INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or “target” for pages apparently lacking from the document photographed is “Missing Page(s)”. If it was possible to obtain the missing page(s) or section; they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of “sectioning” the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.
Hajela, Dhananjay

ON COUNTING POINTS IN HYPERCUBES, ADDITIVE SEQUENCES AND LAMBDA(P) SETS

The Ohio State University

University Microfilms International

300 N. Zeeb Road, Ann Arbor, MI 48106
ON COUNTING POINTS IN HYPERCUBES,
ADDITIVE SEQUENCES AND $\Lambda(p)$ SETS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

Dhananjay Hajela, M.S., M.S.

* * * * *

The Ohio State University

1983

Reading Committee:

Approved By

William B. Johnson
Joseph Rosenblatt
Paul Seymour

William B. Johnson
Adviser
Department of Mathematics
This work is dedicated to my mother and father.
Acknowledgements

There are several people to whom I wish to express my gratitude and appreciation for making this work possible. I would particularly like to thank my advisor Professor William B. Johnson for his interest, advice and many valuable discussions regarding the subject matter of this dissertation. My special thanks go also to Professors Paul Erdös and Paul Seymour for several inspiring discussions.

I have also benefited from conversations with and communications from several mathematicians. I would like to thank B. Baishanski, W. Davis, P. Deligne, G. Edgar, J. Fournier, R. Graham, G. Pisier, D. Ray-Chaudhuri, J. Rosenblatt, K. Ross, G. Schechtman, M. Talagrand and others too numerous to mention.

I would like to thank Laura Brumfield and Jacqueline Jones for expertly typing this dissertation.

Finally I would like to thank my parents for their encouragement and support during the writing of this dissertation and during the many years since I first started my studies.
April 23, 1960

1975

1978

1981

1975-1976

1976-1983

B.S., The Ohio State University, Columbus, Ohio

M.S., Mathematics, The Ohio State University, Columbus, Ohio

M.S., Computer Science, The Ohio State University, Columbus, Ohio

University Fellowship, The Ohio State University, Columbus, Ohio

Teaching Associate, The Ohio State University, Columbus, Ohio

PUBLICATIONS


FIELDS OF STUDY

Major Field: Mathematics


Minor Field: Computer and Information Science

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEDICATION................................. ii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS............................ iii</td>
</tr>
<tr>
<td>VITA...................................... iv</td>
</tr>
<tr>
<td>LIST OF FIGURES........................... vii</td>
</tr>
</tbody>
</table>

Chapter

I. INTRODUCTION.......................... 1

II. COUNTING POINTS IN HYPERCUBES AND CONVOLUTION MEASURE ALGEBRAS

II.1 Introduction.......................... 5
II.2 Counting Points in Hypercubes........... 7

III. $B_h[g]$ SEQUENCES

III.1 Introduction.......................... 25
III.2 Estimates on $F_h(n,g)$ Using Local Theory..... 28
III.3 Estimates on $F_h(n,g)$ Using Trigonometric Polynomials......................... 35
III.4 Estimates on $F_h(n,g)$ Using a Gap Theorem on Primes......................... 44

IV. CONSTRUCTION TECHNIQUES FOR $A(p)$ SETS

IV.1 Introduction.......................... 48
IV.2 Construction in the Dual of the Cantor Group. 53
IV.3 Preliminary Facts........................ 64
IV.4 Construction in $\mathbb{Z}$ and $\mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots \ldots 68$
IV.5 Construction in $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots \ldots 79
IV.6 Construction in $\mathbb{Z}(p^\infty)$ ......................... 88
IV.7 Finite Random $\Lambda(p)$ Sets ......................... 95
IV.8 Some Related Results ................................. 100

LIST OF REFERENCES ......................................... 104
LIST OF FIGURES

| Figure 2.1 | 11 |
| Figure 2.2 | 16 |
| Figure 2.3 | 16 |
| Figure 2.4 | 17 |
| Figure 2.5.1 | 18 |
| Figure 2.5.2 | 18 |
| Figure 2.5.3 | 18 |
| Figure 2.5.4 | 18 |
| Figure 2.5.5 | 18 |
| Figure 2.5.6 | 18 |
| Figure 2.6 | 19 |
| Figure 2.7 | 20 |
I. INTRODUCTION

This dissertation is concerned with three different topics. However all three topics are related in that the methods involved in investigating these topics are concerned with the interaction between certain ideas in combinatorics, number theory and harmonic analysis. Below we give a brief summary of the results obtained. A more detailed account of the results may be found in the introductions to the various chapters.

In chapter II we investigate a combinatorial problem about midpoints of hypercubes and give some applications of it. The results of this chapter were obtained jointly with P. Seymour. It is shown that if $A$ and $B$ are non-empty subsets of $\{0,1\}^n$ (for some $n \in \mathbb{N}$) then $|A + B| \geq (|A||B|)^{\alpha}$ where $\alpha = \frac{1}{3} \log_2 3$. In particular if $|A| = 2^{n-1}$ then $|A + A| \geq 3^{n-1}$ which answers a question of Erdös. It is also shown that if $|A| = 2^{n-1}$ then $|A + A| = 3^{n-1}$ if and only if the points of $A$ lie on a hyperplane in $n$-dimensions. This answers a stronger form of the above conjecture. A generalization of this last result is given in a forthcoming paper of P. Seymour and the author where necessary and sufficient conditions on $A$ and $B$ are given to deal with the extremal case $|A + B| = (|A||B|)^{\alpha}$. The above results also yield an improved version of a
result of Talagrand [48]. We obtain that if $X$ and $Y$ are analytic subsets of the Cantor set $K$ with $m(X)m(Y) > 0$ then

$$\lambda(X + Y) \geq 2(m(X)m(Y))^\alpha$$

where $\alpha$ is as above, $m$ is the usual measure on $K$ and $\lambda$ is Lebesgue measure. This also answers a question of Moran (in more precise terms than the answer given by Talagrand), showing that $m$ is not concentrated on any proper Ralkov system.

Chapter III addresses various problems concerning $B_h[g]$ sequences. An increasing sequence of natural numbers $A = (a_1)$ (finite or infinite) is called $B_h[g]$ if every $n \in \mathbb{N}$ can be written in at most $g$ ways as a sum of $h$ ($h > 2$) elements of $A$. The reader who reads chapter IV will observe that an infinite $B_h[g]$ sequence is a $\Lambda(2h)$ set in $\mathbb{Z}$. It was this interaction in fact which motivated the results of chapter III.

Denote by $F_h(n,g)$ the cardinality of the largest $B_h[g]$ sequence in $\{1, \ldots, n\}$. A well known question asks for bounds on $F_h(n,g)$ (see [20], page 96). We obtain bounds on $F_h(n,g)$ in three different ways, using Banach space theory, using estimates or trigonometrical sums and by using a gap theorem for primes. In turn these bounds on $F_h(n,g)$ yield partial answers to a generalization of a question of Bose and Chowla (communicated to us by Professor Erdős) and of a generalization of a question of Erdős and Turan [14]. Bose and Chowla's question is: given natural numbers $a_1 < a_2 < \ldots < \delta n^3$ (for some $0 < \delta < 1$) does there exist
a \( n_0(\delta) \in \mathbb{N} \) such that for \( n \geq n_0(\delta) \) there is a duplication among the sums \( a_i + a_j + a_k \) (\( 1 \leq j < k \))? Erdős and Turan's question is: if \( A = (a_i)_{i=1}^{\infty} \) is an increasing sequence of natural numbers with \( a_k < ck^2 \) for some \( c > 0 \) and all \( k \), is it true that \[ \sup \{ R(n,A) \} = +\infty \] where \( R(n,A) \) is the number of ways of writing \( n \) as a sum of two elements of \( A \)?

In chapter IV various techniques are presented for constructing \( \Lambda(p) \) sets which are not \( \Lambda(p + \epsilon) \) for any \( \epsilon > 0 \). The main result is that there is a \( \Lambda(4) \) set in the dual of any compact abelian group which is not \( \Lambda(4 + \epsilon) \) for any \( \epsilon > 0 \). Along the way to proving the above assertion we give new constructions of \( \Lambda(p) \) but not \( \Lambda(p + \epsilon) \) sets for any \( \epsilon > 0 \) (and certain values of \( p \)) in duals of compact abelian groups in which such constructions were already known. The main new results in specific dual groups are: there is a \( \Lambda(2k) \) set which is not \( \Lambda(2k + \epsilon) \) in \( \mathbb{Z}(2) \oplus \mathbb{Z}(2) \oplus \ldots \) for all \( k \geq 2, k \in \mathbb{N} \) and \( \epsilon > 0 \) and in \( \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots \) (\( p \) a prime, \( p > 2 \)) for \( 2 \leq k < p, k \in \mathbb{N} \) and \( \epsilon > 0 \) (thus answering in a strong form a question in Lopez and Ross's book [32]).

It is also shown that random infinite integer sequences are \( \Lambda(2k) \) but not \( \Lambda(2k + \epsilon) \) for \( k \geq 2, k \in \mathbb{N} \) and \( \epsilon > 0 \). The reader who reads chapter III will notice that the last assertion is in fact proved by constructing random \( B_h[g] \) sequences. Also finite random \( \Lambda(p) \) sets are investigated
in arbitrary dual groups. Finally various applications to Banach spaces are discussed including the existence of uniformly complemented Hilbertian subspaces and a generalization of the classical gap theorem of Paley.

Notation is introduced in the respective chapters as needed. Any non-standard notation that is needed is defined; however, for the sake of completeness various standard references are given when appropriate. Although the various chapters are interconnected the reader who is so inclined may read each chapter independently of any of the others, since the chapters were so written that they are totally independent of each other.
II. COUNTING POINTS IN HYPERCUBES AND CONVOLUTION MEASURE ALGEBRAS

II.1. INTRODUCTION

In this chapter we consider a problem of Erdős (communicated to us by M. Talagrand): Suppose $A \subseteq \{0,1\}^n$ with $|A| = 2^{n-1}$; is it true that $|A + A| \geq 3^{n-1}$. We also consider the extremal problem of characterizing those sets $A \subseteq \{0,1\}^n$ with $|A| = 2^{n-1}$ such that $|A + A| = 3^{n-1}$.

We now describe the contents of this chapter more fully and also various previous results in this direction. In section 2 we consider the following generalization of the problem of Erdős: Suppose $A, B \subseteq \{0,1\}^n$, $A \neq \emptyset$, $B \neq \emptyset$ (i.e. $A, B$, are non-empty subsets of the vertices of the n-cube, $I^n$), then the number of midpoints of $A, B$ i.e. $|\frac{A + B}{2}|$ is at least $(|A| \cdot |B|)^\alpha$ where $\alpha = \frac{1}{2}\log_23$. Clearly this yields an affirmative answer to Erdős' problem with $A = B$. It is also shown that a necessary and sufficient condition for $|A + A| = 3^{n-1}$ (provided that $|A| = 2^{n-1}$) is that the points of $A$ lie on a hyperplane in $n$-dimensions. This too was a conjecture of Erdős. Weaker results of the above type were obtained by Talagrand (see [Tal]). As an immediate application we obtain the following result: Suppose $\lambda$ is the
Lebesgue measure on $\mathbb{R}$ and let $\mu$ denote the usual Haar measure on the Cantor group $D=\{0,1\}^\mathbb{N}$. If $X$ and $Y$ are analytic subsets of $D$ with $\mu(X)\mu(Y)>0$ then $\lambda(X+Y)\geq 2(\mu(X)\mu(Y))^{\alpha}$ where $\alpha$ is as before (the addition of $X$ and $Y$ is with respect to the usual addition on $\mathbb{R}$ after identifying $D$ with the classical Cantor set in $[0,1]$). A special case of this had been posed as a problem by W. Moran: If $\mu(X)>0$ is $\lambda(X+X)>0$? This special case was solved earlier by M. Talagrand (see [48] who showed that $\lambda(X+X)\geq 2(2\mu(X)-1)$. Moran's interest in this was from the point of view of convolution measure algebras. It shows that $\mu$ cannot be concentrated on proper Raikov systems. The proof of the above statements for the Cantor set has certain features in common with the proof in [48], but is actually somewhat simpler.

The notation we use is standard. For unexplained terminology from harmonic analysis see [17]. As was mentioned in the introduction, the work of this chapter was done jointly with P. Seymour.
II.2 COUNTING POINTS IN HYPER-CUBES

We start in this section by giving an affirmative answer to a generalization of a question of Erdős. Recall Erdős' question from section II.1:
Given \( A \subseteq \{0,1\}^n \) with \( |A| \geq 2^{n-1} \), is it true that \( |A + A| \geq 3^{n-1} \)?
We show the following:

**Theorem 2.1:**

If \( A, B \subseteq \{0,1\}^n \) are non empty then \( |A + B| \geq (|A| |B|)^{\alpha} \) where \( \alpha = \frac{1}{2} \log_2 3 \). (Throughout this section \( \alpha \) is \( \frac{1}{2} \log_2 3 \).

An immediate consequence is (by taking \( A = B \) with \( |A| = 2^{n-1} \)):

**Theorem 2.2:**

If \( A \subseteq \{0,1\}^n \) with \( |A| = 2^{n-1} \) then \( |A + A| \geq 3^{n-1} \).

To prove theorem 2.1 we need two elementary calculus lemmas (for both of these there is probably a suitable reference, but we are unable to find one). Lemma 2.1 was pointed out to us by G. Edgar and simplifies the proof of lemma 2.2.

**Lemma 2.1:**

If \( \alpha_0 < \alpha_1 \ldots < \alpha_n \) and \( a_n \neq 0 \) then \( g(t) = \sum_{k=0}^{n} a_k t^{\alpha_k} \) has at most \( n \) zeros in \( (0, +\infty) \), counting multiplicity.
Proof:

The proof is by induction on $n$. For $n = 0$, $a_0 t^{\alpha_0}$ has no zeros on $(0, \infty)$. If $g(t) = \sum_{k=0}^{n} a_k t^{\alpha_k}$, then $g(t)$ has the same number of zeros in $(0, \infty)$ as $\sum_{k=0}^{n} a_k t^{\alpha_k-\alpha_0} = g(t)/t^{\alpha_0}$.

The derivative $\frac{d}{dt} g(t) = \sum_{k=1}^{n} a_k (\alpha_k - \alpha_0) t^{\alpha_k-\alpha_0-1}$ has at most $n-1$ zeros by induction. So by Rolle's theorem $g(t)$ has at most $n$ zeros. \qed

The next lemma we need is:

Lemma 2.2:

Let $g(a,b) = (ab)^\alpha + ((1-a)(1-b))^{\alpha} + (a(1-b))^{\alpha}$ for $(a,b) \in [0,1] \times [0,1]$ and $h(a,b) = (ab)^\alpha + ((1-a)(1-b))^{\alpha} + (1-a) b)^{\alpha}$ for $(a,b) \in [0,1] \times [0,1]$. Then $\max (g,h) \geq 1$ for all $(a,b) \in [0,1] \times [0,1]$.

Proof:

Assume $a \geq b$ (the case $a \leq b$ is similar). Then $\max (g(a,b), h(a,b)) = g(a,b)$. If $a = 1$ or $b = 0$ then $g(a,b) = b^\alpha + (1-b)^\alpha$ or $g(a,b) = a^\alpha + (1-a)^\alpha$ respectively. In either case $g(a,b) \geq 1$. This leaves the points $(a,b)$ with $a \geq b$, $a < 1$, $b > 0$ to check. We have,
\[
\frac{\partial g}{\partial a} = \alpha (ab)^{\alpha} a^{-1} + \alpha (a(1-b))^{\alpha} a^{-1} - \alpha ((1-a)(1-b))^{\alpha} (1-a)^{-1}.
\]

Setting \( \frac{\partial g}{\partial a} = 0 \) we get,

\[
ag = a^\alpha [b^\alpha + (1-b)^\alpha]
\]

\( \geq a^\alpha \)

So \( g \geq a^{\alpha-1} \) and so \( g \geq 1 \). For \( a = b \) we have to make a special argument since \( g = h \) and \( \max (g, h) \) is not differentiable. So we only have to show that \( \min_{x \in [0,1]} f(x) = 1 \) where

where \( f(x) = x^{2\alpha} + (1-x)^{2\alpha} + x^\alpha (1-x)^\alpha \). We have that,

\[
f'(x) = 2\alpha x^{2\alpha-1} - 2\alpha (1-x)^{2\alpha-1} + \alpha x^{\alpha-1} (1-x)^\alpha - \alpha x^\alpha (1-x)^{\alpha-1}
\]

\[
f''(x) = (2\alpha)(2\alpha-1)x^{2\alpha-2} + (2\alpha)(2\alpha-1)(1-x)^{2\alpha-2} + \alpha(\alpha-1)x^{\alpha-2}(1-x)^\alpha
\]

\[-2\alpha^2 x^{\alpha-1}(1-x)^{\alpha-1} + \alpha(\alpha-1)x^\alpha (1-x)^{\alpha-2}.
\]

So \( f'(\frac{1}{2}) = 0, f''(\frac{1}{2}) = (8\alpha^2 - 6\alpha)(\frac{1}{2})^{2\alpha-2} > 0 \). So \( f \) has a relative minimum at \( \frac{1}{2} \) with \( f(\frac{1}{2}) = 1 \). Now \( \lim_{x \to 0} f'(x) = +\infty \) and \( \lim_{x \to 1} f'(x) = -\infty \), so \( f \) is increasing near 0, decreasing near 1. It is therefore enough to show \( f' \) has at most 3 zeros in \((0,1)\) (counting \( \frac{1}{2} \) and counting multiplicity, also note that \( f(0) = f(1) = 1 \)). Now,
\[
\frac{f'}{ax^a(1-x)^{a-1}} = 2 \frac{x^{a-1}}{(1-x)^{a-1}} - 2 \frac{(1-x)^a}{x^a} + \frac{1-x}{x} - 1
\]

\[
= t - 2t^\alpha + 2t^{1-\alpha} - 1 \equiv P(t),
\]

with \( t = \frac{1-x}{x} \).

Then \( P(t) \) has the same number of zeros on \((0,\infty)\) as \( f' \) has in \((0,1)\). Since \( 1 > \alpha > 1 - \alpha > 0 \), \( P(t) \) has at most three zeros by lemma 2.1, thus concluding the proof.

The proof of theorem 2.1 now follows easily.

**Proof (of theorem 2.1):**

The proof is by induction on \( n \). It is trivial for \( n = 1 \).

From now on we regard \( A \) and \( B \) naturally as subsets of the vertices of the \( n \)-dimensional unit cube \( I^n \) (and \( \frac{A+B}{2} \) as midpoints). We assume the result true for \((n-1)\)-dimensional cubes. Regarding \( I^n \) as the cube (see Figure 2.1),
where each face is $I^{n-1}$ and denote by $a_i = |A \cap F_i|$ and $b_i = |B \cap F_i|$ for $i = 1, 2$ where $F_1$ and $F_2$ are opposite faces.

By induction the number of midpoints gotten from $A$ and $B$ on the face $F_1$ is,

$$\left(2.1\right) \quad \frac{|(A \cap F_1) + (B \cap F_1)|}{2} \geq (a_1 b_1)^\alpha .$$

Similarly for the face $F_2$ we have

$$\left(2.2\right) \quad \frac{|(A \cap F_2) + (B \cap F_2)|}{2} \geq (a_2 b_2)^\alpha .$$

Now considering midpoints generated by $A \cap F_1$ and $B \cap F_2$ (and ignoring the midpoints generated by $A \cap F_2$ and $B \cap F_1$) we get by induction (since they all lie on a hyperplane between $F_1$ and $F_2$) that,
Adding the above inequalities we get,

$$\left| \frac{A + B}{2} \right| \geq (a_1 b_1)^\alpha + (a_2 b_2)^\alpha + (a_3 b_3)^\alpha,$$

since all the midpoints generated in (2.1), (2.2) and (2.3) lie on different planes. Similarly

$$\left| \frac{A + B}{2} \right| \geq (a_1 b_1)^\alpha + (a_2 b_2)^\alpha + (a_3 b_3)^\alpha.$$

So by lemma 2.2, the proof is completed. □

Remark 2.1:

It is natural to ask what happens when more than two sets are taken in theorem 2.1. It seems plausible that given $p \in \mathbb{N}$ and $A_1, \ldots, A_p \subseteq \{0,1\}^n$ that

$$\left| A_1 + \ldots + A_p \right| \geq (|A_1| |A_2| \ldots |A_p|)^\alpha_p$$

where $\alpha_p = \frac{1}{p} \log_2 (p+1)$. Clearly by using the same sort of proof as in theorem 2.1 it is enough to show the following:

Given $b = (b_1, \ldots, b_p) \in \mathbb{I}^p$ and $\pi \in S_p$ (the group of permutations on $\{1,\ldots, p\}$) define by,
and set \( f(b) = \max_{\pi \in S^p} f_\pi(b) \). Is it true that \( f(b) \geq 1 \)? Equivalently without loss of generality by ordering so that \( b_1 \leq ... \leq b_p \), it is enough to show that,

\[
g(b) = (b_1 ... b_p)^{\alpha_p} + ((1-b_1)b_2 ... b_p)^{\alpha_p} + ... + ((1-b_1)...(1-b_p))^{\alpha_p} \geq 1.
\]

This was however not checked.

