Acta Informatica 20, 103–111 (1983)

Acta Informatica

On Sets of Boolean n-Vectors With all k-Projections Surjective

Ashok K. Chandra[1], Lawrence T. Kou[2], George Markowsky[1], and Shmuel Zaks[3]*

[1] IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598, USA
[2] Electrical and Computer Engineering Department, University of California, Davis, California, USA
[3] Technion, Haifa, Israel

Summary. Given a set, S, of Boolean n-vectors, one can choose k of the n coordinate positions and consider the set of k-vectors which results by keeping only the designated k positions of each vector, i.e., from k-projecting S. In this paper, we study the question of finding sets S as small as possible such that every k-projection of S yields all the 2^k possible k-vectors. We solve this problem constructively and almost optimally for $k=2$ and all n. For $k \geqq 3$, the constructive solutions we describe are much larger than an $O(k\,2^k \log n)$ nonconstructive upper bound which we derive. The nonconstructive approach allows us to generate fairly small sets S which have a very high probability of having the surjective k-projection property.

§ 1. Introduction

In this section we introduce the notation used throughout, and give a very simple solution for $k=2$ and all n, having $2\lceil \log n \rceil + 2$ vectors. The second section presents an improved solution for the $k=2$ case and some very tight upper and lower bounds. Section 3 describes constructive solutions for $k \geqq 3$, but the number of vectors required seems excessively large. The final section presents a nonconstructive approach to this problem which demonstrates that the sizes of the solutions in Sect. 3 are excessive.

Notation

a) Let B_n denote the set of all Boolean n-vectors.

b) For integers $n \geqq k$, let $\{n; k\}$ denote the set of all k-subsets of the set $\mathbf{n} = \{1, 2, \ldots, n\}$. If X is a set, $\{X; k\}$ shall denote the set of all k-subsets of X.

---

* Work done while visiting the IBM Thomas J. Watson Research Center

c) For $A \in \{n; k\}$, let Π_A denote the projection of B_n onto B_k in the coordinates designated by A, i.e., if $A = \{a_1 < a_2 < \ldots < a_k\}$ and $v = (v_1, \ldots, v_n) \in B_n$, then $\Pi_A(v) = (v_{a_1}, \ldots, v_{a_k})$. If $X \subset B_n$, then $\Pi_A(X) = \{\Pi_A(v) | v \in X\}$.

d) For any set X, 2^X will denote its power set.

e) Throughout the paper, log shall denote logarithm base 2.

f) We will use $\mathrm{Bin}(m; p)$ to denote the binomial coefficient "m choose p".

g) For any $x \in B_m$ and $y \in B_n$, $x * y \in B_{m+n}$ is defined as the $m+n$ dimensional vector constructed by concatenating x with y.

h) For any set $T \subseteq B_n$, $T \oplus T$ is defined as the set $\{y | y = x * x$ where $x \in T\}$.

i) For any pair of sets $S \in B_m$ and $T \in B_n$, $S * T$ is defined as the set $\{\zeta | \zeta = x * y$ where $x \in S$ and $y \in T\}$.

We say that any set $S \subseteq B_n$ has the k *surjective projection property* if for all $A \in \{n; k\}$, $\Pi_A(S) = B_k$. Where k is clear from the context, we shall simply speak about the surjective projection property. The problem we would like to solve is: given $n \geqq k$, find the smallest integer $s = f(n, k)$, such that $\exists S \subseteq B_n$ having the k surjective projection property with $|S| = s$.

At this point it might be helpful to present a very simple solution for the $k=2$ case. Let S consist of the following vectors:

a) the vector of all zeroes;

b) the vectors which are the rows of the matrix results from writing the integers from 0 to $n-1$ in binary notation as *columns;*

c) the complementary (in B_n) vectors to those in a) and b) above.

Before proving that this solution works for $k=2$, we illustrate what it looks like for $n=5$ in Fig. 1.

0	0	0	0	0
1	0	0	0	0
0	1	1	0	0
0	1	0	1	0
1	1	1	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	0	1

Fig. 1

Note that in general the number of vectors required by the construction is $2\lceil \log n \rceil + 2$.

Pick $A \in \{n; 2\}$. Suppose $A = \{i < j\}$. Since S contains the zero-vector and its complement, $(0,0), (1,1) \in \Pi_A(S)$. Since integers written (in step (b) above) in columns i, j are distinct, they must differ at same bit position. Let v be the vector of S which records the values of that bit position. For example, if $i=1$ and $j=3$, either the second row or the third row in Fig. 1 could be used. In general, $\Pi_A(v)$ will be either $(1,0)$ or $(0,1)$. Since S contains the complement of v, $\Pi_A(S) = B_2$.

