SIAM J. Discrete Math.
Vol. 11, No. 4, pp. 624–632, November 1998

© 1998 Society for Industrial and Applied Mathematics
007

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

DIMENSION OF PROJECTIONS IN BOOLEAN FUNCTIONS[*]

RAMAMOHAN PATURI AND FRANCIS ZANE[†]

Abstract. A projection is a subset of $\{0,1\}^n$ given by equations of the form $x_i = x_j$, $x_i = \bar{x}_j$, $x_i = 0$, and $x_i = 1$, where for $1 \leq i \leq n$, x_i are Boolean variables and $\bar{x}_i$ are their complements. We study monochromatic projections in 2-colorings of an n-dimensional Boolean cube. We also study the dimension of the largest projection contained in a set specified by its density. We prove almost matching lower and upper bounds on the density of a set required to guarantee the existence of a d-dimensional projection. We also prove almost tight upper and lower bounds on the dimension of monochromatic projections in arbitrary Boolean functions. We then prove almost tight upper and lower bounds on the dimension of monochromatic projections in Boolean functions represented by low degree GF(2) polynomials. It follows from these lower bounds that low-degree GF(2) polynomials can define Boolean functions which are close to being extremal with respect to the property of having no large dimensional monochromatic projections.

Key words. projections, Ramsey theory, circuit complexity

AMS subject classifications. 05D10, 68Q15, 68R05

PII. S0895480197318313

1. Introduction.

In this paper, we study monochromatic projections in 2-colorings of an n-dimensional Boolean cube. We also consider the related density question: what is the density required to guarantee the existence of a d-dimensional projection? A projection is a subset of $\{0,1\}^n$ given by equations of the form $x_i = x_j$, $x_i = \bar{x}_j$, $x_i = 0$, and $x_i = 1$, where for $1 \leq i \leq n$, x_i are the Boolean variables and $\bar{x}_i$ are their complements. Thus, a projection is an affine subspace of the n-dimensional $GF(2)$ space $\{0,1\}^n$. The dimension of a projection is its dimension as an affine subspace. A projection P is monochromatic under a Boolean function f if $P \subseteq f^{-1}(1)$ or $P \subseteq f^{-1}(0)$. Projections are closely related to Boolean algebras, whose Ramsey-theoretic properties have been studied extensively [4]. Boolean algebras are projections where equations of the form $x_i = \bar{x}_j$ are not allowed, so the sets are always oriented in a canonical direction. Gunderson, Rödl, and Sidorenko [3] recently obtained almost matching bounds on the density required for the existence of a d-dimensional Boolean algebra. They also obtained almost tight bounds for the dimension of the largest monochromatic Boolean algebras under colorings of the Boolean cube.

In addition to being natural generalizations of Boolean algebras, projections are relevant to the study of circuit complexity of Boolean functions. For example, it is shown in [5] that if the set of satisfying solutions of a 2-CNF (conjunctive normal form with two literals per clause) is large, then it must contain a large dimensional projection. The existence of such *nice* subsets gives one a handle to construct *hard* functions for a given class of Boolean circuits. In particular, Boolean functions which do not have large dimensional monochromatic projections require large size depth-3 unbounded fan-in Boolean circuits with bottom fan-in 2. An interesting open question is whether Boolean functions computable by linear size circuits have $\omega(n^{3/4} \log n)$-dimensional monochromatic projections. A positive answer to this question implies that certain explicitly defined Boolean functions in NC (the class of Boolean functions

[*] Received by the editors March 12, 1997; accepted for publication (in revised form) December 15, 1997; published electronically September 1, 1998.

http://www.siam.org/journals/sidma/11-4/31831.html

[†] Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA 92093 (paturi@cs.ucsd.edu, francis@cs.ucsd.edu).

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

computable by logspace uniform circuits of polylogarithmic depth and polynomial size) require nonlinear circuit size [5]. Proving lower bounds on the circuit size of interesting explicit Boolean functions is a fundamental challenge in complexity theory.

