated theorem of Haagerup [54] which gives a full classification of complex Hadamard matrices of order 5. In the original paper [54] the author combines several clever ideas with lengthy calculations to derive the result, whereas it follows almost for free from the formalism above.

Proposition 3.3.9. ([54]) *Any complex Hadamard matrix of order 5 is equivalent to the Fourier matrix F_5, given by $F_5(j,k) = \omega^{(j-1)(k-1)}$, $(j,k = 1,\ldots,5)$, where $\omega = e^{2i\pi/5}$.*

Proof. Let H_1 be a complex Hadamard matrix of order 5. Then the function $G_1(\gamma) = |\hat{H}_1(\gamma)|^2$ satisfies equation (3.79) for all $\gamma \in \mathbb{Z}^5$. Now, regard each $G_1(\gamma)$ as a *variable* as γ ranges through the following set: $\Gamma = \{\gamma = (\gamma_1,\ldots\gamma_5) \in \mathbb{Z}^5 : |\gamma_1| + \cdots + |\gamma_5| \leq 10\}$. (We remark that it is possible to reduce the number of variables considerably due to permutation equivalences. However, it does not change the essence of the forthcoming argument, only makes the computations much quicker). Let $\rho = (5,-5,0,0,0) \in \mathbb{Z}^5$. Set the following linear programming problem: minimize $G_1(\rho)$ subject to the conditions (3.79), and $G_1(0) = 25$, and $0 \leq G_1(\gamma) \leq 25$ for all $\gamma \in \Gamma$. A short computer code testifies that the solution to this linear programming problem is $G_1(\rho) \geq 25$, which actually implies $G_1(\rho) = 25$. And the same holds for any permutation of ρ.

Also, we may assume without loss of generality that H_1 is normalized (i.e. its first row and column are made up of 1s), and then the information above implies that all other entries of H_1 are 5th roots of unity. It is then trivial to check that there is only one way (up to equivalence) to build up a complex Hadamard matrix from 5th roots of unity, namely the matrix F_5. □

We remark here that all the linear programming problems mentioned in this section have rational coefficients, so no numerical errors are encountered, and each result is certifiable (by hand, if necessary). Let us also remark that Proposition 3.3.9 is the only *non-trivial* result concerning MUHs and MUBs in dimensions $d \leq 5$. The classification of complex Hamamard matrices and MUBs is more or less trivial for $d = 2, 3, 4$ due to the geometry of complex unit vectors. We give here the essence of this classification (for full details see [23]).

Proposition 3.3.10. ([23], [97]*) *In any normalized complete system of MUHs in dimension $d = 3, 4, 5$ all entries of the matrices are dth roots of unity. For $d = 2$ all entries are 4th roots of unity.*

Proof. The proof of this statement is similar to that of Proposition 3.3.9. Let $d = 3, 4, 5$. Assume $H_1, \dots H_d$ is a normalized complete system of MUHs. Then the functions F and G must satisfy the linear constraints (3.80), (3.83), (3.84), (3.85), (3.86). Regarding each $F(\gamma)$ and $G(\gamma)$ as a nonnegative variable (as γ ranges through a sufficiently large cube around the origin in $\mathbb{Z}^d$), a short linear programming code testifies that under these conditions $F(\rho) = d^4$ for all such $\rho \in \mathbb{Z}^d$ which is a permutation of $(d, -d, 0, \dots, 0)$. This means that all entries in all of the matrices must be dth roots of unity. The proof is analogous for $d = 2$ except that in this case we can only conclude $F(4, -4) = 16$, so that the matrices contain 4th roots of unity. □

Let us make a remark here about $d = 4$. In this case it is *not true* that all normalized Hadamard matrices must be composed of 4th roots of unity. However, it is true that a complete system of MUHs must be composed of such. This phenomenon shows up very clearly in our linear programming codes. Writing the constraints (3.79) on $G_1(\gamma)$, and $G_1(0) = 16$, and $0 \leq G_1(\gamma) \leq 16$ does not enable us to conclude that $G_1(\rho) = 16$ with ρ being a permutation of $(4, -4, 0, 0)$. However, writing all the constraints (3.80), (3.83), (3.84), (3.85), (3.86) on the functions F and G we can indeed conclude that $F(\rho) = 4G(\rho) = 256$.

We end this section with a few remarks concerning $d = 6$. If we could similarly conclude that

$$F(\rho) = 6^4 \qquad \text{for all } \rho \text{ being a permutation of } (6, -6, 0, 0, 0, 0) \tag{3.87}$$

then it would mean that a complete system of normalized MUHs in dimension 6 can only be composed of 6th roots of unity. Such a structural information would be wonderful, as it is proven in [12] that no such complete system of MUHs exists. Therefore, we could conclude that a complete system of MUHs does not exist at all. Unfortunately, the constraints (3.80), (3.83), (3.84), (3.85), (3.86) do not seem

to imply (3.87). At least, we have run a linear programming code with γ ranging through as large a cube as possible (due to computational limitations), and could not conclude (3.87). Nevertheless, our main strategy for future research in dimension 6 must be as follows: using the linear constraints on F and G try to establish some structural information on the vectors appearing in a hypothetical complete system of MUHs, and then show by other means (e.g. a brute force computer search) that such constraints cannot be satisfied. We formulate here one conjecture which could be crucial in proving the non-existence of a complete system of MUHs in dimension 6.

Conjecture 3.3.11. ([97]*) *Let H_1 be any complex Hadamard matrix of order 6, not equivalent to the isolated matrix S_6 (cf. [131] for the matrix S_6). Let ρ be any permutation of the vector $(1,1,1,-1,-1,-1)$. Then $g_1(\rho)=0$ for the function g_1 defined in* (3.73).

This conjecture is supported heavily by numerical data. We have tried hundreds of matrices randomly from each known family of complex Hadamard matrices of order 6 (including numerically given matrices from the most recent 4-parameter family [129]). Currently we cannot prove this conjecture, but in Section 3 we will show an example of how it could be used in the proof of non-existence results (cf. Remark 3.3.15). We also mention that the conjecture has recently been proved in [99] for Karlson's 3-parameter family [65] of complex Hadamard matrices of order 6.

3.3.3 Non-existence results

We now turn to non-existence results, namely that complete systems of MUHs with certain properties do not exist. The first of these is that any pair of *real* unbiased Hadamard matrices cannot be part of a complete system of MUHs. In fact, we prove the following stronger statement.

Theorem 3.3.12. ([97]*) *Let $H_1,\dots H_d$ be a complete system of MUHs such that H_1 is a real Hadamard matrix. Then any column vector $\mathbf{v}=(v_1,\dots,v_d)$ of the other matrices $H_2,\dots H_d$ satisfies that $\sum_{k=1}^d v_k^2=0$.*

Proof. Let $0\neq\rho=(r_1,\dots,r_d)\in\mathbb{Z}^d$ be such that $\sum_{k=1}^d r_k=0$ and $\sum_{k=1}^d |r_k|\leq 4$. There are five types of these vectors (up to permutation): $(1,-1,0,\dots,0)$, $(2,-2,0,\dots,0)$, $(2,-1,-1,0,\dots,0)$, $(-2,1,1,0,\dots,0)$, and $(1,1,-1,-1,0,\dots 0)$. Then, Theorem 8 in [11] (or Corollary 2.4 in [92]) shows that the function f defined in (3.77) satisfies

$$f(\rho)=0 \tag{3.88}$$

for all these vectors ρ.

Let $\mathbf{c}_1,\mathbf{c}_2,\dots,\mathbf{c}_{d^2}$ denote the column vectors appearing in the system $H_1,\dots H_d$. For each $\gamma\in\mathbb{Z}^d$ let

$$\mathbf{v}(\gamma)=(\mathbf{c}_1^\gamma,\dots\mathbf{c}_{d^2}^\gamma)\in\mathbb{T}^{d^2} \tag{3.89}$$

for $k=1,\dots d$. Consider the vectors $\gamma_k=(0,\dots 0,2,0,\dots 0)\in\mathbb{Z}^d$ with the 2 appearing in position k. Finally, consider the vector $\mathbf{w}=\sum_{k=1}^d\mathbf{v}(\gamma_k)$, and let us

evaluate $\|\mathbf{w}\|^2$. On the one hand, the vectors $\mathbf{v}(\gamma_k)$ are all orthogonal to each other by (3.88), and they all have length $\|\mathbf{v}(\gamma_k)\|^2 = d^2$, and hence $\|\mathbf{w}\|^2 = d^3$. On the other hand *we know* the first d coordinates of $\mathbf{w}$. Each $\mathbf{v}(\gamma_k)$ has first d coordinates equal to 1, because H_1 is a real Hadamard matrix. Therefore the first d coordinates of $\mathbf{w}$ are all equal to d. Therefore, $\|\mathbf{w}\|^2 \geq d^3$ on account of the first d coordinates. Hence, all other coordinates of $\mathbf{w}$ must be zero, which is exactly the statement of the theorem. □

Theorem 3.3.12 implies immediately the following corollary.

Corollary 3.3.13. ([97]*) *Let $H_1, \dots H_d$ be a complete system of MUHs such that H_1 is a real Hadamard matrix. Then there is no further purely real column in any of the matrices $H_2, \dots, H_d$. In particular, it is impossible to have two real Hadamard matrices in a complete set of MUHs.*

This statement is sharp in the sense that for $d = 2, 4$ the complete systems of MUHs are known to contain *one* real Hadamard matrix. Also, in several dimensions $d = 4n^2$ pairs (and even larger systems) of real unbiased Hadamard matrices are known to exist [14, 57], so that the corollary above is meaningful and non-trivial.

Our next result is a new proof of the fact in dimension 6 the Fourier matrix F_6 cannot be part of a complete system of MUHs. This result is well-known, but the only proof we are aware of uses some computer algebra, while we present an easy conceptual proof here.

