ON EXTENSIONS OF THE GALE-BERLEKAMP SWITCHING PROBLEM AND CONSTANTS OF l_p—SPACES

BY

Y. GORDON AND H. S. WITSENHAUSEN

ABSTRACT

For positive integers n, m and real $p \geqq 1$, let

$$B_p(n,m) = \min_{\varepsilon_{ij}=\pm 1} \max_{\theta_i=\pm 1} \left(\sum_{j=1}^{m} \left| \sum_{i=1}^{n} \theta_i \varepsilon_{ij} \right|^p \right)^{1/p}.$$

Upper and lower bounds for this quantity are derived, extending results of Brown and Spencer for $B_1(n,n)$, corresponding to the Gale-Berlekamp switching problem. For a Minkowski space M of dimenson m, define

$$\delta(M) = \min_{\|x_i\|=1} \max_{\theta_i=\pm 1} \left\| \sum_{i=1}^{m} \theta_i x_i \right\|$$

a quantity investigated by Dvoretzky and Rogers.

In particular, for $n = m$, $1 \leqq p \leqq 2 \leqq q \leqq \infty$ one has

$$n \leqq B_q(n,n) \leqq h(n),$$

$$\left[2^{-n} n \sum_{i=0}^{n} \binom{n}{i} \left| n - 2i \right|^p \right]^{1/p} \leqq B_p(n,n) \leqq n^{1/p-\frac{1}{2}} h(n),$$

$$B_2(n,m) \leqq \left(mn\varphi \left(\frac{m}{n}\right)\right)^{\frac{1}{2}}$$

$$\delta(l_q^n) = n^{1/q} \text{ and } a_p n^{\frac{1}{2}} \leqq \delta(l_p^n) \leqq n^{-\frac{1}{2}} h(n)$$

where $h(n)$ is the smallest Hadamard number not less than n and $\lim n^{-1} h(n) = 1$ as $n \to \infty$, $\varphi(x) > 1$ is defined by $x(\varphi - 1 - \log \varphi) = \log 4$ and a_p is a constant depending only on p.

Received June 6, 1971 and in revised form December 10, 1971

1. The extended Gale-Berlekamp problem

For integers n, $m > 0$, real $p \geqq 1$ let ε denote any n by m matrix with entries ± 1 and θ any n-vector with components ± 1. Define

$$B_p(n,m) = \min_{\varepsilon} \max_{\theta} \left(\sum_{j=1}^{m} \left| \sum_{i=1}^{n} \theta_i \varepsilon_{ij} \right|^p \right)^{1/p}. \tag{1}$$

Consider an n by n board of lights with switches that complement the on/off status of all lights in any desired row or column. The Gale-Berlekamp switching problem is to find the minimum over all initial light patterns of the maximum over all switch positions of $|$ # lights off $-$ # lights on$|$. This is clearly [6]

$$\min_{\varepsilon} \max_{\theta\, \eta} \sum_{i,j=1}^{n} \theta_i \eta_j \varepsilon_{ij} \tag{2}$$

subject to $|\theta_i| = |\eta_j| = |\varepsilon_{ij}| = 1$, which is an alternative expression for $B_1(n,n)$.

In the space l_p^m, that is R^m with the l_p norm, let X denote the set of those vectors with components ± 1. Then the selection of ε amounts to the selection of a sequence of vectors $x_i \in X$, $i = 1, \cdots, n$. In these terms one has

$$\begin{aligned} B_p(n,m) &= \min_{x_i \in X} \max_{\text{signs}} \| \pm x_1 \pm x_2 \pm \cdots \pm x_n \| \\ &= \min_{x_i \in X} \max_{|u_i| \leqq 1} \left\| \sum_{i=1}^{n} u_i x_i \right\| \end{aligned} \tag{3}$$

by convexity. The extension to $p = \infty$ is trivial:

$$B_\infty(n,m) = \min_{\varepsilon} \max_{\theta} \max_{1 \leqq j \leqq m} \left| \sum_{i=1}^{n} \theta_i \varepsilon_{ij} \right| = n \tag{4}$$

by choice of $\theta_i = \varepsilon_{i1}$ for all i.

2. Monotonicity properties

LEMMA 1. *For $1 \leqq p \leqq \infty$ and positive integers n, m,*

(a) *$B_p(n,m)$ is nonincreasing in p for fixed n,m.*

(b) *$m^{-1/p}B_p(n,m)$ is nondecreasing in p for fixed n,m.*

(c) *$B_p(n,m)$ is nondecreasing in m for fixed p,n.*

(d) *$B_p(n,m)$ is nondecreasing in n for fixed p,m.*

PROOF. (a) and (b) hold for the minimax in (1) because the inequalities hold for any fixed choice of ε and θ; (c) holds because an additional term in the sum over j in (1) cannot make a negative contribution; (d) holds because the restriction $u_n = 0$ can only decrease the maximum in (3).

