Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Combinatorial Theory, Series A 109 (2005) 331–338
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

Note

Essential covers of the cube by hyperplanes

Nathan Linial[a], Jaikumar Radhakrishnan[b]

[a] *Institute of Computer Science, Hebrew University, Jerusalem 91904, Israel*
[b] *School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai 400 005, India*

Received 31 October 2003
Available online 12 November 2004

Abstract

A set L of linear polynomials in variables $X_1, X_2, \ldots, X_n$ with real coefficients is said to be an essential cover of the cube $\{0,1\}^n$ if

(E1) for each $v \in \{0,1\}^n$, there is a $p \in L$ such that $p(v) = 0$;
(E2) no proper subset of L satisfies (E1), that is, for every $p \in L$, there is a $v \in \{0,1\}^n$ such that p alone takes the value 0 on v;
(E3) every variable appears (in some monomial with non-zero coefficient) in some polynomial of L.

Let $e(n)$ be the size of the smallest essential cover of $\{0,1\}^n$. In the present note we show that

$$\frac{1}{2}(\sqrt{4n+1}+1) \leqslant e(n) \leqslant \left\lceil \frac{n}{2} \right\rceil + 1.$$

1. Introduction

What is the least number of hyperplanes that cover all the points of $\mathcal{B}_n \triangleq \{0,1\}^n$? The obvious answer is "two". This set is full-dimensional, so no single hyperplane will do, and on the other hand the two hyperplanes $X_1 = 0$ and 1 do. This solution is unsatisfactory, since this is really a one-dimensional solution. For the answer to make sense, we should insist that every variable appears in the equation defining one of the hyperplanes. This is still, however, not a good formulation of the problem, for we may consider the three hyperplanes

E-mail address: jaikumar@tifr.res.in

0097-3165/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2004.07.012

$X_1 = 0, 1$ and $\sum_i X_i = 17$. Granted, now all variables appear, but the last hyperplane is redundant. This already brings us to the main concept under consideration here.

A collection L of linear polynomials in variables $X = \{X_1, X_2, \ldots, X_n\}$ with real coefficients is called an *essential cover* of $\mathcal{B}_n = \{0, 1\}^n$ if

(E1) for each $v \in \mathcal{B}_n$, there is a $p \in L$ such that $p(v) = 0$;
(E2) no proper subset of L satisfies (E1), that is, for every $p \in L$, there is a $v \in \mathcal{B}_n$ such that p alone takes the value 0 on v (we say that v is a *private point* of p);
(E3) every variable appears (in some monomial with non-zero coefficient) in some polynomial of L.

Let $e(n)$ be the size of the smallest essential cover of $\mathcal{B}_n$. In the present note we show that

$$\frac{1}{2}\left(\sqrt{4n+1}+1\right) \leqslant e(n) \leqslant \left\lceil \frac{n}{2} \right\rceil + 1.$$

2. The upper bound

Case $n = 1$: $L = \{X, 1 - X\}$ is an essential cover of $\mathcal{B}_1$ of minimum size.
Case $n = 2$: $L = \{X_1 + X_2 - 1, X_1 - X_2\}$ is an essential cover of $\mathcal{B}_2$ of minimum size.
One can combine these constructions to produce essential covers for other values of n.

Lemma 1. *Suppose* $L_1 = \{p_1, p_2, \ldots, p_{e_1}\}$ *is an essential cover of* $\mathcal{B}_m$ *with variables* $\{X_i : i \in [m]\}$ *and* $L_2 = \{q_1, q_2, \ldots, q_{e_2}\}$ *is an essential cover of* $\mathcal{B}_n$ *with variables* $\{Y_i : i \in [n]\}$. *Then,*

$$L \triangleq \{p_1 + q_1, p_2, \ldots, p_{e_1}, q_2, \ldots, q_{e_2}\}$$

is an essential cover of $\mathcal{B}_{m+n}$ *with variables* $\{X_1, X_2, \ldots, X_m, Y_1, Y_2, \ldots, Y_n\}$.

