123.

Open Systems & Information Dynamics
Vol. 2 No 3 (1994) 1–16
© Nicholas Copernicus University Press

Exhaustive Testing of Almost All Devices with Outputs Depending on Limited Number of Inputs.

L.B. LEVITIN and *M.G. KARPOVSKY*
Boston University, College of Engineering
Boston, MA 02215, USA

(Received October 1994)

The problem is considered of efficient test design for combinational devices with large number n of input variables, where each output depends on at most s input variables. It is shown that the number of test patterns can be reduced drastically if we allow a small fraction ε of all possible outputs not to be tested exhaustively. The effect holds even if ε approaches zero with the increase of n. Upper and lower bounds for the number of test patterns in such tests (called (ε, s)-exhaustive tests) are derived and constructions of the tests are suggested.

1 Introduction

With the increasing variety and complexity of digital devices the problem of their testing becomes more and more complex and important. Since generation of an optimal device-specific test has been shown to be an intractable problem for devices of large complexity [1], it seems to be promising to develop tests which would be applicable to a broad class of devices. In particular, consider the class of combinational devices with n binary inputs, where each output is a Boolean function of at most s input variables. It has been shown recently in a number of papers [2-7] that all such (17, 18) devices can be tested exhaustively by the use of tests with the number of test patterns growing rather moderate with n. However, the number of test patterns in the tests constructed is still far away from theoretical nonconstructive upper bounds.

Basing on the analogy with the situation in information theory, one can expect that the number of test patterns can be reduced substantially if we allow a small fraction ε of all possible outputs not to be tested exhaustively. The effect may hold even if ε approaches zero with the increase of n. This question is explored and answered in affirmative in the present paper. Upper and lower bound for the number of test patterns in such tests (called (ε, s)-exhaustive tests) are derived, and constructions of the tests are suggested.

Such tests may be useful for testing complex VLSI devices when a small fraction of undetected faults can be tolerated.

2 Definitions and Notations

Definition 1 *A test matrix $\hat{T}$ for a combinational device with n inputs is a binary ($\{0,1\}$) matrix with n columns whose rows are test patterns.*

Definition 2 *A test is s-exhaustive for given s inputs if the corresponding s columns of its matrix $\hat{T}$ contain all 2^s binary vectors, as rows.*

Definition 3 *A test $T = T(\varepsilon, n, s)$ is (ε, s)-exhaustive if it is s-exhaustive for any s-tuples which does not exceed ε. A test $T(0, n, s)$ is called an s-exhaustive test.*

s-tuple of inputs except
for a fraction of

L A

Definition 4 *A section of tests $(T(\varepsilon, n, s))$ is asymptotically s-exhaustive, if $\varepsilon \to 0$ when $n \to \infty$.*

Denote:

$N = |T(\varepsilon, n, s)|$ - the number of test patterns in an $(\varepsilon,\ s)$ - exhaustive test $T(\varepsilon, n, s)$;

$f(\varepsilon, n, s) = \min\limits_{T(\varepsilon,n,s)} |T(\varepsilon, n, s)|$;

$\phi(n, s) = f(0, n, s)$.

The function $f(0, n, s)$ and some related functions have been studied in [2, 7-10].

We also call s-tuples for which a given test is s-exhaustive "good s-tuples", and all the other s-tuples are "bad" ones.

3 Lower Bound

First we shall prove a few lemmata which will be used in the further analysis.

Lemma 1

$$f(\varepsilon, n, s) \ \geq \ f(\varepsilon, n-1, s) \tag{3.1}$$

Proof. Let $T(\varepsilon, n, s)$ be an optimal (ε, s)-exhaustive test, i.e. $|T(\varepsilon, n, s)| = f(\varepsilon, n, s)$. Denote by r_i the number of good s-tuples which include the i-th column of the test matrix. The total number G_s of good s-tuples is, obviously,

$$G_s \ = \ \frac{1}{s}\sum_{i=1}^{n} r_i\,. \tag{3.2}$$

The fraction of bad s-tuples is, by assumption, at most ε, that is

$$1-\frac{G_s}{\binom{n}{s}} \;=\; 1-\frac{\sum_{i=1}^{n} r_i}{s\binom{n}{s}} \;\le\; \varepsilon\,. \tag{3.3}$$

Let $r_j = \min_i r_i$. Obviously, $\sum_{i=1}^{n} r_i \ge n r_j$. Delete the j-th column. We obtain a test matrix with $n-1$ columns and $f(\varepsilon,n,s)$ rows. The fraction of bad s-tuples in this matrix is

$$1-\Big(\frac{1}{s}\sum_{i=1}^{n} r_i - r_j\Big)\binom{n-1}{s}^{-1} \;=\; 1-\frac{n\sum_{i=1}^{n} r_i - nsr_j}{(n-s)s\binom{n}{s}} \;\le\; 1-\frac{\sum_{i=1}^{n} r_i}{s\binom{n}{s}} \;\le\; \varepsilon\,. \tag{3.4}$$

Thus the obtained test is (ε,s)-exhaustive, and (3.1) is proved.