We now turn to another conjecture of Erdős: He conjectured that if \( |A| = 2^{n-1} \) with \( A \subseteq \{0,1\}^n \) then \( |A + A| = 3^{n-1} \) if and only if the points of \( A \) lie on a hyperplane in \( n \)-dimensions. We show that this is indeed the case. One direction is trivial.

**Proposition 2.1:**

If \( |A| = 2^{n-1} \), \( A \subseteq \{0,1\}^n \) and the points of \( A \) lie on a hyperplane then \( |A + A| = 3^{n-1} \).
Proof:

It is clearly enough to check that for any $n \geq 1$,
$$|\{0,1\}^n + \{0,1\}^n| = 3^n. $$
This is because with the condition on $A$ we may assume that the points of $A$ are the points of a $(n-1)$ dimensional face of the (rotated, if necessary) cube, $\{0,1\}^n$. □

Next we show that if $|A| = 2^{n-1}$, $A \subseteq \{0,1\}^n$ and $|A + A| = 3^{n-1}$ then the points of $A$ lie on a hyperplane.

Theorem 2.3:

If $A \subseteq \{0,1\}^n$, $|A| = 2^{n-1}$ and $|A + A| = 3^{n-1}$ then $A$ lies on a hyperplane in $n$-dimensions.

Proof:

The proof is by induction on $n$. Clearly it is true for $n=1$ and $n=2$. Note that equality occurs in the inequality of lemma 2.2 (see the proof), when $(a,b) = (0,0),(1,0),(0,1),$ $(1,1)$ or $(i,i)$. So by the proof of theorem 2.1 it follows that for $A,B \subseteq \{0,1\}^{n+1}$, $|A + B| = (|A| \cdot |B|)^\alpha$ implies that one of the following four cases occurs ($F_1$ and $F_2$ are opposite $n$-dimensional faces of $I^{n+1}$):

Case 1: $|F_1 \cap A| = |F_1 \cap B| = 0$

Case 2: $|F_2 \cap A| = |F_2 \cap B| = 0$

Case 3: $|F_1 \cap A| = |F_2 \cap B| = 0$

Case 4: $|F_1 \cap A| = |F_2 \cap A| \text{ and } |F_1 \cap B| = |F_2 \cap B|$. 
In our case with $A=B$ this reduces to:

**Case 1 and Case 2:** $A$ lies on an $n$-dimensional face of $I^{n+1}$. Since $|A| = 2^n$ this implies that $A$ consists of the vertices of a $n$-dimensional cube and lies on a hyperplane in $(n+1)$ dimensional space.

**Case 3:** This case clearly doesn't occur because since we have that $A=B$.

**Case 4:** In this case $|F \cap A| = \frac{1}{2}|A| = 2^{n-1}$ for all $n$-dimensional faces of $F$ of $I^{n+1}$. It follows that

$$|(F \cap A) + (F \cap A)| > 3^{n-1}$$

by theorem 2.2. Since $|A + A| = 3^n$, by the proof of theorem 2.1 it follows that

$$|(F \cap A) + (F \cap A)| = 3^{n-1}$$

by the induction hypothesis, $F \cap A$ lies on a hyperplane in $n$-dimensional space for all faces $F$.

Let us first make the following observation. First some terminology is needed. Regarding $I^{n+1}$ as built out of two opposite $n$-dimensional faces, say $F_1$ and $F_2$ with edges joined (as shown in Figure 2.2), a typical set of "opposite edges" is shown as darkened (i.e. edges are non-trivial) (i.e. $n-2$ dimensional) intersections of two $n$-dimensional faces and "opposite edges" lie on a "diagonal" hyperplane in $(n+1)$ dimensions). The point to note is that $|F \cap A| = \frac{1}{2}|A|$ for all $n$-dimensional faces $F$ means that $|E_1 \cap A| = |E_2 \cap A|$ for all pairs of opposite edges $E_1$ and $E_2$. 
From now on we regard $I^{n+1}$ as two $n$-dimensional cubes (with the edges joined). This is shown in Figure 2.3 (where the edges between the two $n$-dimensional cubes have not been joined for convenience). Each $n$-dimensional cube is drawn below as a cube. The cubes are labeled as $C_1$ and $C_2$ for the rest of the proof.
The proof now splits into two cases.

Case A: \( C_2 \cap A \) lies on a face of \( C_2 \), say \( G_2 \) (see figure 2.3). Then by the fact that opposite edges of \( I^{n+1} \) intersect \( A \) in equal cardinality it follows that \( |G_2 \cap A| = |C_1 \cap A| = 2^{n-1} \). It follows that \( A \) lies on a "diagonal" hyperplane in \((n+1)\) - dimensional space.

Case B: \( C_2 \cap A \) lies on a diagonal hyperplane in \( n \)-dimensional space, so that \( C_2 \cap A \) lies on opposite edges of \( C_2 \) say as shown in figure 2.4 (opposite edges darkened):

![Figure 2.4](image)

Since opposite edges of \( I^{n+1} \) intersect \( A \) in equal cardinality it follows that \( C_1 \cap A \) also lies on a "diagonal" hyperplane in \( n \)-dimensional space. Six subcases arise. \( C_1 \cap A \) can lie on opposite edges as shown on page 18 (opposite edges darkened).
It is easy to see that with respect to the situation in figure 2.4, $C_1 \cap A$ looks like figure 2.5.6 and that $A$ in this case is on a "diagonal" hyperplane in $(n+1)$ dimensions. For example, we show that the case of figure 2.5.1 cannot occur (the other cases are dispensed with in the same manner). Suppose $C_1 \cap A$ is as in figure 2.5.1 and $C_2 \cap A$ as in figure 2.4. Then $I^{n+1}$ looks as shown in figure 2.6 (with edges between $C_1$ and $C_2$ drawn):

![Figure 2.6](image-url)
Looking at the bottom most \( n \)-dimensional cube \( C_3 \) (see figure 2.6) we have \( (C_3 \cap A) \) drawn in dots) in figure 2.7:

![Figure 2.7](image)

But \( C_3 \cap A \) is supposed to lie on a hyperplane which it doesn't.

Accordingly in all cases \( A \) lies on a \((n+1)\) dimensional hyperplane and the proof is complete. \( \square \)

We now show that as an immediate consequence of theorem 2.1 we may obtain more precise results than the results of Talagrand [48], mentioned in the introduction. We first need some notation. \( D = \{0,1\}^\mathbb{N} \) will denote the Cantor group (with the group operation being coordinatewise addition modulo 2). Of course \( D \) is homeomorphic to the classical Cantor set \( K \subset [0,1] \). We make use of this association below freely without further mentioning it. Let \( \mu \) denote the Haar measure on \( D \) i.e. if \( \mu_i \) is the measure \( \mu_i \{0\} = \mu_i \{1\} = \frac{1}{2} \) on the
The proof below uses some of the same techniques as in [7], but is actually simpler.

**Theorem 2.4:**

If $X$ and $Y$ are analytic subsets of $D$ s.t. $\mu(X)\mu(Y) > 0$ then $\lambda(X + Y) \geq 2(\mu(X)\mu(Y))^{\alpha}$.

**Proof:**

Assume without loss of generality that $X$ and $Y$ are compact subsets of $D$. Write $K_n^d = \bigcup_{d \in D_n} I_n, d$ where $I_n, d$ is the interval

$$I_n, d = [d, d + \frac{1}{3^n}]$$

where $D_n$ is the set of all numbers of the form $\sum_{k=1}^{n} d_k \frac{1}{3^k}$ where $d_k \in \{0, 2\}$ for all $k$. Note that

$$I_n, d + I_n, d' = [d + d', d + d' + \frac{2}{3^n}] = 2\left[\frac{d + d'}{2}, \frac{d + d'}{2} + \frac{1}{3^n}\right].$$

The point in writing it this way is that it is easy to write $\frac{d + d'}{2}$ in base 3. To be specific, if $d = \sum_{k=1}^{n} d_k \frac{1}{3^k}$ then

$$d' = \sum_{k=1}^{n} d_k' \frac{1}{3^k} \text{ then } \frac{d + d'}{2} = \sum_{k=1}^{n} d_k + d_k' \frac{1}{3^k} = .d_1...d_n$$

where $d_k' = \frac{d_k + d_k'}{2}$. Set $X_n = \bigcup I_n, d$ and $Y_n = \bigcup I_n, d$

$X_n, d \cap X \neq \emptyset \quad I_n, d \cap Y \neq \emptyset$
Then \( X = \bigcap_n X_n \) and \( Y = \bigcap_n Y_n \). It is easy to see that
\[ X + Y = \bigcap_n (X_n + Y_n), \]
It is therefore enough to show that
\[ \lambda(X_n + Y_n) \geq 2^{\mu(X)\mu(Y)} \alpha \]
for all \( n \). Let \( E \) be the set of all \( d \in D_n \) such that \( I_{n,d} \subseteq X_n^c \) and let \( F \) be the set of all \( d \in D_n \) such that \( I_{n,d} \subseteq Y_n^c \). Then note that
\[ |E| \leq 2^n \mu(X^c) \quad \text{and} \quad |F| \leq 2^n \mu(Y^c). \]
So if \( E' \) is the set of all \( d \in D_n \) such that \( I_{n,d} \cap X \neq \emptyset \) and \( F' \) is the set of all \( d \in D_n \) such that \( I_{n,d} \cap Y \neq \emptyset \) then
\[ |E'| \geq 2^n - 2^n \mu(X^c) = 2^n \mu(X) \]
and \( |F'| \geq 2^n - 2^n \mu(Y^c) = 2^n \mu(Y) \). So by applying theorem 2.1 we have that,
\[ |E' + F'| \geq (2^n \mu(X)2^n \mu(Y))^{\alpha} = 3^n(\mu(X)\mu(Y))^{\alpha}. \]
So \( \lambda(X_n + Y_n) \geq 2^{\mu(X)\mu(Y)} \alpha \) for all \( n \), completing the proof. \( \square \)

Remark 2.2:

Clearly the proof above is valid if we replace \( X \) and \( Y \) analytic by \( X \) measurable, \( Y \) measurable such that \( X + Y \) is measurable, but it is hard to think of a more succinct condition on \( X \) and \( Y \) (other than being analytic) which insures \( X + Y \) measurable.
Remark 2.3:

M. Talagrand had shown earlier (see [48]) that if $X$ is analytic then,

1) $\lambda(X + X) \geq 2(\mu(X) - 1)$
2) $\lambda(X + K) \geq 2 \mu(X)$.

Both of these inequalities are special cases of theorem 2.4 since $x^{2\alpha} \geq 2x - 1$ and $x^\alpha \geq x$ for $x \in [0,1]$.

One application of theorem 2.4 is to convolution measure algebras, especially to the measure algebra $M(\mathbb{R})$. Recall that a Raikov system $R$ on $\mathbb{R}$ is a collection of Borel subsets of $\mathbb{R}$ such that

1) If $E \in R$ and $F \subseteq E$ is an $F_\sigma$ subset of $\mathbb{R}$ then $F \in R$.
2) If $E_1, E_2, \ldots \in R$ then $\bigcup E_j \in R$.
3) If $E_1, E_2 \in R$ then $E_1 + E_2 \in R$.
4) $\{x\} \in R$ for all $x \in \mathbb{R}$.

Using $R$ one may naturally define a closed ideal of $M(\mathbb{R})$ by

$I(R) = \{v \in M(\mathbb{R}) | \|v\|(E) = 0 \text{ for all } E \in R\}$. Theorem 2.4 implies that $\mu$ (the Cantor measure) cannot be concentrated on a proper Raikov system. This answers a question of Moran. Of course this conclusion could have also been made using the results in [48]. Notice also in connection with the above that the measure $\mu$ is an infinite Bernoulli
convolution $\mu = \ast \left[ \sum_{j=1}^{\infty} \frac{1}{j} \delta(0) + \frac{1}{j} \delta(3^{-j}) \right]$ which has independent powers (i.e. $\mu^n \perp \mu^m$ whenever $0 \leq m < n < \infty$). For further details on convolution measure algebras and Raikov systems, see [17].
III. \(B_h[g]\) SEQUENCES

III.1. INTRODUCTION

In this chapter we shall give some partial answers to some well known conjectures of \(\text{Erdős and Turan}\) regarding \(B_h[g]\) sequences (for a definition, see below) and also a related question of \(\text{Bose and Chowla}\). We briefly describe the contents of this chapter and also describe some previous results in this direction.

First we describe some notation which is to be used throughout the paper. Other notation will be introduced locally as needed. In the following we shall be dealing exclusively with increasing sequences of positive integers (which may be finite or infinite). The letter \(A\) is reserved for such a sequence. Now given an \(A, 2 \leq h \in \mathbb{N}\) and \(n \in \mathbb{N}\), denote by \(r_h(n, A)\) the number of representations of \(n\) of the following type:

\[
(1.1) \quad n = a_{j_1} + \ldots + a_{j_h} \text{ with } j_1 \leq \ldots \leq j_h, \quad a_{j_i} \in A \text{ for all } i
\]
Recall that a sequence $A$ is $B_h[g]$ if $r_h(n,A) \leq g \forall n \in \mathbb{N}$, for some $1 \leq g \in \mathbb{N}$. Denote by $F_h(n,g)$ the cardinality of a $B_h[g]$ sequence contained in $\{1,\ldots,n\}$ whose cardinality is maximal among those $B_h[g]$ sequences which are contained in $\{1,\ldots,n\}$. Denote $F_h(n,1)$ by $F_h(n)$ and call a $B_h[1]$ sequence a $B_h$ sequence.

In [14] Erdős and Turan, motivated by some work of Sidon (see [45], [46]), got an estimate for $F_2(n)$. They showed that $F_2(n) < n^1/2 + O(n^{1/4})$. In 1944 Erdös [10] and Chowla [8] (independently) showed $\lim n^{-1/2} F_2(n) \geq 1$ using a theorem of Singer [47]; so in fact $\lim n^{-1/2} F_2(n) = 1$. Next it was shown in [6] by Bose and Chowla that $\lim n^{-1/4} F_h(n) = 1$ for any $2 \leq h \in \mathbb{N}$. In [30] B. Lindström gave a different way to estimate $F_2(n)$ and in [31] he got an estimate for $F_h(n)$. His results are $F_2(n) \leq n^{1/2} + n^{1/4} + 1$ and $F_h(n) \leq (8n)^{1/4} + O(n^{1/6})$.

In section 2 of this chapter we get an upper bound for $F_h(n,g)$ for any $2 \leq h \in \mathbb{N}$ and $1 \leq g \in \mathbb{N}$ using some facts from the "local theory" of Banach spaces. The estimates here are not as good as those that are obtained in section 3 by estimating the norms of some trigonometric sums; nevertheless, they serve as motivation for the proof in section 3.

The estimates obtained on $F_h(n,g)$ in section 3 are used in turn to give partial answers to some other questions. An old question of Bose and Chowla which is related to the above material (communicated to us by Professor Erdős)
Suppose that for \( a_1 \in \mathbb{N}, 1 \leq i \leq n, a_1 < a_2 < \ldots < a_n < \delta n^3 \) for some \( \delta > 0 \); is it true that there is a \( n_0(\delta) \in \mathbb{N} \) such that for \( n \geq n_0(\delta) \) there is a duplication among the sums \( a_i + a_j + a_k \) \((1 \leq j \leq k)\)? (Of course \( \delta < 1 \)). In section 3 we obtain some information on this problem. Also in [44] Erdős and Turan asked if for a sequence \( A = (a_k)_{k=1}^{\infty} \) satisfying \( a_k < c k^2 \) for all \( k \) and some \( c > 0 \), is it true that \( \lim r_2(n, A) = +\infty \)? Evidently a positive solution of this problem would also solve a conjecture of theirs stating that if \( r_2(n, A) > 0 \) for all sufficiently large \( n \) then \( \lim r_2(n, A) = +\infty \). In section 3 we use the estimates on \( F_h(n, g) \) to get some information on the above problem of Erdős and Turan. In section 4 we get another set of estimates on \( F_h(n, g) \) using a result about gaps of consecutive primes. In turn these estimates are used to get a different sort of estimate for the Bose-Chowla problem.

Finally we mention some other notation which will be useful in the sequel. Denote by \( R_h(n, A) \) the number of distinct representations of \( n \) in (1.1) where no ordering is imposed on the \( j_i \). So for a \( B_h[g] \) sequence \( A, R_h(n, A) \leq h 1 g \) since \( R_h(n, A) \leq h 1 r_h(n, A) \) for all \( n \). Finally for measurable functions \( f, g : S^1 \to \mathbb{C} \) denote by \( \langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) \overline{g(e^{i\theta})} \, d\theta \) provided the integral exists. We refer to [20] for standard facts about \( B_h[g] \) sequences and to [52] for the harmonic analysis aspects and any unexplained notation.
III.2. ESTIMATES ON $F_h(n,g)$ USING LOCAL THEORY

We recall some further notation which will be used only in this section. $\mathbb{L}^p_n$ (for $1 \leq p < +\infty$ and $n \in \mathbb{N}$) is $\mathbb{R}^n$ (or $\mathbb{C}^n$) with the norm $||x||_p = (\sum_{i=1}^{n} |x_i|^p)^{1/p}$ (whether it is $\mathbb{R}^n$ or $\mathbb{C}^n$ will be clear from the context). For Banach spaces $X,Y$ we write $X \subseteq^K Y$ (for some $0 < K < \infty$) if there exists an isomorphic embedding, $T: X \rightarrow Y$ such that $||T|| ||T||^{-1} \leq K$. Finally for $Z = \{x_1, \ldots, x_n\} \subseteq X$ denote by $(x_1, \ldots, x_n)_X$ the linear span of $Z$ (note that $Z$ is a closed subspace of $X$ with respect to the norm topology of $X$). Other unexplained notation may be found in [28].

To prove the theorem in this section we shall require two lemmas. The following type of lemma is well-known. We include a proof for the sake of completeness.

Lemma 2.1:

Let $A = \{n_1, \ldots, n_k\}$ be a $B_h[g]$ sequence. Then

$$\left[\frac{e^{int}, \ldots, e^{inkt}}{L_{2h}}\right] \frac{\cap (h|g|)^{1/h}}{e^{int}, \ldots, e^{inkt}} \left[\frac{L_{2h}}{L_{2h}}\right]$$
Proof:

Let \((a_j)^k \in \mathbb{C}^k\) and set \(f(e^{i\theta}) = \sum_{j=1}^k a_j e^{in_j \theta}\).