Proposition 3.3.14. ([97]*) *There exists no complete system of MUHs in dimension 6 which contains the Fourier matrix F_6.*

Proof. Assume by contradiction that such a system $H_1, \dots H_6$ exists, and assume $H_1 = F_6$. Consider the vectors $\gamma_1 = (1, 1, 1, 0, 0, 1)$, $\gamma_2 = (0, 0, 1, 1, 1, 1)$, $\gamma_3 = (1, 1, 0, 1, 1, 0)$, $\gamma_4 = (0, 1, 0, 1, 0, 2)$, $\gamma_5 = (1, 0, 0, 0, 1, 2)$, and $\gamma_6 = (0, 1, 0, 0, 2, 1)$, and consider the corresponding vectors $\mathbf{v}(\gamma_k)$ defined in (3.89), and let $\mathbf{w} = \sum_{k=1}^{6} \mathbf{v}(\gamma_k)$. All the vectors $\mathbf{v}(\gamma_k)$ are orthogonal to each other by (3.88), therefore $\|\mathbf{w}\|^2 = 216$. On the other hand, we know the first 6 coordinates of $\mathbf{w}$. It is easy to calculate that each of these coordinates has modulus 6, and therefore $\|\mathbf{w}\|^2 \geq 216$ on account of the first 6 coordinates. This implies that all the other coordinates of $\mathbf{w}$ must be zero. This yields a polynomial identity for the coordinates of any column vector appearing in the matrices $H_2, \dots, H_6$. Instead of using this identity directly, however, we observe that the same argument applies to the vectors $\gamma_1, \dots \gamma_5$ and $\gamma_6' = (2, 0, 0, 1, 0, 1)$, and $\mathbf{w}' = \mathbf{v}(\gamma_6') + \sum_{k=1}^{5} \mathbf{v}(\gamma_k)$. By considering the difference $\mathbf{w} - \mathbf{w}'$ we conclude that $\mathbf{v}(\gamma_6)$ and $\mathbf{v}(\gamma_6')$ must coincide in the last 30 coordinates. That is, if $(z_1, \dots, z_6)$ is any column vector in the matrices $H_2, \dots H_6$ then $z_2 z_5^2 z_6 = z_1^2 z_4 z_6$, and hence $z_2 z_5^2 = z_1^2 z_4$. Furthermore, one can permute the coordinates of γ_k in a cyclic manner, and the argument remains unchanged, yielding this time $z_5 z_2^2 = z_4^2 z_1$. Dividing these two equations finally gives $z_5/z_2 = z_1/z_4$ for each of the last 30 vectors in our complete system of MUHs. This means, by definition, that the last 30 coordinates of the vectors $\mathbf{v}(0, -1, 0, 0, 1, 0)$ and $\mathbf{v}(1, 0, 0, -1, 0, 0)$ coincide. But this is a contradiction, because these vectors should be orthogonal to each other by (3.88). □

Finally, we discuss a non-existence result which states that the matrices $F_6(a,b)$ of the Fourier family (cf. [131] for a formula of these matrices) cannot be extended to a complete system of MUHs in dimension 6.

Theorem 3.3.15. ([62,97]*) *There exists no complete system $H_1,\dots,H_6$ of MUHs in dimension 6 which contains any of the matrices $F_6(a,b)$ of the Fourier family.*

Proof. This theorem was proved rigorously in [62] by a massive computer search after a discretization scheme. We sketch the proof here, on the condition that Conjecture 3.3.11 is valid. The argument is very elegant, and shows a possible way forward in proving the non-existence of complete systems of MUHs in dimension 6.

First, note that it is equivalent to prove the statement for the transposed family $F_6^T(a,b)$. To see this, assume in general that $H_1,\dots,H_6$ is a complete system of MUHs, and consider the extended system $H_1,\dots,H_6,\sqrt{d}I$ (where I is the identity matrix). Multiplying everything from the left by $\frac{1}{\sqrt{d}}H_1^*$ we see that $\sqrt{d}I, \frac{1}{\sqrt{d}}H_1^*H_2,\dots\frac{1}{\sqrt{d}}H_1^*H_6, H_1^*$ is also a complete system of MUHs. Therefore, H_1 can be part of a complete system of MUHs if and only if H_1^* can. Then conjugating each column in all the matrices we see that H_1^* can be part of a complete system of MUHs if and only if H_1^T can. The significance of this fact is that the transposed family $F_6^T(a,b)$ is technically easier to handle because each member of the family contains the three column vectors $\mathbf{c}_1=(1,1,1,1,1,1)$, $\mathbf{c}_2=(1,\omega,\omega^2,1,\omega,\omega^2)$ and $\mathbf{c}_3=(1,\omega^2,\omega,1,\omega^2,\omega)$, where $\omega=e^{2i\pi/3}$.

Also, it is well-known (see [22]) that a complex Hadamard matrix equivalent to S_6 cannot be part of a complete system of MUHs (in fact, it cannot even be part of a pair of MUHs), so that we can assume without loss of generality that none of $H_1,\dots H_6$ are not equivalent to S_6. The significance of this fact is that now Conjecture 3.3.11 (if true) can be invoked.

Assume now, by contradiction, that $H_1=F_6^T(a,b),H_2,\dots,H_6$ is a complete system of MUHs. One can make a clever selection of vectors in $\mathbb{Z}^6$ such that the same argument as in Proposition 3.3.14 can be used. Namely, let
$\gamma_1=(0,0,0,0,0,0)$, $\gamma_2=(0,0,1,-1,-1,1)$, $\gamma_3=(0,0,1,0,0,-1)$,
$\gamma_4=(0,0,2,-1,-1,0)$, $\gamma_5=(0,1,0,0,-1,0)$, $\gamma_6=1(0,1,1,0,-1,-1)$,
$\gamma_7=(1,0,0,-1,0,0)$, $\gamma_8=(1,0,1,-1,0,-1)$, $\gamma_9=(1,1,0,-1,-1,0)$,
$\gamma_{10}=(1,1,1,-1,-1,-1)$, $\gamma_{11}=(1,-1,1,0,-1,0)$, $\gamma_{12}=(1,0,1,0,-2,0)$,
while let $\gamma'_{11}=(-1,1,1,-1,0,0)$, $\gamma'_{12}=(0,1,1,-2,0,0)$.

For the system $\gamma_1,,\dots,\gamma_{10},\gamma_{11},\gamma_{12}$ all the vectors $\mathbf{v}(\gamma_k)$ are orthogonal to each other by either (3.88) or by Conjecture 3.3.11, so that $\|\mathbf{w}\|^2=|\sum_{k=1}^{12}\mathbf{v}(\gamma_k)|^2=432$. (This is where we use Conjecture 3.3.11.) On the other hand, three coordinates of $\mathbf{w}$ corresponding to the columns $\mathbf{c}_1,\mathbf{c}_2,\mathbf{c}_3$ are known exactly, and they happen to be 12 (the vectors γ_k were chosen accordingly). As in Proposition 3.3.14 this leads us to conclude that all the other 33 coordinates of $\mathbf{w}$ must be zero. The same is true for the vector $\mathbf{w}'$ generated by the system $\gamma_1,,\dots,\gamma_{10},\gamma'_{11},\gamma'_{12}$. By considering the difference $\mathbf{w}-\mathbf{w}'$ we conclude that if $(z_1,\dots,z_6)$ is any column (different from $\mathbf{c}_1,\mathbf{c}_2,\mathbf{c}_3$) in our complete system of MUHs then the identity $\frac{z_1z_3}{z_2z_5}+\frac{z_1z_3}{z_5^2}=\frac{z_2z_3}{z_1z_4}+\frac{z_2z_3}{z_4^2}$ must hold. After simplifying by z_3 and conjugating the equation we get $z_1z_4(z_1+z_4)=z_2z_5(z_2+z_5)$.

By applying a cyclic permutation to the coordinates of the selected γ_k's we can derive in the same manner that $z_2z_5(z_2+z_5) = z_3z_6(z_3+z_6)$. Furthermore, 30 of these columns $(z_1,\dots,z_6)$ – the ones contained in $H_2,\dots,H_6$ – must be unbiased to $\mathbf{c}_1 = (1,1,1,1,1,1)$, and hence they must satisfy $|z_1+\dots+z_6| = \sqrt{6}$. It is not hard to show that there are exactly 56 vectors $(z_1,\dots,z_6)$ satisfying all these constraints (one can write up the solutions exactly). However, one can form pairs among these 56 vectors such that in any pair the two vectors are neither orthogonal nor unbiased to each other. Therefore, our system can contain at most one vector from each pair, i.e. at most 28 vectors, a contradiction. □

We believe that the proof of the non-existence of complete systems of MUHs in dimension 6 will hinge on Conjecture 3.3.11. The reason is that it introduces yet another non-trivial linear constraint on the function G, and these constraints will ultimately lead to a contradiction (maybe indirectly, as in Proposition 3.3.14). Therefore, we would be very interested to see a proof of Conjecture 3.3.11.

3.4 Future prospects

In this section we list some further possible applications of Delsarte's method. It is remarkable that the method is so flexible that it can be applied to several problems coming from different parts of mathematics.

3.4.1 Integer sets avoiding kth powers

It is a famous problem in number theory to give bounds on the cardinality of a set $B \subset \{0,1,\dots,N\}$ such that the differences $b_i - b_j$ avoid the square numbers. The best known lower bound is given by a construction of Ruzsa [114], which provides such a set with $|B| \geq cN^\alpha$ with $\alpha \approx 0.733$ (actually, Ruzsa's construction was recently used in [10] to improve the exponent a tiny bit to $\alpha \approx 0.7334$). The best known upper bound is given by Pintz, Steiger and Szemerédi [107] who prove that $|B| \leq \frac{cN}{(\log N)^{c' \log\log\log\log N}}$.

The same problem can also be asked if we replace the squares with cubes or any kth powers. Interestingly, the application of Delsarte's method seems to be significantly easier if we consider sets avoiding the cubes (or any odd powers) than those avoiding the squares (or any even powers). The reason for lies in the modular formulation of the problem: for a fixed N, what is the maximal cardinality of a set $B \subset \mathbb{Z}_N$ such that $B-B$ avoids quadratic (or cubic) residues? The crucial difference is that cubic residues are symmetric to 0 for any N, while quadratic residues are not.

In these problems it is clear that Delsarte's method can be applied, but it is not at all clear *how to find* the "best" witness function f (cf. the proof of Theorem 3.1.4 in Section 3.1.2), and what upper bound it gives. In a joint work with I. Ruzsa we aim to improve the upper bound of [107]. In the modular formulation of the problems we can prove $|B| \leq N^{1-\delta}$ for the cubic residues, but *not* for the quadratic residues. The transition from the modular case to the original setting of the integers seems equally difficult (and has not yet been done) for the squares and the cubes.

3.4.2 Sets avoiding unit distances

What is the maximal possible asymptotic upper density $m_1(\mathbb{R}^d)$ of a measurable set $B \subset \mathbb{R}^d$ such that $B - B$ avoids the unit sphere (i.e. no two points of B are of distance 1 from each other)? The Frankl and Wilson intersection theorem [42] implies the exponential bound $m_1(\mathbb{R}^d) \leq 1.207^{-d}$, which was improved later by Raigorodskii [109] to $m_1(\mathbb{R}^d) \leq 1.239^{-d}$, using similar ideas. A different approach, based on Delsarte's method and the clever subgraph trick of Lemma 3.2.1, was introduced by Filho and Vallentin in [106]. This method resulted in improved upper bounds for small values of d, but gave the inferior bound $m_1(\mathbb{R}^d) \leq 1.165^{-d}$ asymptotically. However, Bachoc, Pasuello and Thiery [3] managed to combine the ideas of [42, 109] and [106] to obtain the best known asymptotic upper bound $m_1(\mathbb{R}^d) \leq 1.268^{-d}$.

