June 15-18 Barcelona
Balearic Islands

Pseudoexhaustive Tests Based on Error-Correcting Codes.*

L. B. Levitin, M.G. Karpovsky (USA)

Mailing Address:

College of Engineering

Boston University

110 Cummington Street

Boston, MA 02215

* This work has been partially supported by NSF Grant No. DCR-8317763.

Pseudoexhaustive Test Based on Error-Correcting Codes.

L.B. Levitin, M.G. Karpovsky (USA)

Consider a combinational device with m inputs where each output is a Boolean function of at most s binary input variables. The problem of exhaustive testing of such devices ([1] - [5]) can be formulated as follows: construct a binary matrix $T(m,s)$ (rows of $T(m,s)$ are test patterns) with m columns such that all 2^s possible binary vectors appear in each s columns of the matrix. A test with $T(m,s)$ as a test matrix is called s-exhaustive.

It has been shown ([1],[4]) that there exist s-exhautive matrices with a number of rows which grows asymptotically with m as log m (for any fixed value of s). The lower bound on the number of rows also yields the same order of growth. However, no constructions of s-exhaustive tests are known which satisfy these (non-constructive) bounds.

In this paper an iterative procedure for constructing s-exhaustive tests is suggested in which the number of test patterns grows with m as $\log^w m$, where w can be chosen arbitrarily close to 1, i.e. arbitrarily close to the theoretical bound.

Let $T(q,s)$ be an s-exhaustive binary matrix with N rows and q columns. Denote columns of $T(q,s)$ by numbers $0,1,\ldots,(q-1)$. Consider a q-ary matrix $Q = \|q_{ij}\|$ with n rows and m columns ($m \geq q$), where matrix elements $q_{ij} \in \mathbb{Z}_q = \{0,1,\ldots,(q-1)\}$. If now we replace each matrix element of Q by a corresponding column of $T(q,s)$, we obtain a binary matrix M with nN rows and m columns.

Lemma 1. The matrix M is s-exhaustive if the matrix Q has the following property:

Consider any submatrix S of Q with n rows and s columns. Consider now any submatrix R of S with n rows and r columns ($r = 1, \ldots, \lfloor s/2 \rfloor$). Denote the matrix elements of R and those of the complementary submatrix S-R (i.e., of the columns of S not included in R) by, respectively, a_{ig} and b_{ih} ($1 \le i \le n$, $1 \le g \le r$, $1 \le h \le s-r$). For any choice of S and for any choice of R there exists a row $j = j(S,R)$ such that $a_{jg} = b_{jh}$ for any g and h. (Here $\lfloor c \rfloor$ is the integral part of c).

Consider now the set of binary columns which are all possible Hamming differences between the columns of matrix Q. (A component of the Hamming difference is equal to 0 if the corresponding components of the two columns of Q are equal, and it is equal to 1 otherwise).

Lemma 2. The matrix M is s-exhaustive if for any $\lfloor s^2/4 \rfloor$ Hamming differences between the columns of matrix Q there exists a row where all the elements are equal to 1.

Let q now be a prime or a power of a prime, let's take $m=q^k$, $k=2,3\ldots$, and let columns of Q be the codewords of a linear code $C(n,k,d)$ over $GF(q)$, where n is the length, k is the dimension and d is the distance of the code. The following theorem shows how q-ary linear codes can be used to construct s-exhaustive tests.

Theorem 1. The matrix M is s-exhaustive if for the corresponding q-ary linear code $C(n,k,d)$

$$d\lfloor s^2/4 \rfloor > n(\lfloor s^2/4 \rfloor - 1).$$

The best constructions of this type are given by maximum distance separable (MDS) codes which satisfy the singleton bound $n = d+k-1$.

Using the results on MDS codes presented in ([6], Ch. 11) we come to the following conclusion.

<u>Theorem 2</u>. Let $T(q,s)$ be an s-exhaustive test with N test patterns and $q = p^t$, where p is a prime, and t = 1,2,... Then for any k such that

$$q \geq \lfloor s^2/4 \rfloor (k-1)$$

an s-exhaustive test $T(q^k, s)$ can be constructed by use of an MDS code $C(n,k\ d = n-k+1)$ over GF(q) with $n = \lfloor s^2/4 \rfloor (k-1) + 1$. The obtained test $T(q^k, s)$ has

$$nN = (\lfloor s^2/4 \rfloor (k-1) + 1)N$$

test patterns.

It follows from Theorem 2 that in transition from $T(q,s)$ to $T(q^k,s)$ the number of test patterns grows as $\ln^w m$, where m is the number of input variables (i.e., the number of columns in the test matrix), and

$$W = 1 + \frac{\log (\lfloor s^2/4 \rfloor \cdot (k-1)+1) - \log k}{\log k + \log \ln q}$$

Since $w \to 1$ for increasing k and q, the asymptotical growth of the number of test patterns can be made arbitrarily close to the theoretical bound $\ln m$ for any fixed s.

On the other hand, it can be shown that the redundancy $(n-k)/k$ cannot be made arbitrarily small for any construction which uses columns of $T(q,s)$ to build a larger s-exhaustive test $T(q^k,s)$.

<u>Theorem 3</u>. Let $T(q,s)$ be a s-exhaustive test. Consider a q-ary matrix Q with n rows and q^k columns. Then the binary matrix M obtained by

substituting columns of $T(q,s)$ for corresponding matrix elements of Q cannot be s-exhaustive if

$$n \leq (s-1)(k-1).$$

Theorem 3 shows that for s=3 MDS codes give an optimal construction ($n = 2(k-1) + 1$) of the considered type.

The complexity of the test generator is considered. It is shown that a test generator for the tests based on MDS codes can be implemented with an asymptotically minimal number of gates $L(q^k,s) \sim q^k$. A method for such an implementation is suggested.

References

1. A.K. Chandra, L.T. Kou, G. Markowsky, and S. Zaks, "On Sets of Boolean n-Vectors with all k-Projections Surjective", IBM Research Report, RC-8936, July 1981.

2. Z. Barzilai, D. Coppersmith, and A. Rosenberg, "Exhaustive Bit Pattern Generation in Discontinuos Positions, with Applications to VLSI Self-Testing", IBM Research Report RC-8750, March 1981.

3. D.T. Tang and C.L. Chen, "Efficient Exhaustive Pattern Generation for Logic Design", IBM Research Report RC-10064, July 1983.

4. G. Cohen, M. Karpovsky, L. Levitin, Exhaustive Testing of Circuits with Outputs Depending on Limited Number of Inputs", 1984 IEEE International Information Workshop, Caesarea, Israel, 1984.

5. A. Lempel and M. Cohn, "Design of Universal Test Sequences for VLSI", IEEE Trans. on Information Theory, IT-31, No. 1, 10-17, Jan. 1985.

6. F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland Publishing Co., 1978.