# Spectral Techniques for Off-Line Testing and Diagnosis of Computer Systems*

Mark G. Karpovsky, Fellow IEEE

Research Laboratory on Design and Testing of Computer Hardware
Department of Electrical, Computer and Systems Engineering
Boston University
Boston , MA 02215

*Abstract* -In this paper we present some of our recent results on applications of spectral techniques over finite fields to the problems of testing and diagnosis of computer systems.

## I. Linear Transforms for Testing of Computer Systems.

Consider a computer system of (not necessarily identical) processing elements (PEs) (this system may be a computer board, multichip module, array processor or computer network). If the system has $n$ output PEs and every PE has at most $m$ output pins, then the response of the system at any given time can be represented as $y=(y_0, \ldots, y_{n-1})$, where $y_i \in Z_q$, $q=2^m$, $Z_q$ is the field with $q=2^m$ elements and $E\ y \in Z_q^n$.

Let $E \subseteq Z_q^n$ be the set of all possible errors in the system such that as a result of the error $e \in E$ $y$ is replaced by $y+e$.

Problems of compression of test responses for error detection can be formulated in the following way:

**P1.** Given $E \subseteq Z_q^n$, construct a transform $y \mapsto H(y)$,

$$H(y)=\{H_j(y) | j=0,1,\ldots,r-1\}, \quad H_j(y) \in Z_q$$

with minimal $r$ such that

$H(y+e) \neq H(y)$ for all $y \in Z_q^n$ and $e \in E$.

**P2.** Given a distribution $P(E)=\{P_0, P_1, \ldots, P_{M-1}\}$, where $M=q^n$ and $P_i=\text{Prob}\{e=i\}$, construct a transform $y \mapsto H(y)$,

$$H(y)=\{H_j(y) | j=0,1,\ldots,r-1\}, \quad H_j(y) \in Z_q,$$

minimizing $\text{Prob}\{H(y+e)=H(y)\}$ (we assume that all $y \in Z_q^n$ are uniformly distributed).

We note that $Z=H(y) \in Z_q^r$ $(Z=(Z_0, \ldots, Z_{r-1}), Z_j=H_j(y),\ Z_j \in Z_q)$, and if $r \ll n$ by monitoring $Z \in Z_q^r$ instead of $y \in Z_q^n$ one can achieve a considerable reduction in overheads required for testing.

Let us consider the case $r=1$. Select

$$Z=Z_1=H_1(y_0, y_1, \ldots, y_{n-1})=\sum_{i=0}^{n-1} y_i \alpha^i, \qquad (1)$$

where $\alpha$ is a primitive element in $Z_q$, and all the operations in (1) are in $Z_q$ $(n \leq q-1)$,. This approach is known as the signature analysis and it is widely used for off-line testing and for built-in self-testing (BIST) [1, 2].

Computation of the signature, Z, can be implemented in $n$ steps by the following recursive procedure:

$$Z^{(i-1)}=\alpha Z^{(i)}+y_{i-1} \quad (i=n, n-1, n-2, \ldots, 1). \qquad (2)$$

where $Z^{(n)}=0, Z^{(i)} \in Z_q$ and $Z^{(0)}=Z$.

This procedure can be implemented in hardware by a $m$-bit linear feedback shift register (LSFR) with parallel input and with the characteristic equation defined by (2) ($y_{i-1}$ is the new input , $Z^{(i)}$ is the previous state and $Z^{(i-1)}$ is the new state.

The hardware implementation of an $m$-bit LFSR requires only $m$ flip-flops and several XOR gates in feedback loops [1].

We note that $Z_1$ defined by (1) is the first coefficient of the Fourier expansion of $y=(y_0, y_1, \ldots, y_{n-1})$ over $Z_q$ [3, 4]. The network (LSFR) computing $Z_1$ can be considered as a

*This work was supported by the National Science Foundation (USA) under Grant MIP 9208487, the NATO under Grant 910411 and Volkswagen Foundation (Germany).

network computing syndromes for the $q$-ary $(n, n\text{-}1)$ Reed-Solomon code of length $n$ with distance 2 [5]. In a view of this one can see that (1) provides for the solution of **P1** for single errors, i. e. when $E=\{e \mid \|e\|=1\}$, where $\|e\|$ is the number of nonzero components in $e=(e_0,e_1,\ldots,e_{n-1})$ $(e_i=Z_q)$.