Finally, note that S produced above is within a factor of about 2 of the smallest possible set. Let T be any set of vectors $\{v_1, \ldots, v_t\}$ having the surjective projection property. Define Θ: $\{1, \ldots, n\} \to 2^T$ by $\Theta(i) = \{j |$the i-th coordinate of v_j is $1\}$. Since T has the surjective projection property, Θ is injective. Thus $2^t \geqq n$ and $t \geqq \lceil \log n \rceil$. Thus $f(n, k) \geqq \lceil \log n \rceil$.

§ 2. Improved Solution for $k=2$

Let $n(s) = \max\{n | f(n, 2) \leqq s\}$. Thus $n(s)$ is the maximum n for which there is a set of s n-vectors having the 2-surjective projection property.

Theorem 2.1

$$n(2s) = \tfrac{1}{2}\,\mathrm{Bin}(2s; s) = \mathrm{Bin}(2s-1; s-1)$$

$$\mathrm{Bin}(2s; s-1) \leqq n(2s+1) \leqq \tfrac{1}{2}\,\mathrm{Bin}(2s+1; s).$$

Before proving the theorem we need a definition and a lemma.

For $S = \{\vartheta_1, \vartheta_2, \ldots, \vartheta_s\} \subset B_n$ with vectors $\vartheta_1 = (\vartheta_{11}, \ldots, \vartheta_{1n})$ written as rows, the corresponding set of columns is denoted $\mathrm{Col}(S) = \{x_1, x_2, \ldots, x_n\} \subset B_s$ where $x_i = (\vartheta_{1i}, \vartheta_{2i}, \ldots, \vartheta_{si})$.

Lemma 2.2. *Let $S = \{\vartheta_1, \ldots, \vartheta_s\} \subset B_n$, $\mathrm{Col}(S) = \{x_1, \ldots, x_n\}$, and $\bar{x}_i$ denote the complement of x_i, then S satisfies the 2 surjective projection property iff $i \neq j$ implies $x_i \neq x_j$, $x_i \neq \bar{x}_j$, and $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ is an antichain in the lattice B_s.*

Proof. Sufficiency. Suppose $\{x_1, \ldots, \bar{x}_n\}$ is an antichain, where $x_i = (\vartheta_{1i}, \ldots, \vartheta_{si})$. Now let $i < j \leqq n$, and show that $\Pi_{\{i,j\}}(S) = B_2$ as follows: since $\{x_i, x_j\}$ is an antichain, there are $p, q \leqq s$ s.t. $\vartheta_{pi} = 0$, $\vartheta_{pj} = 1$, $\vartheta_{qi} = 1$, $\vartheta_{qj} = 0$; also since $\{x_i, \bar{x}_j\}$ is an antichain, there are $r, t \leqq s$ s.t. $\vartheta_{ri} = 0$, $\vartheta_{rj} = 0$, $\vartheta_{ti} = 1$, $\vartheta_{tj} = 1$.

Necessity. If S satisfies the 2 surjective projection property, all columns are distinct and no column is the complement of another. Let $i < j \leqq n$ and show that $\{x_i, x_j, \bar{x}_i, \bar{x}_j\}$ is an antichain as follows: there are $p, q, r, t \leqq s$ such that $\vartheta_{pi} = 0$, $\vartheta_{pj} = 1$, $\vartheta_{qi} = 1$, $\vartheta_{qj} = 0$ (i.e. $\{x_i, \bar{x}_i\}$, $\{x_j, \bar{x}_j\}$, $\{x_i, x_j\}$, $\{\bar{x}_i, \bar{x}_j\}$ are antichains), and $\vartheta_{ri} = 0$, $\vartheta_{rj} = 0$, $\vartheta_{ti} = 1$, $\vartheta_{tj} = 1$ (i.e. $\{x_i, \bar{x}_j\}$, $\{\bar{x}_i, x_j\}$ are antichains). □

Proof of Theorem. Upper Bound. By Sperner's Lemma [1; p. 99], the largest size of any antichain in B_t is $\mathrm{Bin}(t; [t/2])$. By Lemma 2.2, $2n(s)$ does not exceed the size of a maximal size antichain in B_s, thereby giving the upper bound $n(2s) \leqq \frac{1}{2}\,\mathrm{Bin}(2s+1; s)$, $n(2s+1) \leqq \frac{1}{2}\,\mathrm{Bin}(2s+1; s)$.