Lemma 2

$$f(\varepsilon,n,s) \;\ge\; 2f(\varepsilon,n-1,s-1)\,. \tag{3.5}$$

optimal

Proof.Let $T(\varepsilon,n,s)$ be an (ε,s)- exhaustive test, $|T(\varepsilon,n,s)| = N = f(\varepsilon,n,s)$. Denote by $\lfloor a\rfloor$ the integral part of a, and by $\lceil a\rceil$ the least integer such that $\lceil a\rceil \ge a$. Each column of the test matrix contains at least $\lceil N/2\rceil$ identical elements (zeros or ones). Let $r_k = \max_i r_i$,where r_i is the number of good s-tuples which include the i-th column. Delete the k-th column and all the rows where the k-th column has the element (0 or 1) that occurs at least $\lceil N/2\rceil$ times. We obtain a matrix with $n-1$ columns and at most $\lfloor N/2\rfloor$ rows. Let us estimate the fraction of bad s-tuples in this matrix. Obviously, each good s-tuple in $T(\varepsilon,n,s)$ which includes the k-th column corresponds to exactly one good $(s-1)$-tuple in the reduced matrix. Therefore, the number of good $(s-1)$-tuples is

$(s-1)$

$$G_{s-1} \;\ge\; r_k \;\ge\; \frac{1}{n}\sum_{i=1}^{n} r_i\,.$$

Hence, the fraction of bad $(s-1)$-tuples is

$$1-\frac{G_{s-1}}{\binom{n-1}{s-1}} \;\le\; 1-\frac{r_k}{\binom{n-1}{s-1}} \;\le\; 1-\frac{\sum_{i=0}^{n} r_i}{s\binom{n}{s}} \;\le\; \varepsilon\,. \tag{3.6}$$

Thus ~~we~~ obtained test with at most $\lfloor\frac{1}{2}f(\varepsilon,n,s)\rfloor$ test patterns is $(\varepsilon,s-1)$-exhaustive, which proves the lemma.

the

Lemma 3

$$f(\varepsilon,n,2) \;\ge\; N_{\min}\,, \tag{3.7}$$

where $N_{\min}$ *is the minimum integer value of* N *for which the following inequality holds:*

$$\binom{N-1}{\lfloor N/2 \rfloor} \geq \frac{n}{1+\varepsilon(n-1)} = n^{*}. \tag{3.8}$$

For $n \gg 1$ *and* $\varepsilon \ll 1$,

$$f(\varepsilon, n, 2) \geq \log_2 n^{*} + \frac{1}{2}\log_2 \log_2 n^{*} + \frac{1}{2}\log_2 2\pi. \tag{3.9}$$

Proof. Consider an $(\varepsilon, 2)$ exhaustive test with $|T(\varepsilon, n, 2)| = N$ test patterns. Let us subdivide the n columns of the test into classes such that no two columns belonging to the same class form a good pair. First, let us find out how many such distinct classes exists.

The set $\mathbf{Z}_2^N$ of all binary vectors of length N is a partially ordered set where the relation $x \leq y$ means "x is a descendant of y" (cf. [11,p.33] . (Here $x,\ y \in \mathbf{Z}_2^N$). Denote by $\overline{x}$ the complement (negation) of a binary vector x and by $w(x)$ the Hamming weight of x. Obviously, if $x \leq y$ or $x \leq \overline{y}$, the vectors x and y form a bad pair.

Consider two possible cases.

1) $N = 2m,\ m \in \mathbf{N}$.

Let $S_1 = \{x \mid x \in \mathbf{Z}_2^N,\ w(x) \leq m\}$,
$S_2 = \{x \mid x \in \mathbf{Z}_2^N,\ w(x) \geq m\}$.

Note, that the function

$$F : S_1 \to S_2,\ F(x) = \overline{x} \tag{3.10}$$

is a bijection. Moreover, $S_1 \cup S_2 = \mathbf{Z}_2^N$, $S_1 \cap S_2 = \{x \mid w(x) = m\}$, and $|S_1 \cap S_2| = \binom{2m}{m}$. By Sperner's Lemma [12, 13 p.99], $S_1 \cap S_2 = \{x_i\}$, $i = 1, 2, \ldots, \binom{2m}{m}$, is the maximal antichain in $\mathbf{Z}_2^{2m}$. Therefore by the Dilworth theorem ([14,15 sec. 2.8]), there exists a partition of S_1 into chains of descendants such that any $x_i \in S_1 \cap S_2$ belongs to exactly one chain $Z_i^{(1)}$:

$$S_1 = \bigcup_{i=1}^{\binom{2m}{m}} Z_i^{(1)}, \tag{3.11}$$

where $Z_i^{(1)} \cap Z_j^{(1)} = \emptyset\ (i \neq j)$, $x_i \in Z_i^{(1)}$. Because of (3.10), there exists a partition of S_2 into chains $\{Z_j^{(2)}\}$:

$$S_2 = \bigcup_{j=1}^{\binom{2m}{m}} Z_j^{(2)}, \tag{3.12}$$

such that for any $Z_i^{(1)} = \{y_{ik}\}$, there exists a chain $Z_j^{(2)}$, where $y_{jk} = \overline{y}_{ik}$. (In particular, $x_j = \overline{x}_i \in Z_j^{(2)}$, where $x_i,\ x_j \in S_1 \cap S_2$). We call the chain $Z_j^{(2)} = \{\overline{y}_{ik}\}$

complementary to $Z_i^{(1)} = \{y_{ik}\}$ and denote it $Z_j^{(2)} = \overline{Z}_i^{(1)}$. Obviously, $Z_i = Z_i^{(1)} \cup Z_i^{(2)}$ is a chain, and chains $\{Z_i\}$ form a partition of $\mathbf{Z}_2^{2m}$:

$$\mathbf{Z}_2^{2m} = \bigcup_{i=1}^{\binom{2m}{m}} Z_i \,, \tag{3.13}$$

such that for any $Z_i = Z_i^{(1)} \cup Z_i^{(2)}$ there exists a complementary chain $Z_j = Z_j^{(1)} \cup Z_j^{(2)} = \overline{Z}_i^{(2)} \cup \overline{Z}_i^{(1)} = \overline{Z}_i$.