We are primarily interested in the planar case, $d = 2$. The best known construction, due to Croft [32], gives the lower bound $m_1(\mathbb{R}^2) \geq 0.2293$. The best known upper bound $m_1(\mathbb{R}^2) \leq 0.268$ is given in [106] by a combination of Delsarte's method and the subgraph trick of Lemma 3.2.1. It improves an earlier bound of Székely [128], $m_1(\mathbb{R}^2) \leq 0.279$. However, the conjecture of Erdős, $m_1(\mathbb{R}^2) < 1/4$ remains open. In the near future we plan to tackle this conjecture by combining Delsarte's method, the subgraph trick [106], and earlier ideas of Székely [128], altogether.

3.4.3 Littlewood's conjecture

Here we describe a rather surprising possible application of Delsarte's method. In the original formulation of Littlewood's conjecture it is not at all obvious how Delsarte's method could be of any use.

Littlewood's conjecture states that for all real numbers $\alpha, \beta \in \mathbb{R}$ we have $\liminf n\|n\alpha\|\|n\beta\| = 0$, where $\|x\|$ denotes the distance of x from the closest integer. This conjecture has been open for some 80 years and the strongest result so far asserts that the set of possible exceptions α, β has Hausdorff dimension 0 in the plane [39].

One can only see the relevance of Delsarte's method after reading a combinatorial reformulation of the problem on Tim Gowers' web-blog [46] (actually, I was introduced to the same reformulation by I. Ruzsa a few weeks earlier). Following Gowers, let us assume by contradiction that there exists a counterexample α, β to Littlewood's conjecture. Then there exists a $\delta > 0$ such that $n\|n\alpha\|\|n\beta\| > \delta$, for all n. Now, consider a large even integer M, and take the points $P_j = (j/M, \{ja\}, \{jb\})$ in the 3-dimensional torus $\mathbb{T}^3 = [-1/2, 1/2)^3$, for $j = 1, \ldots M/2$. (Here $\{x\}$ denotes the fractional part of x.) There are $M/2$ such points P_j and they have the property that the difference of any two of them lies outside the hyperboloid $H_\varepsilon = \{(x, y, z) : |xyz| < \varepsilon\}$, where $\varepsilon = \delta/M$. This leads to the fact that for every $\varepsilon > 0$ there must exist c/ε points in the 3-dimensional torus $\mathbb{T}^3 = [-1/2, 1/2)^3$ such that the difference of any two of them falls outside the hyperboloid $H_\varepsilon = \{(x, y, z) : |xyz| < \varepsilon\}$. Therefore, in the language of Delsarte's scheme the underlying group is $\mathcal{G} = \mathbb{T}^3$ and the forbidden set is $A = H_\varepsilon$.

What is the maximum number of points in $\mathbb{T}^3$ such that all the pairwise differences lie outside H_ε? In order to prove Littlewood's conjecture we must show that

this quantity is $o(1/\varepsilon)$. To do so, it is sufficient to exhibit witness functions h_ε on the torus $\mathbb{T}^3$ such that $h_\varepsilon(x) = h_\varepsilon(-x)$, $h_\varepsilon|_{\mathcal{G}\setminus H_\varepsilon} \leq 0$, $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{\mathcal{G}} = \mathbb{Z}^3$, and $h(0)/\hat{h}(0) = o(1/\varepsilon)$. Of course, it is not at all obvious how to construct such functions, but neither is it obvious that such witness functions cannot exist.

In fact, using the duality principle described in the Section 3.1.3, we can also see what is needed to refute Delsarte's method in this setting (i.e. to prove that it cannot lead to the solution of Littlewood's conjecture; but be aware that such a refutation would only mean the failure of Delsarte's method and not the falsity of Littlewood's conjecture). We should find dual-witness functions f_ε on the torus $\mathbb{T}^3$ such that $f_\varepsilon(x) = f_\varepsilon(-x)$, f_ε is supported on H_ε^c, $\hat{f}_\varepsilon(0) = 1$, and $\hat{f}(\gamma) \geq -c\varepsilon$ for all $\gamma \in \mathbb{Z}^3$.

Starting from scratch it is not at all obvious whether the witnesses h_ε or the dual-witnesses f_ε exist. What we know, by duality, is that either h_ε or f_ε exist. Tim Gowers ventured to call it a "win-win" situation. The only way we can "lose" is if we are *not able to decide* whether h_ε or f_ε exists. And this is exactly the situation right now, unfortunately. Nevertheless, this remains a promising approach to Littlewood's conjecture.

3.4.4 Improving the Delsarte bound

The Delsarte bound, in itself, is so strong that it provides the best known asymptotic upper bound in some famous problems. Such is the case of the original setting of Delsarte: the maximum number $A(n, d)$ of binary codewords in $\mathcal{G} = \mathbb{Z}_2^n$ such that any two of them differ in at least d positions. As mentioned in Section 3.1.9, asymptotically, as $d/n \to \gamma$ for some $0 < \gamma < 1$, the best current upper bound is given by McEliece et al. [100] using the Delsarte bound with specific witness functions. Another famous example is the maximal density of sphere-packings in $\mathbb{R}^d$ where the best known asymptotic upper bound is also given by Delsarte's method in [63], and in small dimensions in [29].

Therefore, any improvement on Delsarte's bound could be of paramount importance. We have already seen such an improvement, Lemma 3.2.1, which was introduced in [106]. It led to the improved asymptotic upper bound [3] on the maximal density of sets avoiding unit-distances in $\mathbb{R}^d$, and also to the improved upper bound on the independence number of Paley-graphs in [4]. Here I will describe another possible improvement of the Delsarte bound (not yet published).

Assume that $\mathcal{G}$ is a compact Abelian group, and $A \subset \mathcal{G}$ is a standard set in the sense of Section 3.1. As usual we are looking for the maximal cardinality of a subset $B \subset \mathcal{G}$ such that $(B - B) \cap A = \{0\}$. Assume we have some further restriction on the set B: not only must each $b_j - b_k$ fall into $A^c \cup \{0\}$ but also B must be contained in some prescribed set $C \subset \mathcal{G}$. We can turn this information to an improvement of the Delsarte bound as follows.

Theorem 3.4.1. ([93])* *Let $C \subset \mathcal{G}$ be a measurable subset. Assume h is a witness function as in the Delsarte bound: $h : \mathcal{G} \to \mathbb{R}$, $h(x) \leq 0$ for all $x \in A^c$, $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{\mathcal{G}}$, and the Fourier inversion formula holds for h. Let Null denote the set*

of γ's where $\hat{h}(\gamma) = 0$. Assume furthermore that we have another witness function $K : \mathcal{G} \to \mathbb{C}$ with the following properties: $K(x) \geq 1$ for $x \in C$, $\hat{K}(\mathbf{1}) = 0$, and $\hat{K}(\gamma) = 0$ for all $\gamma \in Null$. Then any $B \subset C$ such that $B - B \subset A^c \cup \{0\}$ satisfies

$$|B| \leq \frac{h(0)}{\hat{h}(\mathbf{1}) + \left(\sum_{\gamma \notin Null} \frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}\right)^{-1}} \tag{3.90}$$

Proof. As in the proof of Lemma 3.3.5 define

$$S = \sum_{\gamma \in \hat{\mathcal{G}}} |\hat{B}(\gamma)|^2 \hat{h}(\gamma). \tag{3.91}$$

We will make use of the non-trivial terms in (3.91). Namely,

$$\left(\sum_{\gamma \neq \mathbf{1}, \gamma \notin Null} |\hat{B}(\gamma)|^2 \hat{h}(\gamma)\right)\left(\sum_{\gamma \neq \mathbf{1}, \gamma \notin Null} \frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}\right) \geq \tag{3.92}$$

$$\left|\sum_{\gamma \neq \mathbf{1}, \gamma \notin Null} \hat{B}(\gamma)\overline{\hat{K}(\gamma)}\right|^2 = \left|\sum_{\gamma \in \hat{\mathcal{G}}} \hat{B}(\gamma)\overline{\hat{K}(\gamma)}\right|^2 = \left|\sum_{x \in \mathcal{G}} B(x)\overline{K(x)}\right|^2 =$$

$$\left|\sum_{x \in C} B(x)\overline{K(x)}\right|^2 \geq |B|^2$$

where we used Cauchy-Schwarz, the assumptions on $\hat{K}(\gamma)$, Parseval, and the assumptions on $B(x)$ and $K(x)$, respectively. Therefore, we get an improved version of (3.70), namely:

$$S \geq |B|^2 \hat{h}(\mathbf{1}) + \frac{|B|^2}{\sum_{\gamma \neq 0, \gamma \notin Null} \frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}}. \tag{3.93}$$

Comparing this with $S \leq h(\mathbf{1})|B|$ (as proven in (3.71)) yields the desired bound (3.90). □

We see that Theorem 3.4.1 requires a combination of two witness functions $h(x)$ and $K(x)$ (as well as a prescribed set C in which B is assumed to be located). Unfortunately, it is not at all clear how to optimize h and K in actual applications. I believe that the best chance to apply (3.90) successfully arises in situations when the Delsarte bound is already sharp. In such cases the sheer *existence of any K* can lead to new results. Such is the case, for example, in the problem of MUBs. It remains to be seen whether Theorem 3.4.1 will be as useful for applications as Lemma 3.2.1 has turned out to be.

4 Cardinality of sumsets

In this chapter we describe some selected results concerning the cardinality of sumsets. The structure and cardinality of sumsets are central objects of study in additive combinatorics.

The results of this chapter are based on the papers [52, 53, 95]. They constitute an important part of my work in additive combinatorics, but the methods here are purely combinatorial and do not use Fourier analysis. For this reason I will keep this chapter shorter.

In Section 4.1 we consider finite sets of integers $A_1, \dots, A_k$ and study the cardinality of the k-fold sumset $A_1 + \cdots + A_k$ compared to those of $(k-1)$-fold sumsets $A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k$. We prove superadditivity and submultiplicativity properties for these quantities in Theorems 4.1.1 and 4.1.2. This section is based on [52].

In Section 4.2 we extend Freiman's inequality on the cardinality of the sumset of a d dimensional set. We also consider different sets related by an inclusion of their convex hull, and one of them added possibly several times, in Theorem 4.2.5. This section is based on [95].

4.1 Superadditivity and submultiplicativity properties

Let $A_1, A_2, \dots, A_k$ be finite sets of integers. How does the cardinality of the k-fold sumset $A_1 + A_2 + \cdots + A_k$ compare to the cardinalities of the $(k-1)$-fold sums $A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k$?

In the special case when all the sets are the same, $A_i = A \subset \mathbb{Z}$, Vsevolod Lev [85] proved that the quantity $\frac{|kA|-1}{k}$ is increasing (where we have used the standard notation for the k-fold sum $A + A + \cdots + A = kA$). The first cases of this result assert that

$$|2A| \geq 2|A| - 1 \tag{4.1}$$

and

$$|3A| \geq \frac{3}{2}|2A| - \frac{1}{2}. \tag{4.2}$$

Inequality (4.1) can be extended to different summands as

$$|A + B| \geq |A| + |B| - 1, \tag{4.3}$$

and this inequality also holds for sets of residues modulo a prime p, the only obstruction being that a cardinality cannot exceed p, i.e.

$$|A + B| \geq \min(|A| + |B| - 1, p); \tag{4.4}$$

this familiar result is known as the Cauchy-Davenport inequality.