Lower Bound. Let S be such that $\mathrm{Col}(S) = \{(b_1, b_2, \ldots, b_s) | b_1 = 0,\ \Sigma b_i = \lceil s/2 \rceil\}$. If $\mathrm{Col}(S)$ is denoted $\{x_1, \ldots, x_n\}$ then it is clear that $\{x_1, \ldots, x_n\} \cap \{\bar{x}_1, \ldots, \bar{x}_n\} = \emptyset$ and $\{x_1, \ldots, x_n\}$, $\{\bar{x}, \ldots, \bar{x}_n\}$ are antichains. Also if $i < j \leqq n$, $\{x_i, \bar{x}_j\}$ is an antichain, because if $x_i = (b_1, \ldots, b_s)$, $\bar{x}_j = (c_1, \ldots, c_s)$, then $b_1 = 0$, $c_1 = 1$, and as

$\Sigma b_i \geqq \Sigma c_i$, there is a p such that $b_p=1$, $c_p=0$. This proves that $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ is an antichain, and by the lemma, S has the 2 surjective projection property. Hence $n(s) \geqq \mathrm{Bin}(s-1; \lceil s/2 \rceil)$ which is the lower bound in the theorem. □

Theorem 2.1 shows that

$$f(n, 2) = \log n + \tfrac{1}{2} \log \log n + O(1),$$

and the lower bound for $n(s)$ gives a constructive solution (upper bound) for $f(n, 2)$ which is within 1 of optimal. The table gives lower and upper bounds on $n(s)$, and $f(n, 2)$. For example, $5 \leqq f(5, 2) \leqq 6$ (for this special case, it can be shown that $f(5, 2) = 6$), and an optimal solution is obtained as follows: write columns consisting of three 0's and three 1's, starting with 0 (compare with Fig. 1). Adding additional columns gives 6 row solutions for $f(n, 2)$ with $n \leqq 10$.

0	0	0	0	0
0	0	0	0	1
0	1	1	1	0
1	0	1	1	0
1	1	0	1	1
1	1	1	0	1

Fig. 2

Conjecture. The lower bound for $n(2s+1)$ in Theorem 2.1 is tight.

It has been shown [5] that the lower bound for $n(2s+1)$ in Theorem 2.1 is indeed tight.

§ 3. Constructive Solutions for $k \geqq 3$

In this section, we shall give a deterministic algorithm to construct a set $M(n, k) \subseteq B_n$ with the k surjective projection property. For every $n \geqq 1$, $k \geqq 1$ and $n \geqq k$, we will first construct an $M(N, k)$ where $N = 2^{\lceil \log n \rceil}$. $M(n, k)$ is then constructed from $M(N, k)$ by setting $M(n, k) = \pi_A(M(N, k))$ where $A \in \{N; n\}$.

Algorithm M

Input: Two integers n and k
Output: A set $M(n, k) \subseteq B_n$ with the k surjective projection property.
1. Set $j = \lceil \log n \rceil$.
2. Set $M(2^0, 1) = \{(0), (1)\}$, $M(2^0, 2) = \phi$, $M(2^0, 3) = \phi, \ldots, M(2^0, k) = \phi$.

3. For $i = 0, 1, 2, \ldots, j-1$ perform 4.
4. For $e = 1, 2, \ldots, k$, set

$$M(2^{i+1}, e) = M(2^i, e) \oplus M(2^i, e) \cup \bigcup_{\ell=1}^{e-1} M(2^i, \ell)^* M(2^i, e-\ell).$$

5. Set $A = \{1, 2, \ldots, n\}$.
6. Set $M(n, k) = \pi_A(M(2^j, k))$.

We now establish the following two lemmas.

Lemma 3.1. *$M(n, k)$ has the k surjective projection property, for all $n \geqq 1$, $k \geqq 1$ and $n \geqq k$.*

Proof. It is sufficient to show that $M(2^{\lceil \log n \rceil}, k)$, produced by Algorithm M has the k surjective projection property, for all $n \geqq 1$, $k \geqq 1$ and $n \geqq k$. We shall give a proof by induction on $j = \lceil \log n \rceil$. For $j = 0$, $M(2^0, 1) = \{(0), (1)\}$ which clearly has the k surjective projection property. Assume $j = 0, 1, \ldots, h$, $M(2^j, k)$ has the k surjective projection property for all $k = 1, 2, 3, \ldots, 2^j$. For $j = h+1$, consider any $A \in \{2^{h+1}; e\}$ where $e \in \{1, 2, \ldots, k\}$. Let $A_1 = \{i \mid i \in A \text{ and } i \leqq 2^h\}$, $A_2 = A - A_1$ and $\ell = |A_1|$. There are three cases.