Then we have that,

\[ f^h(e^{i\theta}) = \sum_{m \geq n_1 + \ldots + n_j = m} a_j e^{im\theta} \]

Since we have that,

\[ (2.1) \quad |\sum a_j \ldots a_j| \leq \sup_m R_h(m, A) |a_j| \ldots |a_j| \]

where \(|a_j^*| \ldots |a_j^*|\) is chosen so as to maximize the products within the sum (2.1), it follows that,

\[ \|f\|_2^h = \sum_{m \geq n_1 + \ldots + n_j = m} a_j \ldots a_j^2 \]

\[ \leq (\sup_m R_h(m, A)^2)(\sum |a_j|^2)^h = \max_m R_h(m, A)^2 \|f\|_2^h \]

the inequality being true because the products \(|a_j^*| \ldots |a_j^*|\) change with \(m\). Since \(A\) is a \(\mathcal{B}_h[a]\) sequence we have that \(\sup_m R_h(m, A) \leq h!g\). Since we clearly have \(\|f\|_2^h \geq \|f\|_2\) and the above inequalities show that \(\|f\|_2^h \leq (h!g)^{1/h} \|f\|_2\) it follows that

\[ \{e^{in_1 t}, \ldots, e^{in_k t}\}_{L^2_h} \xrightarrow{(h!g)^{1/h}} \{e^{in_1 t}, \ldots, e^{in_k t}\}_{L^2} \]
The next lemma that we shall use is a theorem of Marciszewicz and Zygmund (see \cite{33}). Reformulating it to correspond to the above notation we have that,

**Lemma 2.2:**

\[ \{e^{it_1}, \ldots, e^{int}\}_{L_q} \subset K_q L_q^\infty \text{ for any } n \in \mathbb{N} \text{ and } 1 < q < \infty, \text{ where } K_q \text{ is a constant which only depends on } q. \]

\[ K_q \to \infty \text{ as } q \to \infty \text{ or as } q \to 1. \]

We may now prove the following:

**Theorem 2.3:**

\[ F_h(n, g) \leq K_{2h}^2 \frac{1}{2h} \frac{1}{(hk)!} \frac{2}{h} g^2/h n^{1/h} \]

The conclusion can be considerably strengthened as will be seen in subsequent sections, but it can even be made stronger using the proof below, as is pointed out in the remarks following the proof. It is presented in the above form to avoid certain details which are left to the remarks.

**Proof (of theorem 2.3):**

Fix \( n \in \mathbb{N}, 2 \leq h \in \mathbb{N}, 1 \leq g \in \mathbb{N} \). Choose \( A \subseteq \{1, \ldots, n\} \) with the cardinality of \( A \) being \( F_h(n, g) \). Let \( A = \{n_1, \ldots, n_k\} \) and set \( p = 2h \). Certainly we may say that \( \{e^{in_1t}, \ldots, e^{inkt}\}_{L_2} \)
is isometrically isomorphic to $\ell_2^k$ (since $\{e^{injt}\}_{j=1}^k$ are orthogonal to each other). Now we have a canonical embedding

\[
[e^{int}, \ldots, e^{int}]_{L^p} \overset{1}{\longrightarrow} [e^{it}, \ldots, e^{int}]_{L^p}.
\]

It follows from lemmas 2.1 and 2.2 that $\ell_2^k \overset{K_p(h!g)^{1/h}}{\rightarrow} \ell_p^k$. The rest of the argument may be completed using well known arguments in the local theory of Banach spaces (for instance see [3] or [15]).

We may choose operators $T : \ell_2^k \rightarrow \ell_2^k$ and $T^{-1} : (\ell_2^k) + \ell_2^k$ s.t. $\|T^{-1}\|=1$ and $\|T\| \leq K_p(h!g)^{1/h}$. It follows that for any choice of scalars $(\lambda_j)_{j=1}^k \in \mathbb{C}^k$ we have that:

\[
(\Sigma_{j=1}^k |\lambda_j|^2)^{1/2} \leq \| \Sigma_{j=1}^k \lambda_j u_j \|_{L^p^n} \leq K_p(h!g)^{1/h} \| \Sigma_{j=1}^k |\lambda_j|^2 \|^{1/2}
\]

where $u_j = (t_{j,1}, t_{j,2}, \ldots, t_{j,n})$, $j=1, \ldots, k$ are vectors in $\ell_p^n$ so that $u_j = Te_j$ where $(e_j)_{j=1}^k$ is the unit vector basis of $\ell_2^k$ (i.e. $e_j(i) = \delta_{ij}$, $i,j=1, \ldots, k$ and $\delta$ is the Kronecker $\delta$). Let $r_j(t)$ be the Rademacher functions on $[0,1]$ (i.e. $r_j(t) = \text{sign} \sin 2^j \pi t$). Recall Khinchin's inequality which says:

\[
A_p(\Sigma_{j=1}^n |a_j|^2)^{1/2} \leq \| \Sigma_{j=1}^n a_j r_j(t) \|_{L_p(0,1)} \leq B_p(\Sigma_{j=1}^n |a_j|^2)^{1/2}
\]

where $(a_j)_{j=1}^n \in \mathbb{C}^n$ and $0 < A_p, B_p < \infty$ and are independent of $n$. Moreover $B_p \leq (\frac{p}{2})^{1/4}$. Now for each fixed $t \in [0,1]$ by
By integrating this last inequality with respect to \( t \), we get:

\[
\left( \sum_{j=1}^{\infty} R_j(t) t_j, I \right)^{p/2} \leq \left( \sum_{j=1}^{\infty} |t_j, I|^2 \right)^{p/2} \leq \left( \sum_{j=1}^{\infty} |t_j, I|^2 \right)^{p/2}
\]

Now by a duality argument it follows that

\[
\left( \sum_{j=1}^{\infty} |t_j, I|^2 \right)^{1/2} \leq K \left( h^{-1} g \right)^{1/h} \quad \text{for } i = 1, \ldots, n.
\]

To see this compute \( T^* : \ell_q^n \rightarrow \ell_2^k \) (where \( T^* \) is the adjoint of \( T \) and \( 1/p + 1/q = 1 \) via the usual duality). For \( x^\ast \in \ell_q^n \) and \( y \in \ell_2^k \) we have \( T^* x^\ast(y) = x^\ast(Ty) \), in particular with \( x^* = \bar{e}_i(j) = \delta_{ij} \) \( j = 1, \ldots, n \) and \( y = \sum_{j=1}^{k} y_j e_j \) we have

\[
T^* x^\ast(y) = \bar{e}_i(Ty) = \bar{e}_i\left( \sum_{j=1}^{k} y_j T e_j \right) = \bar{e}_i\left( \sum_{j=1}^{k} y_j u_j \right)
\]

\[
= \sum_{j=1}^{k} y_j t_j, I. \quad \text{So } T^* e_i = (t_j, I)_{j=1}^{k} \in \ell_2^k. \quad \text{Now}
\]

\[
\left( \sum_{j=1}^{k} |t_j, I|^2 \right)^{1/2} = || T^* e_i ||_{\ell_2^n} \leq || T^* ||_{\ell_2^n} || e_i ||_{\ell_q^n} = ||T||_{\ell_q^n} = K \left( h^{-1} g \right)^{1/h}
\]
So in (2.3) we get \( k^h = k^{p/2} \leq \left( \frac{p}{2} \right)^{h} \sum_{i=1}^{n} (\| t_j \|_2^2)^{p/2} \leq \left( \frac{p}{2} \right)^{h} k^p (g(h!))^n n \)

\[ \Rightarrow k \leq h^{1/2k} (g(h!))^{2/h} n^{1/h} \]

\[ \Rightarrow F_h(n,g) = \text{card } A = k \leq h^{1/2k} (g(h!))^{2/h} n^{1/h} \]

which concludes the argument.

**Remark 2.4:**

The constant \( K_{2h} \) which goes to \( +\infty \) as \( h \to \infty \) may actually be replaced by a uniform constant \( c \). This is because in lemma 2.2 we can have \( \{\varepsilon t, \ldots, \varepsilon n t\}_{L_q} \to \ell^2 n + 1 \). Since in the next section we obtain much better estimates, even after taking into account this fact in the above proof, we do not pursue it.

**Remark 2.5:**

The following was pointed out to us by W.B. Johnson:

Let \( k = F_h(n,g) \), \( p = 2h \). Define by

\[ \gamma_p^h(\ell^k_2) = \inf \{ \|A\|\|B\| \mid A: \ell^k_2 \to \ell^p_n, B: \ell^p_n \to \ell^k_2 \}, \]

where \( D = 1 = \text{identity on } \ell^k_2 \). Using a variation of the idea of the above proof it is not hard to see that \( \gamma_p^h(\ell^k_2) \leq c(g,h) \)

where \( c(g,h) \) is a function of \( g \) and \( h \) (and may be determined explicitly). On the other hand it is a known consequence of a theorem of Grothendieck (see [16],[19],[27]) that

\[ \gamma_p^h(\ell^k_2) \geq \frac{c' \sqrt[k]{n}}{n^{1/p}} \]

(where \( c' \) is possible to estimate). This
gives the estimate $k = F_h(n, g) \leq \frac{c(g, h)^2}{c_i^2} n^{1/h}$. Again after explicit computations are performed one does not get as good an estimate as in the next section, accordingly we do not pursue this line of inquiry.
III.3. ESTIMATES ON $F^*(n,g)$ USING TRIGONOMETRIC POLYNOMIALS

In this section we obtain sharper estimates on $F^*(n,g)$ than those in the previous section. In the previous section $k^* = F^*(n,g)$ was estimated by calculating how large $k$ could be so that $\ell_2^k$ could be "nicely" embedded in $\ell_p^n$. In particular we used $[e^{it}, \ldots, e^{int}]_{L_q} \subset K_q \rightarrow \ell_q^n$ (see lemma 2.2). While it is natural to use this embedding from the point of view of local theory it is more advantageous to deal directly with $[e^{it}, \ldots, e^{int}]_{L_q}$ (and so the proof that follows is motivated by a careful examination of the proofs in the previous section and also by some other well known ideas in harmonic analysis). We need some trivial computational lemmas first. The reader who is so inclined may skip directly to the proof of theorem 3.6.

Let $m \geq 1$, $N \geq 1$, $m$, $N \in \mathbb{N}$. Let $K_{mN}$ be the usual Fejer Kernel:

$$K_{mN}(e^{i\theta}) = \sum_{n=-mN}^{mN} (1 - \frac{|n|}{mN}) e^{in\theta}$$

Since $K_{mN} \geq 0$ $\|K_{mN}\|_{L_1} = K_{mN}(0) = 1$.

Lemma 3.1:

$$\|K_{mN}\|_{L_2}^2 = \frac{(2m^2N^2 + 1)}{3mN}$$
Proof: We have that:

\[ \|K_{mn}\|_{L^2}^2 = \sum_{n=-mN}^{mN} (1 - \frac{|n|}{mN})^2 \text{ (by Parseval's Theorem)} \]

\[ = 1 + 2 \sum_{n=1}^{mN} (1 - \frac{2n}{mN} + \frac{n^2}{m^2N^2}) \]

An application of the identities \( \sum_{n=1}^{M} n^2 = \frac{M(M+1)}{2} \) and

\( \sum_{n=1}^{M} n^2 = M(M+1)(2M+1)/6 \) finishes the computation. □

Lemma 3.2:

For \( 1 < p < 2 \), \( \|K_{mn}\|_{L^p} \leq \left( \frac{2m^2N^2+1}{3mN} \right)^{1/q} \) where \( 1/p + 1/q = 1 \) as usual.

Proof:

If \( n = 2/q \) then \( 1/p = \frac{1-n}{1} + \frac{n}{2} \), so by Hölder's inequality we have that,

\[ \|K_{mn}\|_{L^p} \leq \|K_{mn}\|_{L^1}^{1-n} \|K_{mn}\|_{L^2}^n \]

\[ = \|K_{mn}\|_{L^2}^{2/q} = \left( \frac{2m^2N^2+1}{3mN} \right)^{1/q} \]

by lemma 3.1. □

Notice that lemma 3.3 takes the place of lemma 2.1.

Lemma 3.3:

Suppose \( A = \{n_1, \ldots, n_k\} \) is a B_1[g] sequence. Denote by

\[ P_A(e^{i\theta}) = \sum_{j \leq k} e^{in_j \theta} \text{. Then } \|P_A\|_{L^{2h}} \leq h!g \|P_A\|_{L^{2h}} \]
Proof: We have that:

\[ \mathcal{P}_A^h = (\sum_{j=1}^{k} e^{ij\theta}h)^h = \sum_{\mathcal{R}_h(n,A) > 0} e^{i\theta} \]

It follows that,

\[ \|\mathcal{P}_A\|_{L^2_h} = \int |\sum_{\mathcal{R}_h(n,A) > 0} e^{i\theta} | d\theta = \sum_{\mathcal{R}_h(n,A) > 0} \mathcal{R}_h(n,A)^2. \]

Let \( D = \{ n | \mathcal{R}_h(n,A) > 0 \} \) and for each \( n \in D \) define by

\[ \phi(n) = \{(a_1, \ldots, a_k) | n = a_1 n_1 + \ldots + a_k n_k, \sum_{i=1}^{k} a_i = k, a_i \in \mathbb{N}, n_1 < n_2 < \ldots < n \} \].

Notice that \(|\phi(n)| = \mathcal{R}_h(n,A)\) and if \( n \neq m \) then \( \phi(n) \cap \phi(m) \neq \emptyset \).

So we have that,

\[ \sum_{\mathcal{R}_h(n,A) > 0} \mathcal{R}_h(n,A)^2 \leq \log \sum_{n \in \mathcal{B}} \mathcal{R}_h(n,A) \]

\[ = \log \sum_{n \in \mathcal{B}} \phi(n) \frac{h!}{a_1! \ldots a_k!} \]

\[ = \log \sum_{a_1 + \ldots + a_k = h} \frac{h!}{a_1! \ldots a_k!} \]

\[ = \log \mathcal{R}_h = \log \|\mathcal{P}_A\|_{L^2_h}^2 \]

So \( \|\mathcal{P}_A\|_{L^2_h} \leq \log \|\mathcal{P}_A\|_{L^2_h}^2 \). □

Lemma 3.4:

\[ \frac{k^{1/2k+1}}{2^{2k-1}} > \frac{(k+1)^{1/2k+1}}{2k+1} \] for \( k \geq 1, k \in \mathbb{N} \).

Proof:

This is done by taking the first six terms of a binomial expansion of both sides. The details are left to the reader. □
Lemma 3.5:

Let $q = 2k$, $k \in \mathbb{N}$. Then we have that

$$\min_{n \in \mathbb{N}} \frac{n^{1/q}}{\frac{1}{2^{k-1}} n} = \min \left( \frac{k^{(1/2k)+1}}{2k-1}, \frac{(k+1)^{(1/2k)+1}}{2k+1} \right)$$

Proof:

Let $f(x) = \frac{x^{1/q+1}}{2^{x-1}}$ for $x > 1$. Then $f' > 0 \iff x > \frac{q+1}{2}$.

Accordingly if $a_n = \frac{n^{1/q}}{2^{-1/n}}$ then $a_1 > \ldots > a_k$ and $a_{k+1} < a_{k+2} < \ldots$.

So $\min_{n \in \mathbb{N}} a_n = \min (a_k, a_{k+1})$. □

We may now prove theorem 3.6:

Theorem 3.6:

Let $h$, $g \in \mathbb{N}$ with $h > 2$, $g > 1$. Then we have

$$F_h(n, g) \leq \frac{4g^{1/h} (h!)^{1/h}}{(3n)^{1/h}} \inf_{m \in \mathbb{N}} \left( \frac{(2mn^2 + 1/m)^{1/2h}}{2^{1/m}} \right)^2$$

Proof:

Choose $A \subseteq \{1, \ldots, n\}$ such that $\text{card } A = F_h(n, g)$.

Let $A = \{n_1, \ldots, n_k\}$. Let $\ell = \left(\frac{n+1}{2}\right)$ (where $[x]$ is the greatest integer in $x$) and set $\tilde{K}_{mn}(e^{i\theta}) = e^{i\ell \theta} K_{mn}(e^{i\theta})$. Note that for $1 \leq j \leq n$, $\tilde{K}_{mn}(j) \geq 1 - \frac{1}{2m}$. It follows that if we set $P_A(e^{i\theta}) = \sum_{j \leq k} e^{i\ell j \theta}$ then

$$\langle P_A, \tilde{K}_{mn} \rangle = \sum_{j \leq k} \tilde{K}_{mn}(j) \geq k \left(1 - \frac{1}{2m}\right).$$
On the other hand we have that,

\[ \langle P_A, \tilde{k}_{mn} \rangle \leq \|P_A\|_{L_{2h}} \|\tilde{k}_{mn}\|_{L(2h)^*} \]  

(where \( \frac{1}{2h} + \frac{1}{(2h)^*} = 1 \))

\[ \leq (g(h!))^{1/2h} \|P_A\|_{L_2} \|\tilde{k}_{mn}\|_{L(2h)^*} \]  

(by lemma 3.3)

\[ \leq g(h!) \left( \frac{2m^2n^2 + 1}{3mn} \right)^{1/2h} \]  

(by lemma 3.2)

So \( g(h!) \left( \frac{2m^2n^2 + 1}{3mn} \right)^{1/2h} \geq k(1 - \frac{1}{2m}) \). So,

\[ F_h(n,g) = k \leq \frac{1}{h} \left( \frac{2m+1}{2m-1} \right)^{1/h} \left( \frac{2m^2n^2 + 1}{3mn} \right)^{1/2h} \]

\[ = \frac{1}{h} \left( \frac{g(h!)}{3n} \right)^{1/h} \left( \frac{2m^2n^2 + 1}{2m-1} \right)^{1/h} \]

Since \( m \) was arbitrary the result follows. □

Remark 3.7:

It is reasonable to think that the de la Vallee Poussin kernel would give better results than the Fejer kernel since for the kernel \( V_{mn} = (m+1) K_{(m+1)n-m} K_{mn} \), \( V_{mn} \ast f \) approximates a function \( f \) by having the same Fourier coefficients as \( f \) over a prescribed interval (indeed this was the way the proof was originally done). However it is easy to check that using \( V_{mn} \) gives the result:

\[ F_h(n,g) \leq \inf_{m \in \mathbb{N}} \left( \frac{2m+1}{2m-1} \right)^{1/h} \left( \frac{6m+2}{3n} \right)^{1/h} \]

and that this result is worse than that in theorem 3.6.
Remark 3.8:

If $A$ is an infinite $B_n[n]$ sequence then note that $A(n) = \text{card} (A \cap \{1, \ldots, n\}) \leq F_h(n,g)$ and so theorem 3.6 gives an estimate for $A(n)$. Of course this is not particularly effective.

The estimate in theorem 3.6 easily gives a partial answer to the following problem which is more general than the Bose - Chowla problem: Given $a_1 < a_2 < \ldots < a_n < n^h$, $a_i \in \mathbb{N}$ for all $1 \leq i \leq n$, $g \geq 0$, $2 \leq h \in \mathbb{N}$ and $1 \leq g \in \mathbb{N}$ can you give a value $\delta_0$ such that if $\delta < \delta_0$ (as above) then there is a $n_0(\delta) \in \mathbb{N}$ such that for $n \geq n_0(\delta)$ more than $g$ of the sums, $a_j + \ldots + a_{j_h}$, $j_1 \leq \ldots \leq j_h$ are the same? Theorem 3.9 gives a value for $\delta_0$.

Theorem 3.9:

Given $g$, $h \in \mathbb{N}$, $g \geq 1$, $h \geq 2$ and $a_1 < \ldots < a_n$ with $a_i \in \mathbb{N}$ for all $1 \leq i \leq n$ we have that $\exists \, \delta_0 = \delta_0(g,h)$ such that for $\delta < \delta_0$ with $a_n < \delta n^h \exists \, n_0(\delta) \in \mathbb{N}$ such that for $n \geq n_0(\delta)$ more than $g$ of the sums $a_{j_1} + \ldots + a_{j_h}$, $j_1 \leq \ldots \leq j_h$ are the same. We may take

$$\delta_0 = 2^{\frac{h}{1}} \ldots \frac{1}{h} \left(\frac{2}{h+1}\right)^{2h}.$$
Proof:

For \( m \in \mathbb{N} \) set \( \eta(m) = \frac{4h g(h)}{m} + 4h g(h)(2m) \),
\( \lambda(m) = 4h + 1 \delta_m g(h) \) and \( \tau(m) = 3\delta (2 - \frac{1}{m})^2 \).

