COMBINATORICA 5 (3) (1985) 205—214

COUNTING POINTS IN HYPERCUBES AND CONVOLUTION MEASURE ALGEBRAS

D. HAJELA and P. SEYMOUR

Received 22 August 1983

It is shown that if A and B are non-empty subsets of $\{0, 1\}^n$ (for some $n \in \mathbf{N}$) then $|A+B| \geqq (|A||B|)^\alpha$ where $\alpha = (1/2)\log_2 3$ here and in what follows. In particular if $|A| = 2^{n-1}$ then $|A+A| \geqq 3^{n-1}$ which anwers a question of Brown and Moran. 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. Necessary and sufficient conditions are also given for $|A+B| = (|A||B|)^\alpha$. The above results imply the following improvement of a result of Talagrand [7]: if X and Y are compact subsets of K (the Cantor set) with $m(X), m(Y) > 0$ then $\lambda(X+Y) \geqq 2(m(X)m(Y))^\alpha$ where m is the usual measure on K and λ is Lebesgue measure. This also answers a question of Moran (in more precise terms) showing that m is not concentrated on any proper Raikov system.

1. Introduction

In this note we consider a problem in [1] (communicated to us by M. Talagrand): suppose $A \subseteqq \{0, 1\}^n$ with $|A| = 2^{n-1}$; is it true that $|A+A| \geqq 3^{n-1}$. We also consider the extremal problem of characterizing those sets $A \subseteqq \{0, 1\}^n$ with $|A| = 2^{n+1}$ such that $|A+A| = 3^{n+1}$.

We now describe the contents of this note more fully and also various previous results in this direction. In Section 2 we consider the following generalization of the problem of Erdős: suppose $A, B \subseteqq \{0, 1\}^n$, $A \neq \emptyset$, $B \neq \emptyset$ (i.e., A, B are non-empty subsets of the vertices of the n-cube, $[0, 1]^n$), then the number of midpoints of A, B i.e., $\left|\frac{A+B}{2}\right|$ is at least $(|A||B|)^\alpha$ where $\alpha = (1/2)\log_2 3$. Clearly this yields an affirmative answer to the 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 is the extremal conjecture. We also state necessary and sufficient conditions for $|A+B| = (|A||B|)^\alpha$. Weaker results of the above type were obtained by Talagrand (see [7]). As an immediate application we obtain the following result: suppose λ is the Lebesgue measure on $\mathbf{R}$ and let μ denote the usual Haar measure on the Cantor group $D = \{0, 1\}^{\mathbf{N}}$. If X and Y are analytic subsets of D with $\mu(X)\mu(Y) > 0$ then $\lambda(X+Y) \geqq 2(\mu(X)\mu(Y))^\alpha$ where α is as before (the addition of X and Y is with respect to

---

AMS subject classification (1980) : 10 E 05

the usual addition on **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 [7]) who showed that $\lambda(X+X)\geqq 2(2\mu(X)-1)$. Moran's interest in this was from the point of view of convolution measure algebras. It shows that μ can not 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 [7], but is actually somewhat simpler.

The notation we use is standard. For unexplained terminology from harmonic analysis see [3]. We wish to thank B. Baishanski, G. Edgar, W. Johnson and M. Talagrand for useful conversations regarding some of the material in this note.

A number of developments have come to our attention since this paper was originally submitted. Firstly W. Moran has brought to our attention joint work of his with G. Brown [2], where they prove independently of us the theorem on the measure of sums of analytic sets of D. He also brought to our attention the work of D. Woodall [8]. Woodall had obtained our theorem 2.1 with a similar proof. However he did not obtain the extremal characterizations which is the main part of our paper. Also in [8] is mentioned the work of R. Hall [4] who obtained some weaker results in regard to theorem 2.1. Also the inequality we conjectured in remark 2.1 has been proved very recently [5]. It gives a generalization of theorem 2.1 as was noticed in remark 2.1. We wish to thank W. Moran for his comments and the referee for telling us that lemma 2.1 may be found in [6].