Motivated by these results Imre Ruzsa asked whether inequality (4.2) can also

be extended to different summands in the following form:

$$|A+B+C| \geq \frac{|A+B|+|B+C|+|A+C|-1}{2}. \tag{4.5}$$

Lev noticed (personal communication) that this is true in the case when the sets have the same diameter. (The diameter of a set is the difference of its maximum and minimum.) In this section we establish this property in general, for an arbitrary number of summands, and with the extra twist that in the k-fold sumset it is sufficient to use the smallest or largest element of at least one of the summands.

Theorem 4.1.1. ([52]*) *Let $A_1, \dots, A_k$ be finite, nonempty sets of integers. Let A_i' be the set consisting of the smallest and the largest elements of A_i (so that $1 \leq |A_i'| \leq 2$). Put*

$$S = A_1 + \cdots + A_k,$$

$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k,$$

$$S_i' = A_1 + \cdots + A_{i-1} + A_i' + A_{i+1} + \cdots + A_k,$$

$$S' = \bigcup_{i=1}^{k} S_i'.$$

We have

$$|S| \geq |S'| \geq \frac{1}{k-1}\sum_{i=1}^{k} |S_i| - \frac{1}{k-1}. \tag{4.6}$$

The possibility to extend inequality (4.2) to residues modulo a prime p was investigated in a paper by Gyarmati, Konyagin, Ruzsa [51]. A naive attempt to extend it in the form

$$|3A| \geq \min\left(\frac{3}{2}|2A| - \frac{1}{2}, p\right)$$

fails unless $|A|$ is very small in comparison to p, and for larger values the relationship between the sizes of $2A$ and $3A$ is complicated.

In a sense, Theorem 4.1.1 means that the cardinality of sumsets grows faster than linear. On the other hand, we show that it grows slower than exponential. For identical summands this means that $|kA|^{1/k}$ is decreasing, which is Theorem 7.5 in Nathanson's book [104].

Here we establish a more general result for different summands.

Theorem 4.1.2. ([52]*) *Let $A_1, \dots, A_k$ be finite, nonempty sets in an arbitrary commutative semigroup. Put*

$$S = A_1 + \cdots + A_k,$$

$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k.$$

We have

$$|S| \leq \left(\prod_{i=1}^{k} |S_i|\right)^{\frac{1}{k-1}}. \tag{4.7}$$

For three summands this inequality was established earlier by Imre Ruzsa, [116, Theorem 5.1]. The proof given in [116] is different and works also for noncommutative groups with a proper change in the formulation. On the other hand, that argument relied on the invertibility of the operation, so we do not have any result for noncommutative semigroups. Neither could we extend that argument for more than three summands, and hence the following question remains open.

Problem 4.1.3. ([52]) *Let $A_1, \dots, A_k$ be finite, nonempty sets in an arbitrary noncommutative group. Put*

$$S = A_1 + \cdots + A_k,$$

$$n_i = \max_{a \in A_i} |A_1 + \cdots + A_{i-1} + a + A_{i+1} + \cdots + A_k| .$$

Is it always true that

$$|S| \leq \left(\prod_{i=1}^{k} n_i \right)^{\frac{1}{k-1}} \quad ? \tag{4.8}$$

The superadditivity property clearly does not hold in such a general setting (as it fails already mod p, see [51]). However, it can easily be extended to torsion-free groups (just as everything that holds for finite sets of integers) with the change of formulation that "smallest" and "largest" do not make sense in such generality.

Theorem 4.1.4. ([52]*) *Let $A_1, \dots, A_k$ be finite, nonempty sets in a torsion-free group $\mathcal{G}$,*

$$S = A_1 + \cdots + A_k,$$

$$S_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k.$$

There are subsets $A_i' \subset A_i$ having at most two elements such that with

$$S_i' = A_1 + \cdots + A_{i-1} + A_i' + A_{i+1} + \cdots + A_k,$$

$$S' = \bigcup_{i=1}^{k} S_i'$$

we have

$$|S| \geq |S'| \geq \frac{1}{k-1} \sum_{i=1}^{k} |S_i| - \frac{1}{k-1}. \tag{4.9}$$

Another natural way of generalizing Theorem 4.1.2 is to restrict the summation of elements to a prescribed addition graph. A possible meaning of this in the case $k = 3$ (and identical sets) could read as follows. We consider a graph $\mathcal{G}$ on our set A; on the right hand side of the proposed inequality we take the number of different sums of connected pairs; on the left hand side we take the number of different sums of those triplets where each pair is connected. However, the resulting inequality, $|A \overset{G}{+} A \overset{G}{+} A|^2 \leq |A \overset{G}{+} A|^3$, can fail spectacularly. Take $A = [1, n]$, let S be some subset of the even integers lying in the interval $(2n/3, 4n/3)$, and connect two elements of A if their sum is in S. Then for every $s_1, s_2, s_3 \in S$ we can find

$a_1, a_2, a_3 \in A$, $a_1 = (-s_1 + s_2 + s_3)/2$, etc., whose pairwise sums give these s_i's. Also, $a_1 + a_2 + a_3 = (s_1 + s_2 + s_3)/2$. Therefore, if S is such that all the triple sums $s_1+s_2+s_3$ are distinct, then the above mapping $(s_1, s_2, s_3) \mapsto (a_1, a_2, a_3)$ is injective, and the left-hand side of the inequality will be at least $\binom{|S|}{3}^2 \approx \frac{1}{36}|S|^6$, much larger than the right hand side, which is $|S|^3$. It would be interesting to say something when the graphs are sufficiently dense.

4.1.1 Proof of superadditivity

In this section we prove Theorems 4.1.1 and 4.1.4.

Proof of Theorem 4.1.1. Both sides of the inequality are invariant under translation, therefore we can assume that the smallest element of each A_i is 0. Also, let us denote the largest element of A_i by a_i. Then S is a subset of the interval $I = [0, a_1 + a_2 + \cdots + a_k]$.

We will use the notation $A_{\le a} := A \cap (-\infty, a]$, and $A_{>a} := A \cap (a, +\infty)$. Consider the sets

$$\begin{array}{ll} (a_1 + S_1)_{>a_1} & (S_2)_{\le a_1} \\ (a_2 + S_2)_{>a_1+a_2} & (S_3)_{\le a_1+a_2} \\ \cdots & \cdots \\ (a_{k-2} + S_{k-2})_{>a_1+\cdots+a_{k-2}} & (S_{k-1})_{\le a_1+\cdots+a_{k-2}} \\ (a_{k-1} + S_{k-1})_{>a_1+\cdots+a_{k-1}} & (S_k)_{\le a_1+\cdots+a_{k-1}} \end{array}$$

We are going to calculate the total cardinality of these sets in two ways. First, each S_i, $2 \le i \le k-1$ contributes two items to this table, an initial segment to a right hand column and a translation of the corresponding final segment to the left hand column of the next row; these add up to $|S_i|$. The set S_1 occurs only as the very first item and it contributes $|S_1| - 1$; the set S_k occurs as the last item and it contributes $|S_k|$. Hence the sum of cardinalities is $\sum |S_i| - 1$.

On the other hand, the two sets in each row are disjoint and they are subsets of S'. Consequently the total size of the sets is at most $(k-1)\,|S'|$. By comparing this upper estimate to the previous sum we obtain

$$(k-1)|S| \ge (k-1)|S'| \ge \sum_{i=1}^{k} |S_i| - 1 \tag{4.10}$$

as claimed. □

Proof of Theorem 4.1.4. This is a standard reduction argument to the case of integers. Let $\mathcal{H}$ denote the subgroup generated by the elements of $\cup_{i=1}^{k} A_i$. As a finitely generated torsion-free group $\mathcal{H}$ is isomorphic to $\mathbb{Z}^d$ for some d, therefore we can assume without loss of generality that $A_i \subset \mathbb{Z}^d$. Then, for a large enough integer m the homomorphism $\phi_m : \mathbb{Z}^d \to \mathbb{Z}$ defined by $(z_1, z_2, \ldots z_d) \mapsto mz_1 + m^2 z_2 + \ldots m^d z_d$ preserves the additive identities of all elements of sumsets involved in the desired inequality (this means that ϕ_m is one-to-one restricted to these elements). Finally, if B_i denotes the image of A_i under ϕ_m then the desired two-element subsets A_i' can be chosen as $A_i' = \phi_m^{-1}(B_i')$. □

4.1.2 Proof of submultiplicativity

In this section we prove Theorem 4.1.2. We begin with a lemma on the size of projections.

Lemma 4.1.5. ([52]*) *Let $d \geq 2$ be an integer, $X_1, \ldots, X_d$ arbitrary sets,*

$$B \subset X_1 \times \cdots \times X_d$$

be a finite subset of their Cartesian product. Let

$$B_i \subset X_1 \times \cdots \times X_{i-1} \times X_{i+1} \times \cdots \times X_d$$

be the corresponding "projection" of B:

$$B_i = \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d) : \exists x \in X_i \text{ such that } (x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_d) \in B\}.$$

We have

$$|B|^{d-1} \leq \prod_{i=1}^{d} |B_i| \,. \tag{4.11}$$

This lemma is not new. It is essentially equivalent to an entropy inequality of Han [56], see also Cover–Thomas [31, Theorem 16.5.1]. It also follows from Shearer's inequality [27] or from Bollobás and Thomason's Box Theorem [17]. We include a proof for convenience.

Proof. We prove this lemma by induction on d. For $d = 2$ the statement is obvious. Assume now that the statement holds for $d-1$, and consider the case d.

Make a list $\{b_1, b_2, \ldots, b_t\}$ of those numbers which appear as a first coordinate of some element in B. Partition the set B according to these first coordinates as

$$B = B(b_1) \cup B(b_2) \cup \cdots \cup B(b_t), \tag{4.12}$$

where

$$B(b_i) = \{(b_i, x_2, x_3, \ldots, x_d) = b : \ b \in B\}. \tag{4.13}$$

By the inductive hypothesis we have $|B(b_i)|^{d-2} \leq |B(b_i)_2| \cdots |B(b_i)_d|$, that is,

$$|B(b_i)|^{\frac{d-2}{d-1}} \leq (|B(b_i)_2| \cdots |B(b_i)_d|)^{\frac{1}{d-1}} \,. \tag{4.14}$$

It is also clear that $|B(b_i)| \leq |B_1|$, and hence

$$|B(b_i)| \leq (|B(b_i)_2| \cdots |B(b_i)_d|)^{\frac{1}{d-1}} \, |B_1|^{\frac{1}{d-1}} \,. \tag{4.15}$$

Using this and Hölder's inequality we obtain

$$|B| = \sum_{i=1}^{t} |B(b_i)| \leq |B_1|^{\frac{1}{d-1}} \sum_{i=1}^{t} \left(|B(b_i)_2| \cdots |B(b_i)_d|\right)^{\frac{1}{d-1}} \leq \tag{4.16}$$

$$\leq |B_1|^{\frac{1}{d-1}} \prod_{j=2}^{d} \left(\sum_{i=1}^{t} |B(b_i)_j| \right)^{\frac{1}{d-1}} = \prod_{j=1}^{d} |B_j|^{\frac{1}{d-1}}, \tag{4.17}$$

which proves the statement. □

We now turn to the proof of Theorem 4.1.2.