Proof. In order to verify that L satisfies (E1), we show that every $v \in \mathcal{B}_{m+n}$ is the root of at least one of the polynomial in L. To see this, write v as $v_1 v_2$, where $v_1 \in \mathcal{B}_m$ and $v_2 \in \mathcal{B}_n$. If $p_2(v_1), p_3(v_1), \ldots, p_m(v_1), q_2(v_2), \ldots, q_n(v_2)$ are all non-zero, then $p_1(v_1) = 0$ and $q_1(v_2) = 0$ (because L_1 and L_2 are essential covers). It follows that $p_1(v_1) + q_1(v_2) = 0$. To show that (E2) holds, we need to verify that each polynomial in L has a private point. For $i = 1, \ldots, e_1$, let v_i be a private point of p_i in $\mathcal{B}_m$; similarly, for $j = 1, \ldots, e_2$, let w_j be a private point of q_j in $\mathcal{B}_n$. Then, for $i = 2, \ldots, e_1$, $v_i w_1$ is the private point of p_i, and for $j = 2, \ldots, e_2$, $v_1 w_j$ is a private point of q_j; also, $v_1 w_1$ is a private point for $p_1 + q_1$. Since L_1 and L_2 are essential, it follows immediately that all variables in $\{X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_m\}$ appear in L; so (E3) holds. □

By combining the essential cover for $\mathcal{B}_2$ with itself k times, we obtain the following essential cover for $\mathcal{B}_{2k}$:

$$L = \{X_{2i-1} - X_{2i} : i = 1, 2, \ldots, k\} \cup \{X_1 + X_2 + \cdots + X_{2k} - k\}.$$

For $n = 2k + 1$, we combine this cover of $\mathcal{B}_{2k}$ with the cover $\{X_n, X_n - 1\}$ for $\mathcal{B}_1$, and obtain

$$\{X_{2i-1} - X_{2i} : i = 1, 2, \ldots, k\} \cup \{X_1 + X_2 + \cdots + X_n - k\} \cup \{X_n - 1\}.$$

We thus have the following theorem.

Theorem 1. *For all $n \geqslant 1$, we have $e(n) \leqslant \lceil \frac{n}{2} \rceil + 1$.*

Remark. (a) It is not hard to verify directly, without recourse to Lemma 1, that the sets defined above are essential covers.

(b) While combining essential covers using Lemma 1, we can choose the polynomials p_1 and q_1 as we wish. By choosing them carefully, we can find an essential cover in which no polynomial has more than four variables. For example, take $n = 2k$ and use variables $X_1, X_2, \ldots, X_k, Y_1, Y_2, \ldots, Y_k$. Then, we have the following essential cover for $\mathcal{B}_n$:

$$\{X_1 + Y_1 - 1\} \cup \{X_i - Y_i + X_{i+1} + Y_{i+1} - 1 : i = 1, 2, \ldots, k - 1\} \cup \{X_k - Y_k\}.$$

3. The lower bound

Preliminaries: In this section, we derive lower bounds on $e(n)$. Let L be an essential cover of $\mathcal{B}_n$. Since (E3) holds, every variable appears in some polynomial in L. Consider a variable X_i and let $p \in L$ be a polynomial in which X_i appears. By (E2), p has a private point σ. Let σ' be the point obtained from σ complementing the value of X_i. Now, p cannot take the value 0 on σ', so (to satisfy (E1)) there must be another polynomial $p' \in L$ that takes the value 0 on σ'. Now, X_i appears in p', or else σ is not a private point of p. We conclude that every variable appears at least twice in L. Let k be the maximum number of variables that appear in any polynomial in L. We immediately have