Thus, we obtain $\frac{1}{2}\binom{2m}{m} = \binom{2m-1}{m} = \binom{N-1}{N/2}$ disjoint classes $C_i = Z_i \cup \overline{Z}_i$, $(i = 1, 2, \ldots, \binom{2m-1}{m})$ each of which does not contain good pairs. (Indeed, for any $x, y \in C_i$, one of four alternatives is valid: $x \leq y$, $y \leq x$, $x \leq \overline{y}$, $y \leq \overline{x}$.)

2)$N = 2m + 1$, $m \in \mathbf{N}$. Take a class $C_i = Z_i \cup \overline{Z}_i$ of binary vectors of length $N - 1 = 2m$. If we extend each vector which belongs to Z_i by assigning an additional component equal to 0, we obtain a chain of vectors of length $N = 2m + 1$. Denote this chain by Z_i0. Then the complementary chain is $\overline{Z_i0} = \overline{Z}_i1$, and $C_{i0} = Z_i0 \cup \overline{Z}_i1$ is a class of $(2m + 1)$-dimensional binary vectors which does not contain good pairs. Similarly $C_{i1} = Z_i1 \cup \overline{Z}_i0$ is another such class. All the classes $\{C_{i0}, C_{i1}\}$ $(i = 1, 2, \ldots, \binom{2m-1}{m})$ are disjoint and form a partition of $\mathbf{Z}_2^{2m+1}$. The number of the classes is $\binom{2m}{m} = \binom{N-1}{\lfloor N/2 \rfloor}$.

Hence, for both even and odd N, the number of classes is $k = \binom{N-1}{\lfloor N/2 \rfloor}$. As a result, the n columns of the test $T(\varepsilon, n, s)$ can be subdivided into k classes (some of them may be empty), such that no class contains good pairs. Let n_i be the number of columns in the i-th class, so that

$$\sum_{i=1}^{k} n_i = n \,.$$

To obtain a good pair, it is necessary to take columns from different classes. Hence, the number of good pairs G_2 is upperbounded by

$$G_2 \leq \sum_{j=1}^{k} \sum_{i=1}^{j-1} n_i n_j = G_2^* \,. \tag{3.14}$$

Obviously,

$$\sum_{j=1}^{k} \sum_{i=1}^{k} (n_i - n_j)^2 = 2(k-1) \sum_{i=1}^{k} n_i^2 - 4G_2^* \geq 0 \,, \tag{3.15}$$

and

$$2G_2^* + \sum_{i=1}^{k} n_i^2 = \left(\sum_{i=1}^{k} n_i \right)^2 = n^2 \,. \tag{3.16}$$

Then, by (3.15) and (3.16),

$$G_2^* \le \frac{n^2(k-1)}{2k}. \tag{3.17}$$

Therefore, the fraction of good pairs is limited by

$$\frac{G_2}{\binom{n}{2}} \le \frac{G_2^*}{\binom{n}{2}} \le \frac{n(k-1)}{(n-1)k}. \tag{3.18}$$

Since, by assumption, the test is $(\varepsilon, 2)$-exhaustive, it is necessary that

$$\frac{n(k-1)}{(n-1)k} \ge 1 - \varepsilon, \tag{3.19}$$

or

$$k \ge \frac{n}{1+\varepsilon(n-1)} = n^*, \tag{3.20}$$

which leads to (3.7). If $n \gg 1$ and $\varepsilon \ll 1$, then $N \gg 1$, and, using Stirling's expansion, we obtain (3.9).

Theorem 1 *(Lower bound).*

$$f(\varepsilon, n, s) \ge 2^{s-2} N_{\min}, \tag{3.21}$$

where $N_{\min}$ is the minimum integer value of N for which the following inequality holds:

$$\binom{N-1}{\lfloor N/2 \rfloor} \ge \frac{n-s+2}{1+\varepsilon(n-s+1)}. \tag{3.22}$$

For $n \gg 1$, $\varepsilon \ll 1$,

$$f(\varepsilon, n, s) > 2^{s-2}(\log_2 n^* + \frac{1}{2}\log_2 \log_2 n^* + \frac{1}{2}\log_2 2\pi) \tag{3.23}$$

where

$$n^* = \frac{n-s+2}{1+\varepsilon(n-s+1)}.$$

Proof. Applying $(s-2)$ times Lemma 2, we obtain:

$$f(\varepsilon, n, s) \ge 2^{s-2} f(\varepsilon, n-s+2, 2),$$

and, by Lemma 3, come to (3.21) and (3.23). Note that a lower bound on $\phi(n, s)$ can be obtained from (3.23) by setting $\varepsilon = 0$ (i.e. $n^* = n - s + 2$). A better lower bound on $\phi(n, s)$ follows from [8].

4 Upper bounds and Test Constructions.

In this section we derive two upper bounds for $f(\varepsilon, n, s)$. A nonconstructive upper bound based on probabilistic reasoning is given by Theorem 2. The upper bound of Theorem 3 makes use of the best s-exhaustive tests. A construction based on simple codes is presented in Theorem 4. The resulting tests are nonlinear (rows of test matrices do not comprise a linear space). Linear (ε, s)-exhaustive tests are constructed in Theorems 5 and 6.