Proof. Let us list the elements of the sets $A_1, A_2, \ldots, A_k$ in some order:

$$A_1 = \{c_{11}, c_{12}, \ldots, c_{1t_1}\},$$

$$A_2 = \{c_{21}, c_{22}, \ldots, c_{2t_2}\},$$

$$\vdots$$

$$A_k = \{c_{k1}, c_{k2}, \ldots, c_{kt_k}\}.$$

For each $s \in S$ let us consider the decomposition

$$s = c_{1i_1} + c_{2i_2} + \cdots + c_{ki_k}, \tag{4.18}$$

where the finite sequence $(i_1, i_2, \ldots, i_k)$, composed of the (second) indices of c_{ji_j}, is minimal in lexicographical order. Let us define a function f from S to the Cartesian product $A_1 \times A_2 \times \cdots \times A_k$, by

$$f(s) = (c_{1i_1}, c_{2i_2}, \ldots, c_{ki_k}) \in A_1 \times \cdots \times A_k. \tag{4.19}$$

This function is well-defined, and it maps the set S to a set $B \subset A_1 \times \cdots \times A_k$ such that $|B| = |A_1 + \cdots + A_k|$. Applying Lemma 4.1.5 to the set B we get

$$|B|^{k-1} \leq |B_1|\,|B_2| \cdots |B_k|. \tag{4.20}$$

Therefore, it is sufficient to show that

$$|B_j| \leq |A_1 + A_2 + \cdots + A_{j-1} + A_{j+1} + \cdots + A_k|. \tag{4.21}$$

This inequality, however, follows easily from the fact that sum of the coordinates is distinct for each element in B_j. Indeed, assume that there exist two elements $z \neq z' \in B_j$ such that

$$z = (c_{1i_1}, c_{2i_2}, \ldots, c_{j-1i_{j-1}}, c_{j+1i_{j+1}}, \ldots c_{ki_k}),$$

$$z' = (c_{1i'_1}, c_{2i'_2}, \ldots, c_{j-1i'_{j-1}}, c_{j+1i'_{j+1}}, \ldots, c_{ki'_k}),$$

and

$$c_{1i_1} + c_{2i_2} + \cdots + c_{ki_k} = c_{1i'_1} + c_{2i'_2} + \cdots + c_{ki'_k}.$$

We may assume that

$$(i_1, i_2, \dots, i_{j-1}, i_{j+1}, \dots, i_k) < (i'_1, i'_2, \dots, i'_{j-1}, i'_{j+1}, \dots, i'_k).$$

in lexicographical order.

Now, $z' \in B_j$ therefore there exists an element $d \in A_j$ and $u \in S$, such that

$$u = c_{1i'_1} + c_{2i'_2} + \cdots + c_{j-1i'_{j-1}} + d + c_{j+1i'_{j+1}} + \cdots + c_{ki'_k},$$

and

$$f(u) = (c_{1i'_1}, c_{2i'_2}, \dots, c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, \dots, c_{ki'_k}) \in B.$$

Note that

$$u = c_{1i_1} + c_{2i_2} + \cdots + c_{j-1i_{j-1}} + d + c_{j+1i_{j+1}} + \cdots + c_{ki_k},$$

also holds. However, with $d = c_{ji_j}$ we have

$$(i_1, i_2, \dots, i_{j-1}, i_j, i_{j+1}, \dots, i_k) < (i'_1, i'_2, \dots, i'_{j-1}, i_j, i'_{j+1}, \dots, i'_k).$$

in lexicographical order, therefore the definition of f implies that $f(u) \neq (c_{1i'_1}, c_{2i'_2}, \dots, c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, \dots, c_{ki'_k})$, a contradiction. □

4.1.3 Generalizations

The results of Section 4.1.1 and 4.1.2 have been generalized in several ways since their publication. In particular, the following generalization of Theorem 4.1.2 was already conjectured in [52], and later proved in [53], and independently in [89]. The paper [89] also proves many interesting entropy-inequality analogues of sumset-inequalities.

Theorem 4.1.6. ([89], [53]*) *Let $A, B_1, \dots B_k$ be finite sets of integers, and $S \subset B_1 + \cdots + B_k$. Then*

$$|S + A|^k \leq |S| \prod_{i=1}^{k} |A + B_1 + \cdots + B_{i-1} + B_{i+1} + \cdots + B_k|. \tag{4.22}$$

Theorem 4.1.2 corresponds to the special case $S = B_1 + \cdots + B_k$. The proof of Theorem 4.1.6 in [53] proceeds via the following generalized Plünnecke-type inequality, proven in [53].

Theorem 4.1.7. ([53]*) *Let $l < k$ be integers, and let A, $B_1, \dots, B_k$ be finite sets in a commutative group $\mathcal{G}$. Let $K = \{1, 2, \dots, k\}$, and for any $I \subset K$ put*

$$B_I = \sum_{i \in I} B_i,$$

$$|A| = m, \quad |A + B_I| = \alpha_I m.$$

(This is compatible with the previous notation if we identify a one-element subset of K with its element.) Write

$$\beta = \left(\prod_{L \subset K, |L|=l} \alpha_L \right)^{(l-1)!(k-l)!/(k-1)!} \tag{4.23}$$

There exists an $X \subset A$, $X \neq \emptyset$ such that

$$|X + B_K| \leq \beta |X|. \tag{4.24}$$

Another generalization was given by Balister and Bollobás in [5]. A collection $\mathcal{C}$ of subsets $C \subset \{1, \ldots, k\}$ is called a uniform m-cover if each $j \in \{1, \ldots, k\}$ is contained in exactly m subsets C.

Theorem 4.1.8. ([5]) *Let $A_1, \ldots, A_k$ be finite sets in a commutative semigroup, and let $S = A_1 + \cdots + A_k$. Let $\mathcal{C}$ be a uniform m-cover, and for any $C \in \mathcal{C}$ let $S_C = \sum_{j \in C} A_j$. Then $|S|^m \leq \prod_{C \in \mathcal{C}} |S_C|$.*

If the sets A_j lie in a torsion-free commutative group then $m(|S| - 1) \geq \sum_{C \in \mathcal{C}} (|S_C| - 1)$.

The proof of the first part of the theorem is based on the following *Box Theorem* of Bollobás and Thomason [17].

Theorem 4.1.9. ([17]) *Given a body $K \subset \mathbb{R}^n$, there is a box $B \subset \mathbb{R}^n$ with $|K| = |B|$ and $|K_A| \geq |B_A|$ for every $A \subset [n]$, where K_A denotes the volume of the projection of the body to the subspace corresponding to A.*

4.2 Sumsets and the convex hull

The aim of this section is to give a lower estimate for the cardinality of certain sumsets in $\mathbb{R}^d$.

We say that a set in $\mathbb{R}^d$ is *proper d-dimensional* if it is not contained in any affine hyperplane. Our starting point is the following classical theorem of Freiman.

Theorem 4.2.1. ([43, Lemma 1.14]) *Let $A \subset \mathbb{R}^d$ be a finite set, $|A| = m$. Assume that A is proper d-dimensional. Then*

$$|A + A| \geq m(d+1) - \frac{d(d+1)}{2}.$$

We will show that to get this inequality it is sufficient to use the vertices (extremal points) of A.

Definition 4.2.2. *We say that a point $a \in A$ is a* vertex *of a set $A \subset \mathbb{R}^d$ if it is not in the convex hull of $A \setminus \{a\}$. The set of vertices will be denoted by* $\operatorname{vert} A$.

The convex hull of a set A will be denoted by $\operatorname{conv} A$.

Theorem 4.2.3. ([95]*) *Let $A \subset \mathbb{R}^d$ be a finite set, $|A| = m$. Assume that A is proper d-dimensional, and let $A' = \operatorname{vert} A$, We have*

$$|A + A'| \geq m(d+1) - \frac{d(d+1)}{2}.$$

This can be extended to different summands as follows.

Theorem 4.2.4. ([95]*) *Let $A, B \subset \mathbb{R}^d$ be finite sets, $|A| = m$. Assume that B is proper d-dimensional and $A \subset \operatorname{conv} B$. We have*

$$|A + B| \geq m(d+1) - \frac{d(d+1)}{2}.$$

Finally we extend it to several summands as follows. We use $kB = B + \cdots + B$ to denote repeated addition. As far as we know even the case of $A = B$ seems to be new here.

Theorem 4.2.5. ([95]*) *Let $A, B \subset \mathbb{R}^d$ be finite sets, $|A| = m$. Assume that B is proper d-dimensional and $A \subset \operatorname{conv} B$. Let k be a positive integer. We have*

$$|A + kB| \geq m\binom{d+k}{k} - k\binom{d+k}{k+1} = \left(m - \frac{kd}{k+1}\right)\binom{d+k}{k}. \tag{4.25}$$

The case $d = 1$ of the above theorems is quite obvious. A natural problem is to try to generalize Theorem 4.1.1 to multidimensional sets.

Problem 4.2.6. ([95]) *Generalize Theorem 4.1.1 to multidimensional sets. A proper generalization should give the correct order of magnitude, hence the analog of* (4.6) *could be of the form*

$$|S| \geq |S'| \geq \left(\frac{k^{d-1}}{(k-1)^d} - \varepsilon\right)\sum_{i=1}^{k} |S_i|$$

if all sets are sufficiently large.

Another natural question is whether an analogue of (4.25) remains valid for different summands.

Problem 4.2.7. ([95]) *Let $A, B_1, \ldots, B_k \subset \mathbb{R}^d$ such that the B_i are proper d-dimensional and*

$$A \subset \operatorname{conv} B_1 \subset \operatorname{conv} B_2 \subset \cdots \subset \operatorname{conv} B_k.$$

Does the esimate given in (4.25) *also hold for $A + B_1 + \cdots + B_k$?*

This is easy for $d = 1$.

4.2.1 A simplicial decomposition

We will need a result about simplicial decompositions. By a *simplex* in $\mathbb{R}^d$ we mean a proper d-dimensional compact set which is the convex hull of $d + 1$ points.

Definition 4.2.8. *Let $S_1, S_2 \subset \mathbb{R}^d$ be simplices, $B_i = \operatorname{vert} S_i$. We say that they are in* regular position*, if*

$$S_1 \cap S_2 = \operatorname{conv}(B_1 \cap B_2),$$

that is, they meet in a common k-dimensional face for some $k \leq d$. (This does not exclude the extremal cases when they are disjoint or they coincide.) We say that a collection of simplices is in regular position if any two of them are.

