Europ. J. Combinatorics (1993) **14**, 79–83

Covering the Cube by Affine Hyperplanes

NOGA ALON AND ZOLTÁN FÜREDI

One can easily cover the vertices of the n-cube by 2 hyperplanes. Here it is proved that any set of hyperplanes that covers all the vertices of the n-cube but one contains at least n hyperplanes. We give a variety of proofs and generalizations.

1. HYPERPLANE COVERINGS OF THE VERTEX SET OF THE CUBE

Let $V = \{1, -1\}^n$ be the vertex set of an n-cube. Alon *et al.* [3] proved the following. For even n the minimum cardinality of a family of hyperplanes of the form $(\mathbf{a}_i, \mathbf{x}) = 0$, where the co-ordinates of each vector $\mathbf{a}_i$ are in $\{-1, 1\}$, the union of which covers V, is n. This result is somewhat surprising because each such hyperplane contains $\binom{n}{n/2} = \Theta(2^n/\sqrt{n})$ vertices in V.

Using arbitrary hyperplanes one can cover all the vertices in V by two parallel ones, and there are several additional ways to obtain a covering by two hyperplanes. But what is the minimum number, $m(n)$, of hyperplanes covering exactly $2^n - 1$ vertices? The problem in this form was proposed by Imre Bárány, who extracted it from Komjáth [5]. Komjáth needed a weaker version (namely, a proof that $m(n) \to \infty$), to deal with an infinite extension of Rado's theorem about regular equation systems. He achieved his aim by proving that $m(n) \geqslant \log_2 n - 2 \log_2 \log_2 n$ for $n \geqslant 2$. On the other hand, taking n faces of the cube meeting in a vertex, it is obvious that $m(n) \leqslant n$. Our first result is an exact determination of $m(n)$ (which turns out to be n). We also establish a number of extensions of that result.

Our proofs apply linear algebra techniques and demonstrate the power of these methods. In order to exhibit the variety of proof methods we try to apply a slightly different method in the proof of each extension. In what follows it is more convenient to consider the cube $\{0, 1\}^n$ instead of $\{-1, 1\}^n$, and we proceed with this convention.

THEOREM 1. *Suppose that the hyperplanes $H_1, H_2 \cdots H_m$ in $\mathbf{R}^n$ avoid $\vec{0}$, but otherwise cover all the other $2^n - 1$ vertices of the unit cube $\{0, 1\}^n$. Then $m \geqslant n$.*

PROOF. We utilize the linear algebraic method from [3]. Let $(\mathbf{a}_i, \mathbf{x}) = b_i$ be an equation defining H_i, where $\mathbf{a}_i, \mathbf{x} \in \mathbf{R}^n$, $b_i \in \mathbf{R}$. Consider the polynomial $P(\mathbf{x}) = \prod_{i=1}^m ((\mathbf{a}_i, \mathbf{x}) - b_i)$. Let $Q(\mathbf{x})$ be the multilinear polynomial obtained from $P(\mathbf{x})$ by replacing repeatedly each occurrence of x_i^d, with $d \geqslant 2$ in the standard representation of $P(\mathbf{x})$ as a sum of monomials, by x_i. Clearly, $Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in \{0, 1\}^n \backslash \{\vec{0}\}$, and $Q(\vec{0}) = P(\vec{0}) \neq 0$. Moreover, $\deg(Q) \leqslant \deg(P) = m$. Thus the theorem follows from the first lemma in the next section. □

2. MULTILINEAR POLYNOMIALS

LEMMA 1. *If $Q(\mathbf{x}) \in Z[x_1, \ldots, x_n]$ is a multilinear polynomial with $Q(\vec{0}) = c \neq 0$ and $Q(\mathbf{x}) = 0$ for $\mathbf{x} \in \{0, 1\}^n \backslash \{\vec{0}\}$, then $Q(\mathbf{x}) = c(x_1 - 1)(x_2 - 1) \cdots (x_n - 1)$. In particular, $\deg(Q) = n$.*

PROOF. Let $Q(\mathbf{x}) := \sum_{I \subset \{1,2,\ldots,n\}} c_I x_I$, where x_I is a shorthand for $\prod_{i \in I} x_i$. We claim

0195-6698/93/020079 + 05 $08.00/0

that $c_I = (-1)^{|I|}c$. To prove this claim we proceed by induction on the size of $|I|$. $c_\varnothing = Q(\vec{0}) = c$. Suppose we have already proved our claim for all $J \subset I$, $J \neq I$, where now $|I| \geq 1$. Consider the vector $\mathbf{e}(I) \in \{0, 1\}^n$ with co-ordinates 1 exactly in the elements of I. Then

$$0 = Q(\mathbf{e}(I)) = \sum_{J \subset I} c_J = \sum_{J \subset I,\, J \neq I} (-1)^{|J|}c + c_I = c\left(\sum_{0 \leq j < i} \binom{i}{j}(-1)^j\right) + c_I = c(-1)^{|I|-1} + c_I. \quad \square$$

3. Using Less Than n Hyperplanes

Corollary 1. *If $n \geq m \geq 1$ then m hyperplanes that do not cover all vertices of the unit n-cube miss at least 2^{n-m} vertices.*

This result can be proved by imitating the argument that supplies a lower bound for the distance of the Reed Muller Codes (see, e.g., [6]). Here we give another proof.