Theorem 2

$$f(\varepsilon, n, s) \leq N_{\min}, \tag{4.1}$$

where $N_{\min}$ *is the minimum integer value of* N *for which the following inequality holds:*

$$\sum_{k=1}^{2^s}(-1)^{k-1}\binom{2^s}{k}(1-k\cdot 2^{-s})^N < \left\lfloor \varepsilon\binom{n}{s}+1\right\rfloor \binom{n}{s}^{-1}. \tag{4.2}$$

More roughly,

$$f(\varepsilon, n, s) < \left\lceil \frac{\log_2 \lfloor \varepsilon\binom{n}{s}+1\rfloor - \log_2 \binom{n}{s} - s}{\log_2(1-2^{-s})} \right\rceil. \tag{4.3}$$

Proof. Consider an ensemble of all possible binary $N \times n$ matrices, each having the same probability 2^{-nN}. It is easy to see that this ensemble is the same as the random matrix obtained by choosing each element equal to 0 or 1 independently and with equal probabilities $p_0 = p_1 = \frac{1}{2}$. Let us calculate the probability that a given s-tuple in such a random matrix is bad. The probability that a given vector of length s occurs in a given row of s-tuple is 2^{-s}. Therefore, the probability of the event $A_i (i = 1, 2, \ldots, 2^s)$ that i-th vector does not occur in any of N rows is

$$\Pr\{\mathrm{A_i}\} = (1-2^{-s})^{\mathrm{N}}. \tag{4.4}$$

Hence, the probability q that the s-tuple is bad, i.e. that at least one of the 2^s binary vectors does not occur in the s-tuple, is

$$\begin{aligned} q &= \Pr\{\bigcup_{\mathrm{i=1}}^{2^s} \mathrm{A_i}\} = \sum_{\mathrm{i}} \Pr\{\mathrm{A_i}\} - \sum_{\mathrm{i,j:i\neq j}} \Pr\{\mathrm{A_i} \cap \mathrm{A_j}\} + \ldots \\ &= \sum_{k=1}^{2^s}(-1)^{k-1}\binom{2^s}{k}(1-k\cdot 2^{-s})^N. \end{aligned} \tag{4.5}$$

Then the probability Q that in a randomly chosen matrix at least $\lfloor \varepsilon\binom{n}{s}+1\rfloor$ s-tuples are bad (which means that the matrix is not (ε, s)-exhaustive) is upperbounded by the union bound:

$$Q \leq \binom{n}{s}\left\lfloor \varepsilon\binom{n}{s}+1\right\rfloor^{-1} q. \tag{4.6}$$

If $Q < 1$, it means that there exists at least one $N \times n$ binary matrix which is (ε, s)-exhaustive.

Thus, we conclude that

$$f(\varepsilon, n, s) \leq N_{\min},$$

where $N_{\min}$ is the minimum integer for which the inequality (4.2) holds.

A rougher but simpler upper bound can be obtained by retaining the first term only in the sum (4.5) (which means taking the union bound for q). Then

$$q < 2^s (1 - 2^{-s})^N .$$

Finding the minimum $N = N_{\min}$, for which inequality

$$q < \binom{n}{s} \left[\varepsilon \binom{n}{s} + 1 \right]^{-1} \cdot 2^s (1 - 2^{-s})^N \leq 1 \tag{4.7}$$

holds, we obtain (4.3). When s is large, (4.3) can be rewritten in a simpler form:

$$f(\varepsilon, n, s) < 2^s \log_2 \frac{2^s}{\varepsilon + \binom{s}{en} s} . \tag{4.8}$$

Corollary 1 *For* $1 \ll s,\ 1/4 \log_2 n$

$$\phi(n, s) \leq 2^s s \log_2 \frac{2en}{s}, \tag{4.9}$$

which is consistent with the upper bounds on $\phi(n, s)$ *obtained in [2], [7] and [8].*

Corollary 2 *For any fixed* $\varepsilon > 0$,

$$2^{s-2}(\log_2 \varepsilon^{-1}) + \frac{1}{2} \log_2(2\pi \log_2 \varepsilon^{-1}) < \lim_{(n-s)\to\infty} f(\varepsilon, n, s) < 2^s \log(2^s \varepsilon^{-1}) . \tag{4.10}$$

Corollary 2 demonstrates a significant difference between s-exhaustive and (ε, s)-exhaustive tests. The size of an optimal (ε, s)-exhaustive test remains finite (bounded from above) for any constant values of ε and s, while the size of an s-exhaustive test must grow with n at least as $\log_2 n$.

Now we show, how (ε, s)-exhaustive tests can be constructed by "horizontal concatenation " of s-exhaustive tests for a smaller number of input variables.

Theorem 3

$$f(\varepsilon, n, s) \leq \phi(r_{\min}, s), \tag{4.11}$$

where $r_{\min}$ *is the minimum integer value of* r, *for which the following inequality holds:*

$$\binom{n}{s}^{-1} \binom{r}{s} \left(\left\lceil \frac{n}{r} \right\rceil^{\frac{n}{r} - \lfloor \frac{n}{r} \rfloor} \left\lfloor \frac{n}{r} \right\rfloor^{\lfloor \frac{n}{r} \rfloor - \frac{n}{r} + 1} \right)^s \geq 1 - \varepsilon . \tag{4.12}$$

For $n \gg s$ and $\varepsilon \ll 1$

$$f(\varepsilon, n, s) \ \leq \ \phi(r, s)\,, \tag{4.13}$$

where

$$r \ = \ \left\lceil \frac{s(s-1)n}{s(s-1) - 2n\ln(1-\varepsilon)} \right\rceil . \tag{4.14}$$