Lemma 4.2.9. ([95]*) *Let $B \subset \mathbb{R}^d$ be a proper d dimensional finite set, $S = \operatorname{conv} B$. There is a sequence $S_1, S_2, \ldots, S_n$ of distinct simplices in regular position with the following properties.*

a) $S = \bigcup S_i$.

b) $B_i = \operatorname{vert} S_i = S_i \cap B$.

c) Each S_i, $2 \leq i \leq n$ meets at least one of $S_1, \ldots, S_{i-1}$ in a $(d-1)$ dimensional face.

We include a proof of this lemma for completeness. This proof was communicated to us by Károly Böröczki.

Proof. We use induction on $|B|$. The case $|B| = 2$ is clear. Let $|B| = k$, and assume we know it for smaller sets (in any possible dimension).

Let b be a vertex of B and apply it for the set $B' = B \setminus \{b\}$. This set may be d or $d-1$ dimensional.

First case: B' is d dimensional. With the natural notation let

$$S' = \bigcup_{i=1}^{n'} S'_i$$

be the prescribed decomposition of $S' = \operatorname{conv} B'$. We start the decomposition of S with these, and add some more as follows.

We say that a point x of S' is *visible* from b, if x is the only point of the segment joining x and b in S'. Some of the simplices S'_i have (one or more) $d-1$ dimensional faces that are completely visible from b. Now if F is such a face, then we add the simplex

$$\operatorname{conv}(F \cup \{b\})$$

to our list.

Second case: B' is $d-1$ dimensional. Again we start with the decomposition of S', just in this case the sets S'_i will be $d-1$ dimensional simplices. Now the decomposition of S will simply consist of

$$S_i = \operatorname{conv}(S'_i \cup \{b\}),\ n = n'.$$

□

The construction above immediately gave property c). We note that it is not really an extra requirement, every decomposition has it after a suitable rearrangement. This just means that the graph obtained by using our simplices as vertices

and connecting two of them if they share a $d-1$ dimensional face is connected. Now take two simplices, say S_i and S_j. Take an inner point in each and connect them by a segment. For a generic choice of these point this segment will not meet any of the $\leq d-2$ dimensional faces of any S_k. Now as we walk along this segment and go from one simplex into another, this gives a path in our graph between the vertices corresponding to S_i and S_j.

4.2.2 The case of a simplex

Here we prove Theorem 4.2.5 for the case $|B| = d+1$.

Lemma 4.2.10. ([95]*) *Let $A, B \subset \mathbb{R}^d$ be finite sets, $|A| = m$, $|B| = d+1$. Assume that B is proper d-dimensional and $A \subset \operatorname{conv} B$. Let k be a positive integer. Write $|A \cap B| = m_1$. We have*

$$|A + kB| = (m - m_1)\binom{d+k}{k} + \binom{d+k+1}{k+1} - \binom{d-m_1+k+1}{k+1}. \tag{4.26}$$

In particular, if $|A \cap B| \leq 1$, then

$$|A + kB| = m\binom{d+k}{k}. \tag{4.27}$$

We have always

$$|A + kB| \geq m\binom{d+k}{k} - k\binom{d+k}{k+1} = \left(m - \frac{kd}{k+1}\right)\binom{d+k}{k}. \tag{4.28}$$

Proof. Put $A_1 = A \cap B$, $A_2 = A \setminus B$. Write $B = \{b_0, \dots, b_d\}$, arranged in such a way that

$$A_1 = A \cap B = \{b_0, \dots, b_{m_1-1}\}.$$

The elements of kB are the points of the form

$$s = \sum_{i=0}^{d} x_i b_i,\ x_i \in \mathbb{Z}\ , x_i \geq 0,\ \sum x_i = k,$$

and this representation is unique. Clearly

$$|kB| = \binom{d+k}{k}.$$

Each element of A has a unique representation of the form

$$a = \sum_{i=0}^{k} \alpha_i d_i,\ \alpha_i \in \mathbb{R}\ , \alpha_i \geq 0,\ \sum \alpha_i = 1,$$

$$a = \sum_{i=0}^{d} \alpha_i b_i,\ \alpha_i \in \mathbb{R}\ , \alpha_i \geq 0,\ \sum \alpha_i = 1,$$

and if $a \in A_1$, then some $\alpha_i = 1$ and the others are equal to 0, while if $a \in A_2$, then at least two α_i's are positive.

Assume now that $a+s = a'+s'$ with certain $a, a' \in A$, $s, s' \in kB$. By substituting the above representations we obtain

$$\sum(\alpha_i + x_i)b_i = \sum(\alpha_i' + x_i')b_i,\ \sum(\alpha_i + x_i) = \sum(\alpha_i' + x_i') = k+1,$$

hence $\alpha_i + x_i = \alpha_i' + x_i'$ for all i. By looking at the integral and fractional parts we see that this is possible only if $\alpha_i = \alpha_i'$, or one of them is 1 and the other is 0. If the second possibility never happens, then $a = a'$. If it happens, say $\alpha_i = 1, \alpha_i' = 0$ for some i, then $\alpha_j = 0$ for all $j \neq i$ and then each a_j' must also be 0 or 1, that is, $a, a' \in A_1$.

The previous discussion shows that $(A_1 + kB) \cap (A_2 + kB) = \emptyset$ and the sets $a + kB$, $a \in A_2$ are disjoint, hence

$$|A + kB| = |A_1 + kB| + |A_2 + kB|$$

and

$$|A_2 + kB| = |A_2|\,|kB| = (m - m_1)\binom{d+k}{k}. \tag{4.29}$$

Now we calculate $|A_1 + kB|$. The elements of this set are of the form

$$\sum_{i=0}^{d} x_i b_i,\ x_i \in \mathbb{Z}\ , x_i \geq 0,\ \sum x_i = k+1,$$

with the additional requirement that there is at least one subscript i, $i \leq m_1 - 1$ with $x_i \geq 1$. Without this requirement the number would be the same as

$$|(k+1)B| = \binom{d+k+1}{k+1}.$$

The vectors $(x_0, \ldots, x_d)$ that violate this requirement are those that use only the last $d - m_1$ coordinates, hence their number is

$$\binom{d-m_1+k+1}{k+1}.$$

We obtain that

$$|A_1 + kB| = \binom{d+k+1}{k+1} - \binom{d-m_1+k+1}{k+1}.$$

Adding this formula to (4.29) we get (4.26).

If $m_1 = 0$ or 1, this formula reduces to the one given in (4.27).

To show inequality (4.28), observe that this formula is a decreasing function of m_1, hence the minimal value is at $m_1 = d+1$, which after an elementary trans-

formation corresponds to the right side of (4.28). Naturally this is attained only if $m \geq d+1$, and for small values of m the right side of (4.28) may even be negative. □

4.2.3 The general case

Proof of Theorem 4.2.5. We apply Lemma 4.2.9 to our set B. This decomposition induces a decomposition of A as follows. We put

$$A_1 = A \cap S_1, A_2 = A \cap (S_2 \setminus S_1), \ldots, A_n = A \cap \big(S_n \setminus (S_1 \cup S_2 \cup \cdots \cup S_{n-1})\big).$$

Clearly the sets A_i are disjoint and their union is A. Recall the notation $B_i = \operatorname{vert} S_i$.

We claim that the sets $A_i + kB_i$ are also disjoint. Indeed, suppose that $a + s = a' + s'$ with $a \in A_i$, $a' \in A_j$, $s \in kB_i$, $s' \in kB_j$, $i < j$. We have

$$\frac{a+s}{k+1} \in S_i, \ \frac{a'+s'}{k+1} \in S_j,$$

and these points are equal, so they are in

$$S_i \cap S_j = \operatorname{conv}(B_i \cap B_j).$$

This means that in the unique convex representation of $(a' + s')/(k+1)$ by points of B_j only elements of $B_i \cap B_j$ are used. However, we can obtain this representation via using the representation of a' and the components of s', hence we must have $a' \in \operatorname{conv}(B_i \cap B_k) \subset S_i$, a contradiction.

This disjointness yields

$$|A + kB| \geq \sum |A_i + kB_i| .$$

We estimate the summands using Lemma 4.2.10.

If $i > 1$, then $|A_i \cap B_i| \leq 1$. Indeed, there is a $j < i$ such that S_j has a common $d-1$ dimensional face with S_i, and then the d vertices of this face are excluded from A_i by definition. So in this case (4.27) gives

$$|A_i + kB_i| = |A_i| \binom{d+k}{k}.$$

For $i = 1$ we can only use the weaker estimate (4.28):

$$|A_1 + kB_1| \geq |A_1| \binom{d+k}{k} - k\binom{d+k}{k+1}.$$

Summing these equations we obtain (4.25). □

Very recently Böröczky, Santos and Serra [18] has investigated the case of equality in (4.25). They called the sets $A, B \subset \mathbb{R}^d$, $A \subset \operatorname{conv} B$, k-critical if equation (4.25) holds with equality, and gave a *full characterization* of k-critical pairs in terms of geometric and arithmetic properties of A and B.

References

[1] N. Alon, A. Orlitsky: *Repeated communications and Ramsey graphs*, IEEE Transactions on Information Theory, **41**, 1276–1289, (1995).

[2] M. Andreatta, C. Agon, E. Amiot: *Tiling problems in music composition: Theory and Implementation*, Proceedings of the International Computer Music Conference, Goteborg, Sweden, 156–163, (2002).

[3] C. Bachoc, A.Passuello, A. Thiery: *The density of sets avoiding distance 1 in Euclidean space*, preprint available at http://arxiv.org/abs/1401.6140

[4] C. Bachoc, M. Matolcsi, I. Z. Ruzsa: *Squares and difference sets in finite fields*, Integers, Vol. 13, Article A77, (2013).

[5] P. Balister, B. Bollobás: *Projections, entropy and sumsets*, Combinatorica, **32**, (2), 125–141, (2012).

[6] A. Balog: *On the distribution of p^θ mod 1*, Acta Math. Hungar. **45**, no. 1-2, 179–199, (1985).

[7] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, F. Vatan: *A New Proof for the Existence of Mutually Unbiased Bases*, Algorithmica **34**, 512–528, (2002).

[8] A. Barg, D. B. Jaffe: *Numerical results on the asymptotic rate of binary codes*, in "Codes and Association Schemes" (A. Barg and S. Litsyn, Eds.), Amer. Math. Soc., Providence, (2001).

[9] K. Beauchamp, R. Nicoara: *Orthogonal maximal Abelian *-subalgebras of the 6×6 matrices*, Linear Algebra Appl. **428**, no. 8-9, 1833–1853, (2008).

[10] R. Beigel, W. Gasarch: *Square-Difference-Free Sets of Size $\Omega(n^{0.7334...})$*, preprint available at http://arxiv.org/abs/0804.4892

[11] A. Belovs, J. Smotrovs: *A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases*. Lecture Notes In Computer Science, Vol. 5393, Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth, Section: Quantum Computing, 50–69, (2008).