In particular for $1 \leqq p \leqq 2$ one has

$$B_p(n,m) \leqq m^{1/p-\frac{1}{2}} B_2(n,m) \tag{5}$$

and for $2 \leqq q \leqq \infty$ one has

$$n = B_\infty(n,m) \leqq B_q(n,m) \leqq B_2(n,m). \tag{6}$$

Also, if $a = \min(n,m)$ and $b = \max(n,m)$ one has for all $p \geqq 1$

$$B_p(a,a) \leqq B_p(n,m) \leqq B_p(b,b) \tag{7}$$

and clearly also

$$B_1(n,m) = B_1(m,n). \tag{8}$$

3. Hadamard numbers

A positive integer n is a Hadamard number if there exists an n by n matrix H with entries ± 1 such that $H^T H = nI$, that is, a Hadamard matrix.

Simple parity arguments show that a Hadamard number must belong to the set $\{1,2\} \cup \{4k;\ k \in Z^+\}$. Whether this set consists wholly of Hadamard numbers remains an open question, a positive answer to which would permit significant sharpening of some of the inequalities in the sequel.

For $n \in Z^+$ let $h(n)$ be the smallest Hadamard number not less than n.

A Kronecker product of Hadamard matrices is clearly again a Hadamard matrix, so that the Hadamard numbers form a monoid under multiplication. In particular, all integers of the form $2^a 12^b$, a, $b \geqq 0$ are Hadamard numbers. Since $\theta = \log 2/\log 12$ is irrational its positive multiples reduced modulo 1, are dense in the unit interval. This implies that

$$n \leqq h(n) \leqq n + o(n). \tag{9}$$

If all multiples of 4 are Hadamard numbers, then $h(n) \leqq n + 3$. In any case

$$h(n) \leqq 2n \tag{10}$$

since 2^a is Hadamard (corresponding to the Sylvester matrices*).

---

* The Kronecker powers of $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

4. Boundes for $B_2(n,n)$ and consequences

THEOREM 1. *One has $n \leqq B_2(n,n) \leqq h(n)$ with equality on the left if and only if n is a Hadamard number.*

PROOF. By (6) one has $n \leqq B_2(n,n)$. Equality is achieved for n a Hadamard number by letting ε be a Hadamard matrix, for indeed

$$\begin{aligned}\sum_j \left(\sum_i \theta_i\varepsilon_{ij}\right)^2 &= \sum_{i,j\,k} \theta_i\varepsilon_{ij}\theta_k\varepsilon_{kj} \\ &= \sum_{i,k} \theta_i\theta_k \sum_j \varepsilon_{ij}\varepsilon_{kj} = \sum_{i\,k} \theta_i\theta_k n\delta_{ik} \\ &= n \sum_i \theta_i^2 = n^2.\end{aligned}$$

If n is not a Hadamard number, then for any matrix ε there will be two distinct indices α, β such that $\Sigma_i\varepsilon_{i\alpha}\varepsilon_{i\beta} \neq 0$. Then letting $\theta_i = \varepsilon_{i\alpha}$ gives $\Sigma_j(\Sigma_i\theta_i\varepsilon_{ij})^2 \geqq (\Sigma_i\theta_i\varepsilon_{i\alpha})^2 + (\Sigma_i\theta_i\varepsilon_{i\beta})^2 = n^2 + (\Sigma_i\varepsilon_{i\alpha}\varepsilon_{i\beta})^2 > n^2$, so that $B_2(n,n) > n$.

By parts (c) and (d) of Lemma 1, one has

$$B_2(n,n) \leqq B_2(h(n),n) \leqq B_2(h(n),h(n))$$

and the right hand side is just $h(n)$ as shown above, completing the proof of Theorem 1.

By virtue of (9) one has

COROLLARY 1. $$\lim_{n\to\infty} n^{-1}B_2(n,n) = 1.$$

Using (6) one obtains

COROLLARY 2. *For* $2 \leqq q \leqq \infty$, $n \leqq B_q(n,n) \leqq B_2(n,n) \leqq h(n)$ *and*

$$\lim_{n\to\infty} n^{-1}B_q(n,n) = 1.$$

5. A Gilbert bound for $B_2(n,m)$

The Gilbert bounding technique of coding theory has been used to obtain asymptotic upper bounds on $B_1(n,n)$ [9], and $B_1(n,m)$ [1].

Here the same idea is used to obtain a bound on $B_2(n,m)$ valid for all finite n and m. This bound is applicable to $B_p(n,m)$ via (5) and (6).