In this paper, we obtain density results for projections using techniques similar to those employed in [3]. We show that the existence of projections requires much lower density than in the case of Boolean algebras. We also obtain bounds on the dimension of the largest monochromatic projections in arbitrary Boolean functions. In addition, we consider the question of constructing Boolean functions which do not have large monochromatic projections. Although we do not have any explicit constructions, we show that there are functions much simpler than arbitrary Boolean functions which have this property. More precisely, we show that there exist degree-q GF(2) polynomials representing Boolean functions which have only $O(q(n \log n)^{1/q})$-dimensional monochromatic projections. It follows that there are Boolean functions represented by logarithmic degree polynomials which are nearly extremal with respect to the size of monochromatic projections. Pudlák, Rödl, and Savichý [6] and Razborov [7] obtained similar "low complexity" probabilistic constructions for combinatorial objects. We also show that the bounds obtained by the probabilistic technique are almost tight: given a degree-q GF(2) polynomial, we show how to construct a $\Omega(qn^{1/q})$-dimensional monochromatic projection.

We first introduce some definitions and state our results precisely. The following sections present the proofs of our results.

1.1. Definitions. Let $[n] = \{1, 2, \ldots, n\}$. Let $B_n = \{0, 1\}^n$ denote the n-dimensional Boolean cube. We will also regard B_n as an n-dimensional $GF(2)$ vector space. A projection $P \subseteq B_n$ is the set of all $(x_1, x_2, \ldots, x_n) \in B_n$ satisfying a system of equations of the form $x_i = x_j$, $x_i = \bar{x}_j$, $x_i = 0$, and $x_i = 1$. x_i are Boolean variables and $\bar{x}_i$ is the complement of x_i. The dimension of a projection is its dimension as an affine subspace. It is convenient to think of a d-dimensional projection as a partition $\{A_0, B_0, A_1, B_1, \ldots, A_d, B_d\}$ of $\{1, 2, \ldots, n\}$ with $A_0, B_0, B_1, \ldots, B_d$ possibly empty. A_0 and B_0 are the sets of variables which are set to 0 and 1, respectively. For $1 \le i \le d$, A_i is nonempty and all its variables are equal to each other. Furthermore, the variables in B_i are equal to each other and equal to the complement of the variables in A_i. We obtain a set of free variables of a projection by selecting a representative from each class A_i for $1 \le i \le d$.

We also need some notation to deal with hypergraphs. A d-uniform hypergraph is a pair $G = (V, E)$ with vertex set V and hyperedge set $E \subseteq \binom{V}{d}$, where $\binom{V}{d}$ is the set of all d-subsets of V. A d-partite d-uniform hypergraph is a $d+1$-tuple $G = (X_1, X_2, \ldots, X_d, E)$, where X_i are pairwise disjoint sets and $(\cup_{i=1}^{d} X_i, E)$ is a d-uniform hypergraph whose edges have exactly one point from each X_i. The sets X_i are called partite sets. The complete d-partite d-uniform hypergraph with two vertices in each partite set and having 2^d edges is denoted by $K^{(d)}(2, 2, \ldots, 2)$. Let $ex(n, H)$ be the maximum number of d-hyperedges in a hypergraph on n vertices which does not contain a copy of H.

1.2. Statement of the results. Let $\rho(n, d)$ denote the maximum density of a subset $A \subseteq B_n$ which does not contain a d-dimensional projection. Our first result gives upper and lower bounds on $\rho(n, d)$.

THEOREM 1.

$$2^{-\frac{n \log(2d+2)}{2^d} - 2} \le \rho(n, d) \le 2^{-\frac{n}{d(2^d - 1)} + 1}.$$

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

Let f be a Boolean function with the domain $\{0,1\}^n$. Let $\tau(f)$ be the dimension of the largest monochromatic projection of f. Let $d_n = \min_f \tau(f)$.