Proof. Consider an s-exhaustive test for r input variables $T(0, r, s)$. Let $|T(0, r, s)| = \phi(r, s)$. Form a matrix of order $\phi(r, s) \times r\lceil n/r \rceil$ by concatenating the rows of $\hat{T}(0, r, s)$ $\lceil n/r \rceil$ times. (Let us call it horizontal concatenation of $\lceil n/r \rceil$ matrices $\hat{T}(0, r, s)$). If $n = r\lceil n/r \rceil - g$, we delete g distinct columns, so that the obtained $\phi(r, s) \times n$ matrix consists of $(r-g)$ groups of $\lceil n/r \rceil$ identical columns and of g groups of $\lfloor n/r \rfloor$ identical columns. Obviously, an s-tuple is good if each column is taken from a different group. Therefore, the number of good s-tuples is

$$G_s \ = \ \sum_{i=0}^{s} \binom{g}{i} \binom{r-g}{s-i} \left\lfloor \frac{n}{r} \right\rfloor^{i} \left\lceil \frac{n}{r} \right\rceil^{s-i}, \tag{4.15}$$

where summation is taken over all non-vanishing terms. Note that a^i is a convex function of i. Therefore, by Jensen inequality,

$$\begin{aligned} G_s \ &\geq \ \binom{r}{s} \left(\left\lfloor \frac{n}{r} \right\rfloor^{g/r} \left\lceil \frac{n}{r} \right\rceil^{1-g/r} \right)^{s} \\ &= \ \binom{r}{s} \left(\left\lfloor \frac{n}{r} \right\rfloor^{\lceil \frac{n}{r} \rceil - \frac{n}{r}} \left\lceil \frac{n}{r} \right\rceil^{1+\frac{n}{r}-\lceil \frac{n}{r} \rceil} \right)^{s} \ = \ G_s^{*}\,. \end{aligned} \tag{4.16}$$

The fraction of good s-tuples in the matrix is $G_s\binom{n}{s}^{-1}$. Hence, for the matrix to be (ε, s)-exhaustive, it is sufficient that

$$G_s^{*}\binom{n}{s}^{-1} \ \geq \ 1 - \varepsilon\,, \tag{4.17}$$

which yields (4.11)-(4.12). If $n \gg s$ and $\varepsilon \ll 1$, then also $r \gg s$. Then, using Stirling's expansion, we obtain from (4.17)

$$r \ \geq \ \frac{s(s-1)n}{s(s-1) - 2n\ln(1-\varepsilon)} \tag{4.18}$$

which results in (4.13)-(4.14).

Theorem 3 shows that the number of test patterns in a (ε, s)-exhaustive test can be substantially smaller, then in an s-exhaustive test.

Corollary 3 *For any fixed ε and s,*

$$\lim_{n\to\infty} f(\varepsilon, n, s) \ \leq \ \phi\left(-\frac{s(s-1)}{2\ln(1-\varepsilon)}, s\right). \tag{4.19}$$

Consider now constructions of (ε, s)-exhaustive tests based on linear codes. Let us remind a simple property of linear tests (e.g. [7]).

Lemma 4 *Consider a $2^k \times n$ test matrix $\hat{T}$ whose rows are all code words of a linear (n, k) code over GF(2). Then an s-tuple ($s \leq k$) is good, iff the s columns are linearly independent over GF(2).*

Proof. If s columns are linearly independent, there exist s linearly independent rows in the corresponding $2^k \times s$ submatrix of $\hat{T}$. Since the rows of $\hat{T}$ form a linear space, the rows of the submatrix contain all the 2^s linear combinations of the s linearly independent rows. Conversely, if the s-tuple is good, the rows of the submatrix contain s linearly independent vectors, and therefore the s columns are also linearly independent.

Let $\hat{H}(s)$ be a matrix formed by the code words of a $(2^s - 1, s)$ simplex code [16, p.30] as the rows. (This is, in fact, the Hadamard matrix over $\{0, 1\}$ with the zero column deleted). The columns of the matrix $\hat{H}(s)$ also form an s-dimensional linear space (except for the zero column).

Lemma 5 *The fraction $\varepsilon_H(s)$ of bad s-tuples in $\hat{H}(s)$ is equal to*

$$\varepsilon_H(s) = 1 - \frac{\prod_{i=0}^{s-1}(2^s - 2^i)}{\prod_{i=1}^{s}(2^s - i)} \tag{4.20}$$

and

$$\beta = \lim_{s \to \infty} \varepsilon_H(s) = 0.711211\ldots \tag{4.21}$$

Proof By lemma 4, the number of good s tuples in $\hat{H}(s)$ is equal to the number of different choices of a basis in the s-dimensional column space. Obviously, $(i+1)$-th basis column can be chosen arbitrarily from $2^s - 2^i$ columns (the total number of the columns minus the number of all linear combinations of the previously chosen i columns),Therefore, the total number of good s-tuples is equal

$$G_s = \frac{1}{s!}\prod_{i=0}^{s-1}(2^s - 2^i) \tag{4.22}$$

and

$$\varepsilon_H(s) = 1 - \frac{G_s}{\binom{2^s-1}{s}} = 1 - \frac{\prod_{i=0}^{s-1}(2^s - 2^i)}{\prod_{i=1}^{s}(2^s - i)} \tag{4.23}$$

Note that $\varepsilon_H(s)$ is a monotone increasing function of s. Remarkably the fraction of good s-tuples has a nonzero limit when $s \to \infty$:

$$1 - \beta \;=\; \lim_{s\to\infty} \frac{G_s}{\binom{2^s-1}{s}} \;=\; 0.288788\ldots. \tag{4.24}$$

which gives (4.21).

Theorem 4

$$f(\varepsilon, n, s) \;\le\; 2^s \left\lceil \frac{\log \varepsilon}{\log \delta(a,s)} \right\rceil, \tag{4.25}$$

where

$$\delta(a,s) \;=\; 1 - (1 - \varepsilon_H(s)) \frac{(2^s-1)!(a\cdot 2^s - a - s)a^s}{(2^s - s - 1)!(a \cdot 2^s - a)!} \tag{4.26}$$

√ !