2. Counting points in hyper-cubes

We start in this section by giving an affirmative answer to a generalization of a question in [1]. Recall the question from the Introduction: Given $A\subseteqq\{0,1\}^n$ with $|A|=2^{n-1}$, is it true that $|A+A|\geqq 3^{n-1}$? We show the following:

Theorem 2.1. *If* $A, B\subseteqq\{0,1\}^n$ *are non empty then* $|A+B|\geqq(|A||B|)^\alpha$ *where* $\alpha=(1/2)\log_2 3$.

Throughout this section α is $(1/2)\log_2 3$.

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

Theorem 2.2. *If* $A\subseteqq\{0,1\}^n$ *with* $|A|=2^{n-1}$ *then* $|A+A|\geqq 3^{n-1}$.

To prove Theorem 2.1 we need two elementary calculus lemmas (for lemma 2.2. 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 $n=0$, $a_0t^{\alpha_0}$ 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 $\frac{d}{dt}\frac{g(t)}{t^{\alpha_0}}=\sum_{k=1}^{n} a_k(\alpha_k-\alpha_0)t^{\alpha_k-\alpha_0-1}$ has at most $n-1$ zeros by induction. So by Rolle's Theorem $g(t)$ has at most n zeros. ∎

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* $(a,b)\in[0,1]\times\times[0,1]$ *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* $\max(g,h)\geqq 1$ *for all* $(a,b)\in[0,1]\times[0,1]$.

Proof. Assume $a\geqq b$ (the case $a\leqq b$ 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 $g(a,b)\geqq 1$. This leaves the points (a,b) with $a\geqq b$, $a<1$, $b>0$ 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 $(\partial g/\partial a)=0$ we get

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

So $g\geqq a^{\alpha-1}$ and so $g\geqq 1$. For $a=b$ we have to make a special argument since $g=h$ and $\max(g,h)$ is not differentiable. We only have to show that $\min_{x\in[0,1]} f(x)=1$ where $f(x)=x^{2\alpha}+(1-x)^{2\alpha}+x^\alpha(1-x)^\alpha$. We have $x\in[0,1]$ that,

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

$$f''(x)=(2\alpha)(2\alpha-1)x^{2\alpha-2}+(2\alpha)(2\alpha-1)(1-x)^{2\alpha-2}+\alpha(\alpha-1)x^{\alpha-2}(1-x)^\alpha-$$
$$-2\alpha^2x^{\alpha-1}(1-x)^{\alpha-1}+\alpha(\alpha-1)x^\alpha(1-x)^{\alpha-2}.$$

Then $f'(1/2)=0$, $f''(1/2)=(8\alpha^2-6\alpha)(1/2)^{2\alpha+2}>0$, and so f has a relative minimum at $1/2$ with $f(1/2)=1$ since $\alpha=(1/2)\log_2 3$. 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 $1/2$ and counting multiplicity, also note that $f(0)=f(1)=1$). Now,

$$\frac{f'}{\alpha x^\alpha(1-x)^{\alpha-1}}=\frac{2x^{\alpha-1}}{(1-x)^{\alpha-1}}-\frac{2(1-x)^\alpha}{x^\alpha}+\frac{1-x}{x}-1=t-2t^\alpha+2t^{1-\alpha}-1\equiv P(t),$$

with $t=(1-x)/x$. 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. In what is to follow, I^n denotes any set obtained from $[0,1]^n$ by translating it or rotating it in n-dimensional space:

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 $[0,1]^n$ $\left(\text{and } \frac{A+B}{2} \text{ as mid-points}\right)$. We assume the result true for $(n-1)$-dimensional cubes. Regarding $[0,1]^n$ as the cube (see Figure 2.1),

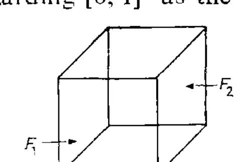

Fig. 2.1

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 we get from A and B on the face F_1 is,

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

Similarly, for the face F_2 we have

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

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 midway between F_1 and F_2) that,

$$\left|\frac{(A\cap F_1)+(B\cap F_2)}{2}\right| \geqq (a_1 b_2)^\alpha. \tag{2.3}$$

Adding the above inequalities we get

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

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

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

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 $p\in\mathbf{N}$ and $A_1,\dots,A_p\subseteq\{0,1\}^n$ that

$$|A_1+\dots+A_p| \geqq (|A_1||A_2|\dots|A_p|)^{\alpha_p}$$

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

Given $b=(b_1,\dots,b_p)\in[0,1]^p$ and $\pi\in S_p$ (the group of permutations on $\{1,\dots,p\}$) define

$$\begin{aligned} f_\pi(b) = {} & (b_{\pi(1)}\dots b_{\pi(p)})^{\alpha_p}+\big((1-b_{\pi(1)})\,b_{\pi(2)}\dots b_{\pi(p)}\big)^{\alpha_p}+ \\ & +\big((1-b_{\pi(1)})(1-b_{\pi(2)})\,b_{\pi(3)}\dots b_{\pi(p)}\big)^{\alpha_p}+\dots \\ & \dots+\big((1-b_{\pi(1)})\dots(1-b_{\pi(p)})\big)^{\alpha_p} \end{aligned}$$

and set $f(b)=\max_{\pi\in S_p} f_\pi(b)$. Is it true that $f(b)\geqq 1$? Equivalently without loss of generality by ordering so that $b_1\leqq\dots\leqq b_p$ it is enough to show that,

$$g(b) = (b_1\dots b_p)^{\alpha_p}+\big((1-b_1)\,b_2\dots b_p\big)^{\alpha_p}+\dots+\big((1-b_1)\dots(1-b)\big)^{\alpha_p} \geqq 1.$$

This was however not checked.

We now turn to an extremal conjecture: the conjecture is 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 simple. We need the following lemma.

Lemma 2.3. *If* $|A|=2^{n-1}$, $A\subseteqq\{0,1\}^n$ *and the points of* A *lie on a hyperplane* H *in* n*-dimensions then*

(a) $H = \{(x_1,\dots,x_n)\in\mathbf{R}^n|x_i=\varepsilon_i$ *for some fixed* $i\}$ *and*

$A = \{(x_1,\dots,x_n)\in\{0,1\}^n|x_i=\varepsilon_i\}$ (*here* $\varepsilon_i=0$ *or* 1); *or*

(b) $H=\{(x_1,\dots,x_n)\in\mathbf{R}^n|x_i-x_j=0\}$ *and* $A=E_1\cup E_2$ *where*

$E_1=\{(x_1,\dots,x_n)\in\{0,1\}^n|x_i=1,\ x_j=1\}$ *and*

$E_2=\{(x_1,\dots,x_n)\in\{0,1\}^n|x_i=0,\ x_j=0\}$; *or*

(c) $H=\{(x_1,\dots,x_n)\in\mathbf{R}^n|x_i+x_j=1\}$ *and* $A=E_1\cup E_2$ *where*

$E_1=\{(x_1,\dots,x_n)\in\{0,1\}^n|x_i=0,\ x_j=1\}$ *and*

$E_2=\{(x_1,\dots,x_n)\in\{0,1\}^n|x_i=1,\ x_j=0\}$.

Proof. The proof is easily seen by induction on n. Clearly it is true for $n=2$ and $n=3$. Assume it is true for n-dimensions. Let $|A|=2^n$, $A\subseteqq\{0,1\}^{n+1}$ and let the points of A lie on a hyperplane H in $n+1$ dimensions. If $A\subseteqq\{(x_1,\dots,x_{n+1})\in\mathbf{R}^n|x_{n+1}=\varepsilon\}$ where $\varepsilon=0$ or 1 then we are clearly in case (a). Otherwise $A\cap\{(x_1,\dots,x_{n+1})\in\mathbf{R}^n|x_{n+1}=\varepsilon\}\neq\emptyset$ for both $\varepsilon=0$ or 1. In this case it easy to see that $|A\cap\{(x_1,\dots,x_{n+1})|x_{n+1}=\varepsilon\}|$ is a power of 2 for both $\varepsilon=0$ and $\varepsilon=1$, say 2^m and 2^l. Since $m,l<n$ and $2^m+2^l=2^n$ it follows that $l=m=n-1$. Let $A_0=A\cap\{(x_1,\dots,x_{n+1})|x_{n+1}=0\}$ and let $A_1=A\cap\{(x_1,\dots,x_{n+1})|x_{n+1}=1\}$. Then by the induction hypothesis A_0 and A_1 lie on hyperplanes H_0 and H_1 respectively of the type in cases (a), (b) or (c). Since A also lies on a hyperplane H, it is now easy to see that H must be of the type in cases (a), (b) or (c). That A now must be of the types described in the lemma also follows since H must be of type (a), (b) or (c), $|A|=2^{n-1}$ and since A lies on H. ∎

In what is to follow we shall call hyperplanes of the sort in cases (b) and (c) of Lemma 2.3 "diagonal" hyperplanes. We can now prove the following proposition.

Proposition 2.1. *If* $|A|=2^{n-1}$, $A\subseteqq\{0,1\}^n$ *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 $n\geqq 1$, $|\{0,1\}^n+\{0,1\}^n|=3^n$. This is because by Lemma 2.3 the points of A are the vertices of a I^{n-1}. Given $1\leqq i_1<i_2<\dots<i_j\leqq n$, where $0\leqq j\leqq n$, define,

$$c(i_1,\dots,i_j) = \{(x_1,\dots,x_n)\in\{0,1\}^n|x_{i_k} = 1 \quad \text{for} \quad k = 1,\dots,j\}.$$

Then $|c(i_1,\dots,i_j)|=2^j$ and so

$$|\{0,1\}^n+\{0,1\}^n| = \sum_{j=0}^{n}\binom{n}{j}2^j = 3^n. \quad ∎$$

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

Theorem 2.3. *If* $A\subseteqq\{0,1\}^n$, $|A|=2^{n-1}$ *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 $(1/2, 1/2)$. So by the proof of Theorem 2.1 it follows that for $A, B \subseteq \{0,1\}^{n+1}$, $|A+B|=(|A||B|)^{\alpha}$ implies that one of the following four cases occurs (F_1 and F_2 are opposite n-dimensional faces of $[0,1]^{n+1}$).

Case 1; $|F_1 \cap A|=|F_1 \cap B|=0$.
Case 2; $|F_2 \cap A|=|F_2 \cap B|=0$.
Case 3; $|F_1 \cap A|=|F_2 \cap B|=0$ or $|F_2 \cap A|=|F_1 \cap B|=0$.
Case 4; $|F_1 \cap A|=|F_2 \cap A|$ 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 $[0,1]^{n+1}$. 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 does not occur since we have $A=B$.

Case 4; In this case $|F \cap A|=(1/2)|A|=2^{n-1}$ for all n-dimensional faces of F of $[0,1]^{n+1}$. It follows that $|(F \cap A)+(F \cap A)| \geqq 3^{n-1}$ 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 observations. First some terminology is needed. Regarding $[0,1]^{n+1}$ 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, that is $(n-1)$-dimensional) intersections of two n-dimensional faces and a set of "opposite edges" are the intersection of a "diagonal" hyperplane in $(n+1)$-dimensions with $[0,1]^{n+1}$). The point to note is that $|F \cap A|=(1/2)|A|$ 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 $[0,1]^{n+1}$ 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. To be specific let $C_1=\{(x_1, \ldots, x_{n+1}) | x_{n+1}=0\} \cap [0,1]^{n+1}$ and let $C_2=\{(x_1, \ldots, x_{n+1}) | x_{n+1}=1\} \cap [0,1]^{n+1}$.

The proof now splits into two cases, according to Lemma 2.3.

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 $[0,1]^{n+1}$ intersect A in equal cardinality it follows that $|G_1 \cap A|=|C_1 \cap A|=2^{n-1}$. It follows that A lies on a "diagonal" hyperplane in $(n+1)$-dimensional space. More precisely, suppose $C_2 \cap A=\{(x_1, \ldots, x_{n+1}) \in \{0,1\}^{n+1} | x_{n+1}=1, x_i=\varepsilon_i\}$ where ε_i is fixed and can be 0 or 1. Then by the above reasoning $C_1 \cap A=$

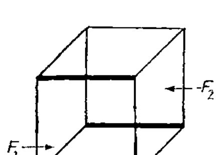

Fig. 2.2

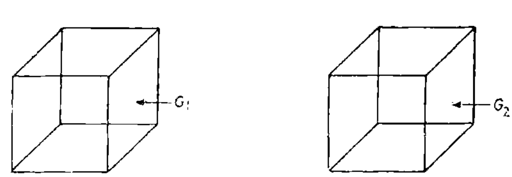

Fig. 2.3

$=\{(x_1, \dots, x_{n+1})\in\{0, 1\}^{n+1} | x_{n+1}=0, x_i=1-\varepsilon_i\}$. So A lies on the "diagonal" hyperplane $x_i+x_{n+1}=1$ in case $\varepsilon_i=0$ and $x_i-x_{n+1}=0$ in case $\varepsilon_i=1$.
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):

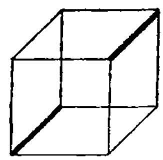

Fig. 2.4

Since opposite edges of $[0, 1]^{n+1}$ intersect A in equal cardinality it follows that $C_1\cap A$ also lies on a "diagonal" hyperplane in n-dimensional space. So the points of $C_2\cap A$ lie on a hyperplane in n-dimensions of the form $x_i-x_j=0$ or $x_i+x_j=1$ for some $1\leq i<j\leq n$ and the points of $C_1\cap A$ can lie on a hyperplane in n-dimensions of the form $x_k-x_l=0$ or $x_k+x_l=1$ for some $1\leq k<l\leq n$ (and so apriori there are $n(n-1)$ possibilities as to how $C_1\cap A$ can lie on a "diagonal" hyperplane). It is now easy to see that in case $C_2\cap A$ lies on the hyperplane $x_i-x_j=0$ (or $x_i+x_j=1$) then $C_1\cap A$ lies on the hyperplane $x_i-x_j=0$ (or $x_i+x_j=1$) and so A lies on the hyperplane in $n+1$ dimensions $x_i-x_j=0$ (or $x_i+x_j=1$). This is so because if the situation is not as described above then it is possible to find an n-dimensional face C_3 of $[0, 1]^{n+1}$ (i.e., an n-dimensional cube) such that $C_3\cap A$ is not on a hyperplane in n-dimensions (i.e., of the type described in Lemma 2.3). The above argument is illustrated when C_1 and C_2 are 3-dimensional cubes. Six subcases arise. $C_1\cap A$ can lie on opposite edges as shown in Figure 2.5 (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 (f) and that A in this case is on a "diagonal" hyperplane in 4 dimensions. For example, we show that the case of figure 2.5 (a) cannot occur (the other cases are dispensed with in the same manner). Suppose $C_1\cap A$ is as in Figure 2.5 (a) and $C_2\cap A$ as in Figure 2.4. Then $[0,1]^4$ looks as shown in Figure 2.6 (with edges between C_1 and C_2 drawn). Looking at the bottom most 3-dimensional cube C_3 (see Figure 2.6) we have ($C_3\cap A$ drawn in dots) in Figure 2.7. But $C_3\cap A$ is supposed to lie on a hyperplane which it does not.

Accordingly in all cases A lies on an $(n+1)$-dimensional hyperplane and the proof is complete. ∎

With some obvious modifications and extensions of the arguments above we can give necessary and sufficient conditions on $A\subseteq\{0, 1\}^n$, $B\subseteq\{0, 1\}^n$ so that $|A+B|=(|A||B|)^\alpha$. Since the proof is much the same as that of Theorem 2.3 we do not give it.

Theorem 2.4. *Let A and B be non-empty subsets of $\{0, 1\}^n$. Then $|A+B|=(|A||B|)^\alpha$ if and only if*

(a) $|A|=|B|=2^m$ *for some* $m\in\mathbf{N}$ *with* $m\leq n$.

(b) *A and B are the vertices of m-dimensional subcubes C_1 and C_2 of $[0, 1]^n$ respectively.*

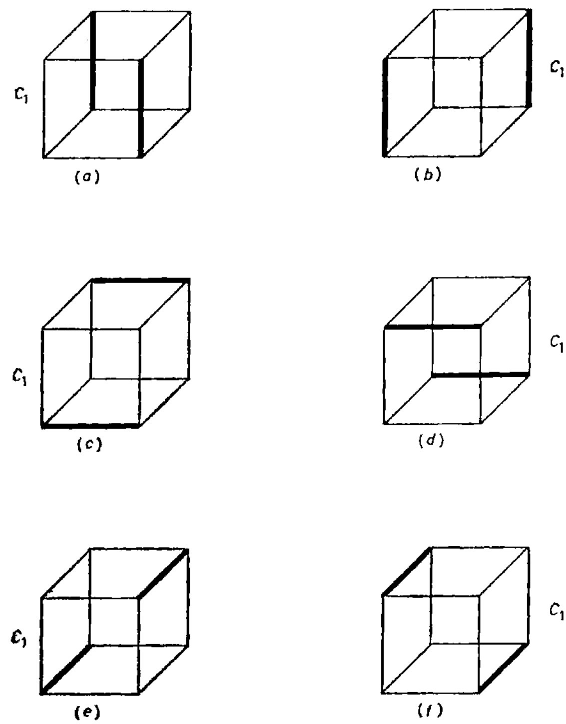

Fig. 2.5

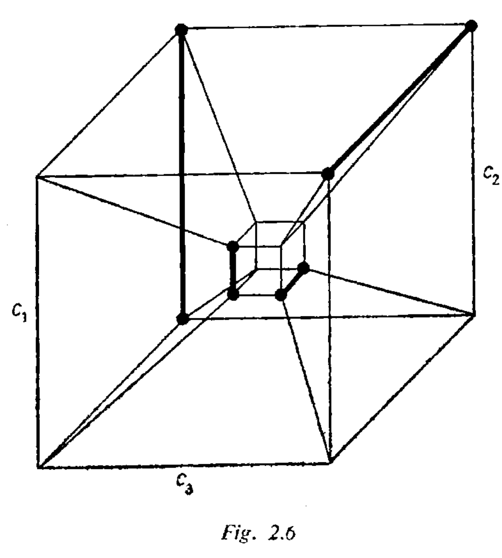

Fig. 2.6

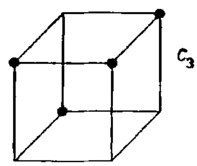

Fig. 2.7

(c) *C_2 is a translate of C_1 (in n-dimensions)*, i.e., *$C_2=C_1+z$ for some $z\in\mathbf{R}^n$.* ∎

We now show that as an immediate consequence of Theorem 2.1 we may obtain more precise results than the results of Talagrand [7] mentioned in the Introduction. We first need some notation. $D=\{0, 1\}^{\mathbf{N}}$ will denote the Cantor group (with the group operation being coordinate-wise addition modulo 2). Of course D is homeomorphic to the classical Cantor set $K\subseteq[0, 1]$. We make use of this association below freely without further mentioning it. Let μ denote the Haar measure on D, i.e., if μ_i is the measure $\mu_i\{0\}=\mu_i\{1\}=1/2$ on the i'th copy of $\{0, 1\}$ in $\{0, 1\}^{\mathbf{N}}$ then μ is the product measure $\mu=\bigotimes_{i=1}^{\infty}\mu_i$. Finally λ is the usual Lebesgue measure on $\mathbf{R}$. The proof below uses some of the same techniques as in [7], but is actually simpler.

Theorem 2.5. *If X and Y are analytic subsets of D such that $\mu(X)\mu(Y)>0$ then $\lambda(X+Y)\geqq 2(\mu(X)\mu(Y))^{\alpha}$.*

Proof. Assume with loss of generality that X and Y are compact subsets of D. Write $K_n=\bigcup_{d\in D_n} I_{n,d}$ where $I_{n,d}$ is the interval $I_{n,d}=\left[d, d+\frac{1}{3^n}\right]$ where D_n is the set of all numbers of the form $\sum_{k=1}^{n}\frac{d_k}{3^k}$ where $d_k\in\{0, 2\}$ for all k. Note that