If $B_2(n,m) \geqq b$ then for any of the 2^{nm} possible matrices ε there is at least one of the 2^n matrices with entries $\theta_i\varepsilon_{ij}$ for which $\Sigma_{j=1}^m(\Sigma_{i=1}^n\theta_i\varepsilon_{ij})^2 \geqq b^2$. It follows that if fewer than 2^{nm-n} distinct matrices ε satisfy $\Sigma_{j=1}^m(\Sigma_{i=1}^n\varepsilon_{ij})^2 \geqq b^2$, then $B_2(n,m) < b$.

Let ε_{ij} be a set of nm independent identically distributed random variables taking the values $+1$ and -1 with probabilities $\frac{1}{2}$. Then $X_j = \sum_{i=1}^{n} \varepsilon_{ij}, j = 1, \cdots, m$ is a set of m independent random variables, with the same centered symmetric binomial distribution with variance n. Let Y be a Gaussian random variable with mean zero and variance n. Efron [3] has observed that all even moments of X_1 beyond the second are strictly less than the corresponding moments of Y. Considering the exponential power series, this implies that for $\lambda > 0$

$$E\{e^{\lambda X_1^2}\} < E\{e^{\lambda Y^2}\}.$$

A Gilbert bound is any number b such that

$$P\left\{\sum_{j=1}^{m} X_j^2 \geqq b^2\right\} < 2^{-n}.$$

Using the Chernoff bound for this probability and the independence of the X_j one obtains

$$\begin{aligned} P\{\Sigma X_j^2 \geqq b^2\} &\leqq E\{e^{\lambda(\Sigma X_j^2 - b^2)}\} \\ &= e^{-\lambda b^2}[E\{e^{\lambda X_1^2}\}]^m \\ &< e^{-\lambda b^2}[E\{e^{\lambda Y^2}\}]^m \\ &= e^{-\lambda b^2}(1 - 2n\lambda)^{-m/2} \end{aligned}$$

for $0 < \lambda < 1/(2n)$, according to the moment generating function of the χ^2 distribution.

This expression is minimized by taking $2n\lambda = 1 - mnb^{-2}$, which gives the following equation for b

$$4\left(\frac{b^2}{mn}\right)^{m/n} = \exp\left(\frac{b^2 - mn}{n^2}\right). \tag{11}$$

Letting $\gamma = m/n$ and $\alpha = b^2/mn$ puts (11) into the form

$$\gamma = \frac{\log 4}{\alpha - 1 - \log \alpha} \tag{12}$$

suitable for calculation (with $\alpha > 1$). This establishes

THEOREM 2. *$B_2(n,m) \leqq (mn\phi(m/n))^{\frac{1}{2}}$ where $\phi(x) > 1$ is defined by $x(\phi - 1 - \log\phi) = \log 4$.*

In particular for $m \ll n$ one has $b \sim 1.18\, n$, while for $n \ll m$ one has $b \sim \sqrt{mn}$. For $m = n$, (12) only yields an insignificant improvement ($b \sim 1.9\, n$) over the bound $b = 2n$ obtainable from (10) and Theorem 1.

6. Bounds for $B_p(n, m)$ and consequences

Theorem 3. *For $1 \leqq p < \infty$ and integers n, m, the following inequality holds:*

$$B_p(n,m) \geqq \left[2^{-n} m \sum_{i=0}^{n} \binom{n}{i} |n-2i|^p\right]^{1/p}.$$

Moreover, there is equality if $m2^{-n+1}$ is an integer.

Proof. The set of 2^n distinct vectors

$$\varepsilon = \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{pmatrix}$$

where $\varepsilon_i = \pm 1$, has a subset E_0 of 2^{n-1} vectors such that for every two distinct vectors ε and ε' in E_0, $\varepsilon \neq \varepsilon'$ and $\varepsilon \neq -\varepsilon'$.

Given any n by m matrix (ε_{ij}) with entries ± 1, let $\eta(\varepsilon)$ denote the number of times in which the column ε or $-\varepsilon$ appears in (ε_{ij}). Then, $\sum_{\varepsilon\in E_0}\eta(\varepsilon) = m$. In addition, for any

$$\theta = \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix}$$

with $\theta_i = \pm 1$, one has

$$\sum_{j=1}^{m} \left|\sum_{i=1}^{n} \theta_i \varepsilon_{ij}\right|^p = \sum_{\varepsilon\in E_0} \eta(\varepsilon) \left|\sum_{i=1}^{n} \theta_i \varepsilon_i\right|^p,$$

therefore

$$B_p(n,m) = \min_{\substack{\Sigma\eta(\varepsilon)=m \\ \varepsilon\in E_0}} \max_{\theta} \left(\sum_{\varepsilon\in E_0} \eta(\varepsilon) \left|\sum_{i=1}^{n} \theta_i\varepsilon_i\right|^p\right)^{1/p}. \tag{13}$$

Suppose now that the minimum is attained for some sequence $\{\eta(\varepsilon)\}$ of non-negative integers, then for this sequence we have the inequality

$$B_p^p(n,m) \geqq 2^{-n} \sum_{\theta} \sum_{\varepsilon\in E_0} \eta(\varepsilon) \left|\sum_{i=1}^{n} \theta_i\varepsilon_i\right|^p$$

$$= 2^{-n} \sum_{\varepsilon\in E_0} \eta(\varepsilon) \sum_{\theta} \left|\sum_{i=1}^{n} \theta_i\varepsilon_i\right|^p = 2^{-n} \sum_{\varepsilon\in E_0} \eta(\varepsilon) \sum_{\theta} \left|\sum_{i=1}^{n} \theta_i\right|^p$$

$$= 2^{-n} m \sum_{\theta} \left|\sum_{i=1}^{n} \theta_i\right|^p = 2^{-n} m \sum_{i=0}^{n} \binom{n}{i} |n-2i|^p.$$

If $m2^{-n+1} = k$ is an integer, set $\eta(\varepsilon) = k$ for every $\varepsilon \in E_0$, then by (13) one has

$$B_p^p(n,m) \leqq m2^{-n+1} \sum_{\varepsilon \in E_0} \left| \sum_{i=1}^{n} \varepsilon_i \right|^p = m2^{-n} \sum_{i=0}^{n} \binom{n}{i} |n-2i|^p$$

and the proof is concluded.

REMARKS. We recall the definition of the p-absolutely summing constant of a Minkowski space (finite-dimensional Banach space) M [5]

$$\pi_p(M) = \max \left\{ \left(\sum_{i=1}^{n} \| x_i \|^p / \max_{\|a\|=1} \sum_{i=1}^{n} |\langle x_i, a\rangle|^p \right)^{1/p} \middle| \; x_i \in M (i = 1,2,\cdots,n) \text{ and } n = 1,2,3,\cdots \right\}.$$

Also, following the Game-Theory point of view of [10], $(\pi_p(M))^{-p} = (v_p(M))^p$ is the value of the zero-sum two player game in which the minimizer selects vector x on the boundary of the unit ball of M, while the maximizer selects vector a on the boundary of the unit ball of M^*, neither player having the knowledge of the other's selection, and the payoff is $|\langle x, a\rangle|^p$.

By [7]

$$\pi_p(l_1^n) = (n^{-p} 2^{-n} \sum_{i=0}^{n} \binom{n}{i} |n-2i|^p)^{-1/p}, \tag{14}$$

and in particular

$$\pi_1(l_1^n) = 2^{n-1} / \binom{n-1}{\left[\frac{n-1}{2}\right]} = n^{\frac{1}{2}} / c(n)$$

where $c(n) = \sqrt{2/\pi} + 0(n^{-1})$.

Let $r_i(t)$ $i = 1,2,\cdots$ be the Rademacher functions in the interval $[0,1]$. By [11, chap. V, th. 8.4] there exist constants a_p and b_p such that if $1 \leqq p < \infty$, then for any integer n and sequence $x_1, \cdots, x_n$ of scalars, the following inequality holds

$$a_p \left(\sum_1^n x_i^2 \right)^{\frac{1}{2}} \leqq \left(\int_0^1 \left| \sum_1^n x_i r_i(t) \right|^p dt \right)^{1/p} \leqq b_p \left(\sum_1^n x_i^2 \right)^{\frac{1}{2}}$$

where $a_p = 1$ if $p \geqq 2$ and $a_p \geqq 2^{1-2/p}$ if $1 \leqq p \leqq 2$, $b_p \leqq \sqrt{k}$ where $2k$ is the smallest even integer for which $2k \geqq p$.

By [5] Theorem 10 if $1 \leqq p \leqq 2 \leqq q < \infty$, then

$$\pi_1(l_1^n) \geqq \pi_p(l_1^n) \geqq n^{\frac{1}{2}} \geqq \pi_q(l_1^n) \geqq b_q^{-1} n^{\frac{1}{2}}.$$

In addition, $\pi_p(l_1^n)$ is increasing if n is increasing, and decreasing to 1 as p increases to ∞. Thus one has

COROLLARY 3. *If* $1 \leqq p \leqq 2$

$$n^{1+1/p}(\pi_p(l_1^n))^{-1} \leqq B_p(n,n) \leqq n^{1/p-\frac{1}{2}}h(n) = n^{1/p+\frac{1}{2}} + o(n^{1/p+\frac{1}{2}}).$$

PROOF. The right hand side inequality follows from (5), (9) and Theorem 1, and the left hand side from Theorem 3 and (14).

REMARK. Brown and Spencer [1] obtained the asymptotic inequality $B_1(n,n) \geqq (\sqrt{2/\pi} + o(1))n^{3/2}$, and Corollary 3 for $p=1$ improves it to $B_1(n,n) \geqq (\sqrt{2/\pi} + O(n^{-1}))n^{3/2}$.

COROLLARY 4. *If* $1 \leqq p < \infty$ *and* n, m *are integers then* $m^{1/p}n(\pi_p(l_1^n))^{-1} \leqq B_p(n,m) \leqq (2^{n-1}[m2^{-n+1}] + 2^{n-1})^{1/p}n(\pi_p(l_1^n))^{-1}$.

PROOF. The right hand side inequality holds by virtue of Lemma 1 (c) and the second part of Theorem 3, since

$$\begin{aligned} B_p(n,m) &\leqq B_p(n, 2^{n-1}[m2^{-n+1}] + 2^{n-1}) \\ &= (2^{n-1}[m2^{-n+1}] + 2^{n-1})^{1/p}n(\pi_p(l_1^n))^{-1}. \end{aligned}$$

The left hand side holds by Theorem 3. As a consequence

COROLLARY 5. $\lim_{m\to\infty} m^{-1/p}B_p(n,m) = n(\pi_p(l_1^n))^{-1}$.

In particular

COROLLARY 6. (i) $B_1(n,m) = B_1(m,n)$ *and*

$$\lim_{m\to\infty} m^{-1}B_1(n,m) = c(n)n^{\frac{1}{2}} = \sqrt{2n/\pi} + 0(n^{-\frac{1}{2}}).$$

(ii) $\lim_{m\to\infty} m^{-\frac{1}{2}}B_2(n,m) = n^{\frac{1}{2}}$.

Theorem 3 may be strengthened:

THEOREM 3*. *If* $1 \leqq p < \infty$ *and* n, m *are integers, then*

$$B_p(n,m) \geqq \max\{n, nm^{1/p}(\pi_p(l_1^n))^{-1}, c(m)nm^{1/p-1/2}\}.$$

PROOF. $B_p(n,m) \geqq B_\infty(n,m) = n$. Moreover,

$$\begin{aligned} B_p(n,m) &\geqq m^{1/p-1}B_1(n,m) = m^{1/p-1}B_1(m,n) \geqq m^{1/p}n(\pi_1(l_1^m))^{-1} \\ &= c(m)nm^{1/p-\frac{1}{2}}. \end{aligned}$$

The rest follows from Theorem 3.

7. Estimates for $B_p(n,m)$

LEMMA 2. *For* $1 \leqq p < \infty$ *and integers* k, m, n,

(i) $B_p(n, mk) \leqq k^{1/p} B_p(n,m)$

(ii) $B_p(nk, m) \leqq k B_p(n,m)$.

PROOF. (i) Let $\varepsilon^\circ = (\varepsilon^\circ_{ij})$ be an n by m matrix such that

$$B_p^p(n,m) = \max_{\theta_i = \pm 1} \sum_{j=1}^{m} \left| \sum_{i=1}^{n} \theta_i \varepsilon^0_{ij} \right|^p .$$

Let $(\varepsilon_{rs}) = (\underbrace{\varepsilon^\circ, \varepsilon^\circ, \cdots, \varepsilon^\circ}_{k})$ be the n by mk matrix. Then

$$B_p^p(n, mk) \leqq \max_{\theta_r = \pm 1} \sum_{s=1}^{mk} \left| \sum_{r=1}^{n} \theta_r \varepsilon_{rs} \right|^p$$

$$= \max_{\theta_r} \sum_{v=1}^{k} \sum_{s=(v-1)m+1}^{vm} \left| \sum_{r=1}^{k} \varepsilon_{rs}\theta_r \right|^p \leqq \sum_{v=1}^{k} \max_{\theta_r = \pm 1} \sum_{s=(v-1)m+1}^{vm} \left| \sum_{r=1}^{n} \theta_r \varepsilon_{rs} \right|^p$$

$$= k B_p^p(n,m).$$

(ii) Let ε° be as above, and let

$$(\varepsilon_{rs}) = \left. \begin{pmatrix} \varepsilon^\circ \\ \vdots \\ \varepsilon^\circ \end{pmatrix} \right\} k$$

be the nk by m matrix. Then

$$B_p^p(nk, m) \leqq \max_{\theta_r = \pm 1} \sum_{s=1}^{m} \left| \sum_{v=1}^{k} \sum_{r=(v-1)n+1}^{vn} \theta_r \varepsilon_{rs} \right|^p$$

$$\leqq \max_{\theta_r} \sum_{s=1}^{m} k^{p-1} \sum_{v=1}^{k} \left| \sum_{r=(v-1)n+1}^{vn} \theta_r \varepsilon_{rs} \right|^p$$

$$\leqq k^{p-1} \sum_{v=1}^{k} \max_{\theta_r} \sum_{s=1}^{m} \left| \sum_{r=(v-1)n+1}^{vn} \theta_r \varepsilon_{rs} \right|^p$$

$$= k.k^{p-1} B_p^p(n,m) = k^p B_p^p(n,m).$$

COROLLARY 7. *If* $1 \leqq p < \infty$ *and* $n < m$, *then*

(i) $B_p(n,m) \leqq (1 + [m/n])^{1/p} B_p(n,n)$

(ii) $B_p(m,n) \leqq (1 + [m/n]) B_p(n,n)$.

PROOF. (i) One has

$$B_p(n,m) \leqq B_p(n, n(1 + [m/n])) \leqq (1 + [m/n])^{1/p} B_p(n,n).$$

Similarly for (ii).

COROLLARY 8. *If* $1 \leqq p \leqq 2$ *and* $n < m$, *then*

$$m^{1/p} n(\pi_p(l_1^n))^{-1} \leqq B_p(n,m) \leqq (n+m)^{1/p} n^{-\frac{1}{2}} h(n).$$

PROOF. Use Theorem 3 and the inequality

$$\begin{aligned} B_p(n,m) &\leqq (1 + m/n)^{1/p} B_p(n,n) \leqq (1 + m/n)^{1/p} n^{1/p - \frac{1}{2}} B_2(n,n) \\ &\leqq (m+n)^{1/p} n^{-\frac{1}{2}} h(n). \end{aligned}$$

COROLLARY 9. *If* $1 \leqq p < 2$ *and* $m < n$, *then*

$$c(m) n m^{1/p - \frac{1}{2}} \leqq B_p(n,m) \leqq (n+m) m^{1/p - 3/2} h(m).$$

PROOF. Use Theorem 3* and the inequality

$$\begin{aligned} B_p(n,m) &\leqq (1 + n/m) B_p(m,m) \leqq (1 + n/m) m^{1/p - \frac{1}{2}} B_2(m,m) \\ &\leqq (n+m) m^{1/p - 3/2} h(m). \end{aligned}$$

COROLLARY 10. *If* $2 \leqq p < \infty$ *and* $m < n$, *then*

$$n \leqq B_p(n,m) \leqq (n+m) m^{-1} h(m).$$

PROOF.

$$\begin{aligned} n &= B_\infty(n,m) \leqq B_p(n,m) \leqq B_2(n,m) \leqq (1 + n/m) B_2(m,m) \\ &\leqq (1 + n/m) h(m). \end{aligned}$$

COROLLARY 11. *If* $2 \leqq p < \infty$, *then* $\lim_{n\to\infty} n^{-1} B_p(n,m) = 1 + o(1)$, *where* $o(1) \to 0$ when $m \to \infty$.

8. A combinatorial generalization

Given integers n, m and any n by m matrix $\varepsilon = (\varepsilon_{ij})$ with entries ± 1, the value $\| \varepsilon \| = \max_{\theta_i, \eta_j = \pm 1} \sum_{i,j} \theta_i \eta_j \varepsilon_{ij}$ is clearly the norm of the corresponding linear operator ε mapping l_∞^n into l_1^m. For any scalar α, $0 < \alpha < nm$, let $\eta(\alpha)$ denote the number of matrices ε which satisfy $\| \varepsilon \| \geqq \alpha$. Obviously $\eta(B_1(n,m)) = 2^{nm}$. By a combinatorial method which originates from [9], one has the following result:

THEOREM 4.

$$\eta(\alpha) \leqq 2^{n+m-1} \left(\frac{nm - \alpha}{2}\right) \binom{nm}{\left[\frac{nm+\alpha}{2}\right]}.$$

PROOF. For every such matrix $\varepsilon=(\varepsilon_{ij})$, say that $\varepsilon\in G(k)$ if ε has k entries equal to $+1$ and $nm-k$ entries equal to -1. $G(k)$ contains then $\binom{nm}{k}$ matrices, and obviously there are at most $2^{n+m-1}\binom{nm}{k}$ matrices ε for which there exist $\theta_i,\ \eta_j=\pm 1$ such that $(\theta_i\eta_j\varepsilon_{ij})\in G(k)$. It follows then that there are at most $2^{n+m-1}\binom{nm}{k}$ matrices ε for which $\|\varepsilon\|=2k-nm$. Therefore, the number $\eta(\alpha)$ cannot exceed the value $\Sigma' 2^{n+m-1}\binom{nm}{k}$, where in Σ' k runs over all the ntegers for which $nm\geqq 2k-nm\geqq\alpha$.

Since $\binom{nm}{k}$ attains its maximum for k in Σ' when k is minimal, and since Σ' contains at most $(nm-\alpha)/2$ terms, it follows that

$$\eta(\alpha)\leqq \Sigma' \leqq 2^{n+m-1}\left(\frac{nm-\alpha}{2}\right)\binom{nm}{\left[\frac{nm+\alpha}{2}\right]}.$$

COROLLARY 12. *If* $\alpha=o(nm)$ *then*

$$\eta(\alpha)\leqq C2^{n+m+nm}\sqrt{nm/8\pi}\,\exp\left(-nm\sum_{i=1}^{\infty}\frac{(\alpha/nm)^{2i}}{2i(2i-1)}\right),$$

where $C=C(n,m,\alpha)\to 1$ *when* $nm\to\infty$. *Moreover, setting* $\alpha=B_1(n,m)$ *this implies that*

$$(B_1(n,m))^2\leqq nm(n+m)(2\ ln\ 2+o(n+m)).$$

PROOF. By [4, cf. chap. VII.6, p. 181, problem 14] we have: If $2k=n+o(n)$, then

$$2^{-n}\binom{n}{k}\sim\sqrt{\frac{2}{n\pi}}\exp\left(-n\sum_{i=1}^{\infty}\frac{\left(\frac{2k}{n}-1\right)^{2i}}{2i(2i-1)}\right).$$

Setting now $k=[(\alpha+nm)/2]$, then by the assumption $\alpha=o(nm)$ and Theorem 4, there exists $C=C(n,m,\alpha)$ which tends to 1 as $nm\to\infty$, such that

$$\eta(\alpha)\leqq C2^{n+m-1}\left(\frac{nm-\alpha}{2}\right)2^{nm}\sqrt{\frac{2}{nm\pi}}\exp\left(-nm\sum_{i=1}^{\infty}\frac{(\alpha/nm)^{2i}}{2i(2i-1)}\right).$$

In particular, if $\alpha=B_1(n,m)$, then $\eta(\alpha)=2^{nm}$, and since by Corollaries 8 and 9

$\alpha = nm.O(\max(n^{-\frac{1}{2}}, m^{-\frac{1}{2}}))$, therefore the above estimate may be used, and as a result we obtain

$$\eta(\alpha) = 2^{nm} \leqq C2^{n+m+nm}\sqrt{\frac{nm}{8\pi}}\exp\left(-nm\sum_{i=1}^{\infty}\frac{(\alpha/nm)^{2i}}{2i(2i-1)}\right).$$

By taking logarithms one has

$$\frac{\alpha^2}{2nm} \leqq nm\sum_{i=1}^{\infty}\frac{(\alpha/nm)^{2i}}{2i(2i-1)} \leqq (n+m)\log 2 + \tfrac{1}{2}\log\left(\frac{nm}{8\pi}\right) + o(1),$$

where the last inequality holds for $\alpha = B_1(n, m)$, and the theorem is established.

9. Some constants of l_p spaces

For a Minkowski space M, $p \geqq 1$ and a positive integer n, let

$$\rho(M,n) = \inf\left\{\max_{\pm}\left\|\sum_{i=1}^{n} \pm x_i\right\|;\ x_i \in M,\ \|x_i\| = 1, i = 1,2,\cdots,n\right\}.$$

$\delta(M) = \rho(M, \dim M)$ is the Dvoretzky-Rogers constant of M. Dvoretzky and Rogers have shown that $\delta(M) \leqq 2(\dim M)^{3/4}$ and conjectured $\delta(M) \leqq (\dim M)^{\frac{1}{2}}$ which holds for dimension 2.

From these definitions one obtains

$$n(\pi_1(M))^{-1} \leqq \rho(M,n). \tag{15}$$

Comparing the definitions of $\rho(l_p^m, n)$ with expression (3) in which $\|x_i\| = m^{1/p}$ and X defines a subset of sequences, gives

$$m^{1/p}\rho(l_p^m, n) \leqq B_p(n,m). \tag{16}$$

THEOREM 5. *Let M be a subspace of $L_p[0,1]$, then*

(i) $\rho(M,n) \geqq n^{1/p}$ *if* $2 \leqq p \leqq \infty$, *with equality if* $l_p^n \subseteq M$.*

(ii) $\rho(M,n) \geqq a_p n^{\frac{1}{2}}$ *if* $1 \leqq p \leqq 2$, *and* $\rho(M,n) \leqq n(\pi_p(l_1^n))^{-1}$ *if* $l_p^{2^{n-1}} \subseteq M$.

(iii) $h(n)n^{-\frac{1}{2}} \geqq \rho(M,n)$ *if* $1 \leqq p \leqq 2$ *and if* $l_p^n \subseteq M$.

PROOF. Obviously, $\rho \overset{\text{def}}{=} \rho(L_p[0,1], n) \leqq \rho(M,n)$. Given $\varepsilon > 0$, there exist $\{f_i\}_{i=1}^n \subset L_p[0,1]$ each of norm 1, such that for every $0 \leqq t \leqq 1$, $\varepsilon + \rho^p \geqq \int_0^1 \left\|\sum_{i=1}^n r_i(t) f_i\right\|^p dt$, where $\{r_i(t)\}$ are the Rademacher functions. Hence

$$\varepsilon + \rho^p \geqq \int_0^1 dt \int_0^1 \left|\sum_{i=1}^n r_i(t) f_i(s)\right|^p ds \geqq a_p^p \int_0^1 \left(\sum |f_i(s)|^2\right)^{p/2} ds.$$

* This notation means that M contains a subspace isometrically isomorphic to l^n.

(i) If $2 \leqq p < \infty$, then $(\Sigma|f_i(s)|^2)^{\frac{1}{2}} \geqq (\Sigma|f_i(s)|^p)^{1/p}$, and since $a_p = 1$ it follows that

$$\varepsilon + \rho^p \geqq n.$$

If in addition $M \supseteq l_p^n$, we have equality by taking for x_i the unit vectors of l_p^n.

(ii) If $1 \leqq p \leqq 2$, then

$$(\Sigma|f_i(s)|^2)^{\frac{1}{2}} \geqq n^{\frac{1}{2}-1/p}(\Sigma|f_i(s)|^p)^{1/p}, \text{ hence}$$

$$\varepsilon + \rho^p \geqq a_p^p n^{p/2-1} \sum_{i=1}^{n} \int |f_i(s)|^p ds = a_p^p n^{p/2}.$$

If in addition $M \supseteq l_p^{2^{n-1}}$, then it follows by (16) that

$$\rho(M,n) \leqq \rho(l_p^{2^{n-1}},n) \leqq (2^{n-1})^{-1/p} B_p(n,2^{n-1})$$
$$= n(\pi_p(l_1^n))^{-1}.$$

(iii) One has $\rho(M,n) \leqq \rho(l_p^n,n) \leqq n^{-1/p}B_p(n,n)$, and the result follows by Corollary 3.

Theorem 5 enables us to estimate $\delta(l_p^n)$

COROLLARY 13. If $1 \leqq p \leqq 2 \leqq q \leqq \infty$, then $\delta(l_q^n) = n^{1/q}$, and $a_p n^{\frac{1}{2}} \leqq \delta(l_p^n) \leqq n^{-\frac{1}{2}}h(n)$.

If all multiples of 4 are Hadamard numbers, this would imply $\delta(l_p^n) \leqq n^{\frac{1}{2}} + 3n^{-\frac{1}{2}}$. Corollary 13 is an improvement on the bound $\delta(l_p^n) \leqq (1 + \sqrt{2})n^{\frac{1}{2}}$ which follows from the bound of Gurari et al. [8] on the Banach-Mazur distance between l_p^n and l_∞^n.

ACKNOWLEDGMENT

The authors are indebted to S. Halfin, J. Lindenstrauss, and C. L. Mallows for fruitful discussions.

REFERENCES

1. T. A. Brown and J. H. Spencer, *Notes on combinatorics: The distribution of coset leaders in a certain code*, Rand Corp. Memorandum RM-6201/3-PR, July 1970.

2. A. Dvoretzky and C. A. Rogers, *Absolute and unconditional convergence in normed linear spaces*, Proc. Nat. Acad. Sci. U.S.A. **36** (1950), 192–197.

3. B. Efron, *Student's t-test under symmetry conditions*, J. Amer. Statist. Assoc. **64** (1969), 1300.

4. W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. I, 2nd ed., New York, 1957.

5. D. J. H. Garling and Y. Gordon, *Relations between some constants associated with finite dimensional Banach spaces*, Israel J. Math. **9** (1971), 346–361.

6. A. M. Gleason, *A search problem in the n-cube*, Proc. Symp. Appl. Math., Vol. **10**, pp. 175–179, Amer. Math. Soc., Providence, R. I., 1960.

7. Y. Gordon, *On p-absolutely summing constants of Banach spaces*, Israel J. Math., **7** (1969), 151–163.

8. V. E. Gurari, M. E. Kadec and V. E. Mazaev, *On the distance between isomorphic L_p spaces of finite dimension*, (Russian), Mat. Sb. **70** (112) (1966), 481–489.

9. J. W. Moon and L. Moser, *An extremal problem in matrix theory*, Mat. Vesnik, **3** (1966), 209–211.

10. H. S. Witsenhausen, *Some games on convex bodies and related inequalities*, J. Math. Anal. Appl. (to appear).

11. A. Zygmund, *Trigonometric Series*, Vol. 1, Cambridge, 1959.

HEBREW UNIVERSITY OF JERUSALEM

AND

LOUISIANA STATE UNIVERSITY

AND

BELL TELEPHONE LABORATORIES, INC.

MURRAY HILL, N. J.