$(a\cdot 2^s - a - s)$

and

$$a \;=\; \lceil n(2^s-1)^{-1} \rceil. \tag{4.27}$$

Proof. Consider a matrix $\hat{H}(s)$ of a simplex $(2^s - 1, s)$ code and form a horizontal concatenation $\hat{A}(a,s)$ of $a = \lceil n(2^s-1)^{-1}\rceil$ such matrices. The fraction p of s-tuples with non-repeating columns chosen from $\hat{A}(a,s)$ is

$$p \;=\; \frac{\binom{2^s-1}{s}a^s}{\binom{a(2^s-1)}{s}} \;=\; \frac{(2^s-1)!(a\cdot 2^s - a - s)a^s}{(2^s-s-1)!(a\cdot 2^s - a)!}. \tag{4.28}$$

~~$(a\cdot 2^s - a^a$~~

$(a\cdot 2^s - a - s)$

Therefore, the fraction $\delta(a,s)$ of bad s-tuples in $\hat{A}(a,s)$ is

$$\delta(a,s) \;=\; 1 - (1 - \varepsilon_H(s))p. \tag{4.29}$$

Let r be the minimum integer such that $\delta^r(a,s) \le \varepsilon$, that is

$$r \;=\; \left\lceil \frac{\log \varepsilon}{\log \delta(a,s)} \right\rceil. \tag{4.30}$$

Consider r matrices $\{\hat{A}_i(a,s)\}(i = 1, 2, \ldots, r)$ obtained by r independent random permutations of the columns of $\hat{A}(a,s)$. Now form an $r \cdot 2^s \times a(2^s - 1)$ matrix $\hat{M}(r,a,s)$ by concatenating the corresponding columns of these r matrices. (We call it vertical concatenation of matrices $\hat{A}_i$). Let $E_i(i = 1, 2, \ldots, r)$ be the event that given s-tuple is bad in matrix $\hat{A}_i(a,s)$. Since the permutations are chosen independently at random, the events E_i are independent. Therefore, the probability that an s-tuple taken from $\hat{M}(r,a,s)$ is bad is $\delta^r(a,s) \le \varepsilon$. Thus, the matrix $\hat{M}(r,a,s)$ is (ε, s)-exhaustive. Then, by applying Lemma 1 $a(2^s - 1) - n$ times we obtain an $r \cdot 2^s \times n$ submatrix which is also (ε, s)-exhaustive. Thus

$$f(\varepsilon, n, s) \le r \cdot 2^s \;=\; 2^s \left\lceil \frac{\log \varepsilon}{\log \delta(a,s)} \right\rceil. \tag{4.31}$$

[illegible]
[illegible]

Corollary 4

$$f(\varepsilon,n,s) \;<\; 2^s\left[\frac{\log\varepsilon}{\log[\varepsilon_H(s)+s(s-1)2^{-s-1}-\varepsilon_H(s)s(s-1)2^{-s-1}]}\right]. \qquad (4.32)$$

Proof.

$$p \;>\; (2^s-1)\prod_{i=1}^{s}(2^s-i) \;>\; 1-s(s-1)2^{-s-1}. \qquad (4.33)$$

Then (4.32) follows from (4.29), (4.31) and (4.33).

Corollary 5

$$f(\varepsilon,n,s) \;<\; 2^s\gamma\log_2(1/\varepsilon) \qquad (4.34)$$

L ε

where

$$\gamma \;=\; -(\log_2\beta)^{-1} \;=\; 2.034\ldots \qquad (4.35)$$

Proof. Note that

$$1-\varepsilon_H(s) \;=\; \prod_{i=1}^{s}(1-2^{-i})\left[\prod_{i=1}^{s}(1-i2^{-s})\right]^{-1}.$$

Taking into account ~~(4.33)~~ we obtain

$$\begin{aligned}\delta(a,s) &= 1-(1-\varepsilon_H(s))p\\ &< 1-(1-2^{-s})^{-s}\prod_{i=1}^{s}(1-2^{-i})\\ &< 1-\prod_{i=1}^{\infty}(1-2^{-i})=\beta,\end{aligned}$$

which, by (4.31), gives (4.34) - (4.35). The upper bound (4.25) is not completely "constructive", since it is obtained using random permutations. Therefore, we give below explicit constructions of linear (ε,s)-exhaustive tests.

Theorem 5 *If $s \le \log_2 n$, there is a construction for a test $T(\varepsilon,n,s)$ such that*

$$|T(\varepsilon,n,s)| \;\le\; [2^{s+1}+s(s-1)]\varepsilon^{-1}, \qquad (4.36)$$

and $T(\varepsilon,n,s)$ is a linear subspace of Z_2^n.