$$|L| \geqslant \frac{2n}{k}. \tag{1}$$

Our lower bound follows by combining this with an algebraic argument using the correspondence between multilinear polynomials with real coefficients and functions from $\mathcal{B}_n$ to $\mathbb{R}$. Formally, we consider the natural homomorphism from the ring $\mathbb{R}[X_1, X_2, \ldots, X_n]$ to the ring of functions from $\mathcal{B}_n$ to $\mathbb{R}$ given by $p \mapsto f_p$, where the $f_p(v) \triangleq p(v)$. The kernel of this map is the ideal I generated by the polynomials $\{X_i^2 - X_i : i = 1, 2, \ldots, n\}$. Hence, we have a ring isomorphism between the ring $R = \mathbb{R}[X_1, X_2, \ldots, X_n]/I$ and the ring of functions from $\mathcal{B}_n$ to $\mathbb{R}$. Every element of $\mathbb{R}[X_1, X_2, \ldots, X_n]/I$ is represented uniquely in the form $p(X) + I$, where $p(X)$ is a multilinear polynomial.

Since $\prod_{p \in L} f_p = 0$, we have that $\prod_{p \in L} p = 0$ in R. In particular, if we fix a polynomial $q \in L$ and let

$$r \triangleq \prod_{p \in L, p \neq q} p,$$

then $r \neq 0$ and $qr = 0$ in the ring R. Note that the degree of r is at most $|L| - 1$.

Lemma 2. *Let q and r be polynomials in R. Suppose q is linear with k ($\geqslant 1$) variables, $r \neq 0$ and $qr = 0$ in R. Then, r has degree at least $\frac{k}{2}$.*

Before we present the proof of this lemma, let us derive our lower bound assuming that it holds. Since the degree of r is at most $|L| - 1$, we see that

$$|L| \geqslant \frac{k}{2} + 1$$

and on combining this with (1) we obtain the required lower bound.

Theorem 2. $|L| \geqslant \max\left\{\frac{2n}{k}, \frac{k}{2} + 1\right\} \geqslant \frac{1}{2}\left(\sqrt{4n+1} + 1\right)$.

We still need to prove Lemma 2.

Proof. Let us assume that $X_1, \ldots, X_k$ are the variables appearing in q. Since $r \neq 0$, we can choose a $v \in \mathcal{B}_n$ such that $r(v) \neq 0$. For $i = k+1, k+2, \ldots, n$, set $X_i = v_i$. We now treat q and r are polynomials in variables $\{X_i : i \in [k]\}$. There is an assignment v' to $\{X_i : i \in [k]\}$ under which r does not evaluate to 0; in fact, $v'_i = v_i$ ($i = 1, 2, \ldots, k$) is such an assignment. We 'shift the origin' to v' by substituting $1 - X_i$ for X_i whenever $v'_i = 1$. We have thus arranged that

(a) q and r are multilinear polynomials with variables $\{X_i : i \in [k]\}$;
(b) q has the form $\sum_{i=1}^{k} \alpha_i X_i$, where $\alpha_i \neq 0$ for $i \in [k]$;
(c) r has degree at most the degree of the original polynomial r, and $r(0) \neq 0$;
(d) $qr = 0$ in R.

To prove our lemma, it is sufficient to show that r has degree at least $\frac{k}{2}$. We present two arguments.

Proof. (1) For $T \subseteq [k]$, let $X_T \triangleq \prod_{i \in T} X_i$. Write $r = \sum_{T \subseteq [k]} \beta_T X_T$. Let d be the degree of r; so, there is a set $T \subseteq [k]$ of size d such that $\beta_T \neq 0$, but for all T' with $|T'| > d$, we have $\beta_{T'} = 0$. If $d = k$, we have nothing to prove because then $d \geqslant \frac{k}{2}$. Assume $d < k$, and let us examine the coefficients of the monomials in qr. Since $qr = 0$ in R, each such coefficient is 0. In particular, for each $S \subseteq [k]$ of size $d+1$ we have

$$\sum_{i \in S} \alpha_i \beta_{S \setminus \{i\}} = 0. \tag{2}$$

For $T \subseteq [k]$, let $\alpha_T \triangleq \prod_{i \in T} \alpha_i$. By dividing both sides of (2) by α_S, we get

$$\sum_{i \in S} \frac{\beta_{S \setminus \{i\}}}{\alpha_{S \setminus \{i\}}} = 0.$$