[12] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej, K. Życzkowski: *Mutually unbiased bases and Hadamard matrices of order six.* J. Math. Phys. **48**, no. 5, 052106, (2007).

[13] R. Berger: *The undecidability of the domino problem*, Memoirs of the Amer. Math. Soc. **66**, 1–72, (1966).

[14] D. Best, H. Kharaghani: *Unbiased complex Hadamard matrices and bases*, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, **2**, 199–209, (2010).

[15] A. Bíró: *Divisibility of integer polynomials and tilings of the integers*, Acta Arithmetica, **118**, 117–127, (2005).

[16] B. Bollobás: *Random Graphs*, (second ed.), Cambridge University Press, Cambridge, (2001).

[17] B. Bollobás, A. Thomason: *Projections of bodies and hereditary properties of hypergraphs*, Bull. London Math. Soc. **27**, 417–424, (1995).

[18] K. J. Böröczky, F. Santos, O. Serra: *On sumsets and convex hull*, to appear in Computational and Discrete Geometry.

[19] D. Bose, S.Madan: *Spectrum is periodic for n-Intervals*, Journal of Functional Analysis, **260**, (1), 308–325, (2011).

[20] J. Bourgain: *Ruzsa's problem on sets of recurrence*, Israel J. Math. **59**, 150–166, (1987).

[21] S. Brierley, S. Weigert: *Maximal sets of mutually unbiased quantum states in dimension six*, Phys. Rev. A (3) **78**, no. 4, 042312, (2008).

[22] S. Brierley, S. Weigert: *Constructing Mutually Unbiased Bases in Dimension Six*, Phys. Rev. A (3) **79**, no. 5, 052316, (2009).

[23] S. Brierley, S. Weigert, I. Bengtsson: *All Mutually Unbiased Bases in Dimensions Two to Five*, Quantum Information and Computing **10**, 803–820, (2010).

[24] P. Butterley, W. Hall: *Numerical evidence for the maximum number of mutually unbiased bases in dimension six*, Physics Letters A **369**, 5–8, (2007).

[25] P. J. Cameron: *Automorphism groups in graphs*, in: R. J. Wilson, L. W. Beineke (Eds.), Selected Topics in Graph Theory, vol. 2, Academic Press, NewYork, 89–127, (1983).

[26] F. R. K. Chung, R. L. Graham, R. M. Wilson: *Quasi-random graphs*, Combinatorica, Volume 9, Issue 4, 345–362, (1989).

[27] F. R. K. Chung, R. L. Graham, P. Frankl, and J. B. Shearer, *Some intersection theorems for ordered sets and graphs*, J. Combin. Theory Ser. A **43**, 23–37, (1986).

[28] S. D. Cohen: *Clique numbers of Paley graphs*, Quaest. Math. **11**, (2), 225–231, (1988).

[29] H. Cohn, N. Elkies: *New upper bounds on sphere packings I.*, Ann. of Math. (2) **157**, no. 2, 689–714, (2003).

[30] E. Coven, A. Meyerowitz: *Tiling the integers with translates of one finite set*, J. Algebra **212**, (1), 161–174, (1999).

[31] T. M. Cover, J. A. Thomas: *Elements of information theory*, Wiley, New York, (1991).

[32] H. T. Croft: *Incidence incidents*, Eureka (Cambridge) **30**, 22–26, (1967).

[33] E. Croot, V. Lev: *Open problems in additive combinatorics*, In: Additive combinatorics, CRM Proc. Lecture Notes Amer. Math. Soc., Providence, RI, **43**, 207–233, (2007).

[34] P. Delsarte: *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. 10, (1973).

[35] P. Dita: *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A, **37**, no. 20, 5355–5374, (2004).

[36] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski: *On mutually unbiased bases*, International Journal of Quantum Information, Vol. **8**, No. 4, 535–640, (2010).

[37] D. E. Dutkay, C-K. Lai: *Some reductions of the spectral set conjecture to integers*, Mathematical Proceedings of the Cambridge Philosophical Society **156**, (2), 123–135, (2014).

[38] D. E. Dutkay, P. E.T. Jorgensen: *On the Universal Tiling Conjecture in Dimension One*, J. Fourier Anal Appl., **19**, 467–477, (2013).

[39] M. Einsiedler, A. Katok, E. Lindenstrauss, *Invariant measures and the set of exceptions to LittlewoodŠs conjecture.* Ann. of Math. 164 (2), (2006), 513-560.

[40] B. Farkas, M. Matolcsi, P. Móra: *On Fuglede's conjecture and the existence of universal spectra*, J. Fourier Anal. Appl., **12**, Number 5, 483–494, (2006).

[41] B. Farkas, Sz. Gy. Révész: Tiles with no spectra in dimension 4, Math. Scand., **98**, 44–52, (2006).

[42] P. Frankl, R. M. Wilson: *Intersection theorems with geometric consequences*, Combinatorica **1**, 357–368, (1981).

[43] G. Freiman: *Foundations of a structural theory of set addition*, American Math. Soc., Providence, R. I., Translated from Russian, Translations of Mathematical Monographs, Vol 37, (1973).

[44] B. Fuglede: *Commuting self-adjoint partial differential operators and a group theoretic problem*, J. Funct. Anal. **16**, 101–121, (1974).

[45] D. Girault-Beauquier, M. Nivat: *Tiling the plane with one tile*, in: Topology and Category Theory in Computer Science, G.M. Reed, A.W. Roscoe, R.F. Wachter (eds.), Oxford Univ. Press, 291–333, (1989).

[46] T. Gowers' web-blog: http://gowers.wordpress.com/2009/11/17/problems-related-to-littlewoods-conjecture-2/

[47] S. Graham, C. Ringrose: *Lower bounds for least quadratic non-residues*, Analytic Number Theory (Allterton Park, IL, 1989), 269–309, (1989).

[48] B. Green: *Counting sets with small sumset, and the clique number of random Cayley graphs*, Combinatorica, **25**(3), 307–326, (2005).

[49] N. Gravin, S. Robins, D. Shiryaev: *Translational tilings by a polytope, with multiplicity*, Combinatorica, to appear.

[50] B. Grünbaum, G.C. Shepard: *Tilings and patterns*, New York: Freeman, (1987).

[51] K. Gyarmati, S. Konyagin, and I. Z. Ruzsa, *Double and triple sums modulo a prime*, CRM Proceedings & Lecture Notes, AMS, Volume 43, 271-278, (2008).

[52] K. Gyarmati, M. Matolcsi, I.Z. Ruzsa: *A superadditivity and submultiplicativity property for cardinalities of sumsets*, Combinatorica, Volume 30, Number 2, Pages 163–174, (2010).

[53] K. Gyarmati, M. Matolcsi, I. Z. Ruzsa: *Plunnecke's inequality for different summands*, Building Bridges Conference, In: Bolyai Society Mathematical Studies, 19; M. Grötschel, G.O.H. Katona(eds.); János Bolyai Mathematical Society and Springer-Verlag, Budapest; 309–320, (2008).

[54] U. Haagerup: *Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory (Rome), Cambridge, MA International Press, 296–322, (1996).

[55] G. Hajós: *Sur la factorization des groupes abéliens*, Casopis Pest Mat. Fys. **74**, 157–162, (1950).

[56] T. S. Han: *Nonnegative entropy measures of multivariate symmetric correlations*, Inform. Contr. **36**, 133–156, (1978).

[57] W. Holzmann, H. Kharaghani, W. Orrick: *On the real unbiased Hadamard matrices*, Contemporary Mathematics, Combinatorics and Graphs, **531**, 243–250, (2010).

[58] A. Iosevich, N. H. Katz, T. Tao: *Convex bodies with a point of curvature do not have Fourier bases*, Amer. J. Math., **123**, (1), 115–120, (2001).

[59] A. Iosevich, N. Katz, T. Tao, *The Fuglede spectral conjecture holds for convex planar domains*, Math. Res. Lett., **10**, (5-6), 559–569, (2003).

[60] Alex Iosevich, M. N. Kolountzakis: *Periodicity of the spectrum in dimension one*, Analysis & PDE, **6-4**, 819–827, (2013).

[61] I. D. Ivanovic: *Geometrical description of quantal state determination*, J. Phys. A **14**, 3241, (1981).

[62] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, M. Weiner: *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, J. Physics A: Mathematical and Theoretical, Vol. 42, Number 24, 245305, (2009).

[63] G. A. Kabatiansky, V. I. Levenshtein: *Bounds for packings on a sphere and in space*, Problems of Information Transmission **14**, 1–17, (1978).

[64] B. R. Karlsson: *H_2-reducible complex Hadamard matrices of order 6*, Linear Algebra and its Applications, Volume 434, Issue 1, 239–246, (2011).

[65] B. R. Karlsson: *Three-parameter complex Hadamard matrices of order 6*, Linear Algebra and its Applications, Volume 434, Issue 1, 247–258, (2011).

[66] A. Klappenecker, M. Rötteler: *Constructions of Mutually Unbiased Bases*, Finite fields and applications, 137–144, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, (2004).

[67] D. J. Kleitman: *On a combinatorial conjecture of Erdős*, J. Comb. Theory **1**, 209–214, (1966).

[68] M. N. Kolountzakis: *Non-symmetric convex domains have no basis of exponentials*, Illinois J. Math., **44**, (3), 542–550, (2000).

[69] M.N. Kolountzakis: *The study of translational tiling with Fourier Analysis*, in Fourier Analysis and Convexity, 131–187, Appl. Numer. Harmon. Anal., Birkhäuser Boston, Boston, MA, (2004).

[70] M.N. Kolountzakis: *Translational tilings of the integers with long periods*, Electr. J. Combinatorics **10**, 1, R22, (2003).

[71] M. N. Kolountzakis, J. C. Lagarias: *Structure of tilings of the line by a function*, Duke Math. J. **82**, 3, 653–678, (1996).

[72] M. N. Kolountzakis, M. Matolcsi: *Tiles with no spectra*, Forum Math., **18**, 519–528, (2006).

[73] M.N. Kolountzakis, M. Matolcsi: *Complex Hadamard matrices and the spectral set conjecture*, Collect. Math., Vol. Extra, 281–291, (2006).

[74] M. N. Kolountzakis, M. Matolcsi: *Algorithms for translational tiling*, Journal of Mathematics and Music, Volume 3, Issue 2, 85–97, (2009).

[75] M. N. Kolountzakis and Sz. Gy. Révész: *Turán's extremal problem for positive definite functions on groups*, J. London Math. Soc. (2), **74**(2), 475–496, (2006).

[76] J. Komlós, M. Sulyok, and E. Szemerédi: *Linear problems in combinatorial number theory*, Acta Math. Hungar. **26**, 113–121, (1975).

[77] S. Konyagin and I. Laba: *Spectra of certain types of polynomials and tiling of integers with translates of finite sets*, J. Number Th. **103**, 2, 267–280, (2003).

[78] M. Krivelevich, B. Sudakov: *Pseudo-random graphs*, in: More Sets, Graphs and Numbers, Bolyai Society Mathematical Studies 15, Springer, 199–262, (2006).