□ Z_{2}^{n}

indeces in italic

Proof. Consider the matrix $\hat{H}(m)$ of a $(2^m-1,m)$ simplex code, where $s<m\le\log_2 n$. By the same reasoning, as in Lemma 5, the fraction p_1 of good s-tuples in $\hat{H}(m)$ is equal to

$$p_1 \;=\; \frac{\prod_{i=0}^{s-1}(2^m-2^i)}{s!\binom{2^m-1}{s}} \;>\; \prod_{i=0}^{s-1}(1-2^{i-m}) \;>\; 1-2^{-m}\sum_{i=0}^{s-1}2^i \;>\; 1-2^{s-m}. \qquad (4.37)$$

Now form a $2^m \times a(2^m - 1)$ matrix $\hat{M}(a, m)$ by the horizontal concatenation of $a = \lceil n(2^m - 1)^{-1} \rceil$ identical matrices $\hat{H}(m)$. The fraction p_2 of s-tuples with nonrepeating columns chosen from $\hat{M}(a, m)$ is equal to

$$p_2 = \frac{a^s \binom{2^m-1}{s}}{\binom{a(2^m-1)}{s}} > \frac{\prod_{i=1}^{s}(2^m - i)}{(2^m - 1)^s} > 1 - s(s-1)2^{-m-1} . \tag{4.38}$$

Therefore, the fraction of good s-tuples in $\hat{M}(a, m)$ is

$$p = p_1 p_2 > (1 - 2^{s-m})(1 - s(s-1)2^{-m-1}) > 1 - 2^{s-m}(1 + s(s-1)2^{-s-1}) . \tag{4.39}$$

The matrix $\hat{M}(a, m)$ is (ε, s)-exhaustive, if

$$2^{s-m}(1 + s(s-1)2^{-m-1} \leq \varepsilon . \tag{4.40}$$

$\lceil s \rceil)$ $(1+s(s-1)2^{-s-}$

The minimum integer value of m which satisfies (4.40) is given by

$$m = s + \lceil \log_2 [1 + s(s-1)2^{-s-1})\varepsilon^{-1}] \rceil \leq s + 1 + \log_2 [(1 + s(s-1)2^{-s-1})\varepsilon^{-1}] . \tag{4.41}$$

By applying Lemma 1 $a(2^m - 1) - n$ times we obtain a $2^m \times n$ submatrix $\hat{T}(\varepsilon, n, s)$ which is (ε, s)-exhaustive. Thus,

$$|T(\varepsilon, n, s)| = 2^m \leq [2^{s+1} + s(s-1)]\varepsilon^{-1} . \tag{4.42}$$

The case $n - s = t \ll n$ calls for special consideration. The following lemma is useful for constructing (ε, s)-exhaustive tests in this case.

Lemma 6 *Suppose that a test matrix is formed by all the code words of a linear (n, k) code as rows. Then an s-tuple is good iff the binary vector v_s which has ones in the corresponding s positions and zeros in the remaining $n - s$ positions does not cover any nonzero code word in the dual (orthogonal) $(n, n - k)$ code.*

Proof. If vector v_s does not cover any nonzero code word of the dual code, then the s-tuple consists of linearly independent columns, and, by Lemma 4, the s-tuple is good. Conversely, if v_s covers a nonzero code word in the dual code, then the columns comprising the s-tuple are linearly dependent, and, by Lemma 4, the s-tuple is bad.

codeword

Theorem 6 *For $n - s = t$ there is a construction for a test $T(\varepsilon, n, n - t)$ such that*

$$|T(\varepsilon, n, n - t)| \leq 2^{n - \lfloor t(\ln t/\varepsilon)^{-1} \rfloor} , \tag{4.43}$$

and $T(\varepsilon, n, n - t)$ is a linear subspace of $\mathbf{Z}_2^n$.

Proof. Consider a linear (n, m) code with a generating matrix which consists of m nonoverlapping (i.e. having no common nonzero components) binary vectors

$x_1, \dots, x_m$ of weights $\lfloor n/m \rfloor$ and $\lceil n/m \rceil$. Obviously, a vector $v_s = v_{n-t}$ covers a nonzero code word of this code iff it covers at least one of the m rows of the generating matrix. The $(n, n-m)$ code dual to the previous one will be used as a test, the code words being the rows of the test matrix $\hat{T}$. By Lemma 6, an $(n-t)$-tuple in the test matrix is bad, iff the corresponding vector v_{n-t} covers at least one of the words $x_1, \dots, x_m$, or, in other words, iff its complement (negation) $\overline{v}_{n-t}$ (which has t nonzero components) does not overlap with at least one of these words.

Denote by $x \cap y = \emptyset$ the fact that two binary words x and y do not overlap. The probability q that an $(n-t)$-tuple chosen at random from the test matrix $\hat{T}$ is bad can be upperbounded by the use of the union bound:

$$\begin{aligned} q &= \Pr\{\exists \mathrm{i} \mid \overline{\mathrm{v}}_{\mathrm{n-t}} \cap \mathrm{x_i} = \emptyset.\ \mathrm{i} = 1, \dots, \mathrm{m}\} \\ &\leq m \cdot \max_i \Pr\{\overline{\mathrm{v}}_{\mathrm{n-t}} \sqcap \mathrm{x_i} = \emptyset\} \\ &= m \cdot \binom{n - \lfloor n/m \rfloor}{t} \binom{n}{t}^{-1} \leq m(1 - 1/m)^t \leq me^{-t/m}. \end{aligned} \qquad (4.44)$$

Hence, our test is $(\varepsilon, n-t)$-exhaustive, if

$$me^{-t/m} \leq \varepsilon. \qquad (4.45)$$

Since the number of test patterns is 2^{n-m}, we are interested in the largest integer m that satisfies (4.45). It is easy to see that (4.45) is fulfilled for

$$m = \lfloor t(\ln(t/\varepsilon))^{-1} \rfloor \leq t(\ln(t/\varepsilon))^{-1}, \quad (\text{assuming } t/\varepsilon \geq e) \qquad (4.46)$$

e italic

which leads to (4.43).

Note that for s-exhaustive tests the best known result is ([4], [7])

$$\phi(n, n-t) \leq \frac{2^n}{t+1}, \qquad (4.47)$$

and thus, for any fixed ε and sufficiently large t, $|T(\varepsilon, n, n-t)| \ll \phi(n, n-t)$.