Thus, if we define $\beta'_T \triangleq \beta_T/\alpha_T$, for $T \subseteq [k]$ of size d, we obtain

$$\sum_{T \subseteq S} \beta'_T = 0,$$

where the sum ranges over subsets T of S of size exactly d. That is, $(\beta'_T : T \subseteq [k], |T| = d)$ constitutes a non-zero solution to the system of linear equations

$$A \cdot \bar{\beta} = 0,$$

where A is the $\binom{k}{d+1} \times \binom{k}{d}$ set inclusion matrix (with rows indexed by sets S of size $d+1$ and columns by sets T of size d, and $A[S,T] = 1$ if $S \supseteq T$ and $A[S,T] = 0$ otherwise). This matrix has rank $\min\{\binom{k}{d}, \binom{k}{d+1}\}$ (this was shown many times, but the first proof we are aware of is in [3]). Since not all β'_T are 0, we have $\binom{k}{d+1} < \binom{k}{d}$, that is, $d \geqslant \frac{k}{2}$.

(2) Let P be the set of variables that appear in q with positive coefficients. By replacing q by $-q$ if necessary, we ensure that $|P| \leqslant \frac{k}{2}$. Set the variables in P to 0. Now, the only assignment to the remaining variables under which q is 0 is the all-zeros assignment. View q and r as non-zero multilinear polynomials in $k' \geqslant \frac{k}{2}$ variables. Since $qr = 0$ and $q(w) \neq 0$ for all $w \in \mathcal{B}_{k'} \setminus \{0\}$, we have $r(w) = 0$ for all $w \in \mathcal{B}_{k'} \setminus \{0\}$. We already know that $r(0) \neq 0$. A result of Alon and Füredi [1] states that in this situation r has degree at least k'. Indeed, the multilinear polynomial $r(0)\prod_{i \in [k] \setminus P}(1 - X_i)$ and r agree on all points in $\mathcal{B}_{k'}$. Since functions on $\mathcal{B}_{k'}$ are represented uniquely by multilinear polynomials, this polynomial must be r; hence, r has degree at least $k' \geqslant \frac{k}{2}$. □

3.1. A lower bound using Sperner's theorem

A lower bound for $e(n)$ can be obtained using a combinatorial argument. This lower bound is weaker than the lower bound derived above using algebraic arguments, but the combinatorial argument is applicable to coverings of the hypercube by structures more general than hyperplanes. In this section, we present the combinatorial lower bound for $e(n)$ and bounds for covering the hypercube by combinatorial structures related to hyperplanes.

The combinatorial lower bound for $e(n)$: Let L be an essential cover of $\mathcal{B}_n$ with variables $\{X_i : 1 \leqslant i \leqslant n\}$. Let $k = \lfloor n^{2/3} \rfloor$. Let L_1 be the subset of L produced by the following greedy procedure.

Initially, $L_1 = \emptyset$.

Let S denote the set of variables that appear in some polynomial in L_1 (so, initially $S = \emptyset$). If there is a polynomial $p \in L \setminus L_1$ such that p has at most k variables outside S, then set $L_1 \leftarrow L_1 \cup \{p\}$. Repeat.

Clearly,

$$|L_1| \geqslant \frac{|S|}{k}.$$

If $|S| \geqslant \frac{n}{2}$, we see that $|L| \geqslant |L_1| = \Omega(n^{1/3})$. If $|S| \leqslant \frac{n}{2}$, then every polynomial in $L_2 \triangleq L \setminus L_1$ has more than k variables outside S. Furthermore, there is an assignment to the variables

in S under which each polynomial in L_1 takes a non-zero value. So, on each of the $2^{n-|S|}$ points of $\mathcal{B}_n$ compatible with this assignment, some polynomial in L_2 takes the value 0. We will show below that any one polynomial in L_2 evaluates to zero on a fraction at most

$$2^{-k}\binom{k}{\lfloor \frac{k}{2} \rfloor} = O(1/\sqrt{k})$$

of such points. So, $|L| \geqslant |L_2| = \Omega(\sqrt{k}) = \Omega(n^{1/3})$.

