COMBINATORICA 5 (4) (1985) 337—342

AN INEQUALITY CONJECTURED BY HAJELA AND SEYMOUR ARISING IN COMBINATORIAL GEOMETRY

H. J. LANDAU, B. F. LOGAN and L. A. SHEPP

Received 31 October 1984

In a recent paper, D. Hajela and P. Seymour proved that for $0\leqq b_1\leqq b_2\leqq 1$, $\alpha=(\log_2 3)/2$,

$$b_1^\alpha b_2^\alpha+(1-b_1)^\alpha b_2^\alpha+(1-b_1)^\alpha(1-b_2)^\alpha\geqq 1,$$

and drew from this inequality a variety of interesting results in combinatorial geometry. They also conjectured a generalization of the inequality to n variables, which they showed to imply a lower bound on the number of different sequences obtained when members of n sets of zero-one sequences are added to one another.

We prove their conjecture, not easy to verify even for small values of n, using complex-variable theory.

Introduction

In a recent paper [1], D. Hajela and P. Seymour derived a variety of interesting results in combinatorial geometry from the inequality

$$[b_1b_2]^\alpha+[(1-b_1)b_2]^\alpha+[(1-b_1)(1-b_2)]^\alpha \geqq 1,$$

which they established for $\alpha=(\log_2 3)/2$ and $0\leqq b_1\leqq b_2\leqq 1$. (This inequality also appeared in [3], with similar applications.) They then conjectured the truth of the following generalization: if $0\leqq b_1\leqq b_2\leqq\ldots\leqq b_n\leqq 1$, $\alpha=n^{-1}\log_2(n+1)$, and

$$f_n(b_1,\ldots,b_n;\alpha)\equiv[b_1b_2\ldots b_n]^\alpha+[(1-b_1)b_2\ldots b_n]^\alpha+[(1-b_1)(1-b_2)b_3\ldots b_n]^\alpha+\ldots$$

$$\ldots+[(1-b_1)(1-b_2)\ldots(1-b_n)]^\alpha, \tag{1}$$

then

$$f_n\geqq 1. \tag{2}$$

On the basis of (2), they concluded that if A_i is a set of vertices of the unit cube (i.e., of sequences whose entries are 0 or 1), $|A_i|$ denotes the cardinality of A_i, and A_i+A_j is the set of all sums of an element from A_i and one from A_j, then

$$|A_1+A_2+\ldots A_n|\geqq(|A_1||A_2|\ldots|A_n|)^{n^{-1}\log_2(n+1)}.$$

But even apart from its applications, the conjecture, which was open already for $n=3$, presents an enticing analytic challenge. We establish it here in a slightly more

AMS subject classification 1980: 26 D 15, general form by proving that, for any $\alpha>0$, f_n is minimized by choosing the b_i to be either 1/2 or 1. Specifically, we show that

$$\min_{0\leqq b_1\ldots\leqq b_n\leqq 1} f_n(b_1, \ldots, b_n; \alpha) = \min\,[1, (n+1)2^{-n\alpha}]. \tag{3}$$

Since the inequality seems to be a matter of real variables, it is perhaps surprising that our proof is based on conformal mapping and Hadamard's three-circle theorem.

Acknowledgement. We are grateful to J. C. Lagarias for having brought this problem to our attention.

Discussion and Proofs

We begin by showing that the minimizing $\{b_i\}$ can be presumed to lie in half of the unit interval.

Lemma 1. *Let* $\alpha>0$, $0\leqq b_1\leqq\ldots\leqq b_n\leqq 1$, *and* f_n *be defined by* (1). *In the problem of minimizing* f_n *by choice of* $\{b_i\}$, *it is sufficient to consider* $1/2\leqq b_1\leqq\ldots\leqq b_n\leqq 1$.