Proof. Induction on $n - m$. The case $n - m = 0$ is obvious, and the case $n - m = 1$ follows from Theorem 1. In general, suppose that $H_1, \ldots, H_m$ miss at least two vertices $\mathbf{x}$ and $\mathbf{y}$. There is a co-ordinate i with $x_i \neq y_i$. Consider the two $(n-1)$-dimensional subcubes $\{\mathbf{v} \in \{0, 1\}^n : v_i = \alpha\}$, where $\alpha \in \{0, 1\}$. Neither is covered by $H_1 \cup \cdots \cup H_m$. So the induction hypothesis implies that these hyperplanes miss at least $2^{(n-1)-m}$ points of each. $\square$

Corollary 2. *If $H_1, \ldots, H_m$ is a minimal set of hyperplanes that cover all vertices of the unit n-cube, then each such a plane contains at least 2^{n+1-m} own vertices, i.e.*

$$\left|(\{0, 1\}^n \cap H_i) \setminus \left(\bigcup_{\substack{1 \leq j \leq m \\ j \neq i}} H_j\right)\right| \geq 2^{n+1-m}. \quad \square$$

4. More Hyperplane Coverings

Let $V = V(h_1, h_2, \ldots, h_n)$ be the set of lattice points $(y_1, \ldots, y_n)$ such that $0 \leq y_i \leq h_i$. Let $\mathbf{v} \in V$, and define $U = V \setminus \mathbf{v}$. Clearly, the points of V can be covered by $\min h_i$ parallel hyperplanes. But to cover U by hyperplanes avoiding $\mathbf{v}$ one cannot improve on the trivial upper bound, $\sum h_i$, obtained by using hyperplanes orthogonal to the standard unit vectors. This is proved in the following theorem.

Theorem 2. *Suppose that the hyperplanes $H_1, H_2 \cdots H_m$ in $\mathbf{R}^n$ avoid $\mathbf{v}$, but their union $H_1 \cup H_2 \cup \cdots \cup H_m$ contains $V(h_1, h_2, \ldots, h_n) \setminus \mathbf{v}$. Then $m \geq h_1 + h_2 + \cdots + h_n$.*

Theorem 1 is a special case of Theorem 2, but here we present a slightly different proof. For $\mathbf{i} = (i_1, \ldots, i_n) \in V$ let $B(i_1, \ldots, i_n, \mathbf{x}) \in Z(x_1, \ldots, x_n)$ be the following polynomial:

$$B(\mathbf{i}, \mathbf{x}) := \prod_{\substack{0 \leq j_1 \leq h_1 \\ j_1 \neq i_1}} (x_1 - j_1) \prod_{\substack{0 \leq j_2 \leq h_2 \\ j_2 \neq i_2}} (x_2 - j_2) \cdots \prod_{\substack{0 \leq j_n \leq h_n \\ j_n \neq i_n}} (x_n - j_n).$$

All these polynomials have degree $\sum h_i$.

Lemma 2. *The polynomials $B(\mathbf{i}, \mathbf{x})$ form a basis of the subspace Z generated by the functions $\{x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} : 0 \leq a_i \leq h_i\}$.*

PROOF OF LEMMA 2. Obviously, every $B(\mathbf{i}, \mathbf{x})$ belongs to Z and the dimension of Z is precisely $\prod (h_i + 1)$, so all we need is to show that the polynomials $B(\mathbf{i}, \mathbf{x})$ are linearly independent. Consider a linear dependence

$$\sum_{\mathbf{i} \in V} \alpha_{\mathbf{i}} B(\mathbf{i}, \mathbf{x}) \equiv 0.$$

For each $\mathbf{i} = (i_1, \ldots, i_n)$ one can substitute $x_j = i_j$ for all j in the above equation. For this $\mathbf{x} = (x_1, \ldots, x_n)$, $B(\mathbf{i}, \mathbf{x})$ is not zero, whereas for all $\mathbf{k} \neq \mathbf{i}$, $B(\mathbf{k}, \mathbf{x}) = 0$ and hence this implies that $\alpha_{\mathbf{i}} = 0$ for all $\mathbf{i}$, completing the proof. □