Fix a polynomial $p \in L_2$ with $k' > k$ variables. Let $p(X) = \sum_{i=1}^{k'} \alpha_i X_i - \beta$. By substituting $1 - X_i$ for X_i whenever necessary, we can assume that the α_i's are all positive. We may view the 0-1 assignments to $X_1, \ldots, X_{k'}$ as subsets of $[k']$. Then, it is easy to see that the roots of this polynomial (corresponding to assignments to variables $(X_i : i \notin S)$) have the form $A \times \{0,1\}^{n-|S|-k'}$, where A is an antichain of subsets of $[k']$. By Sperner's theorem [2,4] the size of the largest antichain of subsets of $[k']$ is at most $\binom{k'}{\lfloor \frac{k'}{2} \rfloor}$. So, the number of roots of p is at most

$$2^{n-|S|-k'}\binom{k'}{\lfloor \frac{k'}{2} \rfloor} = O(2^{n-|S|}/\sqrt{k'}).$$

Coverings using other combinatorial structures: We now consider a combinatorial generalization of hyperplanes and study the problem of covering the hypercube using such structures.

Definition 1. Let $S = P \cup N$ be a partition of $S \subseteq [n]$. Consider the ordering on subsets of S where by $A \leqslant B$ if and only if $A \cap P \subseteq B \cap P$ and $B \cap N \subseteq A \cap N$. An antichain in the resulting partially ordered set is called a *signed antichain of subsets of S* (the elements in P are to be thought of as positive elements and the elements in N are to be thought of as negative elements). The usual antichain of subsets corresponds to the situation when $N = \emptyset$. A *signed antichain cube* (SAC) with support S is a family of subsets $[n]$ of the form

$$\{A \cup B : A \in \mathcal{A} \text{ and } B \subseteq [n] \setminus S\},$$

where $\mathcal{A}$ be a signed antichain of subsets of S. If we restrict $\mathcal{A}$ to be an antichain of subsets of S we get an *antichain cube* (AC) *with support S*.

We may consider essential covers of $\mathcal{B}_n$ (identifying elements of $\mathcal{B}_n$ with subsets of $[n]$ in the natural manner) using SACs: every element of $\mathcal{B}_n$ should appear in some SAC, every element in $[n]$ should be in the support of some SAC, and every SAC should have a private point. Note that the set of points lying on a hyperplane form an SAC. So, the upper bound obtained earlier is still valid. The algebraic proof of the lower bound is no longer valid, but the combinatorial proof can be easily adapted to this setting, yielding the same $\Omega(n^{1/3})$ lower bound.

What about essential covers of $\mathcal{B}_n$ by ACs? The family of hyperplanes $\{\sum_{i=1}^{n} X_i = j : 0 \leqslant j \leqslant n\}$ is an essential cover of $\mathcal{B}_n$ by ACs. We do not know a better upper bound. The lower bound of $\Omega(n^{1/3})$ observed above for essential covers of $\mathcal{B}_n$ by SACs is still valid. We can improve this bound to $\Omega(\sqrt{n})$ if we restrict ourselves to ACs.

To get the lower bound of $\Omega(\sqrt{n})$, we first use a greedy procedure similar to the one used above. Let $k = \lfloor \sqrt{n} \rfloor$. Let L be an essential cover of $\mathcal{B}_n$ by ACs. Let L_1 be the subset of L returned by the following greedy procedure.

Initially, $L_1 = \emptyset$.

Let I denote the union of the supports of the ACs that appear in L_1 (so, initially $I = \emptyset$). If there is an element $C \in L \setminus L_1$ whose support has at most k elements outside S, then set $L_1 \leftarrow L_1 \cup \{C\}$. Repeat.