Proof. We will show that we do not increase the value of f_n if we replace $\{b_i\}$ by $\{b_i'\}$, obtained by reflecting those b_i in (0, 1/2) into (1/2, 1) by the map $b_i\mapsto 1-b_i$, and reordering the resulting sequence. We argue by induction. The assertion is evidently true when $n=1$. Assuming it to be true for $n-1$, we consider it for n. We may suppose that

$$1-b_n \leqq b_1, \tag{4}$$

for otherwise we can reflect all the points $\{b_i\}$ by setting $b_i''=1-b_{n+1-i}$; this transformation does not change the value of f_n, and produces (4). But when (4) holds, b_n remains the largest point even after each b_i in (0, 1/2) has been replaced by $1-b_i$, and so the subsequent reordering does not affect it. Thus the reflection and reordering procedure operates only on $b_1, \ldots, b_{n-1}$. On writing

$$f_n = f_{n-1}b_n^\alpha + [(1-b_1)\ldots(1-b_{n-1})]^\alpha(1-b_n)^\alpha,$$

we see, by the induction hypothesis, that the reflection and reordering can only decrease f_{n-1}, and likewise only lower the distances $\{1-b_i\}$. Thus f_n is not increased, as was to be shown. ∎

In view of Lemma 1 we henceforth assume that all the b_i lie in [1/2, 1], and we begin by considering the minimum of f_n as we vary the largest of the b_i over its permitted domain, keeping the remaining ones fixed. Accordingly, suppose that, for $k\geqq 1$, the k last b_i coincide, $b_{n-k+1}=b_{n-k+2}=\ldots=b_n=b$, and that we wish to minimize f_n for

$$1/2 \leqq b_{n-k} \leqq b \leqq 1. \tag{5}$$

We have

$$\frac{f_n(b_1, \ldots, b_{n-k}, b, \ldots, b; \alpha)}{(1-b_1)^\alpha\ldots(1-b_{n-k})^\alpha} = (1+A)b^{k\alpha}+(1-b)^\alpha b^{(k-1)\alpha}+\ldots+(1-b)^{k\alpha},$$

with

$$1+A = \frac{f_{n-k}(b_1, \ldots, b_{n-k}; \alpha)}{(1-b_1)^\alpha \ldots (1-b_{n-k})^\alpha},$$

so that

(6) $$A \geqq 0.$$

Letting $b^\alpha = x$, $(1-b)^\alpha = y$, the problem becomes to minimize

$$g(x, y) \equiv (1+A)x^k + x^{k-1}y + \ldots + y^k$$

over the curve $x^{1/\alpha} + y^{1/\alpha} = 1$, in that part of the positive quadrant where

(7) $$b_{n-k}^\alpha \leqq x \leqq 1.$$

Since $1/2 \leqq b_{n-k}$, $y \leqq x$ in this region; let us denote by Δ the arc of $x^{1/\alpha} + y^{1/\alpha} = 1$ which lies in $y \leqq x$. We now take advantage of the homogeneity of $g(x, y)$ by introducing the homothetic family of level curves

(8) $$\Gamma_c = \{(x, y) | g(x, y) = c\},$$

in terms of which the problem is to find the least c for which Γ_c intersects Δ in the range (7). To obtain more information about such intersections, we find the slope dy/dx on Γ_c by implicit differentiation

$$\frac{dy}{dx}\Big|_{(x,y)\in\Gamma_c} = -\frac{(1+A)kx^{k-1} + (k-1)x^{k-2}y + \ldots + y^{k-1}}{x^{k-1} + 2yx^{k-2} + \ldots + ky^{k-1}},$$

and, parametrizing Γ_c by $\lambda = y/x$, we obtain

(9a) $$\frac{dy}{dx}\Big|_{(x,y)\in\Gamma_c} = -\frac{(1+A)k + (k-1)\lambda + \ldots + \lambda^{k-1}}{1 + 2\lambda + \ldots + k\lambda^{k-1}}.$$

Proceeding analogously with Δ yields

(9b) $$\frac{dy}{dx}\Big|_{(x,y)\in\Delta} = -\frac{1}{\lambda^\theta}, \quad \theta = \alpha^{-1} - 1.$$

The relation between these slopes is given by the following result of independent interest.

Theorem 1. *Suppose* $0 \leqq a_0 \leqq a_1 \leqq \ldots \leqq a_n \neq 0$, *and let*

(10) $$h_n(z) \equiv \frac{a_0 + a_1 z + \ldots + a_n z^n}{a_n + a_{n-1}z + \ldots + a_0 z^n}.$$

Then

a) $h_n(z)$ *is analytic in* $|z| \leqq 1$;

b) $h_n(z)$ *takes* $|z| \leqq 1$ *into itself;*

c) $h_n(x) = \max\limits_{|z|=x} |h_n(z)|$, $0 \leqq x \leqq 1$.

Proof. We proceed by induction. Let C_n denote the collection of functions having the form (10), with some monotone sequence of coefficients $\{a_k\}$, $0 \leqq k \leqq n$. If $h_1 \in C_1$, $h_1(z)$ is the linear fractional transformation

(11) $$h_1(z) = \frac{\mu + z}{1 + \mu z}, \quad 0 \leqq \mu = a_0/a_n \leqq 1.$$

Ignoring the trivial case $\mu=1$, this function is analytic in $|z|<1$, takes $|z|\leqq 1$ conformally onto itself, and maps $|z|=r<1$ onto a circle with center on the positive real axis, so that the theorem is valid for $h_1(z)$. Now let us suppose that each $h\in C_n$ satisfies a), b), and c). The same is then true for $zh(z)$, and, by the above-mentioned properties of (11), also for

$$\frac{\mu+zh(z)}{1+\mu zh(z)}, \tag{12}$$

with any $0\leqq\mu\leqq 1$. We complete the induction by showing that any $h_{n+1}\in C_{n+1}$ can be so represented. For we can write h_{n+1} in the form (12) by setting

$$h(z)\equiv\frac{h_{n+1}(z)-\mu}{z(1-\mu h_{n+1}(z))}. \tag{13}$$

If

$$h_{n+1}(z)=\frac{a_0+a_1z+\ldots+a_{n+1}z^{n+1}}{a_{n+1}+a_nz+\ldots+a_0z^{n+1}},$$

with $\{a_i\}$ positive monotone sequence, we set

$$\mu=a_0/a_{n+1}\leqq 1,$$

and substitute into (13), obtaining

$$h(z)=\frac{b_0+b_1z+\ldots+b_nz^n}{b_n+b_{n-1}z+\ldots+b_0z^n},$$

with

$$b_i=a_{i+1}a_{n+1}-a_{n-i}a_0\geqq 0,\quad 0\leqq i\leqq n.$$

From the monotonicity of $\{a_i\}$ it follows that $a_{i+2}-a_{i+1}\geqq 0$, while $a_{n-i-1}-a_{n-i}\leqq 0$, hence

$$a_0(a_{n-i-1}-a_{n-i})\leqq a_{n+1}(a_{i+2}-a_{i+1}),\quad -1\leqq i\leqq n-1,$$

or, equivalently, $b_i\leqq b_{i+1}$, $0\leqq i\leqq n-1$. Thus $h\in C_n$, and consequently, by means of the representation (12), C_{n+1} inherits from C_n properties a), b), and c), as was to be shown. ▮

Corollary 1. *With h_n as in (10), the equation*

$$h_n(x)=x^\theta \tag{14}$$

has at most one solution in $0\leqq x<1$ when $\theta>0$, and $h_n(x)<x^\theta$ there when $\theta\leqq 0$.

Proof. By Theorem 1, $h_n(x)$ coincides with the maximum modulus of a function analytic in $|z|\leqq 1$, and so, by Hadamard's three-circle theorem [2, p. 173], $\log h_n(x)$ is an increasing convex function of $\log x$, $0\leqq x\leqq 1$. Thereupon, letting $y=\log x$, and $f(y)\equiv\log h_n(x)$, (14) becomes

$$\frac{f(y)}{y}=\theta,\quad y\leqq 0, \tag{15}$$

with $f(y)$ an increasing convex function of y. But $f(0)=0$, hence, for $y<0$,

$$\frac{f(y)}{y}=\frac{1}{y}\int_0^y f'(t)\,dt=-\frac{1}{-y}\int_y^0 f'(t)\,dt,$$

with $f'(t)$ positive, and increasing by the convexity of f. Thus the quotient represents an average of an increasing function, hence itself increases monotonically as a function of y (between 0 at $y=-\infty$ and $f'(0)$ at $y=0$), so that (15) can have at most one solution for $\theta>0$. For $\theta\leqq 0$, $h_n(x)-x^\theta$ is an increasing function, vanishing at $x=1$, hence is negative in $0\leqq x<1$. ∎

Corollary 2. *With* $0<a_0\leqq\ldots\leqq a_n$ *and* $v>0$, *the equation*

$$\frac{a_0+a_1x+\ldots+a_nx^n}{v+a_k+a_{k-1}x+\ldots+a_0x^n}=x^\theta \tag{16}$$

has exactly one solution in $0\leqq x<1$ *when* $\theta>0$, *and no solutions there when* $\theta\leqq 0$.

Proof. Let $p(x)=a_0+a_1x+\ldots+a_nx^n$ and $q(x)=a_n+a_{n-1}x+\ldots+a_0x^n$. Equivalently to (16), we consider $x^{-\theta}p(x)-q(x)=v$; this has one solution for each $v>0$ if and only if $x^{-\theta}p(x)-q(x)$ is a monotonic function of x where it is positive. By Corollary 1, if $\theta\leqq 0$, $x^{-\theta}p(x)-q(x)<0$ in $0\leqq x<1$, while if $\theta\geqq n$, $x^{-\theta}p(x)-q(x)$ evidently decreases for $x>0$. We therefore restrict to the remaining case, $0<\theta<n$. Since $\theta>0$ and $a_0>0$, $x^{-\theta}p(x)-q(x)\to\infty$ as $x\to 0+$, and has at most a single zero in $0<x<1$ by Corollary 1. Therefore $x^{-\theta}p(x)-q(x)$ is positive in a single interval $I\subset[0,1]$, having $x=0$ as its left endpoint. Moreover, since $(n-\theta)>0$, $(1-x^{n-\theta})$ is positive in $0<x<1$, approaching 1 and 0 at the endpoints. Now in Corollary 1 let us replace a_n by a_n+v, noting that $a_{n-1}\leqq a_n+v$ since $v>0$. We conclude that

$$\frac{p(x)+vx^n}{v+q(x)}=x^\theta$$

has at most one solution, $0\leqq x\leqq 1$, or, equivalently, that the equation

$$x^{-\theta}p(x)-q(x)=v(1-x^{n-\theta}) \tag{17}$$

has at most one solution in $0\leqq x<1$. But this implies that $x^{-\theta}p(x)-q(x)$ is monotone for $x\in I$, else (since it approaches ∞ at $x=0$) it must have a local minimum x_0 interior to I. Then, by choosing $v>0$ so that (17) is satisfied at x_0, we see that $v(1-x^{n-\theta})-[x^{-\theta}p(x)-q(x)]$ is positive in some neighborhood $x_0-\varepsilon<x<x_0$, but is negative near $x=0$, hence must have a zero in addition to x_0. This means that (17) has at least two solutions, a contradiction which establishes the desired monotonicity. ∎

We can now return to the original problem and complete the argument.

Theorem 2. *Let* $\alpha>0$, $0\leqq b_1\leqq\ldots\leqq b_n\leqq 1$, *and* f_n *be defined by* (1). *Then*

$$\min_{(b_i)} f_n=\min\,[1,(n+1)2^{-n\alpha}].$$

Proof. We recall the earlier discussion, which converted the problem of minimizing f_n by choice of b to that of finding the least c for which the level cruve Γ_c of (8) intersects Δ in the range (7). Assume now that $\alpha<1$, and consider the level curve Γ_{1+A}, which passes through the point $(1,0)$, corresponding to $\lambda=y/x=0$. By (9a), the slope of Γ_{1+A} at this point is $-(1+A)k$, while that of Δ is $-\infty$ by (9b), since $\theta>0$. We assert that for $c\leqq 1+A$, Γ_c crosses Δ at most once. For supposing otherwise, let λ_0 and λ_1, with $0<\lambda_0<\lambda_1<1$, be the first two values of λ at which Γ_c and Δ cross. Since Γ_c lies below Δ at $\lambda=0$, Γ_c crosses Δ from below at λ_0, hence the slope of Γ_c is lower than that of Δ at λ_0 (more precisely, at some point in an arbitrarily small neighborhood of λ_0). Analogously, Γ_c crosses Δ from above at λ_1, so that Γ_c has larger slope than does Δ at λ_1. Thus $s(\lambda)\equiv$(slope of Γ_c)$-$(slope of Δ) changes sign at least twice in the range $0<\lambda\leqq\lambda_1$, hence must have at least two zeros there. But on inserting (9a) and (9b) into the definition of $s(\lambda)$, we see by Corollary 2 that s vanishes only once, a contradiction. We conclude, firstly, that Γ_{1+A} crosses Δ at most once. Thus, letting $(\bar{x},\bar{y})$ denote the point of intersection, it follows that $g(x,y)\geqq 1+A$ on the part of Δ where $x\geqq\bar{x}$. Moreover, where $x<\bar{x}$, each point of Δ lies on a distinct Γ_c, hence $g(x,y)$ increases monotonically in x on the part of Δ where $x<\bar{x}$.

Consequently, the minimum of $g(x,y)$ over Δ in the range $b^{\alpha}_{n-k}\leqq x$ occurs at the right-hand end point $x=1$ if $b^{\alpha}_{n-k}\geqq\bar{x}$, and at the left-hand endpoint $x=b^{\alpha}_{n-k}$ otherwise; this corresponds to $b=1$ and $b=b_{n-k}$, respectively, in (5). In the former case,

$$f_n(b_1,\ldots,b_{n-k},b,\ldots,b;\alpha)=f_{n-k}(b_1,\ldots,b_{n-k};\alpha)$$

and we repeat the argument; in the latter case, the minimizing choice of b increases the number of coincident $\{b_i\}$ from the last k to the last $k+1$. Continuing in this way, we see that at the last stage all the remaining b_i coincide, and equal either 1/2 or 1. Thus the possible minima of f_n are restricted to be either 1 or $(k+1)2^{-k\alpha}$ for some $k\leqq n$. But the function $\log(t+1)-t\alpha\log 2$ is concave in t, with value 0 at $t=0$; it therefore necessarily decreases where it is negative. It follows that $(k+1)2^{-k\alpha}$ is a decreasing function of k wherever it lies below 1. Consequently, we have $\min[1,(n+1)2^{-n\alpha}]\leqq\min[1,(k+1)2^{-k\alpha}]$, for each $k\leqq n$, and we conclude that, for $\alpha<1$,

$$\min_{(b_i)} f_n=\min[1,(n+1)2^{-n\alpha}],$$

as was to be shown. For $\alpha\geqq 1$, $\theta\leqq 0$ in (9b). The argument just given then shows that Δ is below Γ_{1+A}, and that each point of Δ lies on a distinct Γ_c with $c\leqq 1+A$. Thus, on Δ, $g(x,y)$ increases monotonically in x, so that $g(x,y)$ is invariably minimized at the left-hand endpoint, and $\min f_n=(n+1)2^{-n\alpha}$. ∎

References

[1] D. Hajela and P. Seymour, Counting points in hypercubes and convolution measure algebras, *Combinatorica*, **5** (1985), 205—214.
[2] E. C. Titchmarsh, *The Theory of Functions*, Oxford Univ. Press, 1939.
[3] D. R. Woodall, A theorem on cubes, *Mathematika* **24** (1977), 60—62.

H. J. Landau, B. F. Logan, L. A. Shepp

AT&T Bell Laboratories
Murray Hill, NJ 07974, U.S.A.