[79] I. Laba: *The spectral set conjecture and multiplicative properties of roots of polynomials*, J. London Math. Soc. (2), **65** (3), 661–671, (2002).

[80] J. C. Lagarias, S. Szabó: *Universal spectra and Tijdeman's conjecture on factorization of cyclic groups*, J. Fourier Anal. Appl., **7** (1), 63–70, (2001).

[81] J. C. Lagarias, Y. Wang: *Tiling the line with translates of one tile*, Inventiones Math. **124**, 341–365, (1996).

[82] J.C. Lagarias and Y. Wang: *Spectral sets and factorizations of finite abelian groups*, J. Funct. Anal. **145**, 73–98, (1997).

[83] N. LeCompte, W. J. Martin, W. Owens: *On the equivalence between real mutually unbiased bases and a certain class of association schemes*, European Journal of Combinatorics, **31**, Issue 6, 1499–1512, (2010).

[84] H. Leptin, D. Müller: *Uniform partitions of unity and locally compact groups*, Adv. Math. **90**, 1, 1–14, (1991).

[85] V. F. Lev: *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory **58**, 79–88, (1996).

[86] J. H. van Lint, R. M. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge, (2nd edition), (2001).

[87] L. Lovász: *Combinatorial Problems and Exercises*, North-Holland, Amsterdam, (2nd edition), (1993).

[88] J. MacWilliams, N. J. A. Sloane: *The Theory of Error Correcting Codes*, Amsterdam, North-Holland, (1977).

[89] M. Madiman, AW. Marcus, P. Tetali: *Entropy and set cardinality inequalities for partition-determined functions*, Random Structures and Algorithms, **40**, (4), 399–424, (2012).

[90] E. Maistrelli, D. B. Penman: *Some colouring problems for Paley graphs*, Discrete Math. **306**, 99–106, (2006).

[91] M. Matolcsi: *Fuglede's conjecture fails in dimension 4*, Proc. Amer. Math. Soc. **133**, no.10, 3021–3026, (2005).

[92] M. Matolcsi: *A Fourier analytic approach to the problem of mutually unbiased bases*, Studia Sci. Math. Hung., Vol. 49, No. 4, 482–491, (2012).

[93] M. Matolcsi: *Improvements on the Delsarte LP-bound*, preprint, (2014).

[94] M. Matolcsi, J. Réffy, F. Szöllõsi: *Constructions of Complex Hadamard matrices via tiling Abelian groups*, Open Systems & Information Dynamics, **14**, 247–263, (2007).

[95] M. Matolcsi, I. Z. Ruzsa: *Sumsets and the convex hull*, In: Additive Number Theory: Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson; David Chudnovsky, Gregory Chudnovsky (eds.), Springer-Verlag, (2010), 221–227.

[96] M. Matolcsi, I. Z. Ruzsa: *Difference sets and positive exponential sums I. General properties*, J. Fourier Anal. Appl., to appear (DOI: 10.1007/s00041-013-9299-9 published online 19. Nov. (2013)).

[97] M. Matolcsi, I. Z. Ruzsa, M. Weiner: *Systems of mutually unbiased Hadamard matrices containing real and complex matrices*, Australasian J. Combinatorics, Volume 55, 35–47, (2013).

[98] M. Matolcsi, F. Szöllõsi: *Towards a classification of 6x6 complex Hadamard matrices*, Open Systems & Information Dynamics, Vol:15, Issue:2, 93–108, (2008).

[99] A. Maxwell, S. Brierley: *On properties of Karlsson Hadamards and sets of Mutually Unbiased Bases in dimension six*, preprint available at http://arxiv.org/abs/1402.4070

[100] R. J. McEliece, E. R. Rodemich, H. Rumsey Jr., L. R. Welch, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Inform. Theory **IT-23**, 157–166, (1977).

[101] P. McMullen: *Convex bodies which tile space by translation*, Mathematika **27**, 113–121, (1980).

[102] H. Minkowski: *Allgemeine Lehrsatze uber die convexen Polyeder*, Nachr. Ges. Wiss. Gottingen., 198–219, (1897).

[103] H. L. Montgomery: *Ten lectures on the interface between analytic number theory and harmonic analysis*, American Mathematical Society, (1994).

[104] M. B. Nathanson: *Additive number theory: Inverse problems and the geometry of sumsets*, Springer, (1996).

[105] D.J. Newman: *Tesselations of integers*, J. Number Th. **9**, 107–111, (1977).

[106] F. M. de Oliveira Filho, F. Vallentin: *Fourier analysis, linear programming, and densities of distance avoiding sets in* $\mathbb{R}^n$, J. Eur. Math. Soc. **12**, 1417–1428, (2010).

[107] J. Pintz, W.L. Steiger, and E. Szemerédi: *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. (2), **37**, 219–231, (1988).

[108] G. Prakash: *Number of sets with small sumset and the clique number of random Cayley graphs*, preprint available at http://arxiv.org/abs/0711.0081v3

[109] A. M. Raigorodskii: *On the chromatic number of a space*, Uspekhi Mat. Nauk 55 (2001), 147–148. English translation in Russian Math. Surveys 55 (2000), 351–352.

[110] P. Raynal, X. Lü, B.-G. Englert: *Mutually unbiased bases in six dimensions: The four most distant bases*, Phys. Rev. A **83**, 062303, (2011).

[111] Sz. Révész: *Turán's extremal problem on locally compact abelian groups*, Anal. Math., **37**, Issue 1, 15–50, (2011).

[112] R.M. Robinson: *Undecidability and nonperiodicity for tilings of the plane*, Invent. Math. **12**, 177–209, (1971).

[113] W. Rudin: *Fourier analysis on groups*, Reprint of the 1962 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, (1990).

[114] I.Z. Ruzsa: *Difference sets without squares*, Periodica Math. Hungar., **15**, 205–209, (1984).

[115] I. Z. Ruzsa: *Connections between the uniform distribution of a sequence and its differences*, Topics in Number Theory (Budapest 1981), Coll. Math. Soc. J. Bolyai, vol. 34, 1419–1443, Akadémiai Kiadó, Budapest, (1984).

[116] I. Z. Ruzsa: *Cardinality questions about sumsets*, Additive combinatorics, 195–205, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, (2007).

[117] I. Z. Ruzsa: *Appendix, in: R. Tijdeman: Periodicity and Almost-periodicity*, More sets, graphs and numbers, 381–405, Bolyai Soc. Math. Stud., 15, Springer, Berlin, (2006).

[118] A. Samorodnitsky: *Extremal properties of solutions for Delsarte's linear program*, manuscript available at http://www.cs.huji.ac.il/ salex/ (1998).

[119] A. Samorodnitsky: *On the Optimum of Delsarte's Linear Program*, Journal of Combinatorial Theory, Series A, **96**, Issue 2, 261–287, (2001).

[120] T. Sanders: *On Roth's theorem on progressions*, Ann. of Math. (2) **174**, no. 1, 619–636, (2011).

[121] A.D. Sands: *On a conjecture of G. Hajós*, Glasgow Math. Journal, **15**, 88–89, (1974).

[122] A.D. Sands: *On the factorization of finite Abelian groups*, Acta Math. Acad Sci. Hungar. **8**, 65–86, (1957).

[123] A.D. Sands: *On the factorization of finite Abelian groups II*, Acta Math. Acad Sci. Hungar. **13**, 153–159, (1962).

[124] A.D. Sands: *On Keller's conjecture for certain cyclic groups*, Proc. Edinburgh Math. Soc. (2), **22**, 17–21, (1977).

[125] J. P. Steinberger: *Tilings of the integers can have superpolynomial periods*, Combinatorica **29**, (4), 503–509, (2009).

[126] S. Szabó: *A type of factorization of finite abelian groups*, Discrete Math., **54**, no. 1, 121–124, (1985).

[127] M. Szegedy: *Algorithms to tile the infinite grid with finite clusters*, In: Proceedings of the 39th Annual Symposium on the Foundations of Computer Science, 137–145, (1998).

[128] L. A. Székely: *Measurable chromatic number of geometric graphs and sets without some distances in Euclidean space*, Combinatorica **4**, 213–218, (1984).

[129] F. Szöllősi: *Complex Hadamard matrices of order 6: a four-parameter family*, J. Lond. Math. Soc. (2) 85, no. 3, 616–632, (2012).

[130] W. Tadej: *Permutation equivalence classes of Kronecker Products of unitary Fourier matrices*, Linear Algebra Appl. 418, no. 2-3, 719–736, (2006).

[131] W. Tadej, K. Życzkowski: *A concise guide to complex Hadamard matrices*, Open Syst. Inf. Dyn., **13**, 133–177, (2006).

[132] T. Tao: *Fuglede's conjecture is false in 5 and higher dimensions*, Math. Res. Lett., **11**, (2-3), 251–258, (2004).

[133] T. Tao, V. H. Vu: *Additive combinatorics*, Cambridge University Press, Cambridge, (2006).

[134] R. J. Vanderbei: *Linear Programming: Foundations and Extensions*, Second Edition, Springer-Verlag, (2001).

[135] B. A. Venkov: *On a class of Euclidean polyhedra*, Vestnik Leningrad Univ. Ser. Math. Fiz. Him. 9 (1954), 11–31 (in Russian).

[136] D. T. Vuza: *Supplementary Sets and Regular Complementary Unending Canons*, Perspectives of New Music, nos 29(2) 22–49; 30(1), 184–207; 30(2), 102–125; 31(1), 270–305, (1991).

[137] Web-page of Geoffrey Exoo with clique numbers of Paley graphs for $7000 < p < 10000$, http://ginger.indstate.edu/ge/PALEY/

[138] Web-page of J. B. Shearer with clique numbers of Paley graphs for $p < 7000$, http://www.research.ibm.com/people/s/shearer/indpal.html

[139] Web-page discussion of clique numbers and plot of the function $s(p)$ for $p < 10000$, http://mathoverflow.net/questions/48591/cliques-paley-graphs-and-quadratic-residues

[140] M. Weiner: *A gap for the maximum number of mutually unbiased bases*, Proc. Amer. Math. Soc. 141, no. 6, 1963–1969, (2013).

[141] R. F. Werner: *All teleportation and dense coding schemes*, J. Phys. A, **34**, 7081–7094, (2001).

[142] P. Wocjan, T. Beth: *New construction of mutually unbiased bases in square dimensions*, Quantum Inf. Comput. **5**, 93–101, (2005).

[143] H.A.G. Wijshoff, J. van Leeuwen: *Arbitrary versus periodic storage schemes and tesselations of the plane using one type of polyomino*, Information and Control **62**, 1–25, (1984).

[144] W. K. Wootters, B. D. Fields: *Optimal state-determination by mutually unbiased measurements*, Ann. Physics **191**, 363–381, (1989).

[145] G. Zauner: *Quantendesigns Ű Grundzüge einer nichtkommutativen Designtheorie*, PhD thesis, Universität Wien, (1999). (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf)