ANNALES DE L'INSTITUT FOURIER

D. J. HAJELA

Construction techniques for some thin sets in duals of compact abelian groups

Annales de l'institut Fourier, tome 36, n° 3 (1986), p. 137-166

<http://www.numdam.org/item?id=AIF_1986__36_3_137_0>

Ann. Inst. Fourier, Grenoble
36, 3 (1986), 137-166

CONSTRUCTION TECHNIQUES FOR SOME THIN SETS IN DUALS OF COMPACT ABELIAN GROUPS

by D.J. HAJELA

1. Introduction.

In this note 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], [4], [6], [23]) 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 $\epsilon > 0$.

We now describe the contents of this note 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 Γ is a $\Lambda(p)$ set if there exists a constant $A_{p,q} > 0$ such that,

$$\left\| \sum_{j=1}^{n} a_j \gamma_j \right\|_{L_p(G)} \leqslant A_{p,q} \left\| \sum_{j=1}^{n} a_j \gamma_j \right\|_{L_q(G)} \tag{1.1}$$

for some $0 < q < p$, for all $n \in \mathbf{N}$ and all $(a_j)_{j=1}^{n} \in \mathbf{C}^n$. 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 [23]).

In section 2 we show that in the dual of the Cantor group D^* (where $D = \{-1, 1\}^{\mathbf{N}}$) there exist $\Lambda(p)$ sets which are not $\Lambda(p+\epsilon)$ for any $\epsilon > 0$, where $p = 2k$ and $2 \leqslant k \in \mathbf{N}$. 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

Key-word: $\Lambda(p)$ sets.

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for D are some ideas from coding theory and in particular it was some remarks of Johnson, Schectman, and Wilson (unpublished) in the $p = 4$ case that led us to general case for D and subsequently to other groups.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 paper 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 $\mathbf{Z}$, $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$ (for an increasing sequence of primes (p_n)), $\mathbf{Z}(p^\infty) = \bigcup_{n \geqslant 0} \mathbf{Z}(p^n)$ (p a prime) and $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$. This is effected by using the results of [6], where this type of idea was used in showing that there are sets which are $\Lambda(p)$ for all $1 \leqslant p < \infty$ but which are not Sidon sets.

In section 4 we give construction for $\mathbf{Z}$ and $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$ While constructions for these two groups are known (see [23], [6]) we give a construction based on a theorem of Bose and Chowla [5] (which was used to assert the existence of finite projective planes). In this section we also generalize a method of Erdös (see [7]) 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 $p = 2k$, $2 \leqslant k \in \mathbf{N}$ almost all integer sequences are $\Lambda(p)$ but not $\Lambda(p + \epsilon)$. We also give in this section a more precise version of the growth of the $\Lambda(4)$ constant of the squares than in [23]. 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 $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$ for $p > 2$. It is shown that for $p > k \geqslant 2$ there are $\Lambda(2k)$ sets which are not $\Lambda(2k + \epsilon)$ for any $\epsilon > 0$ by using certain classical facts about symmetric polynomials. For $k \geqslant p$ 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 [19]).

In section 6 we turn to construction in $\mathbf{Z}(p^\infty) = \bigcup_{n \geq 0} \mathbf{Z}(p^n)$. It is shown that there are $\Lambda(4)$ sets which are not $\Lambda(4 + \epsilon)$ for all $\epsilon > 0$. 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 connection with the above results, one should mention a result of Pisier (unpublished). His result is: Given $A \subseteq G^*, |A| = n$ and given $\delta > 0$ $\exists B \subseteq A, |B| \geq n^{1/2-\delta}$ with $\lambda_4(B) \leq C_\delta$ (where C_δ doesn't depend on n and $\lambda_4(B)$ is the $\Lambda(4)$ constant of B). The interest in such a statement is that the $\Lambda(4 + \epsilon)$ constant of B should be large by suitably choosing $\delta(\epsilon)$. 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 $\Lambda(4 + \epsilon)$ for all $\epsilon > 0$. Also the proof is limited to $\Lambda(4)$ sets. Let us finally point out that the gluing process could be non-trivial as will be seen in section 6.

We will use standard notations and any notation not mentioned in the paper may be found in [22], [27] and [18]. Let us just mention that $|S|$ denotes the cardinality of a set S and $[x]$ denotes the greatest integer function for $x \in \mathbf{R}$.

We wish to thank P. Deligne, J. Fournier, W. Johnson, G. Pisier, D. Ray-Chaudhuri, K. Ross and G. Schectman for useful comments and communications.

2. Construction in the dual of the Cantor group.

In this section we construct a $\Lambda(2k)$ set in D^* which is not $\Lambda(2k + \epsilon)$, for all $\epsilon > 0$, $2 \leq k \in \mathbf{N}$, where $D = \{-1, 1\}^{\mathbf{N}}$ 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 $\epsilon_k : D \longrightarrow \{-1, 1\}$ be defined by $\epsilon_k(x) = x_k$ where $k \in \mathbf{N}$, $k \geq 1$. Then an element of the dual group D^* of D consists of finite products of the ϵ_k. Given a finite subset A of $\mathbf{N}$ let us write, $W_A = \prod_{j \in A} \epsilon_j$.

2.1 Preliminaries.

To construct $\Lambda(p)$ sets which are not $\Lambda(p+\epsilon)$ 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* $2 \leqslant m \in \mathbf{N}$ *and let* $n \in \mathbf{N}$ *such that* $n \geqslant [\log_2 m + 1] + 1$. *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* $k \in \mathbf{N}$, $1 \leqslant k \leqslant m$ *and let* $\{c_1, \ldots, c_k\} \subseteq A$ *and* $\{c_{k+1}, \ldots, c_{2k}\} \subseteq A$ *with* $\{c_1, \ldots, c_k\} \cap \{c_{k+1}, \ldots, c_{2k}\} = \phi$. *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 $n \geqslant [\log_2 m + 1] + 1$ and m is fixed. Regarding $GF(2^n)$ as a vector space over $GF(2)$ we have that dim $GF(2^n) = n$. So let $\{x_1, \ldots, x_n\} \subseteq GF(2^n)$ be a basis for $GF(2^n)$ over $GF(2)$. To $x \in GF(2^n)$ we associate the n-tuple of $0's$ and $1's (a_1^1, \ldots, a_n^1)$ where $x = \sum_{i=1}^{n} a_i^1 x_i$. In what follows we will always maintain the order of the $x_i's$ in any expansion of a given element of $GF(2^n)$. 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. $x^{2k-1} = \sum_{i=1}^{n} a_i^k x_i$ for $1 \leqslant k \leqslant m$. 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 $A = \{a(x) \mid x \in GF(2^n)\}$ 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 $n \geqslant [\log_2 m + 1] + 1$ assures us that such sets do exist for all $1 \leqslant k \leqslant m$). Pick $z_i \in GF(2^n)$ so that $a(z_i) = y_i$, $1 \leqslant i \leqslant 2k$. Now suppose that:

$$\sum_{i=1}^{k} y_i = \sum_{i=k+1}^{2k} y_i \,. \tag{2.1.1}$$

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

$$z_1^{2j-1} + \ldots + z_k^{2j-1} = z_{k+1}^{2j-1} + \ldots + z_{2k}^{2j-1} \tag{2.1.2}$$

for $1 \leqslant j \leqslant k$. Now since $\mathrm{GF}(2^n)$ has characteristic 2 the above condition forces:

$$z_1^j + \ldots + z_k^j = z_{k+1}^j + \ldots + z_{2k}^j \quad \text{for} \quad 1 \leqslant j \leqslant 2k-1 \,. \tag{2.1.3}$$

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

$$\det \begin{bmatrix} 1 & z_1 & z_1^2 & \ldots & z_1^{2k-1} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 1 & z_j & z_j^2 & \ldots & z_j^{2k-1} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 1 & z_{2k} & z_{2k}^2 & \ldots & z_{2k}^{2k-1} \end{bmatrix} = 0 \,.$$

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 $\overline{\lim} \, |A| / |S|^{1/m} \leqslant 1$ (as $|S| \longrightarrow \infty$). In the proposition the set A has

$$|A| = 2^n = |\{0,1\}^{nm}|^{1/m} \,.$$

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 $1 \leqslant m \in \mathbf{N}$ 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 $k_1, \ldots, k_{m-1} \in \mathbf{N}$, $2 \leqslant k_1 < \ldots < k_{m-1}$ s.t. the conditions $\sum_{i=1}^{k} x_i^{k_j} = \sum_{i=k+1}^{2k} x_i^{k_j}$ $j = 1, \ldots, m-1$, k fixed, $k \leqslant m$ and the condition $x_1 + \ldots + x_k = x_{k+1} + \ldots + x_{2k}$ for $x_i \in \mathrm{GF}(p^n)$ force the conditions

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j \qquad j = 1, \ldots, 2k-1.$$

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 $j \leqslant 2m - 1$ can be written as $j = 2^l j_1$ 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

$$\mathrm{A} = \{(x, x^2) \mid x \in \mathrm{GF}(p^n)\}$$

(here we expand x and x^2 in tuple fashion regarding $\mathrm{GF}(p^n)$ as a vector space over $\mathrm{GF}(p)$). Then $|\mathrm{A}| = p^n$ while

$$|\{0, 1, \ldots, p-1\}^{2n}| = p^{2n}$$

and if a, b, c, d are 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 solution with $\{x, y, w, z\} \subseteq \mathrm{GF}(p^n)$ and with x, y, w, z being distinct.

2.1.4) With $m = 2$ in proposition 2.1.1 the proof shows that $\mathrm{A} = \{(x, x^3) \mid x \in \mathrm{GF}(2^n)\}$ 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 [26]). This resemblance was pointed out to us by D.K. Ray – Chaudhuri.

2.2 The Construction.

To begin with we set up a correspondance between certain subsets of the Walsh functions and the sets constructed in the proposition. Fix $2 \leqslant m \in \mathbf{N}$ and choose any $n \geqslant [\log_2 m + 1] + 1$. Let W_k be the Walsh functions generated by $\epsilon_1, \ldots, \epsilon_k$. 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} and 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 then $\prod_{i=1}^{k} W_{A_i} \neq \prod_{i=k+1}^{2k} W_{A_i}$ provided that $k \leqslant m$.

Now pick n_1 so that $n_1 = \min \{2^j \mid 2^j \geqslant [\log_2 m + 1] + 1\}$. Now define $n_{j+1} = 2n_j$ for $j \geqslant 1, j \in \mathbf{N}$. Finally put $E = \bigcup_{j \geqslant 1} A_{mn_j}$. Note that $A_{mn_j} \subseteq A_{mn_{j+1}}$, by the construction and because $GF(2^{n_{j+1}}) \supseteq GF(2^{n_j})$ 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 $\Lambda(2m + \epsilon)$ set for all $\epsilon > 0$.

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 $\epsilon > 0$ and put $p = 2m + \epsilon$. Then $[W_{mn_j}]_p$ (closed linear span of W_{mn_j} in p-norm) is isometric to $l_p^{2^{n_j m}}$, for a fixed $j \geqslant 1$. 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 $\chi_I \in [W_{mn_j}]_p$ (of course here we are looking upon the $\epsilon_k{}'s$

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 $\Lambda(p)$ set then $\lambda_p(A_{mn_j}) \leqslant A$ where A is the $\Lambda(p)$ 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 enbeddable in $l_p^{2^{n_j m}}$ is less than 2^{n_j}. It follows $\lambda_p(A_{mn_j}) \longrightarrow +\infty$ as $j \longrightarrow +\infty$. This is a contradiction. We give a more precise computation of $\lambda_p(A_{mn_j})$ below. The proof here is easily adapted from [10].

PROPOSITION 2.2.1. – *For any* $m \geqslant 1$, $j \geqslant 1$ *and* $\epsilon > 0$ *we have that* $\lambda_p(A_{mn_j}) \geqslant c(p) \mid A_{mn_j} \mid^{1/2-m/p}$ *where* $p = 2m + \epsilon$ *and* $c(p) = 1/p^{1/2p}$.

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

$$\Big(\sum_{j=1}^{k} \mid a_j^2 \mid\Big)^{1/2} \leqslant \Big\| \sum_{j=1}^{k} a_j w_j \Big\|_p \leqslant \lambda_p(A_{mn_j}) \Big(\sum_{j=1}^{k} \mid a_j \mid^2\Big)^{1/2} \quad . \quad (2.2.1)$$

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

$$\begin{aligned} k^{p/2} &\leqslant \int_0^1 \Big\| \sum_{j=1}^{k} r_j(t)\, x_j \Big\|^p dt \\ &= \sum_{i=1}^{n} \int_0^1 \Big| \sum_{j=1}^{k} r_j(t)\, x_{j,i} \Big|^p dt \\ &\leqslant B_p \sum_{i=1}^{n} \Big(\sum_{j=1}^{k} \mid x_{j,i} \mid^2\Big)^{p/2} \end{aligned} \quad (2.2.2)$$

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

$$\Big(\sum_{j=1}^{k} |x_{j,i}|^2\Big)^{p/2} \leqslant \lambda_p^p\,(A_{mn_j}). \tag{2.2.3}$$

By plugging (2.2.3) into (2.2.2) and using that $B_p \leqslant p^{1/2}$ (for $p > 2$) it follows that,

$$k^{p/2} \leqslant B_p\, n\, \lambda_p^p\,(A_{mn_j}) = B_p\, k^m\, \lambda_p^p\,(A_{mn_j}) \leqslant p^{1/2}\, k^m\, \lambda_p^p\,(A_{mn_j}).$$

It follows that: $\lambda_p\,(A_{mn_j}) \geqslant c(p)\,|A_{mn_j}|^{1/2-m/p}$. □

We show next that $\lambda_{2m}\,(A_{mn_j}) \leqslant c$ where $c = c(m)$. It follows immediately that $\lambda_{2m}\,(E) \leqslant c$, since $A_{mn_j} \subseteq A_{mn_{j+1}}$.

PROPOSITION 2.2.2. – *For any* $m \geqslant 2$ *and* $j \geqslant 1$ *we have* $\lambda_{2m}\,(A_{mn_j}) \leqslant c$ *where* $c = c(m)$.

Proof. – Fix $j \geqslant 1$. Let $w_1, \ldots, w_N$ be the elements of $A_{mn_j}(N = 2^{n_j})$. Set $f = \sum_{j=1}^{N} a_i w_i$ where $(a_i)_{i=1}^{N} \in \mathbf{C}^N$ and set $A = \sum_{i=1}^{N} |a_i|^2$ and $B = \sum_{i \neq j} a_i \bar{a}_j\, w_i w_j$. We first observe that,

$$\Big|\int B^k\Big| \leqslant c_k\, A^k \tag{2.2.4}$$

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

$$\int B^k = \int \Big(\sum_{i \neq j} a_i \bar{a}_j\, w_i w_j\Big)^k$$

$$= \int \sum_{i_1 \neq i_1', \ldots, i_k \neq i_k'} a_{i_1} \bar{a}_{i_1'} \ldots a_{i_k} \bar{a}_{i_k'}\, w_{i_1} \ldots w_{i_k}\, w_{i_1'} \ldots w_{i_k'}.$$

By the second property in proposition 2.1.1

$$\int w_{i_1} \ldots w_{i_k}\; w_{i_1'} \ldots w_{i_k'} = 0$$

unless there is a pairing so that $i_j = i_l$ or i_n' for some l and n for each $1 \leqslant j \leqslant k$ and similarly for i_j' $(1 \leqslant j \leqslant k)$. So

$$\Big|\int B^k\Big| \leqslant \sum_{\text{all pairings}} |a_{i_1}|\,|a_{i_1'}| \ldots |a_{i_k}|\,|a_{i_k'}|. \tag{2.2.5}$$

For a fixed pairing P we certainly have

$$A^k \geqslant \sum_{P} |a_{i_1}|\ |a_{i_1'}| \cdots |a_{i_k}|\ |a_{i_k'}|$$

since A^k has all products of length k of squares i.e. $|a_i|^2$. Note that only a finite number of pairings exist and this number only depends on m (and k). So (2.2.4) follows.

Now $|f|^2 = \left(\sum_{i=1}^{N} a_i w_i\right)\left(\sum_{i=1}^{N} \bar{a}_i w_i\right) = A + B$.

It follows that $\|f\|_2^{2m} = A^m$ and

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

$$= A^m + \int m A^{m-1} B + \int \sum_{k \geqslant 2}^{m} \binom{m}{k} A^{m-k} B^k$$

$$= A^m + \sum_{k \geqslant 2}^{m} \binom{m}{k} A^{m-k} \int B^k.$$

So $$\|f\|_{2m}^{2m} = \left|\|f\|_{2m}^{2m}\right| \leqslant A^m + \sum_{k \geqslant 2}^{m} \binom{k}{m} A^{m-k} \left|\int B^k\right|$$

$$\leqslant A^m \left[1 + \sum_{k \geqslant 2}^{m} \binom{m}{k} c_k\right]$$

with the last inequality following by the use of (2.2.4). Setting $c^{2m} = c(m)^{2m} = 1 + \sum_{k \geqslant 2}^{m} \binom{m}{k} c_k$ we have

$$\|f\|_{2m}^{2m} \leqslant c^{2m} \|f\|_2^{2m} \quad \text{and so} \quad \|f\|_{2m} \leqslant c \|f\|_2 . \qquad \square$$

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_{mn_j} instead of "inductive" ones

(i.e. $A_{mn_j} \subseteq A_{mn_{j+1}}$). We choose to use the latter type of blocks just because this feature was implicit in the construction of proposition 2.1.1.

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 [6] and the proof in [6] was based on ideas in [23]. From now on if E is $\Lambda(p)$ 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 $L_p^E = \{f \in L_p \mid \hat{f}(\chi) = 0 \text{ if } \chi \notin E\}$.

PROPOSITION 3.1. – *Let* $G \subseteq \Gamma$ (*dual of some compact abelian group*) *be a group with* $|G| < +\infty$. *Let* Λ *be* $\Lambda(q)$ *for some* $q > 2$. *Then* $\lambda_q(\Lambda) \geqslant |G \cap \Lambda|^{1/2} / |G|^{1/q}$.

Remark 3.1. – It is obvious from [6] 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 [6]. It is an obvious modification of the proof in [6]. A similar estimate appears in [4] but the proof is somewhat different. We require the following definition.

DEFINITION 3.1. – *Let* Γ *be an abelian group and let* $2 \leqslant n \in \mathbf{N}$. *For all* $\Lambda \subset \Gamma$ *denote by* $R(\Lambda, n)$ *all functions*

$$f: \Lambda \longrightarrow N \text{ s.t. } \sum_{\chi \in \Lambda} f(\chi) = n.$$

For $\gamma \in \Gamma$, $R(\Lambda, n, \gamma)$ *denotes all* f *s.t.* $\sum_{\chi \in \Lambda} \chi^{f(\chi)} = \gamma$ and $f \in R(\Lambda, n)$.

PROPOSITION 3.2. – *Let* G *be a compact abelian group with dual group* Γ *and assume that* $|R(\Lambda, n, \gamma)| \leqslant M$ *for all* $\gamma \in \Gamma$ *and some* $\Lambda \subseteq \Gamma$. *Then* $\lambda_{2n}(\Lambda) \leqslant (M(n!))^{1/2n}$ (*here* $n \geqslant 2$).

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

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

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

Now by Holder's inequality

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

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

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

So $\|f\|_{2n}^{2n} = \sum |b_\gamma|^2$ (by Parseval's identity)

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

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

$$= M(n!) \left(\sum |a(x)|^2 \right)^n \quad \text{(by the multinomial expansion)}$$

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

So $\lambda_{2n}(\Lambda) \leqslant (M n!)^{1/2n}$. □

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 [6] for the purpose of studying Sidon sets. We start with the following obvious proposition (for a proof see [6]).

PROPOSITION 3.3. – *Let* G *be a compact abelian group and* H *a closed subgroup. Then* Λ *is a* $\Lambda(p)$ *set in* $(G/H)^*$ $(1 < p < \infty)$ *if and only if* Λ *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 [6].

PROPOSITION 3.4. – *Let* G *be an infinite abelian group. Then* G *contains a subgroup of one of the following types:*

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

Proof. – Let $\tau(G)$ be the torsion subgroup of G. If $\tau(G) \neq G$ then $G \supseteq \mathbf{Z}$. So assuming $\tau(G) = G$ write $G = \oplus G_p$ where G_p are the p-primary components. If there are infinitely many components then $G \supseteq \mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$. 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 [21]). Denote by $\alpha(B) = \sup_{b \in B} 0(b)$ where $0(b)$ is the order of b. If $\alpha(B) = +\infty$ then B will contain infinitely many cyclic groups in it's decomposition, so $B \supseteq \mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$. If $\alpha(B) < \infty$ then $G_p = B \oplus G_p/B$ (see [21]). If $G_p/B = \{0\}$ then $G_p = B$ and so B will contain infinitely many cyclic groups in its decomposition and so $B \supseteq \mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$. If $G_p/B \neq \{0\}$ then $G_p/B = \Sigma \oplus \mathbf{Q} \oplus \mathbf{Z}(p^\infty)$, because G_p/B is divisible. Since $\mathbf{Q}$ is not torsion and G_p is, $G_p/B = \Sigma \oplus \mathbf{Z}(p^\infty)$. So at least one $\mathbf{Z}(p^\infty)$ appears since $G_p/B \neq \{0\}$. It follows that $G \supseteq \mathbf{Z}(p^\infty)$. □

4. Constructions in $\mathbf{Z}$ and $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$

Constructions in $\mathbf{Z}$ and $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$ are well known ([23], [6]). We will give a slightly different type of construction here.

Our starting point is the following theorem of Bose and Chowla (see [5]).

PROPOSITION 4.1. – *Let* $m = p^n$ *(where* p *is a prime,* $n \in \mathbf{N}$*) and* $q = (m^{r+1} - 1)/m - 1$ *for some* $r \in \mathbf{N}$. *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* $d_{i_1} + \ldots + d_{i_r}$, $0 \leqslant i_1 \leqslant i_2 \leqslant \ldots \leqslant i_r \leqslant m$ *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 [6] with a different conclusion.

PROPOSITION 4.2. – *If* $n > 3m6^m$ *(for some* $m \in \mathbf{N}$*) then we can find* $A \subseteq \mathbf{Z}_n$ *such that* $|A| \geqslant \dfrac{n^{1/m}}{(3^{m+1}m)^{1/m}}$ *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* $1 \leqslant i_1 \leqslant \ldots \leqslant i_m$.

Proof. – Choose n as above. Set $x = \dfrac{n^{1/m}}{3^{(1/m)+1}m^{1/m}}$. Then $x > 2$ and so there exists a prime p (by Bertrands's theorem, [15]) s.t. $[x] + 1 < p < 2[x] + 2$. So $x < p < 2x + 2 < 3x$ (since $x > 2$) i.e. there exists a prime p s.t. $\dfrac{n^{1/m}}{3^{1/m+1}m^{1/m}} < p < \dfrac{n^{1/m}}{3^{1/m}m^{1/m}}$.

Set $q = \dfrac{p^{m+1}-1}{p-1}$. By proposition 4.1 there exists $a_1, \ldots, a_p$ (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

$$a_{i_1} + \ldots + a_{i_m} < mq < 3p^m m < n.$$

So the m-sums are also distinct mod n. Also

$$|A| = p > \frac{n^{1/m}}{3^{1/m+1}m^{1/m}} = \frac{n^{1/m}}{(3^{m+1}m)^{1/m}}. \qquad \square$$

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 $\epsilon > 0$, $\pi((1+\epsilon)n) - \pi(n) \longrightarrow +\infty$ as $n \longrightarrow +\infty$ (and so there is a prime $p, n < p < (1+\epsilon)n$ if n is large) by the prime number theorem. This would have yielded a somewhat larger set A 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 $\mathbf{Z}$ which are not $\Lambda(2k+\epsilon)$, for all $\epsilon > 0$.

PROPOSITION 4.3. – *There is a set* $F \subseteq \mathbf{Z}$ *which is* $\Lambda(2k)$ *but not* $\Lambda(2k+\epsilon)$ *for* $\epsilon > 0$, *where* $k \geqslant 2$.

Proof. – Let (p_n) be an increasing sequence of primes. By proposition 4.1 there exist sets $E_n \subseteq \mathbf{Z}$ s.t. $|E_n| \geqslant p_n$, $E_n \subseteq \left[0, \frac{p_n^{k+1}-1}{p_n - 1}\right]$ s.t. k-sums out of E_n are distinct (we are now adding in $\mathbf{Z}$ and looking upon these sums). Set $F_1 = E_1$ and set $a_i = k \max F_{i-1}$ (for $i \geqslant 2$) and $F_i = a_i E_i$. Set $F = \bigcup_{i \geqslant 1} F_i$. It is clear that F is $\Lambda(2k)$ by proposition 3.2. To see F is not $\Lambda(2k+\epsilon)$, let $A_n = \left\{ a_n m \mid m \in \mathbf{N}, 0 \leqslant m \leqslant \frac{p_n^{k+1}-1}{p_n - 1} \right\}$ and note that $|F_n \cap A_n| \geqslant p_n \geqslant \frac{1}{(k+1)^{1/k}} |A_n|^{1/k}$. By a theorem of Rudin the cardinality of the intersection of a $\Lambda(2k+\epsilon)$ set with an arithmetic progression can't be so large (see [23], 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 $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$, one may build analogous examples.

PROPOSITION 4.4. – *There is a set* $E \subseteq \mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \oplus \ldots$ *which is* $\Lambda(2k)$ *but not* $\Lambda(2k+\epsilon)$.

Proof. – Assume without loss of generality that $p_n > 3k6^k$ for all $n \geqslant 1$. By proposition 4.2. there exists $E_n \subseteq \mathbf{Z}(p_n)$ s.t.

$|E_n| \geqslant \dfrac{p_n^{1/k}}{(3^{k+1}k)^{1/k}}$ 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 $\mathbf{Z}(p_1) \oplus \mathbf{Z}(p_2) \ldots$ in the cannonical fashion. By proposition 3.2 E is $\Lambda(2k)$ and since

$$\lambda_{2k+\epsilon}(E) \geqslant |E \cap \mathbf{Z}(p_n)|^{1/2} / p_n^{1/2k+\epsilon}$$

$$\geqslant \frac{1}{(3^{k+1}k)^{1/k}} p_n^{1/2k-1/2k+\epsilon} \longrightarrow +\infty \quad \text{as} \quad n \longrightarrow +\infty$$

(by proposition 3.1), E is not $\Lambda(2k+\epsilon)$. □

Remark 4.1. – Notice that the growth "locally" of $\lambda_{2k+\epsilon}(E)$ 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 $\mathbf{Z}$ by considering a method of Erdös. We first introduce a biased coin tossing space on the set of integer sequences Ω (increasing subsequences of $\mathbf{N}$). Let X_n be 2-valued random variables (independent) for $n \geqslant 1$, with $P(X_n = 0) = 1 - p_n$ and $P(X_n = 1) = p_n$ for $0 < p_n < 1$ and $(p_n)_{n=1}^{\infty}$ a given sequence. It is natural to call Ω a biased coin tossing space: The probability space on which the X_n's are defined can naturally be taken to be the Cantor set $D = \{0,1\}^{\mathbf{N}}$. 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 nth coordinate. Using the natural identification between Ω and D we have a coin tossing measure on Ω.

For different choices of (p_n) we get different probability spaces (though by a theorem of Kakutani [16] if p_n' is sufficiently close to p_n for all n, the spaces are the same). We denote a generic sequence of Ω by $(a_k)_{k=1}^{\infty}$. We always choose (p_n) so that $\sum_{n \geqslant 1} p_n = +\infty$. 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 [13]).

PROPOSITION 4.5. – *Let* $(X_n)_{n\geqslant 1}$ *be a sequence of independent random variables on a probability space* (Ω, F, μ). *Let* $S_n = \sum_{i\leqslant n} X_i$ *and suppose that:* 1) $E(X_i) > 0$ 2) $\lim_{i\to\infty} E(S_i) = +\infty$ 3) $\sum_{i\geqslant 1} \frac{\mathrm{Var}(X_i)}{E(S_i)^2} < +\infty$. *Then with probability* 1, *we have*

$$(S_n - E(S_n))/E(S_n) \longrightarrow 0.$$

As an immediate consequence we have in our case :

PROPOSITION 4.6. – *Let* $(X_n)_{n\geqslant 1}$ *and* Ω *be as in our case. If in addition to the previous conditions on* $(p_n)_{n=1}^{\infty}$ *we have*

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

then a.a. $\omega \in \Omega$

$$\frac{X_1 + \ldots + X_n}{p_1 + \ldots + p_n} \longrightarrow 1.$$

It follows that a.a. $\omega \in \Omega$ *we have*

$$\lim_{k\to+\infty} \frac{\sum_{i\leqslant a_k} p_i}{k} = 1$$

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* $2 \leqslant l \in \mathbf{N}$, $0 < \epsilon < 1/l$ *and set* $c = \frac{1 - l\epsilon}{l}$. *Let* $p_k = \frac{c}{k^{(1-1/l)+\epsilon}}$ *for* $k \in \mathbf{N}$. *Let* $(a_k)_{k=1}^{\infty} \in \Omega$ *be a random sequence. Then with probability* 1 *we have*

$$|R((a_k)_{k=1}^{\infty}, l, n)| \leqslant [1/l\epsilon]$$

except for finitely many n.

The case $l = 2$ is classical and due to Erdös and Renyi [8]. The proposition above is proved with some minor modifications to their proof. For a detailed proof in the case of $l = 2$ see [8]. 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 an* $0 < \epsilon < 1/l$ *s.t. with probability* 1 *we have* $a_k \sim k^{l+\delta}$.

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

$$\lim_{k \to \infty} \frac{\sum_{i \leqslant a_k} p_i}{k} = 1$$

since we have that

$$p_1 + \ldots + p_n = c \sum_{k \leqslant n} \frac{1}{k^{(1-1/l)+\epsilon}} \sim c \frac{n^{(1/l)-\epsilon}}{1/l - \epsilon} = n^{1/l-\epsilon}$$

and since $\sum_{n \geqslant 1} \frac{p_n(1-p_n)}{(p_1 + \ldots + p_n)^2} \leqslant \sum_{n \geqslant 1} \frac{p_n}{(p_1 + \ldots + p_n)^2} < +\infty$ since $\sum_{n \geqslant 1} \frac{1}{n^{1+1/l+\epsilon}} < +\infty$. So $\lim_{k \to +\infty} \frac{a_k^{\frac{1-l\epsilon}{l}}}{k} = 1$ which implies $a_k \sim k^{l+\delta}$ by choosing $\epsilon = \frac{\delta}{l(l+\delta)}$. □

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* $l \in \mathbf{N}$, $l \geqslant 2$. *Set* $p = 2l$ *and let* $\eta > 0$. *Then a.a. subsequences* $A = (a_k)_{k=1}^{\infty}$, *are* $\Lambda(2l)$ *but not* $\Lambda(2l + \eta)$.

Proof. – By proposition 4.7 and proposition 3.2 a.a. subsequences A are $\Lambda(2l)$ and $a_k \sim k^{l+\delta}$ for any fixed δ, $0 < \delta < \eta/2$. One may now conclude that A is not $\Lambda(2l + \eta)$ by using Rudin's proposition on arithmetic progressions (see [23]), but an alternative argument is: By a theorem of Marcinkiewicz and Zygmund (see [27]), $[e^{it}, \ldots, e^{int}]_q \overset{k_q}{\cong} l_q^n$ for any $1 < q < \infty$ where the constant

of isomorphism k_q doesn't depend on n. If (a_k) is $\Lambda(2l+\eta)$ then the 2 and $2l+\eta$ norms agree on $(a_k)_{k=1}^{\infty}$, but we can pack $[n^{1/l+\delta}]$ a_k's in $1, \ldots, n$, so arguing as in proposition 2.2.1 we have that,

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

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

Note that the case $l=2$ in proposition 4.8 gives $a_k \sim k^{2+\delta}$ for any $\delta > 0$ being $\Lambda(4)$. This is a priori somewhat surprising in view of the fact that $a_n = n^2$ is not $\Lambda(4)$ (see [23]). One may give a refinement of this result by calculating $\lambda_4((k^2)_{k\leqslant n})$ by using essentially the same techniques as in [23]. We first recall the following result of Landau (see [14]) (and also due independently to Ramanujan (see [14])). This is the only additional result needed in the technique of [23].

PROPOSITION 4.10. – *Let* $x \in \mathbf{R}_+$. *Let* $B(x)$ *be the cardinality of* $n \leqslant x$, $n \in \mathbf{N}$ *which are representable as sums of two squares. Then* $B(x) \sim \dfrac{Kx}{(\log x)^{1/2}}$ *where* $K = \left(\dfrac{1}{2} \prod_{\substack{p=3 \pmod 4 \\ p \text{ prime}}} \dfrac{1}{1-p^{-2}}\right)^{1/2} = .764\ldots$

PROPOSITION 4.11. – *Let* $n \in \mathbf{N}$. *We have for all* $\epsilon > 0$ *there exists* $N_\epsilon \in \mathbf{N}$ *s.t.* $\lambda_4((k^2)_{1<k\leqslant n}) \geqslant (1-\epsilon)\, c(\log n)^{1/8}$ *where* $n \geqslant N_\epsilon$ *and* $c = \pi/2 \dfrac{2^{1/8}}{K^{1/4}}$ *where* K *is as in proposition 4.10.*

Remarks. – 4.2) It should be noted that while the previous constructions yielded $\Lambda(p)$ sets which were not $\Lambda(p+\epsilon)$ for all $\epsilon > 0$, the construction in proposition 4.9 is not uniform i.e. for a fixed $\eta > 0$ a.a subsequences $A = (a_k)_{k=1}^{\infty}$ are $\Lambda(2l)$ but not $\Lambda(2l+\eta)$. This may be the price one has to pay for random constructions.

4.3) It should be noted that $\lambda_4((k^2)_{1\leqslant k\leqslant n}) = O(n^\delta)$ 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 [15]) and because of proposition 3.2.

5. Construction in $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots (p > 2)$.

In this section we will show that for $p > m$ there is a $\Lambda(2m)$ set in $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$ which is not $\Lambda(2m + \epsilon)$ for all $\epsilon > 0$. For $m \geqslant p$ 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 $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$. 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 [6]. One may perform a modification of the proof in [6]. The modification of the proof of proposition 2.2.2 is much more cumbersome. We require the following definition:

DEFINITION 5.1. – *Let* Γ *be an abelian group and let* $2 \leqslant n \in \mathbf{N}, 2 \leqslant p \in \mathbf{N}$. *For* $\Lambda \subseteq \Gamma$ *denote by* $R_p(\Lambda, n)$ *all functions* $f: \Lambda \longrightarrow \mathbf{N}$ *s.t.* $f(X) \leqslant p - 1$ *for all* $X \in \Lambda$ *and* $\sum_{X \in \Lambda} f(X) = n$. *For* $\gamma \in \Gamma$, $R_p(\Lambda, n, \gamma)$ *denotes all* f *s.t.* $\prod_{X \in \Lambda} X^{f(X)} = \gamma$ *and* $f \in R_p(\Lambda, n)$.

PROPOSITION 5.1. – *Let* G *be a compact abelian group with dual group* Γ *and assume that* $\Lambda \subseteq \Gamma$ *has elements only of order* p, $p \geqslant 2$. *Also assume* $|R_p(\Lambda, m, \gamma)| \leqslant M$ *for all* $\gamma \in \Gamma$ *and for all* m *s.t.* $2 \leqslant m \in \mathbf{N}$, $m \leqslant n \in \mathbf{N}$. *Then*

$$\lambda_{2n}(\Lambda) \leqslant M^{1/2n} \left(\left[\frac{n}{p} \right] + 1 \right)^{1/n} (n!)^{1/n}.$$

We now turn to the construction of $\Lambda(q)$ sets in

$$\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots .$$

We will try to follow the ideas embodied in section 2. Fix $2 \leqslant m \in \mathbf{N}$. Suppose we could show the following for all $n \in \mathbf{N}$, $n \geqslant n(m)$: 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) $|A_n| \geqslant p^n$

2) If

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

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

Then identifying the dual group of $\mathbf{Z}(p)^{\mathbf{N}}$ with finite tuples of $0's, \ldots, p-1's$ as in section 2; we way construct the required types of $\Lambda(p)$ sets. This is done by patching the sets A_n as in section 2. $|A_n| \geqslant p^n$ and proposition 3.1 ensures that the patched set is not $\Lambda(2m+\epsilon)$ for all $\epsilon > 0$ 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 $\mathbf{Z}(p) \oplus \mathbf{Z}(p) \oplus \ldots$).

Proposition 2.1.1 suggests that A_n may be built by considering a suitable choice of $(k_i)_{i=1}^m \in \mathbf{N}^m$ and letting,

$$A_n = \{(x^{k_1}, \ldots, x^{k_m}) \mid x \in \mathrm{GF}(p^n)\}$$

with $1 = k_1 < k_2 < \ldots < k_m$ (we regard $\mathrm{GF}(p^n)$ as a vector space over $\mathrm{GF}(p)$ and expand x^{k_i} in a basis expansion and put in the coordinates in place of x^{k_i}, 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 $x \longrightarrow x^{k_1}$ is an automorphism for $\mathrm{GF}(p^n)$ (fixing $\mathrm{GF}(p)$). 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 $2 \leqslant m \in \mathbf{N}$ and p be a prime which are fixed. Let $n \in \mathbf{N}$, $\{y_1, \ldots, y_m\} \subseteq \mathrm{GF}(p^n)$ and

$$1 = k_1 < k_2 < \ldots < k_m$$

with the $k_i \in \mathbf{N}$ for all i. Consider the system of equations:

$$(*) \qquad \begin{aligned} x_1^{k_1} + \ldots + x_m^{k_1} &= y_1 \\ x_1^{k_2} + \ldots + x_m^{k_2} &= y_2 \\ &\vdots \\ x_1^{k_m} + \ldots + x_m^{k_m} &= y_m \end{aligned}$$

By a "solution" to this system we mean an $(x_1, \ldots, x_m) \in \mathrm{GF}(p^n)^m$ 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_i's, $1 = k_1 < k_2 < \ldots < k_m$ s.t.

$$g(n, y_1, \ldots, y_m, k_1, \ldots, k_m) \leqslant C$$

for some $C \in \mathbf{N}$ uniformly in n and $\{y_i, \ldots, y_m\}$? Of course one may replace uniformity in n by working in the algebraic closure $A = \bigcup_{n \geqslant 1} \mathrm{GF}(p^n)$ and considering the equivalent problem of getting a bound on the number of solutions (to (*) 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* $k_i = i$, $1 \leqslant i \leqslant m$ *then* $g(n, y_1, \ldots, y_m, 1, 2, \ldots, m) \leqslant m!$

Proof. – Fix $n \in \mathbf{N}$. 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 (*)) are the same is automatic since $p > m$. We will show that the assumption,

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

implies that set of x_i's, $1 \leqslant i \leqslant m$ counting multiplicity is the same as the set of x_i's $m+1 \leqslant i \leqslant 2m$ counting multiplicity. Let $y_1, \ldots, y_m$ be indeterminates adjoined to $\mathrm{GF}(p^n)$. 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 Newtons's identities (see [25]) the σ_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

$$(\lambda - x_1) \ldots (\lambda - x_m) = (\lambda - x_{m+1}) \ldots (\lambda - x_{2m})$$

for all $\lambda \in \mathrm{GF}(p^n)$. So some $x_i (1 \leqslant i \leqslant m)$ is the same as an x_j $x_j (m+1 \leqslant j \leqslant 2m)$. By relabelling the x_i's we can have $x_m = x_{2m}$. Cancelling these from the equations

$$\sum_{i=1}^{m} x_i^j = \sum_{i=m+1}^{2m} x_i^j, \quad j = 1, \ldots, m,$$

we may repeat the above argument with the equations

$$\sum_{i=1}^{m-1} x_i^j = \sum_{i=1}^{2m-1} x_i^j, \quad j = 1, \ldots, m-1$$

(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 $m \geqslant p$ the problem 5.1 is much more difficult and no solution seems to be known. The following remarks are due to P. Deligne.

Remarks. — 5.1) For a fixed set of y_i's, $\{y_1, \ldots, y_m\} \subseteq \mathrm{A}$ (see problem 5.1) if the variety of solutions consists of isolated points then by Bezout's theorem they are at most $\prod_1^m k_j$ of them. For Bezout's theorem see [20].

5.2) If there are infinitely many solutions to (*) on the algebraic closure A then there is a formal power series :

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

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 $\sum_i \mathrm{X}_i(t)^{k_j}$ 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 $g(n_j, y_1, \ldots, y_m, k_1^{(j)}, \ldots, k_m^{(j)}) \leqslant C$ 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 $k_1^{(j)} = 1$ for all j), some subsequence (n_j) of $\mathbf{N}$ s.t. $n_j \longrightarrow +\infty$ and for all $\{y_1, \ldots, y_m\} \subseteq \mathrm{GF}(p^{n_j})$.

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.

6. Construction in $\mathbf{Z}(p^\infty)$.

We construct a $\Lambda(4)$ set in $\mathbf{Z}(p^\infty)$ 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

$$E_k \subseteq \mathbf{Z}(p^{n_k}) + x_k$$

(for some $n_k \longrightarrow +\infty$, some $x_k \in \mathbf{Z}(p^\infty)$), $k = 1, 2, \ldots$ such that

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

2) $|R(\bigcup_k E_k, 2, \gamma)| \leqslant 1$ for all $\gamma \in \mathbf{Z}(p^\infty)$.

By the remark 3.1 and (1) it follows that $\bigcup_k E_k$ is not $\Lambda(4+\epsilon)$ for all $\epsilon > 0$ and proposition 3.2 and (2) insure that $\bigcup_k E_k$ 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 $F_k's$) are constructed by induction. The main tool will be a well-known theorem of Turan's in extremal graph theory [3].

PROPOSITION 6.1. — *The maximal graph on n vertices without an l-clique is achieved by splitting the n vertices into l-1 sets of cardinality* $\left[\frac{n}{l-1}\right]$ *and* $\left[\frac{n}{l-1}\right] + 1$ *and placing an edge between any pair of vertices in different sets. If*

$$n = (l-1)m + r, \quad 0 \leqslant r < l-1$$

then the cardinality of the number of edges of this graph is

$$1 + \binom{n}{2} - r\binom{m+1}{2} - (l-1-r)\binom{m}{2}.$$

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-subsets of* S) *with* $|A| \geqslant \frac{n(n-1)}{2} - \left(\frac{n}{2} - 1\right)$ *then*

$$A \supseteq P_2(B) \quad \text{for} \quad B \subseteq S \quad \text{with} \quad |B| \geqslant \frac{n}{2}.$$

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 $l = k+1$, $m = l$, $r = 0$, so that $n = (l-1)m + r$. If

$$|A| \geqslant 1 + \binom{n}{2} - k\binom{2}{2} = 1 + \frac{n}{2}(n-2)$$

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 $n = (l-1)m + r$ with $l = k+1$, $m = 2$, $r = 1$.

By proposition 6.1. if $|A| \geqslant \frac{(n-1)^2}{2} - 1$ 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

$$A = \{\{a, b\} \mid 1 \leqslant a \leqslant n,\ n+1 \leqslant b \leqslant 2n\}.$$

Then $|A| = \frac{n^2}{2}$ yet $A \not\supseteq P_2(B)$ for any B with $|B| \geqslant 3$. 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 $|A| > \binom{n}{2} - \binom{q}{2}$ then by Ramsey's theorem $A \supseteq P_2(B)$ for some B with $|B| = q$. Unfortunately q is only about log n (see [12]). 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* $\mathbf{Z}(p^\infty)$ *which is not* $\Lambda(4+\epsilon)$ *for all* $\epsilon > 0$.

Proof. – Assume $E_1, \ldots, E_k$ have been constructed with the two properties discussed above (and so $|R\left(\bigcup_{j \leq k} E_j, 2, \gamma\right)| \leqslant 1$ for all $\gamma \in \mathbf{Z}(p^\infty)$). 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 $E' \subseteq \mathbf{Z}(p^{n_{k+1}}) + x_{k+1}$ for some $n_{k+1} \in \mathbf{N}(n_{k+1} > n_k)$ and $x_{k+1} \in \mathbf{Z}(p^\infty)$, $|E'| \geqslant c p^{n_{k+1}/2}$ and $|R(E \cup E', 2, \gamma)| \leqslant 1$ for all $\gamma \in \mathbf{Z}(p^\infty)$. First choose $F_1 \subseteq \mathbf{Z}(p^m)$, $n_{k+1} = m > n_k$ (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 $|F_1| \geqslant c\, p^{m/2}$ (all constants in this proof are denoted by c and are independent of n_k) and finally that 2-sums from $F_1 \bmod (p^m)$ are distinct according to proposition 4.2.

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

Case 1 : $a' + b' = c' + d$; $\{a', b', c'\} \subseteq F_1$, $d \in E$ $\{a', b'\} \neq \{c', d\}$.

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

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 $E \cap F_1 = \phi$. We may assume this because m may be chosen so large that $|F_1 \backslash E| \geqslant c\, p^{m/2}$. $F_2 = F_1 \backslash E$ 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 $(F_2 + F_2 - F_2) \cap E = \phi$. By choosing n large enough $E \subset \mathbf{Z}(p^n)$. Assume m much larger than n and $F_2 \subset \mathbf{Z}(p^m)$ with $|F_2| > cp^{m/2}$. Choose n' larger than m and pick

$$x \in \mathbf{Z}(p^{n'}) \backslash \mathbf{Z}(p^m). \text{ Set } F_3 = F_2 + x.$$

Then $(F_3 + F_3 - F_3) \cap E = \phi$, otherwise $x \in \mathbf{Z}(p^m)$. Also

$$|F_3| = |F_2|, \quad F_3 \subseteq \mathbf{Z}(p^m) + x$$

and 2-sums out of F_3 are still distinct in $\mathbf{Z}(p^\infty)$. F_3 will be the new F_2. Of course we may assume $F_3 \cap E = \phi$ by taking m large and considering $F_3 \backslash E$ if needed.

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

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

Case 2 (b) : Now we want to avoid $a' + b = c' + d$ with $\{a', b\} \neq \{c'. d\}$. The fact that $F_5 \cap E = \phi$ (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

$$((F_5 - F_5) \backslash \{0\}) \cap (E - E) \backslash \{0\}) = \phi .$$

Since differences in F_5 are unique, if we set

$$G = (F_5 - F_5 \backslash \{0\}) \backslash (E - E] \{0\})$$

then by choosing m large we can have $|G|$ as "close" to

$$|F_5 - F_5 \backslash \{0\}|$$

as we want. Define a map $\phi : (F_5 \times F_5)\backslash\Delta \longrightarrow (F_5 - F_5)\backslash\{0\}$ where $\Delta = \{(f, f) \mid f \in F_5\}$ by $\phi(a', b') = a' - b'$. Then ϕ is bijective. Define $\Psi : F_5 \times F_5\backslash\Delta \longrightarrow P_2(F_5)$ by $\Psi(a', b') = \{a', b'\}$. Then Ψ 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. $|B| \geqslant c|F_5|$ 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. □

For $\Lambda(p)$ sets with $p > 4$ we have some troubles. This is because neither the translation technique nor the technique 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. Translation obviously doesn't work and to use the other technique 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* $2 \leqslant k \in \mathbf{N}$ *then there is a* $\Lambda(2k)$ *set which is not* $\Lambda(4k - 4 + \epsilon)$ *for all* $\epsilon > 0$ *in* $\mathbf{Z}(p^\infty)$.

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

THEOREM 6.5. – *For any compact abelian group* G *there is a* $\Lambda(4)$ *set in* G* *which is not* $\Lambda(4 + \epsilon)$ *for all* $\epsilon > 0$.

BIBLIOGRAPHY

[1] G. BACHELIS and S. EBENSTEIN, On $\Lambda(p)$ sets, *Pacific. J. Math.*, 54 (1974), 35-38.

[2] G. BENKE, An Example in the Theory of $\Lambda(p)$ Sets, *Bollettino U.M.I.*, (5) 14-A (1977), 506-507.

[3] B. BOLLOBAS, Graph Theory, An Introductory Course, *Graduate Texts in Math*, Vol. 63 (1979).

[4] A. BONAMI, Etude des Coefficients de Fourier des fonctions de $L^p(G)$, *Ann. Inst. Fourier*, Grenoble, 20, fasc. 2 (1970), 335-402.

[5] R. BOSE and S. CHOWLA, Theorems In The Additive Theory of Numbers, *Comment. Math. Helv.*, 37 (1962/1963), 141-147.

[6] R. EDWARDS, E. HEWITT and K. ROSS, Lacunarity for Compact Groups I, *Indiana University Math. Journal*, 21 (1972), 787-806.

[7] P. ERDOS, Problems and Results in Additive Number Theory, *Colloque sur la Théorie des Nombres*, Bruxelles (1955), 127-137.

[8] P. ERDOS and A. RENYI, Additive Properties of Random Sequences of Positive Integers, *Acta. Arith.*, 6 (1960), 83-110.

[9] P. ERDOS and J. SPENCER, *Probabilistic Methods in Combinatorics*, Academic Press, 1974.

[10] T. FIGIEL, J. LINDENSTRAUSS and V. MILMAN, The dimension of Almost Spherical Sections of Convex Bodies, *Acta. Math.*, 139 (1977), 53-94.

[11] C. GRAHAM and O.C. MCGEHEE, *Essays in Commutative Harmonic Analysis*, Springer-Verlag, 1979.

[12] R. GRAHAM, B. ROTHSCHILD and J. SPENCER, *Ramsey Theory*, Wiley Interscience, 1980.

[13] H. HALBERSTAM and K. ROTH, *Sequences*, Oxford University Press, 1966.

[14] G. HARDY, *Ramanujan*, Chelsea, 1959.

[15] G. HARDY and E. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford, 1938.

[16] S. KAKUTANI, On the Equivalence of Infinite Product Measures, *Ann. of Math.*, 49 (1948), 214-224.

[17] J. KOLMOS, M. SULYOK and E. SZEMEREDI, Linear Problems in Combinatorial Number Theory, *Acta. Math. Sci. Hungar.*, 26 (1975), 113-121.

[18] J. LINDENSTRAUSS and L. TZAFRIRI, *Classical Banach Spaces I*, Springer-Verlag, 1977.

[19] J. LOPEZ and K. ROSS, *Sidon Sets*, Marcel Dekker, 1975.

[20] D. MUMFORD, Introduction to Algebraic Geometry, *Harvard Lecture Notes*, 1967.

[21] J. ROTMAN, *The Theory of Groups*, Allyn – Bacon, 1973.

[22] W. RUDIN, *Fourier Analysis on Groups*, Interscience Publishers, 1962.

[23] W. RUDIN, Trigonometric Series With Gaps, *J. Math. Mech.*, 9 (1960), 203-227.

[24] H. RYSER, Combinatorial Mathematics, *Carus Mathematical Monographs* 14, Mathematical Association of America, 1963.

[25] B.L. VAN DER WAERDEN, *Modern Algebra*, Ungar, 1953.

[26] J.H. VAN LINT, Introduction to Coding Theory, *Graduate Texts in Mathematics*, 86, Springer-Verlag, 1980.

[27] A. ZYGMUND, *Trigonometric Series*, Cambridge University Press, 1959.

Manuscrit reçu le 30 septembre 1983
révisé le 23 août 1985.

D.J. HAJELA,
Bell Communications Research
435 South Street, MRE 2P-372
Morristown N.J. 07960 (USA).