Note that \( \tau(m) > 0 \iff \delta < \delta_m \) where \( \delta_m \) is defined by
\[
\delta_m = \frac{3}{2} \frac{1}{4h g(h)} (2 - \frac{1}{m})^{2h}.
\]

Suppose \( a_1 < \ldots < a_n < 6h \) for some \( \delta < \delta_m \) and no more than \( g \) of the sums \( a_{j_1} + \ldots + a_{j_h} \), \( j_1 \leq \ldots \leq j_h \) are the same, no matter how big \( n \) is. Then \( r_h(k,A) \leq g \forall k \in \mathbb{N} \) for \( A = (a_i)_{i=1}^n \). It follows that
\[
F_h(\{\delta h + 1\}, g) > n.
\]
However it is the case that,
\[
F_h(\{\delta h + 1\}, g) \leq \frac{4g^{1/h}(h)_{1/h}^{(2m(\delta h + 1)^2 + 1/m)^{1/h}}}{3^{1/h} \delta^{1/h} n^{1/h}} \leq \frac{4g^{1/h}(h)_{1/h}^{(2m(\delta h + 1)^2 + 1/m)^{1/h}}}{3^{1/h} \delta^{1/h} n^{1/h}} = (*) \text{ (by definition)}. \]

Now it is easily checked that \( (*) < n \) is equivalent to \( \eta(m) < n^{2h} \tau(m) - n^h \lambda(m) \). This last inequality is certainly true if \( n > \max \left( \frac{(2n(m))^{1/2h}}{\tau(m)}, \frac{(2\lambda(m))^{1/h}}{\tau(m)} \right) = \mathbb{N} \) (by definition).

So for \( n > \mathbb{N} \), \( F_h(\{\delta h + 1\}, g) < n \). This contradiction shows that \( \delta_m \) works as a choice for \( \delta_0 \), in the statement of theorem 3.9. Since \( m \) was arbitrary, we may in fact take \( \delta_0 = \sup \delta_m \).

Lemmas 3.4 and 3.5 then give that we may take
\[
\delta_0 = \frac{3}{2} \frac{1}{4h g(h)} (2 - \frac{1}{h+1})^{2h}.
\]
We finally make some comments on the question of Erdos and Turan mentioned at the beginning of the paper. Recall that it asked: If a sequence $A = \{a_k\}_{k=1}^{\infty} \subseteq \mathbb{N}$ satisfies $a_k < c k^2$ for all $k$ and some $c > 0$, is it true that $\prod R_2(n,A) = +\infty$? Clearly it is equivalent to: given $A = \{a_k\}_{k=1}^{\infty}$ a sequence of natural numbers with $\sup_n R_2(n,\{a_k\}_{k=1}^{\infty}) < +\infty$ we have the following: given $c > 0$ there exists $n \in \mathbb{N}$ for which $a_n \geq c n^2$. A more general question one can ask is the following: given $A = \{a_k\}_{k=1}^{\infty} \subseteq \mathbb{N}$ (of course as usual $A$ is strictly increasing) with $\sup_n R_h(n,A) < +\infty$ do we have that given $c > 0$, there exists $n \in \mathbb{N}$ for which $a_n \geq c n^h$? We suspect that the answer to this is in the affirmative. At any rate, it follows immediately from theorem 3.6 that for a $B_h[g]$ sequence $A = \{a_k\}_{k=1}^{\infty}$, $\prod a_k > 0$. Accordingly given any $B_h[g]$ sequence $(a_n)_{n=1}^{\infty}$ and $c > 0$ there exist infinitely many $n$ for which $a_n \geq c \frac{n^h}{\phi(n)}$ for any $\phi(n) \rightarrow \infty$. So we have the following:

**Theorem 3.10:**

Let $A = \{a_n\}_{n=1}^{\infty}$ be a $B_h[g]$ sequence. Then we have that,

(a) $\prod a_n \to 0$

(b) Given $c > 0$ and any $\phi(n) \to +\infty$ (as $n \to \infty$) $a_n \geq c \frac{n^h}{\phi(n)}$ for infinitely many $n$. 
Remark 3.11:

A different way of putting (a) (but obviously equivalent) is to say that: Given a $B(h,g)$ sequence $A=(a_n)_{n=1}^\infty$, $\exists c_0 = c_0(g,h) > 0$ s.t. for $0 < c < c_0$ $\exists$ infinitely many $n$ s.t. $a_n > cn^h$. An explicit expression for $c_0$ may be given using theorem 3.6, but it is rather messy; so we leave it.

Remark 3.12:

Theorem 3.10(b) shows that the above analysis "almost" gives the Erdős-Turan conjecture, since $\phi(n)$ can be arbitrarily slow growing.
III.4. ESTIMATES ON $F_h(n,g)$ USING A GAP THEOREM ON PRIMES

In this section we shall get a different set of estimates on $F_h(n,g)$ in a simple fashion using a gap theorem on consecutive primes. We need the following fact on gaps between consecutive primes:

\textbf{Theorem 4.1} [23]:

If $(p_n)_{n=1}^{\infty}$ is the sequence of primes $p_{n+1} - p_n \leq M_0 \ p_n^\theta$ where $\theta$ may be taken to be $\frac{11}{20} + \epsilon$ for any $\epsilon > 0$, where $M_0 > 0$ (may be calculated).

We shall also need the following result of Bose and Chowla (see [6]) already mentioned in the introduction:

\textbf{Theorem 4.2:}

For $2 \leq h \in \mathbb{N}$ and $p$ any prime $F_h(p^h) \geq p$.

The two theorems enable us to prove rather simply that:

\textbf{Theorem 4.3:}

Let $\delta > 1$, $2 \leq h \in \mathbb{N}$, $1 \leq g \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$F_h(n,g) \leq \delta (h! gh)^{1/h} n^{1/h}$$

for $n \geq n_0(h,g,\delta)$. (For an explicit value of $n_0(g,h,\delta)$, see the proof.)
Proof:

Clearly we have \( (\frac{m}{h})^{\leq h} n \) where we write \( m = F_h(n,g) \) for convenience. This is because if \( A = \{n_1, \ldots, n_K\} \subseteq \{1, \ldots, n\} \) with \( \text{card } A = F_h(n,g) \) then to each subset \( \{n_{j_1}, \ldots, n_{j_h}\} \) we can associate the sum \( n_{j_1} + \ldots + n_{j_h} \) (which is duplicated at most \( g \) times) and \( n_{j_1} + \ldots + n_{j_h} \leq h n \). Then we have that:

\[
\begin{align*}
    m^h \left(1-\frac{1}{m}\right) \ldots \left(1-\frac{1-h-1}{m}\right) &= [m(m-1) \ldots (m-(h-1))] / h! \leq h n.
\end{align*}
\]

Using the elementary inequality

\[
\prod_{i \leq N} (1-n_i) \geq 1 - \sum_{i \leq N} n_i \text{ for } 0 < n_i < 1 \text{ V } i \leq N \text{ and the identity } \sum_{i=1}^{N} i = \frac{N(N+1)}{2},
\]

we have that \( (1 - \frac{h(h-1)}{2m})^{m^{\leq h} n} \). It is therefore enough to prove that \( 1 - \frac{h(h-1)}{2m} \geq \frac{1}{\delta^h} \) for \( n \geq n_0 \) for some \( n_0 \). We show that we may take \( n_0 \geq \max \left(2^h, \left(2M_0^\theta\right)^{h/1-\theta}, \left(\frac{h(h-1)}{\delta^h-1}\right)^h\right) \) where \( M_0 \) is from theorem 4.1 and \( \theta = \frac{1}{11} + \epsilon \) (take \( \theta \) to be some fixed value in the sequel). To see this: We have \( F_h(p^h) \geq p \) for \( p \) a prime (theorem 4.2). So if \( n \geq 2^h \) then \( p \leq n^{1/h} \leq p^i \) for some consecutive primes \( p \) and \( p^i \). Also \( p^i - p = O(p_0^\theta); \) so that \( F_h(n) \geq F_h(p^h) \geq p = n^{1/h} + (p - n^{1/h}) \geq n^{1/h} - M_0 n^{\theta/h} \).
So \( F_h(n) \geq \frac{1}{2} n^{1/h} \) for \( 1 - h_0 \leq n \leq \frac{9-1}{n} \), i.e. \( n \geq (2M_0)^{h/1-\theta} \).

(the very last part of the argument above is adapted from [201]). So \( F_h(n, g) \geq F_h(n) \geq \frac{1}{2} n^{1/h} \) for \( n \geq \max(2^h, (2M_0)^{h/1-\theta}) \).

Now \( 1 - h(h-1) \geq \frac{1}{\delta h} \) is equivalent to \( m \geq \frac{h(h-1)}{2(1-1/\delta h)} \), which is true by requiring in addition to the above lower bound on \( n, \frac{1}{2} n^{1/h} \geq \frac{h(h-1)}{2(1-1/\delta h)} \), which finishes the proof.

There are a number of disadvantages to the estimates of theorem 4.3. Firstly the proof is simple only modulo the deep theorem 4.1 and the non-trivial theorem 4.2, while the proof of theorem 3.6 is self-contained. Secondly theorem 4.3 is only a slight improvement (in terms of the order of the estimates) over theorem 3.6. Thirdly theorem 3.6 gives an estimate for \( F_h(n, g) \forall n \in \mathbb{N} \) while theorem 4.3 gives an estimate only for quite large \( n \).

Just as theorem 3.6 was used to give an estimate for the "generalized Bose-Chowla problem", so does theorem 4.3. We conclude this section with these estimates. The proof is obvious and similar to that of theorem 3.9 (though much simpler) and is accordingly left to the reader.

**Corollary 4.4:**

Let \( \delta > 1, 1 \leq g \leq \mathbb{N} \) and \( 2 \leq h \leq \mathbb{N} \). Then there is \( n_0 > 0 \).
(depending only on \( g, h \) and \( \delta \)) s.t. for every \( \eta < \eta_0 \) there is an \( \eta_0(\eta) \in \mathbb{N} \) so that for \( n > \eta_0(\eta) \) (\( \eta_0 \) also depends on \( g, h \) and \( \delta \)) the following happens:

Given \( n \) integers \( 0 < a_1 < \ldots < a_n < n^h \) consider sums of the type \( a_{j_1} + \ldots + a_{j_h} \) where \( 1 \leq j_1 \leq \ldots \leq j_h \leq n \). Then among these sums there are more than \( g \) of them which are the same. We may take \( \eta_0 = \frac{1}{\delta^h(h!)(gh)} \).
IV. CONSTRUCTION TECHNIQUES FOR $\Lambda(p)$ SETS

IV.1. INTRODUCTION

In this chapter we give construction techniques for $\Lambda(p)$ sets in various groups. As a consequence we are able to recapture previous results on these sets (see e.g. [2], [5], [9], [43]) as well as prove some new results. In particular we show that in the dual of any compact abelian group there exists a $\Lambda(4)$ set which is not $\Lambda(4+\epsilon)$ for any $\epsilon > 0$. Several applications of $\Lambda(p)$ sets are also presented.

We now describe the contents of this chapter more fully. Let us recall the definition of a $\Lambda(p)$ set for $G$ a compact abelian group: If $\Gamma = \{\gamma_i\}_{i=1}^\infty \subseteq G^*$ ($G^*$ is the dual group of $G$) then $\Gamma$ is a $\Lambda(p)$ set if there exists a constant $A_p, q > 0$ such that,

\[
(1.1) \quad \|\sum_{j=1}^n a_j \gamma_j \|_{L_p(G)} \leq A_p, q \|\sum_{j=1}^n a_j \gamma_j \|_{L_q(G)}
\]
for some $0 < q < p$, for all $n \in \mathbb{N}$ and all $(a_j)_{j=1}^n \in \mathbb{C}^n$. By an application of Holder's inequality it is easily seen that if the above holds for some $0 < q < p$ then it holds for all $0 < r < p$ (see [43]).

In section 2 we show that in the dual of the Cantor group $D^*$ (where $D = (-1, 1)^\mathbb{N}$) there exist $\Lambda(p)$ sets which are not $\Lambda(p+c)$ for any $c > 0$, where $p = 2k$ and $2 < k \in \mathbb{N}$. Some of the results in this section follow from more general results in the following sections, but we have given proofs specifically adapted to $D$. This is because the construction in $D$ is particularly revealing and shows some of the basic ideas used in other constructions. Essential to the construction for $D$ are some ideas from coding theory and in particular it was some remarks of Johnson, Schectman, and Wilson (unpublished) in the $p=4$ case that led us to general case for $D$ and subsequently to other groups.

In section 3 some preliminary results used for the rest of the chapter are proved. In particular the study of $\Lambda(p)$ sets for general compact abelian groups is reduced to the study of $\Lambda(p)$ sets in a few special groups, namely in the dual groups $\mathbb{Z}$, $\mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots$ (for an increasing sequence of primes $(p_n)$), $\mathbb{Z}(p^\infty) = \bigcup_{n \geq 0} \mathbb{Z}(p^n)$ ($p$ a prime) and $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$. This is effected by using
the results of [9], where this type of idea was used in showing that there are sets which are $\Lambda(p)$ for all $1 \leq p < \infty$ but which are not Sidon sets.

In section 4 we give constructions for $\mathbb{Z}$ and $\mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots$. While constructions for these two groups are known (see [43], [9]) we give a construction based on a theorem of Bose and Chowla [6] (which was used to assert the existence of finite projective planes). In this section we also generalize a method of Erdős (see [11]) which shows that with respect to a certain biased coin tossing measure on the space of integer sequences almost all sequences have a prescribed rate of growth and that an arbitrary integer can be written in a bounded number of ways as a sum of elements of a given random integer sequence. This result easily yields that for $p=2k$, $2 \leq k \in \mathbb{N}$ almost all integer sequences are $\Lambda(p)$ but not $\Lambda(p+\varepsilon)$. We also compute in this section a more precise version of the growth of the $\Lambda(4)$ constant of the squares than in [43]. It is somewhat surprising that the sequence constructed in the $p=4$ case above are like squares, since the squares are not $\Lambda(4)$.

In section 5 we turn to the dual group $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$ for $p>2$. It is shown that for $p>k \geq 2$ there are $\Lambda(2k)$ sets which are not $\Lambda(2k+\varepsilon)$ for any $\varepsilon>0$ by using certain classical facts
about symmetric polynomials. For $k \geq p$ we don't have a construction but it is shown that one possible approach is to reduce the problem to one about counting rational points in a certain variety. This problem in algebraic geometry however appears to be rather delicate. The results of section 2 along with those in section 5 constitute a strong form of a solution to a problem in Lopez and Ross's book "Sidon Sets", page 171 (see [32]).

In section 6 we turn to construction in $\mathbb{Z}(p^\omega) = \bigcup_{n \geq 0} \mathbb{Z}(p^n)$. It is shown that there are $\Lambda(4)$ sets which are not $\Lambda(4+\varepsilon)$ for all $\varepsilon > 0$. One also obtains construction for $\Lambda(2k)$ sets ($k > 2$). The main idea here is that one may reduce to a well known theorem of Turan's in extremal graph theory.

In section 7 we study finite random $\Lambda(4)$ sets. Some easy modifications of the following theorem of Pisier (unpublished) are obtained: Given $A \subseteq G^*$, $|A| = n$ and given $\delta > 0$ there exists $B \subseteq A$, $|B| \geq n^{1/2 - \delta}$ s.t. $\lambda_4(B) \leq C_\delta$ (where $C_\delta$ doesn't depend on $n$ and $\lambda_4(B)$ is the $\Lambda(4)$ constant of $B$). In the final section of this chapter some applications are presented. In particular a generalization of a theorem of Pelczynski and Rosenthal [37] concerning the existence of uniformly complemented Hilbertian subspaces and a different proof of a theorem of Kwapien and Pelczynski [26] (which generalizes the classical gap theorem of Payley [36]) are presented.
We will use standard notations and any notation not mentioned in the chapter may be found in [42], [52] and [28]. Let us just mention that \(|S|\) denotes the cardinality of a set \(S\) and \([x]\) denotes the greatest integer function for \(x \in \mathbb{R}\).
IV.2. CONSTRUCTION IN THE DUAL OF THE CANTOR GROUP

In this section we construct a $\Lambda(2k)$ set in $D^*$ which is not $\Lambda(2k+\varepsilon)$, for all $\varepsilon > 0$, $2 \leq k \in \mathbb{N}$, where $D = \{-1,1\}^\mathbb{N}$ is the Cantor group. Recall that the set of characters for $D$ is the Fourier-Walsh system: For $x = (x_n) \in D$ we let $\varepsilon_k: D + \{-1,1\}$ be defined by $\varepsilon_k(x) = x_k$ where $k \in \mathbb{N}$, $k \geq 1$. Then an element of the dual group $D^*$ of $D$ consists of finite products of the $\varepsilon_k$. Given a finite subset $A$ of $\mathbb{N}$, let us write, $W_A = \prod_{j \in A} \varepsilon_j$.

2.1 Preliminaries

To construct $\Lambda(p)$ sets which are not $\Lambda(p + \varepsilon)$ we shall use the proposition below which states that among certain tuples of 0's and 1's one can find a large set of tuples whose elements when added together have distinct sums.

Proposition 2.1.1:

Let $2 \leq m \in \mathbb{N}$ and let $n \in \mathbb{N}$ such that $n \geq \lceil \log_2 m + 1 \rceil + 1$. Then among the $2^{mn}$ tuples of 0's and 1's i.e. $\{0,1\}^{mn}$, one can find a subset $A \subseteq \{0,1\}^{mn}$ with the following properties:

1) $|A| = 2^n$
2) Let $k \in \mathbb{N}$, $1 \leq k \leq m$ and let $\{c_1, \ldots, c_k\} \subseteq A$ and
\( \{c_{k+1}, \ldots, c_{2k}\} \subseteq A \) with \( \{c_1, \ldots, c_k\} \cap \{c_{k+1}, \ldots, c_{2k}\} = \emptyset \).

Then \( c_1 + \ldots + c_k \neq c_{k+1} + \ldots + c_{2k} \) (the addition of two tuples is performed coordinatewise modulo 2).  

**Proof:**

Let GF\((2^n)\) denote the Galois field of \(2^n\) elements where \(n\) is chosen so that \(n \geq \lceil \log_2 m + 1 \rceil + 1\) and \(m\) is fixed.

Regarding GF\((2^n)\) as a vector space over GF\((2)\) we have that \(\dim \text{GF}(2^n) = n\). So let \(\{x_1, \ldots, x_n\} \subseteq \text{GF}(2^n)\) be a basis for \(\text{GF}(2^n)\) over GF\((2)\). To \(x \in \text{GF}(2^n)\) we associate the \(n\)-tuple of \(0\)'s and \(1\)'s \((a_1^1, \ldots, a_n^1)\) where \(x = \sum_{i=1}^{n} a_i^1 x_i^1\). In what follows we will always maintain the order of the \(x_i^1\)'s in any expansion of a given element of \(\text{GF}(2^n)\). In a similar fashion associate to each odd power \(x^{2k-1}\) of \(x\) its \(n\)-tuple \((a_1^k, \ldots, a_n^k)\) i.e. \(x^{2k-1} = \sum_{i=1}^{n} a_i^k x_i^k\) for \(1 \leq k \leq m\).

Finally associate to \(x\) the \(mn\) tuple of \(0\)'s and \(1\)'s \(a(x) = (a_1^1, \ldots, a_n^1, \ldots, a_1^k, \ldots, a_n^k, \ldots, a_1^m, \ldots, a_n^m)\).