The proof of Theorem 2 now follows the previous proof. Consider the polynomial $P(\mathbf{x}) = \prod_{i=1}^{m} ((\mathbf{a}_i, \mathbf{x}) - b_i)$. Let $Q(\mathbf{x}) \in Z$ be the polynomial obtained from $P(\mathbf{x})$ by replacing repeatedly each occurrence of $x_i^{h_i+1}$ by $x_i^{h_i+1} - (\prod_{0 \leq j \leq h_i} (x_i - j))$ (which is a polynomial of degree at most h_i in x_i.) Clearly,

$$Q(\mathbf{x}) = 0 \tag{1}$$

for all $\mathbf{x} \in U$, and $Q(\mathbf{v}) = P(\mathbf{v}) \neq 0$. Apply Lemma 2 to write Q as a linear combination $Q(\mathbf{x}) = \sum_{\mathbf{i} \in V} \alpha_{\mathbf{i}} B(\mathbf{i}, \mathbf{x})$. Substituting here an $\mathbf{x} = \mathbf{i} \in U$, (1) implies that $\alpha_{\mathbf{i}} = 0$ for all $\mathbf{i} \in U$. However, Q is not identically 0, so $Q(\mathbf{x}) = cB(\mathbf{v}, \mathbf{x})$ for some $0 \neq c \in \mathbf{R}$. Hence $m = \deg(P) \geq \deg(Q) \geq \deg B(\mathbf{v}, \mathbf{x}) = \sum_{i=1}^{n} h_i$. □

5. A Common Generalization for Bricks over any Field

For a sequence of positive integers $\mathbf{s} = (s_1, \ldots, s_n)$, let $M(\mathbf{s}, l)$ denote the minimum of the product of n positive integers $y_i \leq s_i$ the sum of which is at least l. For $l \leq n$ we have $M = 1$, and for $l \geq \sum s_i$ we define $M = \prod s_i$. One can give a formula, but let us leave it in this form.

THEOREM 4. *Let* $\mathbf{F}$ *be an arbitrary field, let* $S_1, \ldots, S_n$ *be non-empty subsets of* $\mathbf{F}$, $|S_i| = s_i$, *and let* B *be the set* $S_1 \times S_2 \times \cdots \times S_n$. *If* m *hyperplanes do not cover* B *completely, then they miss at least* $M(\mathbf{s}, (\sum s_i) - m)$ *points of* B.

Observe that if $\sum y_i = \sum s_i - m$ and if $y_i \leq s_i$ are positive integers then one can make the union of the hyperplanes miss exactly $\prod y_i$ points by taking $s_i - y_i$ hyperplanes of the form $x_i = s$ for $s_i - y_i$ distinct members $s \in S_i$ for all i.

To prove the above theorem it clearly suffices to prove the following:

THEOREM 5. *Any polynomial* $P(x_1, \ldots, x_n)$ *of degree* m *which does not vanish on all of* B *is non-zero on at least* $\min \prod y_i$ *points of* B, *where the minimum is taken over all positive integers* $y_i \leq s_i$ *the sum of which is at least* $(\sum s_i) - m$.

PROOF. The proof is by induction on n. The result is trivial for $n = 1$, as a (non-zero) polynomial of degree m can have at most m distinct roots. Write $s = s_1$. Define $Q(x_1) = \prod_{i \in S_1} (x_1 - i) = x_1^s - q(x_1)$ and let us reduce P modulo Q; namely, replace in P, repeatedly, every occurrence of x_1^s by $q(x_1)$. Observe that this does not change the value of P on points of B, and in the end we obtain a polynomial, call it $R(x_1, \ldots, x_n)$, of total degree at most m, the degree in x_1 of which is at most $s - 1$. Clearly, it is not identically zero, as it is non-zero on some points of B.

For each possible substitution for $x_1 \in S_1$ we now obtain $R_{x_1}(x_2, \ldots, x_n)$, a polynomial in $x_2, \ldots, x_n$. Not all of these substitutions give the zero polynomial.

Denote by y the number of substitutions that do not give the zero polynomial on $B_1 := S_2 \times \cdots \times S_n$: that is, let $Y := \{x_1 \in S_1 : R_{x_1}(\mathbf{x}) \neq 0 \text{ for some } \mathbf{x} \in B_1\}$ and put $y := |Y|$.

CLAIM. *Each polynomial obtained from* $(R(x_1, \ldots, x_n)$ *by a substitution of a value from* Y *to* x_1 *(which is not the zero polynomial on* B_1*, by the definition of* Y*), is of degree at most* $m - s_1 + y$ *on* B_1.

PROOF OF CLAIM. Write $R(x_1, \ldots, x_n) = R_1 x_1^{s-1} + R_2 x_1^{s-2} + \cdots + R_s$, where R_i is a polynomial of degree at most $m - s + i$ in $x_2, \ldots, x_n$. The values of each polynomial $R_i(x_2, \ldots, x_n)$ over B_1 can be considered as a vector $\mathbf{r}_i$ from the space $\mathbf{F}^{B_1}$.

For $s - y$ substitutions of x_1, namely for $x_1 \in (S_1 \backslash Y)$, we obtain a linear equation $\vec{0} = x_1^{s-1}\mathbf{r}_1 + \cdots + x_1\mathbf{r}_{s-1} + \mathbf{r}_s$. As the coefficients of the vectors $\mathbf{r}_{y+1}, \mathbf{r}_{y+2}, \ldots, \mathbf{r}_s$ form a Vandermonde matrix, this matrix is non-singular. So one can express these vectors, as linear combinations of $\{x_1^{s-1}\mathbf{r}_1 + \cdots + x_1^{s-y}\mathbf{r}_y : x_1 \in (S_1 \backslash Y)\}$. We can thus express the polynomials $R_{y+1}, R_{y+2}, \ldots, R_s$ as linear combinations of $R_1, \ldots, R_y$ (on B_1), and the degree of each of these is at most $m - s_1 + y$, proving the claim. □

Note that we did not prove that the polynomial $R_{x_1}(x_2, \ldots, x_n)$ is of degree at most $m - s + y$, we have only proved that there is a polynomial $T_{x_1}(x_2, \ldots, x_n)$ such that $\deg T \leq m - s + y$, and $T_{x_1}(\mathbf{x}) = R_{x_1}(\mathbf{x})$ for all $\mathbf{x} \in B_1$.

It thus follows that the number of points of B on which our polynomial $R(\mathbf{x})$ is not zero is at least y times G, where G is (by induction) the minimum possible value of the product of $n - 1$ positive integers $y_2, \ldots, y_n$, with $y_i \leq s_i$, the sum of which is at least $(\sum_{2 \leq i \leq n} s_i) - m + s - y$. Taking $y = y_1$ we obtain the desired result. □

6. ANOTHER PROOF FROM NULLSTELLENSATZ

SKETCH. Another proof for Theorem 1 can be obtained (in a way that resembles the one in [3]), by using Hilbert's Nullstellensatz. The polynomial $P(\mathbf{x})$ defined in the proof in Section 1 vanishes on the zero set of the ideal $\mathcal{I}$ generated by $x_1^2 - x_1$, $x_2^2 - x_2, \ldots, x_n^2 - x_n$ and $(x_1 - 1)(x_2 - 1) \cdots (x_n - 1)$. Thus a power of P should belong to $\mathcal{I}$. One can next show that in fact $P \in \mathcal{I}$, too. Finally, another argument proves that $P(\mathbf{x})$ vanishes identically if its degree is less than n. This proof can be probably extended to the general case too.

Another proof for Theorem 2 can be obtained using the following lemma proved in [2]. If $S_1, \ldots, S_n$ are sets of integers, $|S_i| = h_i$ and $P(x_1, \ldots, x_n)$ is a polynomial of $x_1, \ldots, x_n$ that vanishes on all points of $S_1 \times S_2 \times \cdots \times S_n$ but is not identically zero then $\deg(P) \geq h_1 + \cdots + h_n$.

Several additional algebraic proofs with a similar flavour can be found in [4] and in [1].

ACKNOWLEDGMENTS

We would like to thank Imre Bárány for helpful comments. N.A.'s research was supported by a United States Israel BSF grant. Z.F.'s research was supported in part by the Hungarian National Science Foundation under grant No. 1812.

REFERENCES

1. N. Alon, Tools from higher algebra, in: *Handbook of Combinatorics*, North Holland, to appear.
2. N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica*, **12** (1992), 125–134.

3. N. Alon, E. E. Bergmann, D. Coppersmith and A. M. Odlyzko, Balancing sets of vectors, *IEEE Trans. Inform. Theory*, **34** (1988), 128–130.
4. L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics, with Applications to Geometry and Computer Science* (book preliminary version 2), University of Chicago, September 1992.
5. P. Komjáth, Partitions of vector spaces, *Studia Sci. Math. Hungar.*, to appear.
6. F. J. MacWillams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, 1977.

Received 23 May 1992 and accepted 23 September 1992

NOGA ALON
Department of Mathematics,
Raymond and Beverly Sackler Faculty of Exact Sciences,
Tel Aviv University, Tel Aviv, Israel
noga@math.tau.ar.il
and
ZOLTÁN FÜREDI
Department of Mathematics, University of Illinois,
Urbana, Illinois 61801, U.S.A.
zoltan@math.uinc.edu
and
Mathematical Institute of the Hungarian Academy of Sciences,
P.O. Box 127, 1364 Budapest, Hungary