Case 1. $\ell = 0$.

By the construction in step 4 of Algorithm M, we have $M(2^{h+1}, e) \supseteq M(2^h, e) \oplus M(2^h, e)$. Therefore,

$$\begin{aligned} \pi_A M(2^{h+1}, e) &\supseteq \pi_A[M(2^h, e) \oplus M(2^h, e)] \\ &= \pi_{A_2} M(2^h, e) \\ &= B_e. \end{aligned}$$

Case 2. $\ell = e$.

Following the same argument as in Case 1, we have

$$\begin{aligned} \pi_A M(2^{h+1}, e) &\supseteq \pi_A[M(2^h, e) \oplus M(2^h, e)] \\ &= \pi_{A_1} M(2^h, e) \\ &= B_e. \end{aligned}$$

Case 3. $0 < \ell < e$.

In this case, by the construction in step 4 of Algorithm M, we have $M(2^{h+1}, e) \supseteq M(2^h, \ell)^* M(2^h, e-\ell)$. Hence

$$\begin{aligned} \pi_A M(2^{h+1}, e) &\supseteq \pi_A[M(2^h, \ell)^* M(2^h, e-\ell)] \\ &= \pi_{A_1} M(2^h, \ell)^* \pi_{A_2} M(2^h, e-\ell) \\ &= B_e. \end{aligned}$$

Therefore, we have shown that in all three cases, $\pi_A M(2^{h+1}, e) \supseteq B_e$. The proof is thus completed. □

In the following lemma, we give an upper bound for the size of $M(n, k)$.

Lemma 3.2. *$f(n,k) \leqq |M(n,k)| \leqq 2^k \lceil \log n \rceil^{k-1}$, for all $n \geqq 2$, $k \geqq 1$.*

Proof. We shall prove this lemma by induction on $j = \lceil \log n \rceil$. Notice that we consider the cases where $n \geqq 2$ to avoid the trivial situation when $n=1$ and $\lceil \log n \rceil = 0$. For $j = \lceil \log 2 \rceil = 1$, from Algorithm M, we have $M(2,1) = \{(0,0), (1,1)\}$, $M(2,2) = \{(0,0),(0,1),(1,0),(1,1)\}$, $M(2,3) = \phi$, $M(2,4) = \phi, \ldots, M(2,k) = \phi$. It is easy to check that $|M(2,k)| \leqq 2^k \lceil \log 2 \rceil^{k-1}$ for all $k \geqq 1$. Assume $|M(n,k)| \leqq 2^k \lceil \log n \rceil^{k-1}$ for all $k \geqq 1$ and for all $j = 1, 2, \ldots, h$. For $j = \lceil \log n \rceil = h+1$, we have, for all $e = 1, 2, \ldots, k$,

$$\begin{aligned} |M(n,e)| &\leqq |M(2^{h+1}, e)| \\ &\leqq |M(2^h, e)| + \sum_{\ell=1}^{e-1} |M(2^h, \ell)| \times |M(2^h, e-\ell)| \\ &\leqq 2^e h^{e-1} + \sum_{\ell=1}^{e-1} 2^\ell h^{\ell-1} \times 2^{(e-\ell)} h^{e-\ell-1} \\ &= 2^e h^{e-1} + (e-1) 2^e h^{e-2} \\ &= 2^e (h^{e-1} + (e-1) h^{e-2}) \\ &\leqq 2^e (h+1)^{e-1}. \end{aligned}$$

Therefore the lemma is true for $j = \lceil \log n \rceil = h+1$. The proof is thus completed. □

These recursive solutions can be further improved. For doing this we modify step 4 of Algorithm M. First we observe that for $e=3$ one can have

$$M(2^{i+1}, 3) = M(2^i, 3) \oplus M(2^i, 3) \cup M(2^i, 2) \oplus \overline{M(2^i, 2)}$$

where $\overline{M(n,k)}$ is the set obtained from $M(n,k)$ by exchanging 0's and 1's, and where $T \oplus \bar{T}$, for a set $T \subseteq B_n$, is defined as the set $\{y \mid y = x * \bar{x}$ where $x \in T\}$ ($\bar{x}$ is the vector obtained from x by exchanging 0's and 1's). A case analysis (similar to the one found in the proof of Lemma 3.1) shows that $M(2^{i+1}, 3)$ thus constructed has the 3 surjective projection property. Let $A = \{a, b, c\}$. If all $a, b, c \leqq 2^i$ (or if all $a, b, c > 2^i$) then $\Pi_A(M(2^i, 3) \oplus M(2^i, 3)) = B_3$. Otherwise, without loss of generality, let $a < b \leqq 2^i$, $c > 2^i$. Say $c = 2^i + d$. If $d \neq a, b$ then again $\Pi_A(M(2^i, 3) \oplus M(2^i, 3)) = B_3$. On the other hand, if d equals one of a, b, say, $a < b = d$ then $\Pi_A(M(2^i, 3) \oplus M(2^i, 3)) = \{000, 011, 100, 111\}$ and $\Pi_A(M(2^i, 2) \oplus M(2^i, 2)) = \{001, 010, 101, 110\}$, from which $M(2^{i+1}, 3) = B_3$.

This yields

$$|M(2^{i+1}, 3)| \leqq |M(2^i, 3)| + |M(2^i, 2)|$$

which together with the results in Sect. 2, yield

$$\begin{aligned} |M(2^{i+1}, 3)| &\leqq |M(2^i, 2)| + |M(2^{i-1}, 2)| + \ldots \\ &\leqq \frac{i^2}{2} + O(i \log i) \end{aligned}$$

and if $\lceil \log n \rceil = i+1$ then

$$f(n,3) \leqq |M(n,3)| \leqq |M(2^{i+1}, 3)| \leqq \tfrac{1}{2} \lceil \log n \rceil^2 + O(\log n \log \log n).$$

Next we construct, in a similar manner, solutions for $e \geqq 4$, as follows:

$$\begin{aligned} M(2^{i+1}, e) = {} & M(2^i, e) \oplus M(2^i, e) \cup M(2^i, e-1) \oplus \overline{M(2^i, e-1)} \\ & \cup \bigcup_{\ell=2}^{e-2} M(2^i, \ell) * M(2^i, e-\ell). \end{aligned}$$

It can be shown that $M(n,k)$, as constructed by this modified algorithm, has the k surjective projection property. The proof, being similar to that of Lemma 3.1, is omitted.

For small values of e a closer look at these structures can improve the solution. For example, for $e=4$ one might have

$$\begin{aligned} M(2^{i+1}, 4) = {} & M(2^i, 4) \oplus M(2^i, 4) \cup M(2^i, 3) \oplus \overline{M(2^i, 3)} \\ & \cup \{0^{2^i}, 1^{2^i}\} * M(2^i, 2) \cup M(2^i, 2) * \{0^{2^i}, 1^{2^i}\} \end{aligned}$$

where 0^t or 1^t is a vector of t 0's or 1's respectively. Hence

$$|M(2^{i+1}, 4)| \leqq |M(2^i, 4)| + |M(2^i, 3)| + 4 |(M(2^i, 2)|$$

which yields

$$f(n,4) \leqq |M(n,4)| \leqq \tfrac{1}{6} \lceil \log n \rceil^3 + O(\log^2 n \log \log n).$$

Following a preliminary version of this paper [2], other explicit constructions have been found showing [3] that

$$f(n,k) \leqq \frac{2^n}{n-k+1}$$

and

$$f(n,k) \leqq \mathrm{Bin}(n; \lfloor k/2 \rfloor) + \mathrm{Bin}(n; k - \lfloor k/2 \rfloor - 1)$$

which are useful for large k, and [4]

$$f(n,k) = O(g(k) \cdot (\log n)^\alpha)$$

for some function g and $\alpha = \log(\lfloor k^2/4 \rfloor + 1)$, which is useful for constant k.

§ 4. The Probabilistic Approach

In this section, we present a simple probabilistic argument which shows that for constant k we can find S's with the surjective projection property which are considerably smaller than the sets constructed in Sect. 3. Furthermore, this argument provides an estimate of the likelihood that a set S of a certain size chosen at random has the surjective projection property. It turns out that the probability is quite high even for fairly small sets.

Our probability space, $\mathscr{P}$, shall be $\{B_n; r\}$ where r is an integer. For each $A \in \{n; k\}$, $w \in B_k$, we define a random variable $Q_{A,w}$ by $Q_{A,w}(S)=0$ if $w \in \Pi_A(S)$ and $Q_{A,w}(S)=1$ otherwise. Finally, define a random variable

$$Q=\sum_A \sum_w Q_{A,w}.$$

Clearly, S has the surjective projection property iff $Q(S)=0$. We wish to compute the expected value of Q, i.e., $E(Q)$. This is most easily done in terms of the expected values of the $Q_{A,w}$'s, i.e. the $E(Q_{A,w})$'s, Now $Q_{A,w}(S)$ is 1 iff S does not contain any of the 2^{n-k} vectors v for which $\Pi_A(v)=w$. Thus $E(Q_{A,w}) = \mathrm{Bin}(2^n-2^{n-k}; r)/\mathrm{Bin}(2^n; r)$ for all A, w whence

$$E(Q)=2^k \times \mathrm{Bin}(n; k) \times \mathrm{Bin}(2^n-2^{n-k}; r)/\mathrm{Bin}(2^n; r).$$

Since $1 \leqq a < b$ implies that $a/b > (a-1)/(b-1)$, $E(Q_{A,w})$ is bounded above by $(2^n-2^{n-k})^r/2^{nr}=(1-2^{-k})^r$.

Thus $E(Q) < 2^k \times \mathrm{Bin}(n; k) \times (1-2^{-k})^r$. If we can find a value for r for which $E(Q)<1$, then $Q(S)=0$ for some S, since $Q(S)$ is always a nonnegative integer.

Theorem 4.1. *For $r=\lceil k 2^k \ln n \rceil$ and $n \geqq 2$, there exists $S \in \{B_n; r\}$ having the surjective projection property.*

Proof. From the above discussion, one need only demonstrate that $E(Q)<1$. Since $E(Q)<2^k \times \mathrm{Bin}(n; k) \times (1-2^{-k})^r$, $\mathrm{Bin}(n; k) < n^k/k!$ and $(1-2^{-k}) < \exp(-2^{-k})$, $E(Q) < (2^k/k!)\, n^k \exp(-2^{-k} r)$. For $r=\lceil k 2^k \ln n \rceil$, we get $E(Q)<(2^k/k!)<1$ for $k>3$. For $k \leqq 3$, the estimate can be refined as the reader can easily check to get the same result. □

Corollary 4.2. *The probability that S chosen at random has the surjective projection property is $\geqq 1-E(Q)$.*

Proof

$$E(Q)=\sum_{i=0}^{\infty} i \times \mathrm{Prob}\{Q=i\} \geqq \sum_{i=1}^{\infty} \mathrm{Prob}\{Q=i\} = 1-\mathrm{Prob}\{Q=0\}. \quad \square$$

The following table uses Corollary 4.2 to make some estimates of the likelihood of failing to pick an S at random which has the surjective projection property.

Table 2

n	k	r	Upper bound on Prob$(Q>0)$
32	5	500	0.823
32	5	1,000	10^{-7}
32	5	1,500	1.34×10^{-14}
1,000	5	1,100	0.18
1,000	5	2,200	1.22×10^{-16}
1,000	5	3,300	8.32×10^{-32}

Note that for $k=5$ the number of vectors we need to use to guarantee a high rate of success is not abnormally large even for $n=1{,}000$. It seems likely that the probabilistic approach might supply a practical solution for $k \geqq 3$, since its failure can be made less than the probability of failure of any more elaborate scheme. Alternatively, the probabilistic approach can be used to generate a set S and check that it indeed has the surjective projection property.

Acknowledgement. The authors would like to acknowledge that the problem considered in this paper arose from some discussions with David Patch and Richard Zumbach.

References

1. Birkhoff, G.: Lattice Theory. Am. Math. Soc., Providence, Rhode Island, 1967
2. Chandra, A.K., Kou, L.T., Markowsky, G., Zaks, S.: On sets of Boolean n-vectors with all k-projections surjective. Technical report RC 8936, IBM Research, Yorktown Heights, July 1981
3. Tang, D.T., Woo, L.S.: Exhaustive test pattern generation with constant weight vectors. Technical report RC 9442, IBM Research, Yorktown Heights, June 1982
4. Tang, D.T., Chen, C.L.: Personal communication, Aug. 1982
5. Kleitman, D.J., Spencer, J.: Families of k-independent sets. Discrete Math. **6**, 255–262 (1973)

Received August 24, 1981/October 6, 1982