5 Asymptotically s-exhaustive sequences of tests.

Let us explore now the asymptotic behaviour of (ε, s)-exhaustive tests when $\varepsilon \to 0$ with $n \to \infty$. Denote by $\psi_\sigma(n, s)$ the number of test patterns in a test $T(\varepsilon, n, s)$ which belongs to an asymptotically s-exhaustive sequence of tests $(T(\varepsilon, n, s)) = \sigma$, i.e. $|T(\varepsilon(n), n, s[= \psi_\sigma(n, s)$ for any $T(\varepsilon(n), n, s) \in \sigma$.

Theorem 7 i. *For any asymptotically s-exhaustive sequence of tests there exists a function $h_\sigma(n-s)$ such that*

$$h_\sigma(n-s) \to \infty \qquad \text{when} \qquad (n-s) \to \infty, \qquad (5.1)$$

and

$$\psi_\sigma(n,s) \ \geq\ 2^s h_\sigma(n-s)\,. \tag{5.2}$$

ii. *For any $h(n)$ such that*

$$h(n) \to \infty \qquad \textit{when} \qquad n \to \infty \tag{5.3}$$

there exists an asymptotically s-exhaustive sequence of tests σ such that

$$\psi_\sigma(n,s) \ \leq\ 2^s h(n)\,. \tag{5.4}$$

Proof. i. Consider an asymptotically s-exhaustive sequence of tests σ.

Let

$$h_\sigma(n-s) \ =\ 2^{-2}\cancel{\log_2}\frac{n-s+2}{1+\varepsilon(n-s+1)}\,, \tag{5.5}$$

$\vdash\!\dashv \log_2$

where $\varepsilon = \varepsilon(n)$ is the fraction of bad s-tuples in the test $T(\epsilon, n, s) \in \sigma$. Obviously, if $\varepsilon = \varepsilon(n) \to 0$ when $n \to \infty$, then $h_\sigma(n-s) \to \infty$ when $(n-s) \to \infty$. Thus, by Theorem 1,

$$\psi_\sigma(n,s) \ \geq\ f(\varepsilon, n, s) \ \geq\ 2^s h_\sigma(n-s)\,. \tag{5.6}$$

ii. Let

$$\varepsilon \ =\ \varepsilon(n) \ =\ 2^{-h(n)/\gamma}\,, \tag{5.7}$$

where γ is given by (4.35).

$$\text{If } \ h(n) \to \infty \quad \text{when } \ n \to \infty, \quad \text{then } \ \varepsilon(n) \to 0 \quad \text{when } \ n \to \infty\,. \tag{5.8}$$

Take a sequence of (ε, s)-exhaustive tests such that $f(n, s) = f(\varepsilon(n), n, s)$. By (5.8) this sequence is asymptotically s-exhaustive. On the other hand, by (4.34),

$\ulcorner\ \psi_6$

$$\psi_\sigma(n,s) \ <\ 2^s\gamma\log_2(1/\varepsilon) \ =\ 2^s h(n)\,. \tag{5.9}$$

The meaning of the first part of Theorem 7 is that for $\varepsilon \to \infty$ with $n \to \infty$ the number of test patterns must increase faster than 2^s, if $(n-s) \to \infty$. In particular, it cannot remain bounded even for a constant s. The second part of the theorem shows, however, that this additional factor $h(n)$ can be chosen to grow arbitrarily slow with n. It means that $\psi_\sigma(n,s)$ can grow much slower than $\phi(n,s)$. Thus, by sacrificing an infinitesimal fraction of all possible output functions, we can gain substantially with the number of test patterns.

References

[1] A.K. Ibarra and S. Sahni, IEEE Trans. Comput. C-24, 242 (1975).

[2] A.K. Chandra, L.T. Kau, G. Markowsky, and S. Zaks, IBM Research Report RC-8336 (1981).

[3] Z. Barzilai, D. Coppersmith, and A. Rosenberg, IBM Research Report RE-8750 (1981).

[4] D.T. Tang and L.S. Wao, IBM Research Report RC-9442 (1982).

[5] D.T. Tang and C.L. Chen, IBM Research Report RC-10064 (1983).

[6] A. Lempel and M. Cohn, IEEE Trans. Inform. Theory 31, 10 (1985).

[7] G. Cohen, M. Karpovsky, and L. Levitin, *1984 IEEE Int. Workshop on Inform. Theory*, Caesarea, Israel 1984.

[8] D.J. Kleitman and J. Spencer, Discrete Mathematics 6, 255 (1973).

[9] P. Erdos, P. Frankl, and Z. Furedi, J. Combin. Theory A 33, 158 (1982).

[10] D.J. Kleitman, J. Shearer, and D. Sturtevant, Combinatorica 1, 381 (1981).

[11] W.W. Peterson, *Error-Correcting Codes*, Mass. Inst. Tech., Cambridge, (1961).

[12] D. Lubell, J. Combin. Theory 1, 299 (1966).

[13] G. Birkhoff, *Lattice Theory*, Amer. Math. Society, Providence, 1961.

[14] R.P. Dilworth, Ann. of Math. 51, 161 (1950).

[15] L.R. Ford and D.R. Fulkerson, *Flows in Networks*, Princeton Univ. Press, Princeton, 1962.

[16] F.J MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ., Amsterdam-New York-Oxford, 1978.

[17] L.B. Levitin, and M.G. Karpovsky, 1986 IEEE Int. Symposium on Inform. Theory, Ann Arbor, MI, USA, 1986

[18] G. Freiman, E. Lipkin, and L.B. Levitin, Discrete Mathematics, 70, 137 (1988)