We claim that \(A = \{a(x) \mid x \in \text{GF}(2^n)\}\) has the desired properties. Clearly \(|A| = 2^n\) because the first \(n\) coordinates of \(a(x)\) are the basis expansion for \(x\). To see the second property let \(\{y_1, \ldots, y_k\} \subseteq A\) and \(\{y_{k+1}, \ldots, y_{2k}\} \subseteq A\) where the two sets are disjoint (note that the condition \(n \geq \lceil \log_2 m + 1 \rceil + 1\) assures us that such sets do exist for all \(1 \leq k \leq m\)). Pick \(z_i \in \text{GF}(2^n)\) so that \(a(z_i) = y_i\), \(1 \leq i \leq 2k\). Now suppose that:
\[(2.1.1) \quad \sum_{i=1}^{k} y_i = \sum_{i=k+1}^{2k} y_i \]

Then by virtue of \(a(z_i) = y_i\) we have that:

\[(2.1.2) \quad z_1^{2j-1} + \ldots + z_k^{2j-1} = z_{k+1}^{2j-1} + \ldots + z_{2k}^{2j-1}\]

for \(1 \leq j \leq k\). Now since \(GF(2^n)\) has characteristic 2 the above condition forces:

\[(2.1.3) \quad z_1^j + \ldots + z_k^j = z_{k+1}^j + \ldots + z_{2k}^j\quad \text{for} \quad 1 \leq j \leq 2k - 1.\]

This follows by taking \(1 \leq j \leq 2k-1\), writing it as \(j = 2^l j'\) where \(j'\) is odd and raising equation (2.1.2) corresponding to \(j'\) to the \(2^l\)th power. Letting \(u_i = (1, z_i, \ldots, z_i^{2k-1})\) for \(1 \leq i \leq 2k\) the last equation in turn forces \(\{u_i\}_{i=1}^{2k}\) to be linearly independent. So,

\[\det \begin{bmatrix}
1 & z_1 & z_1^2 & \ldots & z_1^{2k-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & z_j & z_j^2 & \ldots & z_j^{2k-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & z_{2k} & z_{2k}^2 & \ldots & z_{2k}^{2k-1}
\end{bmatrix} = 0.\]

But the above is the Van der Monde determinant and is so also \(\prod_{i>j} (z_i - z_j) \neq 0\) since the \(z_i\) are distinct. This contradiction means that \(A\) has the second property.
Remarks:

2.1.1) Notice that the above type of result is the best possible of its kind in the sense that if one is given a set $S$ with a binary operation $+$, which has the closure property with respect to $S$, then for the maximal subset $A \subseteq S$ with the second property in the above proposition one has $\frac{|A|}{|S|^{1/m}} \leq 1$ (as $|S| \to \infty$). In the proposition the set $A$ has $|A| = 2^n = |\{0,1\}^n|^{1/m}$.

2.1.2) In view of the remark above it follows that the result in the proposition doesn't generalize to the characteristic $p$ case ($p>2$) with the above proof. To see this fix $1 \leq m \in \mathbb{N}$ and choose a prime $p > 2m-1$. In order for the above proof to work and to choose a maximal subset (as in the above remark) one must choose exponents $k_1, \ldots, k_{m-1} \in \mathbb{N}$, $2 \leq k_1 < \ldots < k_{m-1}$ s.t. the conditions $\sum_{i=1}^{k} x_i^{k_j} = \sum_{i=k+1}^{2k} x_i^{k_j}$ for $j=1, \ldots, m-1$, $k$ fixed, $k \leq m$ and the condition $x_1 + \ldots + x_k = x_{k+1} + \ldots + x_{2k}$ for $x_i \in \text{GF}(p^n)$ force the conditions $\Sigma_{i=1}^{k} x_i^{j} = \Sigma_{i=k+1}^{2k} x_i^{j}$ for $j=1, \ldots, 2k-1$. If $k = m$ for example this is clearly not automatic (since $p > 2m-1$). In some sense what is special about the $p=2$ case is that any $j \leq 2m-1$ can be written as $j = 2^lj_1$ with $j_1 = 1 \pmod{2}$ and all the odd exponents have already been chosen so that the conditions are forced.
2.1.3) For fields whose characteristic is not 2 an alternative approach is discussed in section 5. As an example of one case in the non characteristic 2 situation, pick a prime $p > 2$. Set $A = \{(x, x^2) | x \in GF(p^n)\}$ (here we expand $x$ and $x^2$ in tuple fashion regarding $GF(p^n)$ as a vector space over $GF(p)$). Then $|A| = p^n$ while $|\{0, 1, \ldots, p-1\}^{2n}| = p^{2n}$ and if $a, b, c, d$ are in $A$ (all distinct) then $a + b \neq c + d$. To see this simply observe that $x + y = w + z$ and $x^2 + y^2 = w^2 + z^2$ have no solutions with $\{x, y, w, z\} \subseteq GF(p^n)$ and with $x, y, w, z$ being distinct.

2.1.4) With $m = 2$ in proposition 2.1.1 the proof shows that $A = \{(x, x^3) | x \in GF(2^n)\}$ works. This case corresponds to a standard construction in coding theory (see remark 2.1.5).

2.1.5) We finally point out that the construction in the proof of the proposition is the same type of construction as that of certain well known cyclic codes (particularly BCH codes) (see [50]). This resemblance was pointed out to us by D. K. Ray-Chaudhuri.

2.2 The Construction:

To begin with we set up a correspondence between certain subsets of the Walsh functions and the sets constructed in the proposition. Fix $2 \leq m \in \mathbb{N}$ and choose any $n \geq \lceil \log_2 m + 1 \rceil + 1$. Let $W_k$ be the Walsh functions
generated by \( e_1, \ldots, e_k \). For \( W_A \in W_{mn} \) construct the following tuple of 0's and 1's (of length \( mn \)):

\[
S_{W_A}(i) = \begin{cases} 
1 & \text{if } i \in A \\
0 & \text{if } i \notin A 
\end{cases}
\]

Note that given \( W_A, W_B \in W_{mn} \) and their associated tuples \( S_{W_A}, S_{W_B} \), the tuple for \( W_A W_B \), \( S_{W_A W_B} = S_{W_A} + S_{W_B} \) (mod 2).

By the construction in proposition 2.1.1 it follows that we can find a set \( A_{mn} \) of Walsh functions satisfying the following properties:

1) \( A_{mn} \subseteq W_{mn} \)

2) \( |A_{mn}| = 2^n \)

3) If \( W_{A_i} \in A_{mn}, i = 1, \ldots, 2k \) are distinct Walsh functions provided that \( k \leq m \) then \( \prod_{i=1}^{k} W_{A_i} \neq \prod_{i=k+1}^{2k} W_{A_i} \).

Now pick \( n_1 \) so that \( n_1 = \min \{ 2^j \mid 2^j \geq \lfloor \log_2 m + 1 \rfloor + 1 \} \).

Now define \( n_{j+1} = 2n_j \) for \( j \geq 1 \), \( j \in \mathbb{N} \). Finally put \( E = \bigcup_{j \geq 1} A_{mn_j} \).

Note that \( A_{mn_j} \subseteq A_{mn_{j+1}} \), by the construction and because \( GF(2^{n_{j+1}}) \supseteq GF(2^n) \) as a subfield because \( n_j \mid n_{j+1} \).

We will show that:

1) \( E \) is a \( \Lambda(2m) \) set

2) \( E \) is not a \( \Lambda(2m + \varepsilon) \) set for all \( \varepsilon > 0 \)
We show (2) first. This easily follows from some material in section 3. We choose to give however a different proof than is usual by using some well-known techniques from the local theory of Banach spaces. Fix \( \varepsilon > 0 \) and put \( p = 2m + \varepsilon \).

Then \([W_{mn_j}]_p \) (closed linear span of \( W_{mn_j} \) in \( p \)-norm) is isometric to \( \ell^2_{2^m n_j m} \), for a fixed \( j \geq 1 \). This is because of the obvious fact that if \( D_{mn_j} \) is the set of dyadic intervals of length \( 2^{-n_j m} \) on \([0,1]\) and \( I \in D_{mn_j} \) then \( X_I \in [W_{mn_j}]_p \) (of course here we are looking upon the \( \varepsilon_k \)'s as Rademacher functions on \([0,1]\)). Let \( \lambda_p(A_{mn_j}) \) be the constant of equivalence between the \( L_p \) and \( L_2 \) norms on \([A_{mn_j}]_p \). If \( E \) is a \( A(p) \) set then \( \lambda_p(A_{mn_j}) \leq A \) where \( A \) is the \( A(p) \) constant of \( E \). Now \( \dim [A_{mn_j}]_p = 2^n j \). It is a well known fact that the maximal dimension of Hilbertian subspaces which are uniformly embeddable in \( \ell^2_{2^m n_j m} \) is less than \( 2^n j \). It follows \( \lambda_p(A_{mn_j}) + \infty \) as \( j \to \infty \). This is a contradiction.

We give a more precise computation of \( \lambda_p(A_{mn_j}) \) below. The proof here is easily adapted from [15].

**Proposition 2.2.1:**

For any \( m \geq 1 \), \( j \geq 1 \) and \( \varepsilon > 0 \) we have that

\[
\lambda_p(A_{mn_j}) \geq c(p) |A_{mn_j}|^{1/2 - m/p} \quad \text{where} \quad p = 2m + \varepsilon \quad \text{and} \quad c(p) = 1/p^{1/2p}.
\]
Proof:

Let $w_1, \ldots, w_k$ be the Walsh functions in $A_{mnj}$ ($k = 2^{nj}$). For any choice of scalars $(a_j)_{j=1}^k$ we have,

$$
(2.2.1) \quad \left( \sum_{j=1}^{k} |a_j|^2 \right)^{1/2} \leq \left\| \sum_{j=1}^{k} a_j w_j \right\|_p \leq \lambda_p(A_{mnj}) \left( \sum_{j=1}^{k} |a_j|^2 \right)^{1/2}
$$

Let $(r_j)_{j=1}^k$ be the Rademacher functions and let $(x_j)_{j=1}^k \subseteq \ell_p^{2njm}$ be vectors which correspond to $w_j$ under the isometry between $[W_{mnj}]_p$ and $\ell_p^{2njm}$. Let $x_j = (x_{j,i})_{i=1}^n$ where $n = 2^{njm}$. By the left hand side of (2.2.1) and Khinchin's inequality we have,

$$
(2.2.2) \quad k^{p/2} \leq \int_0^1 \left\| \sum_{j=1}^{k} r_j(t)x_j \right\|_p dt = \sum_{i=1}^{n} \left( \int_0^1 \left| \sum_{j=1}^{k} r_j(t)x_{j,i} \right|_p dt \right)^{p/2} \leq B_p \sum_{i=1}^{n} \left( \sum_{j=1}^{k} |x_{j,i}|^2 \right)^{p/2}
$$

where $B_p$ is the upper Khinchin constant. By dualizing the right hand side of (2.2.1) we get that,

$$
(2.2.3) \quad \left( \sum_{j=1}^{k} |x_{j,i}|^2 \right)^{p/2} \leq \lambda_p^p(A_{mnj})
$$

By plugging (2.2.3) into (2.2.2) and using that $B_p \leq p^{1/2}$ (for $p>2$) it follows that,
\[ k^{p/2} \leq B_{p,n} \lambda_p^p(A_{mnj}) = B_p k^m \lambda_p^p(A_{mnj}) \leq p^{z} k^m \lambda_p^p(A_{mnj}). \]

It follows that: \( \lambda_p(A_{mnj}) \geq c(p) |A_{mnj}|^{1/2-m/p}. \)

We show next that \( \lambda_{2m}(A_{mnj}) \leq c \) where \( c = c(m) \). It follows immediately that \( \lambda_{2m}(E) \leq c \), since \( A_{mnj} \subseteq A_{mnj+1} \).

**Proposition 2.2.2:**

For any \( m \geq 2 \) and \( j \geq 1 \) we have \( \lambda_{2m}(A_{mnj}) \leq c \) where \( c = c(m) \).

**Proof:**

Fix \( j \geq 1 \). Let \( w_1, \ldots, w_N \) be the elements of \( A_{mnj} \) (N=2^{nj}).

Set \( f = \Sigma_{i=1}^N a_i w_i \) where \( (a_i)_{i=1}^N \in \mathbb{C}^N \) and set \( A = \Sigma_{i=1}^N |a_i|^2 \) and \( B = \Sigma_{i \neq j} a_i \omega_j w_i w_j \). We first observe that,

\[ (2.2.4) \quad |\int B^k| \leq c_k A^k \]

where \( c_k \) depends only on \( k \) and \( m \) (here \( 1 \leq k \leq m \)). This is because:

\[ \int B^k = \int (\Sigma_{i \neq j} a_i \overline{a_j} w_i w_j)^k \]

\[ = \int \sum_{i_1 \neq i_1', \ldots, i_k \neq i_k'} a_{i_1} \overline{a_{i_1'}} \ldots a_{i_k} \overline{a_{i_k'}} w_{i_1} \ldots w_{i_k} w_{i_1'} \ldots w_{i_k'} \]
By the second property in proposition 2.1.1

\[ \int w_{i_1} \cdots w_{i_k} \cdots w_{i_k} = 0 \text{ unless there is a pairing so that } i_j = i_1 \text{ or } i_n \text{ for some } 1 \text{ and } n \text{ and for each } 1 \leq j \leq k \text{ and similarly for } i_j' \ (1 \leq j \leq k). \text{ So } \]

\[ (2.2.5) \quad \left| \sum_{\text{all pairings}} |a_{i_1}| |a_{i_1}'| \cdots |a_{i_k}| |a_{i_k}'| \right| \]

For a fixed pairing \( P \) we certainly have

\[ A^k \geq \sum_P |a_{i_1}| |a_{i_1}'| \cdots |a_{i_k}| |a_{i_k}'| \text{ since } A^k \text{ has all products of length } k \text{ of squares i.e. } |a_i|^2. \text{ Note that only a finite number of pairings exist and this number only depends on } m \text{ (and } k). \text{ So } (2.2.4) \text{ follows.} \]

Now \( |f|^2 = (\sum_{i=1}^N a_i w_i) (\sum_{i=1}^N \overline{a_i w_i}) = A + B \).

It follows that \( \left| f \right|_{2m}^{2m} = A^m \text{ and } \)

\[ \left| f \right|_{2m}^{2m} = \int (A + B)^m = \int \sum_{k=0}^m \binom{m}{k} A^{m-k} B^k \]

\[ = A^m + \int m A^{m-1} B + \int \sum_{k \geq 2} \binom{m}{k} A^{m-k} B^k \]

\[ = A^m + \sum_{k \geq 2} \binom{m}{k} A^{m-k} \int B^k \]

So \( \left| f \right|_{2m}^{2m} = \left| f \right|_{2m}^{2m} \leq A^m + \sum_{k \geq 2} \binom{m}{k} A^{m-k} \int B^k \]

\[ \leq A^m [1 + \sum_{k \geq 2} \binom{m}{k} c_k] \]
with the last inequality following by the use of (2.2.4).

Setting $c^{2m} = c(m)^{2m} = 1 + \sum_{k \geq 2}^{m} (\binom{m}{k}) c_k$, we have

$$||f||_{2m}^{2m} \leq c^{2m} ||f||_2^{2m}$$

and so $||f||_{2m} \leq c ||f||_2$. □

Remarks:

(2.2.1) The result in proposition 2.2.2 easily follows from material in section 5, but the proof above is somewhat different from that in section 5 and is especially simple.

(2.2.2) The reader will observe that we could also have built our example on "disjoint" blocks $A_{mnj}$ instead of "inductive" ones (i.e. $A_{mnj} \subseteq A_{mnj+1}$). We choose to use the latter type of blocks just because this feature was implicit in the construction of proposition 2.1.1.
IV.3. PRELIMINARY FACTS

In this section we state some simple results which are used in the rest of the paper. We start with a result which states that $\Lambda(p)$ sets are thin from the point of view of the groups they contain. A generalization of this result is in [9] and the proof in [9] was based on ideas in [43]. From now on if $E$ is a $\Lambda(p)$ set for $p > 2$ then the $\Lambda(p)$ constant of $E$, $\lambda_p(E)$ is the constant of equivalence between the $L_p$ and $L_2$ norms on $L_p^E = \{ f \in L_p \mid \hat{f}(x) = 0 \text{ if } x \notin E \}$.

**Proposition 3.1:**

Let $G \leq \Gamma$ (dual of some compact abelian group) be a group with $|G| < +\infty$. Let $\Lambda$ be $\Lambda(q)$ for some $q > 2$. Then

$$\lambda_q(\Lambda) \geq |G \cap \Lambda|^{\frac{1}{2}} / |G|^{1/q}.$$

**Remark 3.1:**

It is obvious from [9] that the above result is valid not only for finite groups but also translates of finite groups.

The next result improves the estimate of the $\Lambda(p)$ constant involved over that in [9]. It is an obvious modification of the proof in [9]. A similar estimate appears in [5] but the proof is somewhat different. We require the following definition.
**Definition 3.1:**

Let $\Gamma$ be an abelian group and let $2 \leq n \in \mathbb{N}$. For all $\Lambda \subseteq \Gamma$ denote by $R(\Lambda, n)$ all functions $f : \Lambda \rightarrow \mathbb{N}$ s.t. $\sum_{x \in \Lambda} f(x) = n$. For $\gamma \in \Gamma$, $R(\Lambda, n, \gamma)$ denotes all $f$ s.t. $\sum_{x \in \Lambda} f(x) = \gamma$ and $f \in R(\Lambda, n)$.

**Proposition 3.2:**

Let $G$ be a compact abelian group with dual group $\Gamma$ and assume that $|R(\Lambda, n, \gamma)| \leq M$ for all $\gamma \in \Gamma$ and some $\Lambda \subseteq \Gamma$. Then $\lambda_{2n}(\Lambda) \leq (M(n!))^{1/2n}$ (here $n \geq 2$).

**Proof:**

Let $f = \sum_{x \in A} a(x)x$ for some finite set $A \subseteq \Lambda$. By the multinomial expansion we have

$$f^n = \sum_{g \in R(A, n)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} (a(x)x)g(x)$$

$$= \sum_{\gamma \in \Gamma} b_{\gamma} \text{ where } b_{\gamma} = \sum_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} a(x)g(x)$$

Now by Holder's inequality

$$|b_{\gamma}|^2 \leq \left( \sum_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} |a(x)| \right) \left( \sum_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} 2g(x) \right)$$

$$\leq \left( \sup_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} |a(x)| \right) \left( \sum_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} 2g(x) \right)$$

$$\leq M n! \sum_{g \in R(A, n, \gamma)} \frac{n!}{\prod_{x \in A} g(x)!} \prod_{x \in A} |a(x)| 2g(x)$$
So $\|f\|_{2n}^2 = \sum |b_{\gamma}|^2$ (by Parseval's identity)

$$\leq M(n!) \sum_{\gamma \in \Gamma} (\prod_{x \in A} a(x))^2 \prod_{x \in A} |a(x)|^2 g(x)$$

$$\leq M(n!) \sum_{g \in G(A,n)} (\prod_{x \in A} a(x))^2 \prod_{x \in A} |a(x)|^2 g(x)$$

$$= M(n!) (\sum_{x \in A} |a(x)|^2)^n \text{ (by the multinomial expansion)}$$

$$= M(n!) \|f\|_2^{2n}$$

So $\lambda_{2n}(A) \leq (M(n!))^{1/2n}$.

The last result of this section reduces the study of $\Lambda(p)$ sets for general compact abelian groups to a few special cases. A result of this type was stated in [9] for the purpose of studying Sidon sets. We start with the following obvious proposition (for a proof see [9]).

Proposition 3.3:

Let $G$ be a compact abelian group and $H$ a closed subgroup. Then $A$ is a $\Lambda(p)$ set in $(G/H)^*$ $(1 < p < \infty)$ if and only if $A$ is a $\Lambda(p)$ set in $G^*$.

Proposition 3.3 shows that we may reduce our study to $\Lambda(p)$ sets in the list of groups in proposition 3.4. For a slightly different proof of this simple fact, see [9].
Proposition 3.4:

Let $G$ be an infinite abelian group. Then $G$ contains a subgroup of one of the following types:

1) $\mathbb{Z}$
2) $\mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots$ for some increasing sequence of primes $(p_n)_{n=1}^{\infty}$
3) $\mathbb{Z}(p^\infty)$ and
4) $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$ for some $p$ (prime).

Proof:

Let $\tau(G)$ be the torsion subgroup of $G$. If $\tau(G) \neq G$ then $G \cong \mathbb{Z}$. So assuming $\tau(G) = G$ write $G = \bigoplus G_p$ where $G_p$ are the $p$-primary components. If there are infinitely many components then $G \cong \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots$. If there are finitely many components then $|G_p| = +\infty$ for some $p$. Then $G_p$ (for this value of $p$) contains a basic subgroup $B$ (see [41]). Denote by $\alpha(B) = \sup_{b \in B} \text{ord}(b)$ where $\text{ord}(b)$ is the order of $b$. If $\alpha(B) = +\infty$ then $B$ will contain infinitely many cyclic groups in its decomposition, so $B \cong \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$.

If $\alpha(B) < +\infty$ then $G_p = B \oplus G_p/B$ (see [41]). If $G_p/B = \{0\}$ then $G_p = B$ and so $B$ will contain infinitely many cyclic groups in its decomposition and so $B \cong \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$.

If $G_p/B \neq \{0\}$ then $G_p/B = \mathbb{Z} \oplus Q \oplus \mathbb{Z}(p^\infty)$, because $G_p/B$ is divisible. Since $Q$ is not torsion and $G_p$ is $\bigoplus G_p/B = \mathbb{Z} \oplus \mathbb{Z}(p^\infty)$. So at least one $\mathbb{Z}(p^\infty)$ appears since $G_p/B \neq \{0\}$. It follows that $G \cong \mathbb{Z}(p^\infty)$. □
IV.4. CONSTRUCTIONS IN \( \mathbb{Z} \) AND \( \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots \)

Constructions in \( \mathbb{Z} \) and \( \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots \) are well known ([43], [9]). We will give a slightly different type of construction here. Our starting point is the following theorem of Bose and Chowla (see [6]).

**Proposition 4.1:**

Let \( m = p^n \) (where \( p \) is a prime, \( n \in \mathbb{N} \)) and \( q = (m^{r+1} - 1)/m - 1 \) for some \( r \in \mathbb{N} \). Then we can find \( m + 1 \) integers (less than \( q \)) \( d_0 = 0, d_1 = 1, d_2, \ldots, d_m \) s.t. the sums \( d_{i_1} + \ldots + d_{i_r}, 0 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m \) are all different mod \( q \).

Proposition 4.1 is for \( m \) being powers of primes (and this was what was needed to construct finite projective planes). Proposition 4.2 is an extension. A similar argument appears in [9] with a different conclusion.

**Proposition 4.2:**

If \( n > 3m^6^m \) (for some \( m \in \mathbb{N} \)) then we can find \( A \subseteq \mathbb{Z}_n \) such that \( |A| \geq \frac{n^{1/m}}{(3^m+1)/m} \) and the sums \( a_{i_1} + \ldots + a_{i_m} \) are distinct mod \( n \) where \( \{a_{i_1}, \ldots, a_{i_m}\} \subseteq A \) and \( 1 \leq i_1 \leq \ldots \leq i_m \).
**Proof:**

Choose \( n \) as above. set \( x = \frac{n^{1/m}}{3^{1/m + 1/m^{1/m}}} \). Then \( x > 2 \) and so there exists a prime \( p \) (by Bertrand's theorem, [22]) s.t. \( \lfloor x \rfloor + 1 < p < 2\lfloor x \rfloor + 2 \). So \( x < p < 2x + 2 < 3x \) (since \( x > 2 \)) i.e. there exists a prime \( p \) s.t.

\[
\frac{n^{1/m}}{3^{1/m + 1/m^{1/m}}} < p < \frac{n^{1/m}}{3^{1/m^{1/m}}}.
\]

Set \( q = \frac{p^{m+1} - 1}{p - 1} \). By proposition 4.1 there exist \( a_1, \ldots, a_p \) (less than \( q \)) s.t. \( m \)-sums of the \( a \)'s are distinct (mod \( q \)). Set \( A = \{a_1, \ldots, a_p\} \). Then we have that \( a_1^{m} + \ldots + a_m^m < mq < 3p^m < n \). So the \( m \)-sums are also distinct mod \( n \). Also

\[
|A| = p > \frac{n^{1/m}}{3^{1/m + 1/m^{1/m}}} = \frac{n^{1/m}}{(3^{m^{1/m}})^{1/m}}.
\]

Since it is not particularly important as to how large \( n \) should be in proposition 4.2 to make it true we could have used the prime number theorem instead of Bertrand's theorem in the proof above. This is because for all \( \varepsilon > 0 \),

\[
\pi((1 + \varepsilon)n) - \pi(n) \to +\infty \text{ as } n \to +\infty \text{ (and so there is a prime } p, n < p < (1 + \varepsilon)n \text{ if } n \text{ is large) by the prime number theorem. This would have yielded a somewhat larger set } A \text{ in proposition 4.2. Since this is of no importance in what follows we choose to use Bertrand's theorem.}
\]

One may now easily construct \( \Lambda(2k) \) sets in \( \mathbb{Z} \) which are not \( \Lambda(2k + \varepsilon) \), for all \( \varepsilon > 0 \).
Proposition 4.3:

There is a set \( F \subseteq \mathbb{Z} \) which is \( \Lambda(2k) \) but not \( \Lambda(2k + \varepsilon) \) for \( \varepsilon > 0 \), where \( k \geq 2 \).

Proof:

Let \( (p_n) \) be an increasing sequence of primes. By proposition 4.1 there exist sets \( E_n \subseteq \mathbb{Z} \) s.t. \( |E_n| \geq p_n \), \( E_n \subseteq [0, \frac{p_{n+1} - 1}{p_n - 1}] \) s.t. \( k \)-sums out of \( E_n \) are distinct (we are now adding in \( \mathbb{Z} \) and looking upon these sums).

Set \( F_1 = E_1 \) and set \( a_i = \max_{j \geq 1} F_{i-1} \) (for \( i \geq 2 \)) and \( F_i = a_i E_i \). Set \( F = \bigcup_{i \geq 1} F_i \). It is clear that \( F \) is \( \Lambda(2k) \) by proposition 3.2. To see \( F \) is not \( \Lambda(2k + \varepsilon) \), let \( A_n = \{ a_n m \mid m \in \mathbb{N}, 0 \leq m \leq \frac{p_{n+1} - 1}{p_n - 1} \} \) and note that \( |F_n \cap A_n| \geq p_n^{1/(k+1)} |A_n|^{1/k} \). By a theorem of Rudin the cardinality of the intersection of a \( \Lambda(2k + \varepsilon) \) set with an arithmetic progression can't be so large (see [43], one can't quite use proposition 3.1, but certainly one can use appropriate generalizations of it. Since this is the only time we need anything other than proposition 3.1 we don't state the general results). □

It should be clear that by using proposition 4.2 on "disjoint blocks" of \( \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots \), one may build analogous examples.

Proposition 4.4:

There is a set \( E \subseteq \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots \) which is \( \Lambda(2k) \) but not \( \Lambda(2k + \varepsilon) \).
Proof:
Assume without loss of generality that $p_n > 3k6^k$ for all $n \geq 1$. By proposition 4.2 there exists $E_n \subseteq \mathbb{Z}(p_n)$ s.t. $|E_n| \geq \frac{p_n}{(3k+1)^{1/k}}$ and $k$-sums out of $E_n$ are distinct mod $p_n$.

Set $E = \bigcup_{n=1}^{\infty} E_n$ with each $E_n$ embedded in $\mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \cdots$ in the canonical fashion. By proposition 3.2 $E$ is $\Lambda(2k)$ and (by proposition 3.1), $E$ is not $\Lambda(2k+c)$. □

Remark 4.1:
Notice that the growth "locally" of $\lambda_{2k+c}(E)$ for the sets $E$ constructed in propositions 4.3 and 4.4 are "power type" and compare this with proposition 2.2.1.

We now look at some infinite random $\Lambda(p)$ sets in $\mathbb{Z}$ by considering a method of Erdős. We first introduce a biased coin tossing space on the set of integer sequences $\Omega$ (increasing subsequences of $\mathbb{N}$). Let $\chi_n$ be 2-valued random variables (independent) for $n \geq 1$, with $P(\chi_n = 0) = 1 - p_n$ and $P(\chi_n = 1) = p_n$ for $0 < p_n < 1$ and $(p_n)_{n=1}^{\infty}$ a given sequence. It is natural to call $\Omega$ a biased coin tossing space: The probability space on which the $\chi_n$'s are defined can naturally be taken to be the Cantor set $D = \{0,1\}^\mathbb{N}$. On each factor introduce the probability $P_n(\{0\}) = 1 - p_n$ and $P_n(\{1\}) = p_n$. 
Then the $P$ above is just $P = \bigotimes_{n=1}^{\infty} P_n$ and the $X_n$'s are the projection onto the $n$th coordinate. Using the natural identification between $\Omega$ and $D$ we have a coin tossing measure on $\Omega$.

For different choices of $(p_n)$ we get different probability spaces (though by a theorem of Kakutani [24] if $(p_n)$ is sufficiently close to $p_n$ for all $n$, the spaces are the same). We denote a generic sequence of $\Omega$ by $(a_k)_{k=1}^{\infty}$. We always choose $(p_n)$ so that $\sum_{n=1}^{\infty} p_n = +\infty$. This insures that the sequence $(a_k)_{k=1}^{\infty}$ is infinite with probability 1 (by Borel-Cantelli). Recall the following simple variant of the strong law of large numbers (see [20]).

**Proposition 4.5:**

Let $(X_n)_{n\geq 1}$ be a sequence of independent random variables on a probability space $(\Omega, F, \mu)$. Let $S_n = \sum_{i=1}^{n} X_i$ and suppose that: 1) $E(X_i) > 0$ 2) $\lim_{n\to\infty} E(S_n) = +\infty$ 3) $\sum_{i=1}^{\infty} \frac{\text{Var}(X_i)}{E(S_i)^2} < +\infty$ Then with probability 1, we have

$$\frac{(S_n - E(S_n))}{E(S_n)} \to 0.$$ 

As an immediate consequence we have in our case:

**Proposition 4.6:**

Let $(X_n)_{n\geq 1}$ and $\Omega$ be as in our case. If in addition to the previous conditions on $(p_n)_{n=1}^{\infty}$ we have

$$\sum_{n=1}^{\infty} \frac{p_n(1-p_n)}{(p_1 + \ldots + p_n)^2} < +\infty$$

then a.a. $\omega \in \Omega$
\[
\frac{x_1 + \ldots + x_n}{p_1 + \ldots + p_n} \to 1
\]

It follows that a.a. \( \omega \in \Omega \) we have

\[
\lim_{k \to \infty} \frac{\sum_{i \leq a_k} p_i}{k} = 1
\]

with \((a_i)\) being a generic sequence.

The essence of the method is that by choosing \((p_k)_{k=1}^\infty\) carefully we impose a growth rate on almost all sequences by proposition 4.6. This in turn forces some nice properties to hold.

**Proposition 4.7:**

Let \(2 < \ell \in \mathbb{N}, 0 < \varepsilon < 1/\ell\) and set \(c = \frac{1-\ell\varepsilon}{\ell}\). Let

\[
p_k = \frac{c}{k(1-1/\ell)+\varepsilon}
\]

for \(k \in \mathbb{N}\). Let \((a_k)_{k=1}^\infty \in \Omega\) be a random sequence. Then with probability 1 we have \(|R((a_k)_{k=1}^\infty, \ell, n)| \leq \lfloor 1/\ell \varepsilon \rfloor\) except for finitely many \(n\).

The case \(\ell = 2\) is classical and due to Erdös and Renyi [12]. The proposition above is proved with some minor modifications to their proof. For a detailed proof in the case of \(\ell=2\) see [12]. Let us also note the following consequence of proposition 4.6.
Proposition 4.8:

With the same hypotheses as in proposition 4.7 we have that for each \( \delta > 0 \), there exists a \( 0 < \epsilon < 1/j \) such that with probability 1 we have \( a_k \sim k^{j+\delta} \).

Proof:

By proposition 4.6 we have a.a. \((a_k) \in \Omega\) that

\[
\lim_{k \to \infty} \frac{\sum_{i \leq a_k} p_i}{k} = 1 \quad \text{since we have that}
\]

\[
p_1 + \ldots + p_n = c \sum_{k \leq n} \frac{1}{k(1-1/j)+\epsilon} \sim c \frac{n^{(1/j)-\epsilon}}{1/j-\epsilon} = n^{1/j-\epsilon}
\]

and

\[
\sum_{n \geq 1} p_n(1-p_n) \sum_{n \geq 1} (p_1 + \ldots + p_n) = \frac{1}{n^{1+1/j+\epsilon}} < +\infty \quad \text{since}
\]

\[
\sum_{n \geq 1} \frac{1}{n^{1+1/j+\epsilon}} < +\infty \quad \text{So} \lim_{k \to +\infty} \frac{a_k}{k^{j-\epsilon}} = 1 \quad \text{which implies}
\]

\[
a_k \sim k^{j+\delta} \quad \text{by choosing} \quad \epsilon = \frac{\delta}{j(j+\delta)}.
\]

We can now easily construct \( \Lambda(p) \) sets (in fact most integer sequences will do) that are not \( \Lambda(p + \epsilon) \). We have the following:

Proposition 4.9:

Let \( \ell \in \mathbb{N}, \ell \geq 2 \). Set \( p = 2\ell \) and let \( n > 0 \). Then a.a. subsequences \( A = (a_k)_{k=1}^\infty \), are \( \Lambda(2\ell) \) but not \( \Lambda(2\ell+n) \).
Proof:

By proposition 4.7 and proposition 3.2 a.a. subsequences A are $A(2\ell)$ and $a_k \sim k^{\ell+\delta}$ for any fixed $\delta$, $0 < \delta < \eta/2$. One may now conclude that A is not $A(2\ell + \eta)$ by using Rudin's proposition on arithmetic progressions (see [43]), but an alternative argument is: By a theorem of Marcinkiewicz and Zygmund (see [43]), $[e^{1t}, \ldots, e^{int}]_q \approx k_q^{\ell_n}$ for any $1 < q < \infty$ where the constant of isomorphism $k_q$ does not depend on $n$. If $(a_k)$ is $A(2\ell + \eta)$ then the $2$ and $2\ell + \eta$ norms agree on $(a_k)_{k=1}^\infty$, but we can pack $[n^{1/\ell+\delta}]$ $a_k$'s in $1, \ldots, n$, so arguing as in proposition 2.2.1 we have that,

$$\lambda_{2\ell+n}((a_k) \geq c(\ell, \eta) n^{(n-2\delta)/(2\ell-2\delta)(2\ell+\eta)}$$

where $c(\ell, \eta)$ is a constant depending on $\ell$ and $\eta$. Since $\delta < \eta/2$ we have a contradiction. $\square$

Note that the case $\ell = 2$ in proposition 4.8 gives $a_k \sim k^{2+\delta}$ for any $\delta > 0$ being $A(4)$. This is a priori somewhat surprising in view of the fact that $a_n = n^2$ is not $A(4)$ (see [43]). Here we give a refinement of this result by calculating $\lambda_4((k^2)_{k\leq n})$ by using essentially the same technique as in [43]. We first recall the following result of Landau (see [21]) (and also due independently to Ramanujan (see [21])).
Proposition 4.10:

Let \( x \in \mathbb{R}_+ \). Let \( B(x) \) be the cardinality of \( n \leq x, n \in \mathbb{N} \) which are representable as sums of two squares. Then \( B(x) \sim \frac{K x}{(\log x)^{\frac{3}{4}}} \) where \( K = \left( \prod_{p \text{ prime, } p=3(\text{mod } 4)} 1 - \frac{1}{p^2} \right)^{\frac{1}{4}} \approx 0.764 \ldots \)

We shall also need the following proposition (see [22]).

Proposition 4.11:

\[ \left( |R'((k^2),2,1)| + \ldots + |R'((k^2),2,n)| \right)/n \rightarrow \pi/4 \text{ as } n \to +\infty, \]

where \( R' \) allows one to count permutations of the \( 2 \)-sums of squares which represent an element of \( \mathbb{N} \).

Proposition 4.12:

Let \( n \in \mathbb{N} \). We have for all \( \varepsilon > 0 \) there exists \( N_\varepsilon \in \mathbb{N} \) s.t. \( \lambda_k((k^2)_{1 \leq k \leq n}) \geq (1 - \varepsilon) c \left( \log n \right)^{1/8} \) where \( n \geq N \) and \( c = \pi/2 \frac{\log 2}{K^{1/4}} \) where \( K \) is as in proposition 4.10.

Proof:

Let \( \mu = \) counting measure on \( \mathbb{N} \). Write \( r_n = |R'((k^2),2,n)| \) and let \( A = \{ n \in \mathbb{N} \mid r_n \geq 1 \} \) and let \( E_n = \{ k^2 \mid 1 \leq k \leq n \} \).

Consider \( f(e^{i\theta}) = e^{i\theta} + e^{i2^2\theta} + \ldots + e^{i n^2\theta} = \sum_{k \leq n} e^{ik^2\theta} \). Then we have that \( f^2(e^{i\theta}) = r_0 + r_1 e^{i\theta} + \ldots + r_n e^{i n^2\theta} + \ldots \). So we have,
\[ r_1 n^2 r_k^2 < \| f \|_q^q \cdot \lambda_q^q (E_n) \| f \|_p^p = \lambda_q^q (E_n)n^2 \] which implies \[ \lambda_q^q (E_n) \geq \frac{1}{n^2} \Sigma_1^r r_k^2. \]

Also we have that,

\[ \int_1^n r_m du(m) = \int_1^n r_m x_A du(m) \leq (\int_1^n r_m^2 du)^{1/2} \mu(A \cap [1,n^2])^{1/2}. \]

It follows that,

\[ \int_1^n r_m^2 du \geq (\int_1^n r_m du(m))^2 \geq (1 - \epsilon)^2 \frac{\pi^2}{16} \frac{n^2}{\mu(A \cap [1,n^2])} \]

if \( n \geq N'_e \) say (by proposition 4.11). So

\[ \lambda_q^q (E_n) \geq (1 - \epsilon)^2 \frac{\pi^2}{16} \frac{n^2}{\mu(A \cap [1,n^2])} \quad \text{for } n \geq N'_e. \]

By proposition 4.10 \( \frac{n^2}{\mu(A \cap [1,n^2])} \geq (1 - \epsilon)^2 \frac{(\log n^2)^{1/2}}{K} \)

if \( n \geq N''_e \). So for \( n \geq N_e = \max (N'_e, N''_e) \) we have that

\[ \lambda_q^q (E_n) \geq (1 - \epsilon)^4 \frac{2^{1/8}}{K} (\log n)^{1/2} \frac{\pi^2}{16}, \text{ so that} \]

\[ \lambda_q^q (E_n) \geq (1 - \epsilon) \frac{\pi^2}{2} \frac{2^{1/8}}{K^{1/4}} (\log n)^{1/8} = (1 - \epsilon) c(\log n)^{1/8}. \qed \]

Remarks:

4.2) The same argument shows that if \( E \) is a subsequence of integers s.t. average order of \( |R(E,h,n)| \) is finite while \( A = \{ n \mid |R(E,h,n)| > 0 \} \) has density \( 0 \), then

\[ \lambda_{2h}(E \cap \{1, \ldots, n\}) \to ^\infty \text{ as } n \to \infty. \]
4.3) While the above result is surprising in view of proposition 4.9, it turns out that squares are the exceptional case. Indeed it is known that e.g. there exists sequence \((a_j)\) s.t. \(a_j = j^2 + O(\log j)\) and density \(\{a_j\} + \{a_k\} > 0\) (see [20]).

4.4) It should be noted that while the previous constructions yielded \(\Lambda(p)\) sets which were not \(\Lambda(p + c)\) for all \(c > 0\), the construction in proposition 4.9 is not uniform i.e. for a fixed \(n > 0\) a.a subsequences \(A = (a_k)_{k=1}^\infty\) are \(\Lambda(21)\) but not \(\Lambda(21 + n)\). This may be the price one has to pay for random constructions. This becomes clearer in section 7.

4.5) It should be noted that \(\lambda((k^2)_{1 \leq k \leq n}) = O(n^\delta)\) for any \(\delta > 0\). This follows from the fact that \(|R(\{k^2\}_{k=1}^\infty, 2, n)| = O(n^\delta)\) for all \(\delta > 0\) (see [22]) and because of proposition 3.2.
In this section we will show that for \( p > m \) there is a \( \Lambda(2m) \) set in \( \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots \) which is not \( \Lambda(2m + \varepsilon) \) for all \( \varepsilon > 0 \). For \( m \geq p \) we don't have a construction but we indicate a possible solution. Prior to this however we need an appropriate analog of proposition 2.2.2. Proposition 3.2 is not useful when most elements have small order, such as in \( \mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots \). One may prove the appropriate generalization of proposition 2.2.2 by suitable modifications of its proof, however we choose to improve the estimates in [9]. We will perform a modification of the proof in [9]. The modification of the proof of proposition 2.2.2 is much more cumbersome. We require the following definition.