THEOREM 2.

$$\log n - \log\log n + o(1) \le d_n \le \log n + \log\log\log n + o(1).$$

Compared to the more restricted class of Boolean algebras, the dimension of the largest projection which exists in an arbitrary subset of B_n is much larger. Let $\rho^{BA}(n,d)$ and d_n^{BA} be the analogues of $\rho(n,d)$ and d_n defined for Boolean algebras rather than projections. The corresponding results for these quantities from [3] are

$$c_1(d)n^{-\frac{d}{2^{d+1}-2}(1-o(1))} \le \rho^{BA}(n,d) \le c_2(d)n^{-\frac{1}{2^d}}$$

and

$$\log\log n - (1+o(1))\log\log\log n \le d_n^{BA} \le \log\log n + \log\log\log n.$$

We next consider the problem of constructing objects that match the bounds established earlier. We show that the set of codewords of a "good" code (that is, a code with constant rate and linear distance) can only contain bounded dimensional projections. However, our technique involving codes does not help us in constructing sets of size $c2^n$ whose largest projection has dimension $O(\log n)$. Furthermore, it is not clear how to use codes to construct Boolean functions with no large monochromatic projections, since the set of noncodewords may contain large projections.

Although we could not construct such Boolean functions, our next result shows that simple functions exist which do not contain monochromatic projections of dimension larger than $\log n + \log\log\log n$. We use low-degree GF(2) polynomials to represent Boolean functions. Using a probabilistic argument, we obtain the following.

COROLLARY 1. *There are degree q GF(2) polynomials whose largest monochromatic projection has dimension $O(q(n\log n)^{1/q})$.*

At the extreme end, we have the following.

COROLLARY 2. *There exists a GF(2) polynomial of degree $\lceil \log n + \log\log\log n + o(1)\rceil$ which has no monochromatic projections of dimension greater than $\lceil \log n + \log\log\log n + o(1)\rceil$.*

We also prove that this bound is almost tight.

COROLLARY 3. *Every degree q GF(2) polynomial contains a monochromatic projection of dimension $\Omega(qn^{1/q})$.*

Open problems.

1. Construct a Boolean function with the largest monochromatic projection of dimension $O(\log n)$.
2. Construct degree q GF(2) polynomials with the largest monochromatic projection of dimension $O(q(n\log n)^{1/q})$.

2. Dimension of projections in arbitrary Boolean functions. We adopt the techniques of Erdős [2] and Gunderson, Rödl, and Sidorenko [3] to obtain upper and lower bounds on the density required to guarantee the existence of a d-dimensional projection.

LEMMA 2.1. *For r-uniform, r-partite hypergraphs with n/r nodes in each part,*

$$ex(n, K^{(r)}(2,\ldots,2)) \le 2(n/r)^{r-\frac{1}{2^{r-1}}}$$

when $n \ge 16r$.

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

Proof. Let $G = (X_1, X_2, \dots, X_r, E)$. The proof is by induction on r.

If $r = 2$, the lemma says that every $(\frac{n}{2}, \frac{n}{2})$-node bipartite graph (X_1, X_2, E) with $|E| \geq 2(\frac{n}{2})^{\frac{3}{2}}$ has a 4-cycle. The number of pairs of nodes (counted with repetition) in X_2 with a common neighbor in X_1 is $m = \sum_{v \in X_1} \binom{\deg(v)}{2}$. If this is larger than $\binom{n/2}{2}$, the number of distinct pairs of nodes in X_2, then some pair is counted twice, and a 4-cycle exists. m is minimized when every node in X_1 has average degree $\frac{|E|}{(n/2)} > 2\sqrt{\frac{n}{2}}$. In this case, $m = \frac{n}{2}\binom{2\sqrt{n/2}}{2} > \binom{n/2}{2}$ for $n \geq 0$.