As before, $|L_1| \geqslant \frac{|I|}{k}$. If $|I| = n$, we have $|L| \geqslant |L_1| = \sqrt{n}$. If $|I| < n$, L_1 is a proper subset of L, and there is a set $S \subseteq I$ that is not in any of the ACs in L_1 (because no proper subset of L covers $\mathcal{B}_n$). Consider the $n - |I|$ dimensional subcube consisting of those subsets of $[n]$ whose intersection with I is exactly S. Note that the restriction of an AC in $L - L_1$ to this subcube is an AC whose support has at least $k + 1$ elements. We thus obtain a subcube of $\mathcal{B}_n$, that is covered by a set L' (with $|L'| \leqslant |L|$) of ACs all of whose supports have at least $k + 1$ elements. In this situation the following lemma implies that $|L| \geqslant |L'| \geqslant k + 2 > \sqrt{n} + 1$.

Lemma 3. *Let $\mathcal{C}$ be a cover of $\mathcal{B}_m$ by ACs such that the support of each element of $\mathcal{C}$ has size at least k. Then, $|\mathcal{C}| \geqslant k + 1$.*

Proof. Let π be a random permutation of $[n]$. Consider the chain of sets $\emptyset = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_n$, where $A_i \triangleq \{\pi(1), \pi(2), \ldots, \pi(i)\}$. We will show that the expected number of elements of this chain that appear in any one AC in $\mathcal{C}$ is at most $(m + 1)/(k + 1)$. Since there are $m + 1$ elements in this chain, it follows that $|\mathcal{C}| \geqslant k + 1$.

Fix some $C \in \mathcal{C}$. To estimate the number elements of C in the random chain, it will be convenient to generate the permutation π using the following two-step experiment. Suppose S is the support of C and S has ℓ elements. Let $\mathcal{A}$ be the antichain of subsets of S associated with C.

Step 1: Pick a random permutation $\sigma = (i_1, i_2, \ldots, i_\ell)$ of S, with each of the $\ell!$ possibilities being equally likely.

Step 2: Extend σ to a random permutation π of $[m]$, by inserting the elements of $[m] \setminus S$ one after another into the gaps. That is, we insert the first element into one of the $\ell + 1$ gaps at random, insert the second element into the resulting $\ell + 2$ gaps at random, and so on.

Clearly, the permutation π thus generated is equally likely to be any of the $m!$ permutations of $[m]$. Consider the situation after σ has been chosen in Step 1. Since $\mathcal{A}$ is an antichain, there is at most one position $j \in \{0, \ldots, \ell\}$ for which the set $B_j = \{i_1, i_2, \ldots, i_j\}$ is in $\mathcal{A}$. Now, consider the extension π of σ generated in Step 2, and the resulting chain $(A_i : 0 \leqslant i \leqslant m)$. If A_i is in C, then, $B_j \subseteq A_i$ and (unless $j = \ell$) $A_i \subset B_{j+1}$. That is, the number of elements of the random chain that are in C is at most one plus the number of elements of $[m] - S$ that appear between i_j and i_{j+1} in π (When $j = 0$, we consider all elements that appear to the left of i_1 in π, and when $j = \ell$ we consider the elements that appear to the right of i_ℓ in π.) Thus, for each choice of σ in Step 1, the (conditional) expected number of elements the random chain shares with C is at most $1 + \frac{m-\ell}{\ell+1} = \frac{m+1}{\ell+1}$. Our claim follows from this by averaging over the choices of σ in the Step 1. $\square$

References

[1] N. Alon, Z. Füredi, Covering the cube by affine hyperplanes, Europ. J. Combin. 14 (1993) 79–83.
[2] I. Anderson, Combinatorics of Finite Sets, Clarendon Press, Oxford, 1987.
[3] D.H. Gottlieb, A certain class of incidence matrices, Proc. Amer. Math. Soc. 17 (1966) 1233–1237.
[4] E. Sperner, Ein Satz über Untermenger einer edlichen Menge, Math. Z. 27 (1928) 544–548.