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

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 $d=\sum_{k=1}^{n}\frac{d_k}{3^k}$ and $d'=\sum_{k=1}^{n}\frac{d'_k}{3^k}$ then $\frac{d+d'}{2}=\sum_{k=1}^{n}\frac{d_k+d'_k}{2}\frac{1}{3^k}=.\,d''_1\dots d''_n$ where $d''_k=\frac{d_k+d'_k}{2}$. Set $X_n=\bigcup_{I_{n,d}\cap X\neq\emptyset} I_{n,d}$ and $Y_n=\bigcup_{I_{n,d}\cap Y\neq\emptyset} I_{n,d}$. 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 $\lambda(X_n+Y_n)\geqq 2(\mu(X)\mu(Y))^{\alpha}$ 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 $|E|\leqq 2^n\mu(X^c)$ and $|F|\leqq 2^n\mu(Y^c)$. 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 $|E'|\geqq 2^n-2^n\mu(X^c)=2^n\mu(X)$ and $|F'|\geqq 2^n-2^n\mu(Y^c)=2^n\mu(Y)$. So by applying Theorem 2.1 we have that

$$|E'+F'| \geqq (2^n\mu(X)2^n\mu(Y))^\alpha = 3^n(\mu(X)\mu(Y))^\alpha.$$

So $\lambda(X_n+Y_n) \geqq 2(\mu(x)\mu(Y))^\alpha$ for all n, completing the proof. ∎

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 [7]) that if X is analytic then,
1) $\lambda(X+X) \geqq 2(2\mu(X)-1)$,
2) $\lambda(X+K) \geqq 2\mu(X)$.

Both of these inequalities are special cases of Theorem 2.5 since $x^{2\alpha} \geqq 2x-1$ and $x^\alpha \geqq x$ for $x \in [0, 1]$.

One application of Theorem 2.5 is to convolution measure algebras, especially to the measure algebra $M(\mathbf{R})$. Recall that a Raikov system R on $\mathbf{R}$ is a collection of Borel subsets of $\mathbf{R}$ such that

1) If $E \in \mathbf{R}$ and $F \subseteqq E$ is an F_σ subset of $\mathbf{R}$ 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 $x \in \mathbf{R}$.

Using R one may naturally define a closed ideal of $M(\mathbf{R})$ by $I(R) = \{v \in M(\mathbf{R}) | |v|(E)=0$ for all $E \in R\}$. Theorem 2.5 implies that μ (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 [7]. Notice also in connection with the above that the measure μ is an infinite Bernoulli convolution $\mu = \mathop{*}\limits_{j=1}^{\infty} \left[\frac{1}{2}\delta(0)+\frac{1}{2}\delta(3^{-j})\right]$ which has independent powers (i.e., $\mu^n \perp \mu^m$ whenever $0 \leqq m < n < \infty$). For further details on convolution measure algebras and Raikov systems, see [3].

References

[1] G. Brown and W. Moran, *L.M.S. Research Symposium on Functional Analysis and Stochastic Processes*, Durham (England), August 1974.

[2] G. Brown and W. Moran, Raikov Systems an Radicals in Convolution Measure Algebras, *J. London Math. Soc.*, **28** (1983), 531—542.

[3] C. Graham and O. C. McGehee, *Essays in Commutative Harmonic Analysis*, Springer-Verlag, 1979.

[4] R. Hall, A Problem in Combinatorial Geometry, *J. London Math. Soc.*, *(2)*, **12** (1976), 315—319.

[5] H. Landau, B. Logan and L. Shepp, An Inequality Conjectured by Hajela and Seymour Arising in Combinatorial Geometry, *Combinatorica*, **5** (1985), 337—342.

[6] G. Pólya and G. Szegő, *Problems and Theorems in Analysis*, Springer-Verlag, 1976.

[7] M. Talagrand. Solution d'un Probleme de R. Haydon, *Publications du Department de Mathematiques Lyon*, 12—2 (1975), 43—46.

[8] D. Woodall, A Theorem on Cubes. *Mathematika* **24** (1977), 60—62.

D. HAJELA and P. SEYMOUR

Bell Communications Research, Inc.
435 South Street
Morristown, NJ 07960
U.S.A.