If $r > 2$, by hypothesis $|E| \geq 2(\frac{n}{r})^{r - \frac{1}{2^{r-1}}}$. We first find two nodes $a_1, a_2 \in X_r$ for which there are many pairs of hyperedges $(y_1, \dots, y_{r-1}, a_1)$ and $(y_1, \dots, y_{r-1}, a_2)$. We then select those two nodes for part r of the r-partite graph $K^{(d)}(2, 2, \dots, 2)$, and use induction to select the remaining parts. To show that such a pair of nodes exist, we use the following lemma.

LEMMA 2.2 (Erdős). *Let S be a set of N elements, $y_1, \dots, y_N$, and let $A_i, 1 \leq i \leq k$, be subsets of S. Let w be such that $\sum_i |A_i| \geq \frac{kN}{w}$. If $k \geq 2l^2w^l$, then there exist $A_{i_1}, \dots, A_{i_l}$ such that $|\cap_j A_{i_j}| \geq \frac{N}{2w^l}$.*

Now, apply the lemma with S as the set of all $(r-1)$-tuples from $X_1 \times \cdots \times X_{r-1}$ and A_i as the set of all such tuples which, when extended by the ith element of X_r, belong to E. Then $N = (\frac{n}{r})^{r-1}, k = n/r, w = \frac{1}{2}(\frac{n}{r})^{\frac{1}{2^{r-1}}}$, and $l = 2$. Since $n \geq 16r$, the condition on k in the lemma is satisfied. There exist a_1, a_2 which have

$$\frac{N}{2w^2} \geq \frac{(\frac{n}{r})^{r-1}}{2(\frac{1}{2}(\frac{n}{r})^{\frac{1}{2^{r-1}}})^2} \geq 2\left(\frac{n}{r}\right)^{(r-1) - \frac{1}{2^{r-2}}}$$

$(r-1)$-tuples in common. By induction, there exists a $K^{(r-1)}(2, \dots, 2)$ among these $(r-1)$-tuples. This can then be extended to a $K^{(r)}(2, \dots, 2)$ by extending each such $(r-1)$-tuple $(y_1, \dots, y_{r-1})$ to $(y_1, \dots, y_{r-1}, a_1)$ and $(y_1, \dots, y_{r-1}, a_2)$. □

We now apply the lemma to obtain an upper bound on $\rho(n, d)$, the density required to guarantee the existence of a d-dimensional projection.

LEMMA 2.3. *For $n \geq 4$,*

$$\rho(n, d) \leq 2^{-\frac{n}{d(2^d - 1)} + 1}.$$

Proof. We only consider the case where $d \leq \log n$ since, otherwise, the theorem is vacuously true.

Given a set A with $|A| \geq 2^{n(1 - \frac{1}{d(2^d-1)}) + 1}$, one can obtain a d-dimensional projection as follows.

Partition $[n]$ into d classes, X_i, such that the largest class size is $\lceil n/d \rceil$ and the smallest class size is $\lfloor n/d \rfloor$. Consider the following d-uniform, d-partite hypergraph H. The ith part H_i will have $2^{|X_i|}$ vertices, indexed by $\{0,1\}^{|X_i|}$. For each point $a \in A$, include the hyperedge $(a|_{X_1}, \dots, a|_{X_d})$ obtained by restricting a to the set of coordinates which appear in X_i.

Since this mapping between points and hyperedges is bijective, H has $2^{n(1 - \frac{1}{d(2^d-1)}) + 1}$ hyperedges, and by the construction, H is d-uniform, d-partite with $d2^{n/d}$ vertices. By the preceding lemma, and by the hypothesis $n \geq 4$, it follows that H must contain a $K^{(d)}(2, 2, \dots, 2)$, which we denote by $G = (Y_1, Y_2, \dots, Y_d, E')$.

Given any two points of $\{0,1\}^m$ for $m \geq 1$, we can obtain a one-dimensional projection by the following: for each coordinate, if both points have the same value in that coordinate, set the corresponding variable to that constant value. Since the

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

points are distinct, there is at least one coordinate which is 0 on one point and 1 on the other. Fix one such coordinate and a variable to denote the value in that position. All variables that were not set to constants are equated to this variable or its negation so that the collection of equations determines precisely the two points.

It is now clear that the Cartesian product $Y_1 \times Y_2 \times \cdots \times Y_d$ is a d-dimensional projection. □

Lemma 2.4.

$$\rho(n,d) \geq 2^{-\frac{n\log(2d+2)}{2^d}-2}$$

for all sufficiently large n.

Proof. Define $\varepsilon = 2^{-\frac{n\log(2d+2)}{2^d}-2}$. Consider the random set A obtained by selecting each element of $\{0,1\}^n$ independently with probability $\delta = 2\varepsilon$.

The probability that this set is smaller than $\varepsilon 2^n$ is at most (using the Chernoff bound [1]) $e^{-\frac{\varepsilon}{4}2^n}$.

Also, for any fixed d-dimensional projection P, the probability that P is contained in A is δ^{2^d}. The number of such projections is at most $(2d+2)^n$. Thus, the probability that such a randomly generated A has sufficiently large size and does not contain any d-dimensional projection is at least

$$1-(2\varepsilon)^{2^d}(2d+2)^n - e^{-\frac{\varepsilon}{4}2^n}.$$

For sufficiently large n, this probability is greater than zero, and thus there exists such a set A with $|A| \geq 2^{-\frac{n\log(2d+2)}{2^d}-2}2^n$ which contains no d-dimensional projections. □

The bounds from the lemmas are summarized in the following theorem.

Theorem 3.

$$2^{-\frac{n\log(2d+2)}{2^d}-2} \leq \rho(n,d) \leq 2^{-\frac{n}{d(2^d-1)}+1}.$$

Corollary 4. *Let d_n be the largest value such that every A with $|A| \geq 2^{n-1}$ contains a projection of dimension d_n.*

$$\log n - \log\log n + o(1) \leq d_n \leq \log n + \log\log\log n + o(1)$$

for all sufficiently large n.

For Boolean functions f, we state the following corollary.

Corollary 5. *If f is a Boolean function on n variables, then f has a monochromatic projection of dimension at least* $\log n - \log\log n + o(1)$.

Using a probabilistic argument very similar to the one used in Lemma 2.4, we obtain the following.

Corollary 6. *There are Boolean functions whose largest monochromatic projection has size at most* $\log n + \log\log\log n + o(1)$ *for all sufficiently large n.*

3. Explicit constructions.

Although we showed that high density sets with no large projections exist, the question of constructing such sets remains open. In this section, we give some constructions of sets which contain no large projections. We first show that the set of codewords of a good code has the property that it contains no projections of greater than constant dimension. However, these sets have very low density, and it is not clear how to extend this technique to construct sets with high density but no large projections. Instead, we show that a randomly chosen low

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

degree GF(2) polynomial is not constant on any large dimensional projection, with high probability. While this does not give an explicit construction of a set with the desired properties, it does show that there exist easily computed sets which have no large projections.

3.1. Explicit constructions using codes.

We start with a simple observation: if a set A contains a d-dimensional projection, then the set A has two points at a Hamming distance of at most n/d: if P is a d-dimensional projection, then it must contain a part with at most n/d variables, and by fixing all the variables outside the part consistent with the projection, we get two points which are at a distance of at most n/d. If A is a set of codewords for a code with rate r and distance δ, then A has size 2^{rn} and cannot contain a projection of dimension larger than n/δ. We can use constructions of linear codes to come up with "dense" sets with no large projections [8]. For example, for $0 < r < 1$, Justesen codes can be constructed with rate r and minimum distance at least $c_r n$ for some constant c_r for infinitely many n. Such codes can only include projections of bounded dimension.

For sets with constant density, it is easy to see that they can have at most constant minimum distance. Thus, this technique does not allow us to construct sets of size $c2^n$ which is guaranteed not to have projections of size $o(n)$.

3.2. Projections in functions defined by low degree GF(2) polynomials.

The results of the previous section leave open the question of constructing sets of size $c2^n$ with no large projections. Moreover, it is not clear how to apply the ideas in the previous section to construct Boolean functions with no large monochromatic projections. In particular, it is an interesting open question to construct Boolean functions whose largest monochromatic projection has dimension $O(\log n)$. Although we fall short of answering this question, we show that there are simple objects which define Boolean functions without large monochromatic projections. In particular, we consider Boolean functions defined by GF(2) polynomials and estimate the dimension of the largest monochromatic projection as a function of degree of the polynomial. Let $\delta(d)$ denote the largest degree such that all polynomials of smaller degree have a monochromatic d-dimensional projection. We provide almost tight upper and lower bounds on $\delta(d)$. From these bounds, it follows that there are $\lceil \log n + \log\log\log n + o(1)\rceil$-degree GF(2) polynomials such that the corresponding Boolean functions have no monochromatic projections of dimension larger than $\log n + \log\log\log n$.

Let $f(x_1, \ldots, x_n)$ be a GF(2) polynomial of degree q. Let P be projection of dimension d, and let $\{y_1, \ldots, y_d\}$ be a set of representative free variables for P. To restrict a polynomial to a projection, replace each variable by the corresponding representative free variable or its negation, as appropriate. It is clear that the polynomial f, when restricted to the projection P, is a polynomial in $\{y_i\}$ of degree at most q. The following lemma shows that there exist low-degree polynomials which do not have large monochromatic projections. A special case of this lemma appears in [5].

LEMMA 3.1. *For $d \geq \lceil \log n + \log\log\log n + o(1)\rceil$ and all sufficiently large n,*

$$\delta(d) \geq Q_1(d),$$

where $Q_1(d)$ is the least integer such that $\sum_{i=0}^{Q_1(d)} \binom{d}{i} > n\log(2d+2) + 1$.

Proof. Let $q = Q_1(d)$. Also, fix a projection P of dimension d. Let $V_1 = \{x_1, \ldots, x_d\}$ be a set of representative free variables for P, and let V_2 be the set of all other variables.

Consider the following method of generating random elements from the space of GF(2) polynomials in the variables V_1 of degree at most q: select a polynomial

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

uniformly at random from the space of all GF(2) polynomials in variables $V_1 \cup V_2$ of degree at most q, then restrict it to the projection P. The polynomials over the variables V_1 correspond to the cosets of the additive group of polynomials which are zero when restricted to P. Therefore, it is easy to see that this distribution is uniform in the space of polynomials in variables V_1 of degree at most q. Hence, the probability that a randomly chosen polynomial is constant when restricted to the projection P is at most $2^{1-\sum_{i=0}^{q}\binom{d}{i}}$.

Since there are at most $(2d+2)^n$ projections of dimension d, the probability that a randomly chosen GF(2) polynomial of degree at most q has any monochromatic projection of dimension d is at most

$$(2d+2)^n 2^{1-\sum_{i=0}^{q}\binom{d}{i}}.$$

Given the definition of q, it follows that this probability is less than 1. Thus, there exists a polynomial of degree at most q which has no monochromatic projection of dimension d. □

Corollary 7. *There exists a degree q GF(2) polynomial whose largest monochromatic projection has dimension $O(q(n\log n)^{1/q})$.*

At the extreme end, we have the following.

Corollary 8. *There exists a GF(2) polynomial of degree $\lceil \log n + \log\log\log n + o(1)\rceil$ which has no monochromatic projection of dimension greater than $\lceil \log n + \log\log\log n + o(1)\rceil$.*

As far as dense sets with no large projections are concerned, we obtain the following corollary.

Corollary 9. *There exists a set of size 2^{n-1} defined by a degree d GF(2) polynomial which does not contain projections of dimension greater than $O(q(n\log n)^{1/q})$.*

We now show how to construct a monochromatic projection given an arbitrary low-degree polynomial.

Theorem 4.

$$\delta(d) \le Q_2(d),$$

where $Q_2(d)$ is the greatest integer such that

$$2d+2+Q_2(d)\sum_{j=1}^{Q_2(d)-1}\binom{2d+3}{j} \le n.$$

Proof. Define $x^I = \prod_{x\in I} x_i$.

Let $f(x_1,\ldots,x_n) = \sum_{I\subset[n]} a_I x^I$ be an arbitrary polynomial of degree at most $q = Q_2(d)$ which is not identically 1. We will construct a d-dimensional projection which is a subset of $\{(x_1,\ldots,x_n) | f(x_1,\ldots,x_n) = 0\}$.

The projection will be constructed in several phases. Initially, all variables $V_0 = \{x_1,\ldots,x_n\}$ are available and we have a projection P_0 where all variables are free. Let $R_0 = \emptyset$. During phase i, a nonempty set $A_i \subseteq V_{i-1}$ of available variables are equated among themselves to obtain a new projection P_i from P_{i-1}, and those variables become unavailable, that is, $V_i = V_{i-1} - A_i$. Then a representative free variable is selected from A_i and added to R_{i-1} to obtain R_i. At the end of each phase, we maintain the invariant that $f(x_1,\ldots,x_n)$, when restricted to P_i, does not contain any monomials of degree 2 or more which involve only the variables from R_i.

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

We now select a nonempty set of available variables while maintaining the invariant. Assume we are at the beginning of phase $i+1$. By the induction hypothesis, the polynomial f restricted to P_i does not contain any monomials of degree 2 or higher involving only the variables in R_i. Let x_{r_i} be the representative variable for A_i, and define

$$f_i = \sum_{I \subseteq R_i} x^I \sum_{J \subseteq V_i, |I \cup J| \leq q} a_{I \cup J} x^J.$$

f_i is f restricted to P_i. We now select a nonempty subset of variables $A_{i+1} \subseteq V_i$ in the following way.

Let $I \subseteq R_i$ be such that $1 \leq |I| \leq q-1$ and

$$g_I = \sum_{J \subseteq V_i, 1 \leq |J| \leq q-|I|} a_{I \cup J} x^J.$$

g_I is a polynomial in the variables V_i and it is the coefficient of the term x^I in f_i except for the constant term. If $|I| \geq 2$, the constant coefficient of the term x^I in f_i is 0 by the induction hypothesis. If $|I| = 1$, then we will be dealing with a linear term which is not considered in the invariant. Note that if x is the characteristic vector of a set of variables to be chosen for A_{i+1} with representative variable $x_{r_{i+1}}$, then $g_I(x)$ is the coefficient of the term $x^I x_{r_{i+1}}$ when f is restricted to the projection P_{i+1}. Since g_I has no constant term, it evaluates to 0 when all the variables in V_i are set to 0. Now define

$$g = 1 + \prod_{I \subseteq R_i, 1 \leq |I| \leq q-1} (1 + g_I).$$

g is 0 exactly when all g_I are 0. The degree of g is at most $q \sum_{j=1}^{q-1} \binom{i}{j}$ and it is not identically equal to 1 since an assignment of 0's to the variables in V_i makes $g = 0$. If x is any nonzero solution of the equation $g = 0$, let A_{i+1} be the set of all variables in V_i which are set to 1 in x. Let P_{i+1} be the projection obtained from equating the variables in A_{i+1}. Also, update R_i to get R_{i+1} by adding a representative free variable for the class A_{i+1}. By the definition of g, f when restricted to P_{i+1} does not contain any monomials of degree 2 or more involving only the variables in R_{i+1}.

We now show that there is at least one nonzero solution to $g = 0$ with a "small" number of ones in the solution, thus ensuring that we can choose a small but nonempty set of variables to form the new part A_{i+1}. To show this, we use the following fact.

FACT 1. *Any GF(2) polynomial $T(x_1, \ldots, x_m)$ in m variables of degree at most $k < m$ which is not identically 1 must have a nonzero solution with at most $k+1$ ones.*

Proof. Find a maximal degree monomial M of T and select a variable which does not appear in M. Set this variable to 1 and set all other variables that do not appear in M to 0. After this assignment, T still contains the monomial M and thus is not identically 1. Hence, it has a solution containing at most k ones. Altogether, we have a nonzero solution with at most $k+1$ ones. □

Returning to the proof of the theorem, in step i, the degree of g is at most $q \sum_{j=1}^{q-1} \binom{i}{j}$ and so by Fact 1, there exists a solution with at most $1 + q \sum_{j=1}^{q-1} \binom{i}{j}$ ones. We continue this process, selecting A_i at each step, until there are no longer enough variables remaining. Let P_t be the final projection we obtain in this process. At this point, we make three modifications to P_t to obtain the desired projection. First,

Downloaded 10/01/13 to 132.239.1.231. Redistribution subject to SIAM license or copyright; see http://www.siam.org/journals/ojsa.php

all remaining available variables are set to 0. This ensures that f restricted to the projection has degree at most 1. Second, if f restricted to the projection has a nonzero constant term, set one of the free variables to 1. Finally, pair up all remaining free variables, and equate the variables of each pair (if the number of free variables is odd, set one free variable to 0) to get the final projection P. At this point, the polynomial f restricted to the projection P is identically 0. Moreover, P has at least $(t-2)/2$ free variables. We have

$$\sum_{i=1}^{2d+2}\left(1+q\sum_{j=1}^{q-1}\binom{i}{j}\right)=2d+2+q\sum_{j=1}^{q-1}\sum_{i=1}^{2d+2}\binom{i}{j}=2d+2+q\sum_{j=1}^{q-1}\binom{2d+3}{j}\le n$$

by the choice of q, thus guaranteeing $t \ge (2d+2)$. Therefore, P has at least d free variables, completing the proof of the theorem. □

COROLLARY 10. *Every degree q $GF(2)$ polynomial contains a monochromatic projection of dimension $\Omega(qn^{1/q})$.*

REFERENCES

[1] N. ALON, J. SPENCER, AND P. ERDŐS, *The Probabilistic Method*, Wiley-Interscience, New York, 1992.

[2] P. ERDŐS, *On extremal problems of graphs and generalized graphs*, Israel J. Math., 2 (1964), pp. 183–190.

[3] D.S. GUNDERSON, V. RÖDL, AND A. SIDORENKO, *Extremal problems for sets forming Boolean algebras and complete partite hypergraphs*, J. Combin Theory Ser. A, to appear.

[4] J. NEŠETŘIL, *Ramsey theory*, in Handbook of Combinatorics, Vols. 1, 2, R.L. Graham, M. Grötschel, and L. Lovász, eds., Elsevier, Amsterdam, 1995, pp. 1331–1403.

[5] R. PATURI, M.E. SAKS, AND F. ZANE, *Exponential lower bounds for depth 3 Boolean circuits*, in Proc. Annual ACM Symposium on Theory of Computing, El Paso, TX, 1997, ACM, New York, pp. 56–91.

[6] P. PUDLÁK, V. RÖDL, AND P. SAVICKÝ, *Graph complexity*, Acta Inform., 25 (1988), pp. 515–535.

[7] A.A. RAZBOROV, *Bounded depth formulae in the basis $\{\&, \oplus\}$ and some combinatorial problems*, in Complexity of Algorithms and Applied Mathematical Logic, S. I. Adian, ed., VINITI, Moscow, 1988, pp. 149–166 (in Russian).

[8] J.H. VAN LINT, *Introduction to Coding Theory*, 2nd ed., Springer-Verlag, New York, 1992.