**Definition 5.1:**

Let \( \Gamma \) be an abelian group and let \( 2 \leq n \in \mathbb{N}, 2 \leq p \in \mathbb{N} \). For \( \Lambda \subseteq \Gamma \) denote by \( \mathcal{R}_p(\Lambda, n) \) all functions \( f: \Lambda \to \mathbb{N} \) s.t. \( f(X) \leq p - 1 \) for all \( X \in \Lambda \) and \( \sum \mathbf{1}_f(X) = n \). For \( \gamma \in \Gamma \), \( \mathcal{R}_p(\Lambda, n, \gamma) \) denotes all \( f \) s.t. \( \prod_{X \in \Lambda} f(X) = \gamma \) and \( f \in \mathcal{R}_p(\Lambda, n) \).

**Proposition 5.1:**

Let \( G \) be a compact abelian group with dual group \( \Gamma \) and assume that \( \Lambda \subseteq \Gamma \) has elements only of order \( p \), \( p > 2 \).
Also assume $|R_p(\Lambda, m, \gamma)| \leq M$ for all $\gamma \in \Gamma$ and for all $m$ s.t. $2 \leq m \leq n$. Then $\lambda_{2n}(\Lambda) \leq M^{1/2n}([n/p] + 1)^{1/n}(n!)^{1/n}$.

**Proof:**

Let $f = \sum_{X \in B} b(X)X$ for some finite set $B \subseteq \Lambda$. Also assume without loss of generality that $b(X) \geq 0$ for all $X \in B$. By the multinomial expansion we have

$$f^n = \sum_{\gamma \in \Gamma} \left( \sum_{g \in R(B, n, \gamma)} \prod_{X \in B} b_X g(x)^Y \right) \prod_{X \in B} b_X g(x)^Y \prod_{Y \in \Gamma} \sum_{\gamma \in \Gamma} b_{\gamma} \gamma$$

Denote by $M(g) = \prod_{X \in B} b_X g(x)^Y$ and by $j = \lfloor n/p \rfloor$. Given $g \in R(B, n)$ write $g(x) = d(x)p + e(x)$ where $0 \leq e(x) \leq p - 1$ and $d(x) \geq 0$.

So $\sum d(x) = i$ for some $i \in \{0, 1, \ldots, j\}$. So for all $g \in R(B, n)$ there exists a unique $i \in \{0, 1, \ldots, j\}$; $d \in R(B, i)$ and $e \in R_p(B, n-pi)$. For each $i \in \{0, 1, \ldots, j\}$ write $R_p(B, n-pi, \gamma)$ as $S(i)$ ($\gamma$ will be fixed for the time being). For a fixed $e \in S(i)$ let $T(i, e) = \{g \in R(B, n, \gamma) | g = pd + e \}$ for some $d$). So $R(B, n, \gamma) = \bigcup_{i=0}^j (U_{e \in S(i)} T(i, e))$. Writing

$$m(i, e) = \sum_{g \in T(i, e)} M(g) \prod_{X \in B} b_X g(x),$$

we have that

$$b_{\gamma} = \sum_{i=0}^j \sum_{e \in S(i)} m(i, e).$$

Now we have,
\[ m(i, e) = \sum_{g \in \mathcal{T}(i, e)} M(g) \left( \prod_{x \in B} b(x)^{p_d(x)} \right) \left( \prod_{x \in B} b(x)^{e(x)} \right). \quad \text{So,} \]

\[ m(i, e) \leq n! \prod_{x \in B} b(x)^{e(x)} \left[ \sum_{d \in R(B, i)} M(d) \prod_{x \in B} (b(x)^p)^{d(x)} \right]. \]

where \( M(d) = \frac{1}{\prod_{x \in B} d(x)^{T}}. \quad \text{So,} \]

\[ m(i, e)^2 \leq (n!)^2 \prod_{x \in B} b(x)^{2e(x)} \left( \sum_{x \in B} b(x)^{p_i} \right)^2 \]

\[ \leq (n!)^2 \left( \sum_{x \in B} b(x)^2 \right)^{p_i} \prod_{x \in B} b(x)^{2e(x)} \]

\[ = (n!)^2 \left( \prod_{x \in B} b(x)^{2e(x)} \right) \|f\|_2^{2p_i} \tag{5.1} \]

So \( b^2_Y = \left( \sum_{i=0}^{J} \sum_{e \in S(i)} m(i, e) \right)^2 \)

\[ \leq \left( \sum_{i=0}^{J} \sum_{e \in S(i)} m(i, e)^2 \right) \sup_{i} |S(i)|(j + 1) \]

(by Holder's inequality)

\[ \leq M(j + 1) \sum_{i=0}^{J} \sum_{e \in S(i)} m(i, e)^2 \quad \text{(by assumption)} \]

\[ \leq M(j+1)(n!)^2 \sum_{i=0}^{J} \|f\|_2^{2p_i} \sum_{e \in S(i)} \prod_{x \in B} b(x)^{2e(x)} \]

(by 5.1)
So
\[ \|f\|_{2n}^2 = \sum_{\gamma \in \Gamma} b_{\gamma}^2 \]
\[
\leq M(j + 1)(n!)^2 \sum_{\gamma \in \Gamma} \sum_{i=0}^{j} \|f\|^{2p_1}_2 \sum_{\gamma \in \Gamma} e_{\gamma} R_p(B, n-p_1, y) \\
\sum_{x \in B} b(x)^2 e(x) \\
\leq M(j + 1)(n!)^2 \sum_{i=0}^{j} \|f\|^{2p_1}_2 \sum_{\gamma \in \Gamma} e_{\gamma} R_p(B, n-p_1) \\
\sum_{x \in B} b(x)^2 e(x) \\
\] 

(\text{where } M(e) = \frac{(n-p_1)!}{\prod_{x \in B} e(x)!})

\[
\leq M(j + 1)(n!)^2 \sum_{i=0}^{j} \|f\|^{2p_1}_2 \|f\|^{2n-2p_1}_2 \\
= M(j + 1)^2(n!)^2 \|f\|^{2n}_2 \\
\]

So
\[ \lambda_{2n}(\Lambda) \leq M^{1/2n}(\left[\frac{n}{p}\right] + 1)^{1/n} (n!)^{1/n}. \]
We now turn to the construction of $\Lambda(q)$ sets in $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$. We will try to follow the ideas embodied in section 2. Fix $2 \leq m \in \mathbb{N}$. Suppose we could show the following for all $n \in \mathbb{N}$, $n \geq n(m)$: there exists $A_n \subseteq \{0,1,\ldots,p-1\}^{mn}$ (which is regarded as an abelian group with the group operation on tuples being coordinate-wise addition mod $p$) s.t.

1) $|A_n| \geq p^n$

2) If $\alpha_n = \sup \left( |R_p (A_n, k, x)| \right) \in \{0,\ldots,p-1\}^{mn}$, $2 \leq k \leq m$

then $\sup_n \alpha_n < +\infty$.

Then identifying the dual group of $\mathbb{Z}(p)^{\mathbb{N}}$ with finite tuples of $0$'s,...,$p-1$'s as in section 2; we may construct the required types of $\Lambda(p)$ sets. This is done by patching the sets $A_n$ as in section 2. $|A_n| \geq p^n$ and proposition 3.1 ensures that the patched set is not $\Lambda(2m + \varepsilon)$ for all $\varepsilon > 0$ and $\sup_n \alpha_n < +\infty$ ensures using proposition 5.1 that the $A_n$'s have a uniform (in $n$) $\Lambda(2m)$ constant (and thus a union of $A_n$'s is $\Lambda(2m)$; with the $A_n$'s built on "disjoint blocks" of $\mathbb{Z}(p) \oplus \mathbb{Z}(p) \oplus \ldots$).

Proposition 2.1.1 suggests that $A_n$ may be built by considering a suitable choice of $(k_i)_{i=1}^m \in \mathbb{N}^m$ and letting, $A_n = \{(x^{k_1},\ldots,x^{k_m}) \mid x \in GF(p^n)\}$ with $1 = k_1 < k_2 < \ldots < k_m$ (we regard $GF(p^n)$ as a vector space over $GF(p)$ and expand $x^{k_i}$ in a basis expansion and put in the coordinates in place
of \(x^{k_1}\), so that \(A_n \subseteq \{0, \ldots, p-1\}^{mn}\). The choice of \(k_1=1\) insures that \(|A_n| = p^n\). (Actually any choice for \(k_1\) will work so long as \(x + x^{k_1}\) is an automorphism for \(GF(p^n)\) (fixing \(GF(p)\)). Since the automorphisms form a cyclic group of order \(n\), the most "convenient" choice is \(k_1 = 1\). The main problem is making sure that \(\sup_n \alpha_n < +\infty\).

In view of the above remarks it is easy to see that we may reduce to the following problem on Diophantine equations over finite fields:

**Problem 5.1:**

Let \(2 \leq m \in \mathbb{N}\) and \(p\) be a prime which are fixed. Let \(n \in \mathbb{N}\), \((y_1, \ldots, y_m) \subseteq GF(p^n)\) and \(1 = k_1 < k_2 < \ldots < k_m\) with the \(k_i \in \mathbb{N}\) for all \(i\). Consider the system of equations:

\[
\begin{align*}
\sum_{i=1}^{k_1} x_i & = y_1 \\
\sum_{i=1}^{k_2} x_i & = y_2 \\
& \vdots \\
\sum_{i=1}^{k_m} x_i & = y_m
\end{align*}
\]

By a "solution" to this system we mean an \((x_1, \ldots, x_m) \in GF(p^n)^m\) which satisfies (*) and for which the number of non-zero \(x_i\)'s which are the same in \((x_1, \ldots, x_m)\) is at most \(p-1\). Denote by \(g(n, y_1, \ldots, y_m, k_1, \ldots, k_m)\) the number of solutions to the above system (*). The question then is: Can one
find one fixed set of $k_1$'s, $1 = k_1 < k_2 < \ldots < k_m$ s.t.
$g(n, y_1, \ldots, y_m, k_1, \ldots, k_m) \leq C$ for some $C \in \mathbb{N}$ uniformly in $n$ and $\{y_1, \ldots, y_m\}$? Of course one may replace uniformity in $n$ by working in the algebraic closure $A = \bigcup_{n \geq 1} \text{GF}(p^n)$ and considering the equivalent problem of getting a bound on the number of solutions (to (1)) of the type $(x_1, \ldots, x_m) \in A^m$ (with no more than $p-1$ of the non-zero $x_i$'s being the same)) uniformly for $\{y_1, \ldots, y_m\} \subseteq A$.

We now show that at least for $p > m$, one may solve the above problem quite simply.

**Proposition 5.2:**

If $p > m$ and one chooses $k_i = i$, $1 \leq i \leq m$ then
$g(n, y_1, \ldots, y_m, 1, 2, \ldots, m) \leq m!$

**Proof:**

Fix $n \in \mathbb{N}$. The condition that at most $p-1$ of the non-zero $x_i$'s in $(x_1, \ldots, x_m)$ ($(x_1, \ldots, x_m)$ being a solution of (1)) are the same is automatic since $p > m$. We will show that the assumption,

$$\Sigma_{i=1}^m x_i^j = \Sigma_{i=m+1}^{2m} x_i^j \text{ for } j = 1, \ldots, m$$

implies that set of $x_i$'s, $1 \leq i \leq m$ counting multiplicity is the same as the set of $x_i$'s $m+1 \leq i \leq 2m$ counting multiplicity. Let $y_1, \ldots, y_m$ be indeterminates adjoined
to $\text{GF}(p^n)$. Denote by $s_k(y_1,\ldots,y_k) = \sum_{i=1}^k y_i^k$ and by $\sigma_1,\ldots,\sigma_m$ the elementary symmetric functions in $y_1,\ldots,y_m$. By Newton's identities (see [49]) the $\sigma_i$'s can be written as polynomials in the $s_k$'s since $p > m$. It follows that $\sigma_i(x_1,\ldots,x_m) = \sigma_i(x_{m+1},\ldots,x_{2m})$ for $i = 1,\ldots,m$. So $(\lambda - x_1)\cdots(\lambda - x_m) = (\lambda - x_{m+1})\cdots(\lambda - x_{2m})$ for all $\lambda \in \text{GF}(p^n)$. So some $x_i(1 \leq i \leq m)$ is the same as an $x_j$ for some $1 < j < 2m$. By relabelling the $x_i$'s we can have $x_m = x_{2m}$. Cancelling these from the equations $\sum_{i=1}^m x_i^j = \sum_{i=m+1}^{2m} x_i^j$, $j = 1,\ldots,m$, we may repeat the above argument with the equations $\sum_{i=1}^{m-1} x_i^j = \sum_{i=1}^{2m-1} x_i^j$, $j = 1,\ldots,m-1$ (the equation with $j = m$ is ignored since it is of no further value) to conclude that $x_{m-1} = x_{2m-1}$ after relabelling the $x_i$'s. The procedure can be continued to terminate the argument. □

Proposition 5.2 therefore gives the required construction for $\Lambda(p)$ sets for $p > m$. For $m \geq p$ the problem 5.1 is much more difficult and no solutions seem to be known. The following remarks are due to P. Deligne.

Remarks:

5.1) For a fixed set of $y_i$'s, $(y_1,\ldots,y_m) \subseteq A$ (see problem 5.1) if the variety of solutions consists of isolated points then by Bezout's theorem they are at most $\prod_{i=1}^m k_i$ of them. For Bezout's theorem see [35].
5.2) If there are infinitely many solutions to (*) on the algebraic closure $A$ then there is a formal power series:

$$ (X_i(t)) = X(t) : X(t) = \sum_{k=0}^{\infty} x^{(k)} t^k $$

which is formally a solution with $x^{(1)} \neq 0$ (i.e. one of $x_i^{(1)} \neq 0$) and

1) $\sum_i x_i^{(0)k_j} = y_j$

2) For all $k > 0$, the coefficient of $t^k$ in $\sum_i X_i(t)^k$ is 0.

No use has been made of the above however.

5.3) One may weaken the problem (since the reader will observe this is all that is really required for the construction) by requiring only that $g(n_j, y_1, \ldots, y_m, k_1^{(j)}, \ldots, k_m^{(j)}) \leq c$ uniformly for some sequence of sets of $k_i$'s (i.e. the set of $m$ $k_i$'s is allowed to change with $n_j$, however $k_i^{(j)} = 1$ for all $j$), some subsequence $(n_j)$ of $\mathbb{N}$ s.t. $n_j \to +\infty$ and for all $\{y_1, \ldots, y_m\} \subseteq GF(p^{n_j})$.

However Professor Deligne thinks that solving the weaker problem for a thin set of $n_j$'s does not really help much and presumably a solution of the weaker problem will in fact enable one to solve problem 5.1.
IV.6. CONSTRUCTION IN $\mathbb{Z}(p^\infty)$

We construct a $\Lambda(4)$ set in $\mathbb{Z}(p^\infty)$ which is not $\Lambda(4 + \epsilon)$ for all $\epsilon > 0$. Some results are also possible for $\Lambda(p)$ sets, $p > 4$. The construction will be done by showing the existence of sets $E_k \subseteq \mathbb{Z}(p^{n_k}) + x_k$ (for some $n_k + \infty$, some $x_k \in \mathbb{Z}(p^\infty)$), $k=1,2,\ldots$ such that

1) $|E_k| > c p^{n_k/2}$ (c independent of k)

2) $|R(U_{k=1}^\infty E_k, 2, \gamma)| \leq 1$ for all $\gamma \in \mathbb{Z}(p^\infty)$.

By the remark 3.1 and (1) it follows that $U_{k=1}^\infty E_k$ is not $\Lambda(4 + \epsilon)$ for all $\epsilon > 0$ and proposition 3.2 and (2) insure that $U_{k=1}^\infty E_k$ is $\Lambda(4)$. The idea of the construction is that by proposition 4.2 it is easy to construct $F_k$ satisfying (1) and having 2-sums out of $F_k$ being distinct. The sets $E_k$ (are modified $F_k$'s) and constructed by induction. The main tool will be a well-known theorem of Turan's in extremal graph theory [4].

Proposition 6.1:

The maximal graph on $n$ vertices without an $1$-clique is achieved by splitting the $n$ vertices into $1$-1 sets of cardinality $[n/(1-\epsilon)]$ and $[n/(1-\epsilon)] + 1$ and placing an edge between any pair of vertices in different sets. If $n = (1 - 1)m + r$, 88
0 ≤ r < 1-1 then the cardinality of the number of edges of
this graph is \(1 + \binom{n}{2} - r\binom{m+1}{2} - (1-1-r)\binom{m}{2}\). The following
proposition follows trivially from proposition 6.1.

**Proposition 6.2:**

Let \(S\) be a set with \(|S| = n\). If \(A \subseteq P_2(S)\) (all 2-sub-
sets of \(S\)) with \(|A| \geq \frac{n(n-1)}{2} - \binom{n}{2}\) then \(A \supseteq P_2(B)\) for
\(B \subseteq S\) with \(|B| \geq \frac{n}{2}\).

**Proof:**

We think of \(S\) as the vertices of a graph \(G\) where an
edge \(\{a, b\}\) is in \(G\) if and only if \(\{a, b\} \in A\). We show that
if \(A\) has cardinality at least as much as above then \(G\) has
a \(n/2\) clique.

**Case 1:** If \(n = 2k\) for some \(k\), then set \(l = k + 1\), \(m = 2,\)
\(r = 0\), so that \(n = (1 - 1)m + r\). If
\(|A| \geq 1 + \binom{n}{2} - k\binom{2}{2} = 1 + \frac{n}{2}(n - 2)\) then there exists a \(B\)
s.t. \(|B| = n/2 + 1\) and \(A \supseteq P_2(B)\) by proposition 6.1.

**Case 2:** If \(n = 2k + 1\) for some \(k\) write \(n = (1 - 1)m + r \)
with \(l = k + 1\), \(m = 2, r = 1\). By proposition 6.1 if
\(|A| \geq \frac{(n-1)^2}{2} - 1\) then there exists \(B\) with \(|B| = \frac{n+1}{2}\) and
\(A \supseteq P_2(B)\).

So the result follows by comparing case 1 and case 2. □
Remark 6.1:

If \( S = \{1, 2, \ldots, 2n\} \) then put
\[
A = \{\{a, b\} \mid 1 \leq a \leq n, \ n + 1 \leq b \leq 2n\}.
\]
Then \( |A| = \frac{n^2}{2} \)
yet \( A \not\subseteq P_2(B) \) for any \( B \) with \( |B| > 3 \). This shows the
sharpness of proposition 6.1.

Remark 6.2:

If \( |S| = n \) and \( n > N(q) \) and \( A \subseteq P_2(S) \) is such that
\( |A| > \binom{n}{2} - \binom{2}{2} \) then by Ramsey's theorem \( A \supseteq P_2(B) \) for some
\( B \) with \( |B| = q \). Unfortunately \( q \) is only about \( \log n \) (see [18]).
For our application we need the size of \( B \) to be proportional
to \( n \).

We now start the inductive construction. Since some
of the details are cumbersome, we shall not give all details
especially if it is obvious as to what to do.

Proposition 6.3:

There is a \( \Lambda(4) \) set in \( \mathbb{Z}(p^\infty) \) which is not \( \Lambda(4 + \varepsilon) \)
for all \( \varepsilon > 0 \).

Proof:

Assume \( E_1, \ldots, E_k \) have been constructed with the two
properties discussed above (and so \( |R(\bigcup_{j \leq k} E_j, 2, \gamma)| \leq 1 \) for
all \( \gamma \in \mathbb{Z}(p^\infty) \)). Denote \( E = \bigcup_{j \leq k} E_j \) and let \( E' = E_{k+1} \) which
is to have the properties (and will be constructed below)
that \( E' \subseteq \mathbb{Z}(p^{n_{k+1}}) + x_{k+1} \) for some \( n_{k+1} \in \mathbb{N} \) (\( n_{k+1} > n_k \)) and \( x_{k+1} \in \mathbb{Z}(p^{\omega}) \), \( |E'| \geq c p^{n_{k+1}/2} \) and \( |R(E \cup E', 2, \gamma)| \leq 1 \) for all \( \gamma \in \mathbb{Z}(p^{\omega}) \). First choose \( F_1 \subseteq \mathbb{Z}(p^m) \), \( n_{k+1} = m > n_k \) (\( m \) is much bigger than \( n_k \)), we will choose \( m \) so big that a number of properties will be satisfied. We leave its size unspecified because it will be clear that such an \( m \) will exist), and so that \( |F_1| > c p^{m/2} \) (all constants in this proof are denoted by \( c \) and are independent of \( n_k \)) and finally that 2-sums from \( F_1 \mod(p^m) \) are distinct according to proposition 4.2.

Considering the possible interactions between \( E \) and \( F_1 \) we have 3-cases which may violate \( R(E \cup F_1, 2, \gamma) \leq 1 \) for all \( \gamma \in \mathbb{Z}(p^{\omega}) \).

**Case 1:** \( a' + b' = c' + d; \) \( \{a', b', c', d\} \subseteq F_1 \), \( d \in E \)

\( \{a', b'\} \neq \{c', d\} \).

**Case 2:** (a) \( a' + b' = c + d; \) \( \{a', b'\} \subseteq F_1 \), \( \{c, d\} \subseteq E \)

\( \{a', b'\} \neq \{c, d\} \), and (b) \( a' + b = c' + d; \) \( \{a', c', d\} \subseteq F_1 \), \( \{b, d\} \subseteq F_1 \).

**Case 3:** \( a' + b = c + d \) and \( a' \in F_1 \), \( \{b, c, d\} \subseteq E \), \( \{a', b\} \neq \{c, d\} \).

We discuss each of these 3 cases separately. Our starting out assumption will be that \( E \cap F_1 = \emptyset \). We may assume this because \( m \) may be chosen so large that \( |F_1 \setminus E| \geq c p^{m/2} \). \( F_2 = F_1 \setminus E \) will be the new \( F_1 \). All
primed elements from this point will be from our possible new set and unprimed ones from the old set.

Case 1: We want to avoid \(a' + b' = c' + d', (a',b') \neq (c,d)\). It is enough to have \((F_2 + F_2 - F_2) \cap E = \emptyset\). By choosing \(n\) large enough \(E \subseteq \mathbb{Z}(p^n)\). Assume \(m\) much larger than \(n\) and \(F_2 \subseteq \mathbb{Z}(p^m)\) with \(|F_2| \geq cp^{m/2}\). Choose \(n'\) larger than \(m\) and pick \(x \in \mathbb{Z}(p^{n'}) \setminus \mathbb{Z}(p^m)\). Set \(F_3 = F_2 + x\). Then 
\[(F_3 + F_3 - F_3) \cap E = \emptyset \text{ otherwise } x \in \mathbb{Z}(p^m)\]. Also
\[|F_3| = |F_2|, F_3 \subseteq \mathbb{Z}(p^m) + x\text{ and }2\text{-sums out of }F_3 \text{ are still distinct in }\mathbb{Z}(p^\infty)\). \(F_3\) will be the new \(F_2\). Of course we may assume \(F_3 \cap E = \emptyset\) by taking \(m\) large and considering \(F_3 \setminus E\) if needed.

Case 3: We want to avoid \(a' + b = c + d\) with \((a',b) \neq (c,d)\). This time we want \((F_3 \cap E + E - E) = \emptyset\). It should be clear to the reader that the translation technique of case 1 will again work, giving a new set \(F_4 \subseteq \mathbb{Z}(p^m) + y\) for some \(y \in \mathbb{Z}(p^\infty)\). We should remark that when using the translation technique in succession we might have to translate using elements of larger and larger \(\mathbb{Z}(p^n)\)'s so as not to cancel the effect of previous translations. Again we may assume that \(F_4 \cap E = \emptyset\).

Case 2(a): We want to avoid \(a' + b' = c + d\). This time we want \((F_4 + F_4) \cap (E + E) = \emptyset\). Again this can be handled as above with a new set \(F_5 \subseteq \mathbb{Z}(p^m) + z\) for some \(z \in \mathbb{Z}(p^\infty)\).

Case 2(b): Now we want to avoid \(a' + b = c' + d\) with \((a',b) \neq (c',d)\). The fact that \(F_5 \cap E = \emptyset\) (which we may assume) and \((a',b) \neq (c',d)\) means that we may assume
a', b, c', d are all different. It is enough to show that
\((F_5 - F_5 \setminus \{0\}) \cap (E - E \setminus \{0\}) = \emptyset.\) Since differences
in \(F_5\) are unique, if we set \(G = (F_5 - F_5 \setminus \{0\}) \cap (E - E \setminus \{0\})\)
then by choosing \(m\) large we can have \(|G|\) as "close" to
\(|F_5 - F_5 \setminus \{0\}|\) as we want. Define a map
\(\phi: (F_5 \times F_5) \setminus \Delta \to (F_5 - F_5 \setminus \{0\})\) where
\(\Delta = \{(f, f) \mid f \in F_5\}\) by \(\phi(a', b') = a' - b'.\) Then \(\phi\) is bi-
jective. Define \(\psi: F_5 \times F_5 \setminus \Delta \to P_2(F_5)\) by \(\psi(a', b') = \{a', b'\}.\)
Then \(\psi\) is surjective with \(|\psi^{-1}(\{a', b'\})| = 2\) for all
\((a', b') \in P_2(F_5).\) Let \(A = \psi \phi^{-1}(G).\) Then \(|A|\) is as "close"
to \(|P_2(F_5)|\) as we want (by choosing \(m\) large). If we know
there exists \(B \subseteq F_5\) s.t. \(|B| \geq c|F_5|\) and \(P_2(B) \subseteq A\) then we
would be done by setting \(F_6 = B.\) That this can be done is
guaranteed by proposition 6.2. (by choosing \(m\) large enough).

Now \(E_{k+1} = F_6\) and \(m = n_{k+1}\) works. \(\square\)

For \(\Lambda(p)\) sets with \(p > 4\) we have some troubles. This
is because neither the translation technique nor the tech-
nique of case 2(b) (suitably generalized) helps in dealing
with the case e.g. when we want to avoid \(a' + b' + c = e' + f' + g\)
(using the notation of the proof) in the \(\Lambda(6)\) case. Trans-
lation obviously doesn't work and to use the other tech-
nique would mean that 4-sums from our new set (which we
want to adjoin) would have to be distinct (or at least meet
the requirement of proposition 3.2) in which case we only
would have the new construction being not $\Lambda(8 + \epsilon)$. In any case it is at least possible to show:

**Proposition 6.4:**

If $2 \leq k \in \mathbb{N}$ then there is a $\Lambda(2k)$ set which is not $\Lambda(4k - 4 + \epsilon)$ for all $\epsilon > 0$ in $\mathbb{Z}(p^\infty)$.

Let us also note that from the work of the previous sections we have as a particular consequence:

**Proposition 6.5:**

For any compact abelian group $G$ there is a $\Lambda(4)$ set in $G^*$ which is not $\Lambda(4 + \epsilon)$ for all $\epsilon > 0$. 
Recently G. Pisier proved the following (unpublished):
If $G$ is a compact abelian group with dual group $\Gamma$ and $A \subseteq \Gamma$ has $|A| = n$, $n \geq N$ ($N$ absolute), then given $\delta > 0$ there exists $B \subseteq A$ s.t. $|B| \geq n^{1-\delta}$ with $|R_2(B,2,\gamma)| \leq c(\delta)$ where $c(\delta)$ only depends on $\delta$ and not on $n$ (of course we don't care whether this statement is true for $n \geq N$ ($N$ absolute instead of $n \geq 1$)). The interest in such a statement is that $\lambda_{4+c}(B)$ would be large by suitably choosing $A$ (by proposition 3.1) and by choosing $\delta(c)$. On the other hand $\lambda_4(B) \leq f(c(\delta))$ for some $f$ by propositions 3.2 and 5.1.

Note that it is necessary to use $R_2$ instead of just $R$ since e.g. if $G = \mathbb{Z}(2)^{\mathbb{N}}$ then $\gamma + \gamma = e$ for all $\gamma \in G^*$. This bad behaviour is of course a reflection on the connectedness of $G$. If $G$ is connected then such behaviour doesn't arise, while $G = \mathbb{Z}(2)^{\mathbb{N}}$ is extremally disconnected.

One should therefore be able to glue such $B$'s together to find bad $\Lambda(4)$ sets. The problem of course is that one doesn't obtain $\Lambda(4)$ sets which are $\Lambda(4+c)$ for all $c > 0$. Also the proof is limited to $\Lambda(4)$ sets. The proof is a simple probabilistic argument similar in spirit to the method of Erdös described in section 4, but somewhat simpler (since the construction is random "most $B$'s work). Let
us finally point out that the gluing process could be non-trivial as seen in section 6. In proposition 7.1 we discuss some complements to the above result, which are proved in the same way as Pisier's result. One can ask what happens as \( \delta \to 0 \). The result below shows that we can at least get logarithmic growth in the \( \Lambda(4) \) constant of \( B \). Since the proofs are much the same we only prove (b).

**Proposition 7.1**

Let \( G \) be a compact abelian group with dual group \( \Gamma \) and let \( A \subseteq \Gamma \) with \( |A| = n \). Then we have the following for \( n \geq N \) (\( N \) absolute):

(a) (Pisier) Given \( \delta > 0 \), a random subset \( B \subseteq A \) with \( |B| \geq n^{1-\delta} \) has \( |R_2(B,2,\gamma)| \leq \lfloor 1/\delta \rfloor + 1 \) for all \( \gamma \in \Gamma \).

(b) A random subset \( B \subseteq A \) with \( |B| \geq \frac{n^{\frac{3}{2}}}{2} \) has \( |R_2(B,2,\gamma)| \leq \log n \) for all \( \gamma \in \Gamma \).

(c) A random subset \( B \subseteq A \) with \( |B| \geq \frac{n^{\frac{3}{2}}}{\log n} \) has \( |R_2(B,2,\gamma)| \leq \log n / \log \log n \) for all \( \gamma \in \Gamma \).

**Proof:**

(b) Let \( \{\xi_i\}_{i=1}^n \) be an independent identically distributed sequence of random variables on some probability space \((\Omega,\mathcal{F},\mathbb{P})\) with \( \mathbb{P}(\xi_i = 1) = \frac{1}{2} \frac{n}{n^{\frac{3}{2}}} \) and \( \mathbb{P}(\xi_i = 0) = 1 - \frac{1}{2} \frac{n^{\frac{3}{2}}}{n} \) for all \( 1 \leq i \leq n \). A random subset of \( A \) is \( B(\omega) = \{\gamma_i | \xi_i(\omega) = 1\} \) for \( \omega \in \Omega \) where \( A = \{\gamma_1, \ldots, \gamma_n\} \). Note that
\[ |B(\omega)| = \sum_{i=1}^{n} \zeta_i(\omega). \] Also note that for \( \gamma \in \Gamma \)

\[ |R_2(B,2,\gamma)| = \sum_{i=1}^{n} \zeta_i(\omega) \zeta_j(\omega) \]

\( \{ \gamma_i, \gamma_j \} \subseteq B(\omega) \)

\( \gamma_i \neq \gamma_j, \gamma_i + \gamma_j = \gamma \)

Fix \( \lambda > 1 \). Since \( P(\zeta_i \zeta_j = 1) = 1/4n \) and since the \( \zeta_i \) are independent we get,

\[ E(\lambda^{|R_2(B,2,\gamma)|}) = E(\lambda^{\sum_{i=1}^{n} \zeta_i \zeta_j}) \]

\[ = \prod_{i,j} E(\zeta_i \zeta_j) \]

\[ \leq (\frac{\lambda}{4n} + (1 - \frac{1}{4n}))^n |R_2(B,2,\gamma)| \]

(because \( |A| = n \))

\[ \leq (1 + \frac{1}{4n}(\lambda - 1))^n \]

\[ \leq \exp n \big(\frac{1}{4n} (\lambda - 1)\big) \]

So by Chebyshev’s inequality,

\[ P(\omega \mid |R_2(B,2,\gamma)| > \log n ) \leq \lambda^{-\log n} \exp \frac{\lambda - 1}{4} \]

Setting \( \lambda = 9 \) gives,

\[ P(\omega \mid |R_2(B,2,\gamma)| > \log n ) \leq \frac{e^2}{9 \log n} \]

So \( P(\text{there exists } \gamma \text{ s.t. } |R_2(B,2,\gamma)| > \log n ) \leq \binom{n}{2} \frac{e^2}{9 \log n} \)

\[ \leq \frac{e^2}{2} \frac{n^2}{9 \log n} < \frac{1}{2} \]

if \( n \geq N \) (\( N \) absolute). So we have
\[ P(\omega \mid |R_2(B(\omega), 2, \gamma)| < \log n \text{ for all } \gamma \in \Gamma) > \frac{1}{2} \text{ if } n \geq N. \]

On the other hand,

\[ P(\omega \mid |B(\omega)| > \frac{n^{\frac{1}{2}}}{2}) = P(\sum_{i=1}^{n} \xi_i(\omega) > \frac{n^{\frac{1}{2}}}{2}) \]

\[ = 1 - \sum_{1 \leq n^{\frac{1}{2}}/2}^{n^{\frac{1}{2}}} \binom{n}{i} \left(\frac{1}{2n} \right)^i \left(1 - \frac{1}{2n}\right)^{n-1} \]

\[ > 1 - 2n^{\frac{1}{4}} \left(\frac{2n^{\frac{1}{2}} - 1}{2n^{\frac{1}{2}} - \frac{1}{2}}\right)^n - \frac{n^{\frac{1}{2}}}{4} \]

\[ + 1 \text{ as } n \to \infty. \]

It follows that there exists \( N \in \mathbb{N} \) s.t. for \( n \geq N \) there exists \( B \) which satisfies the conclusion of (b). \( \Box \)

The result in proposition 2.1.1 and its analogies suggest the following problem of Pisier.

**Problem 7.1:**

(a) Given \( A \subseteq \Gamma, |A| = n, (\Gamma \text{ dual of a compact abelian } \text{G}) \) does there exist a subset \( B \subseteq A \) with \( |B| \geq c \, n^{\frac{1}{2}} \) and

\[ |R_2(B, 2, \gamma)| \leq c' \text{ where } c \text{ and } c' \text{ are independent of } A \text{ and } n? \]

(b) Can one pick such a \( B \) randomly?

Two partial answers are available. First in [25] it is shown that if \( G = S^1 \) and \( A \subseteq \mathbb{Z} \) has \( |A| = n \) then we may find \( B \subseteq A \) with \( |B| \geq c \, n^{\frac{1}{2}} \) and \( |R_2(B, 2, m)| \leq 1. \) Unfortunately the proof relies very heavily on properties of \( \mathbb{Z} \). Secondly
let $p$ be a prime $p \equiv 3 \pmod{4}$ and set $n = 2p$ and $V = n^2 + n + 1$. Let $A = \mathbb{Z}(V)$. Then for any $B \subseteq A$ with $|R_2(B, 2, a)| \leq 1$ for all $a \in A$, $|B| \leq n$. This follows easily from the fact that there are no finite projective planes of order $n$ (see [44]). This suggests that $c$ and $c'$ in problem 7.1(a) might be small and large respectively.

Finally G. Pisier informs us that a result similar to proposition 7.1(a) had been discovered some years earlier (unpublished) by Y. Katznelson.
IV.8. SOME RELATED RESULTS

The existence of $\Lambda(p)$ sets which are not $\Lambda(p + \epsilon)$ for all $\epsilon > 0$ creates some very strange situations. By use of the examples in previous sections, we get functions in $L_p$ whose Fourier coefficients grow strangely (this follows from the equivalent formulations in [43], also see [5],[32]), spaces without lust (which are translation invariant) and embed in spaces with nice properties (see [38]) and also some applications to multipliers (see e.g. [17]). The above type of sets are also known to give examples of translation invariant uncomplemented Hilbertian spaces in $L_p$ for various values of $p$ (see [40]). We point out a simple positive situation below. It was pointed out to us by W. Johnson that this observation had already been made for $L_p$ $(1 < p < \infty)$ by Pelczynski and Rosenthal (see [37]) with our proof being similar to theirs. Accordingly we refer the reader to [37] and we merely state the proposition below.

**Proposition 8.1:**

Let $X$ be a Banach space s.t.
1) $X$ has type 2 and embeds in a space with unconditional basis, or
2) $X$ has cotype 2 and has an unconditional basis.
Let $Y \subseteq X$ with $Y \cong \ell_2$. Then there exists $K < \infty$ (independent of $Y$, $K$ only depends on the type 2 constant and the unconditional basis constant in the first case and the cotype 2 and the unconditional basis constant in the second case) and $Z \subseteq Y$ with $d(Z, \ell_2) \leq K$ and a projection $P : X \to Z$ with $\|P\| \leq K$.

Recall that if $(n_k)_{k=1}^{\infty} \subseteq \mathbb{N}$ is a sequence such that $n_{k+1} > \lambda n_k$ for some $\lambda > 1$ then $[e^{i n_k t}]_{k=1}^{\infty}$ is isomorphic to $\ell_2$ and complemented in $H_1$ according to the classical gap theorem of Payley (see [36]). Pelczynski and Kwapien proved a generalization of this: If $X \subseteq H_1$, is such that $X \cong \ell_2$ then $X \cong Y$ with $Y$ complemented (see [26]). The proposition below is a slightly stronger form of their result.

**Proposition 8.2:**

There exists $0 < K < \infty$ such that if $X \subseteq H_1$ is such that $X \cong \ell_2$ then $X \cong Y$ with $d(Y, \ell_2) \leq K$ and there is a projection $P : H_1 \to Y$ with $\|P\| \leq K$.

**Proof:**

The proof follows at once from proposition 8.1, the fact that $H_1$ is cotype 2 and has an unconditional basis (see [7], [34] or [51]). $\square$
Remarks:

8.1) It is unclear to us as to the situation in the first case of proposition 8.1 when $X$ is merely type 2 or the situation when $X$ has cotype 2 and just embeds in space with unconditional basis but doesn't have an unconditional basis itself. Also can one construct an order continuous lattice with type 2 failing the conclusion? It is known that if $Y \subseteq X$ and $X$ is an order continuous lattice then $Y \supseteq Z$ with $Z$ having an unconditional basis (see [29]).

8.2) It is natural to conjecture that if $X$ has type $p > 1$ and has an unconditional basis then the conclusion of proposition 8.1 is true. This is not so. Linderstrauss and Tzafriri construct an Orlicz space (so it has even got a symmetric basis) which contains an $\ell_2$ (but no complemented ones) and has type $2 - \varepsilon$ for all $\varepsilon > 0$ and cotype $2 + \varepsilon$ for all $\varepsilon > 0$. (see [28]). This was pointed out to us by W. Johnson.

8.3) Finally suppose that $X$ has type $p > 1$ and is cotype 2 and $\ell_2 \hookrightarrow X$, does $\ell_2$ embed complementably in $X$? The finite dimensional version is true (see [39]).

8.4) The basic question for $\Lambda(p)$ sets for $p > 2$ is whether there exist $\Lambda(p)$ sets which aren't $\Lambda(p + \varepsilon)$ for all $\varepsilon > 0$. For $1 \leq p < 2$ the basic question is whether every $\Lambda(1)$ set is already $\Lambda(2)$ since it is an easy consequence of a theorem of Rosenthal that a $\Lambda(p)$ set is already a $\Lambda(p + \varepsilon)$ set for
some $c > 0$ if $1 \leq p < 2$ (see [1]). Another way of asking the question for $1 \leq p < 2$ is to ask whether every K-convex ideal of $L_1(G)$ has type 2.

For the definition of K-convexity, and its relationship to the type of a Banach space, see [39].
LIST OF REFERENCES


[51] P. Wojtaszczyk, The Franklin System is an Unconditional Basis in $H_1$, Preprint.