Let us consider the efficiency of the signature analysis defined by (1) for solution of **P2**. In this case we assume that errors in different components of $y$ are independent (components of $e$ are independent), and all components of $e$ have the same distribution

$$P(e)=(P_0,P_1,\ldots,P_{q-1})$$

$$\left(q=2^m,\ P_i=\text{Prob}\{e_j=i \mid \text{for all } j=0,1,\ldots,n-1\}\right).$$

We will present below our results on probabilities $P_{AL}=\text{Prob}\{H_1(y+e)=H_1(y)\}$ (which are also known as masking or aliasing probabilities) for three important classes of error distributions which correspond to so called "symmetrical errors", "independent errors", and "errors of a given multiplicity".

For symmetrical errors we assume [6, 7, 8]:

$$P_i=\begin{cases}1-p, & i=0;\\ p(2^m-1)^{-1}, & i\neq 0.\end{cases}\quad \text{for some } 0<p<1 \qquad (3)$$

In this case using results from [6, 10] it is possible to show that

$$P_{AL}=\text{Prob}\{H(y+e)=H(y)\}=$$
$$=2^{-m}\left[1-2^m(1-p)^n+(2^m-1)(1-2^m p(2^m-1)^{-1})\right]. \qquad (4)$$

For independent errors [6, 7, 9] we consider every $e_j\in Z_q$ $(q=2^m)$ as an $m$-bit binary vector, and we assume that distortions in the binary components of the vectors are independent. If $\|i\|$ is a number of ones in the binary representation of $i$ $(i=0,1,\ldots,2^{m-1})$, then we have for independent errors

$$P_i=\binom{m}{\|i\|}p_b^{\|i\|}(1-p_b)^{m-\|i\|}, \qquad (5)$$

where $p_b$ is a probability of a distortion of one bit, and for $n=c(2^m-1)$ we have [6, 7]

$$P_{AL}=2^{-m}\left[1-(2^m-1)(1-2p_b)^{cm2^{m-1}}\right]-(1-p_b)^{c(2^m-1)m}. \qquad (6)$$

For errors of a given magnitude [6]

$$P_i=\begin{cases}1-p, & i=0;\\ p, & i=a;\\ 0, & \text{otherwise;}\end{cases}\quad \text{for some } a\in Z_q-0 \qquad (7)$$

and for $n=2^m-1$

$$P_{AL}=2^{-m}\left[1-(2^m-1)(1-2p)^{2^{m-1}}\right]-(1-p)^{2^m-1}. \qquad (8)$$

For large $n$, (say, $n>50$) for all three models $P_{AL}\to 2^{-m}$. Analysis of aliasing probabilities for benchmark circuits [6] shows that for small $n$ the independent error model predicts minimum aliasing, and the symmetrical model predicts aliasing more accurately than the other models.

Let us consider now the case $r>1$. In this case we select the following system of $r$ $q$-ary functions

$$Z_j=H_j(y_0,y_1,\ldots,y_{n-1})=\sum_{i=0}^{n-1}y_i\alpha^{ji} \qquad (9)$$

$$(j=0,1,\ldots,r-1)$$

($\alpha$ is a primitive in $Z_q$, $q=2^m$).

This approach is known as multisignature analysis, and it was also used for off-line testing and diagnosis [11, 12, 13]. The hardware implementation of this approach requires $r$ $m$-bit LFSRs with characteristic equations

$$Z^{(i-1)}=\alpha^j Z^{(i)}+y_{i-1},\ Z^{(n)}=0,\ Z^{(0)}=Z_j;\ j=0,1,\ldots,r-1. \qquad (10)$$

In this case $Z_0,Z_1,\ldots,Z_{r-1}$ defined by (9) are the first $r$ coefficients of the Fourier expansion of $y=(y_0,\ldots,y_{n-1})$ over $Z_q$. The network computing $Z_0,Z_1,\ldots,Z_{r-1}$ ($r$ $m$-bit LFSRs) computes syndromes for the $q$-ary $(n, n\text{-}r)$ Reed-Solomon codes of length $n$ with distance $r+1$. Thus, (9) provides for the minimal solution of **P1** for the case when at most $r$ components of $e=(e_0,e_1,\ldots,e_{n-1})$ are not equal to 0, i. e. at most r components of $y=(y_0,\ldots,y_{n-1})$ are distorted $(E=\{e \mid 0<\|e\|\le r\})$. For a large $n$ we have for the above error models $P_{AL}\to 2^{-rm}=q^{-r}$ for all $e$ such that $\|e\|>r$. $(P_{AL}=0 \text{ for } 0<\|e\|\le r)$.

Let us consider a more general case when the set, $E$, of errors is defined by the topology of the system.

Let $X$ be the set $\{X_0,X_1,\ldots,X_{N-1}\}$ of $N$ processing elements. Consider a digraph G having X as a set of vertices and a set $U=\{U_0,U_1,\ldots,U_{M-1}\}$ of directed edges ( $m$-

bit communication links) between vertices of $G$. We shall also assume that the graph has no cycles and all $n$ output vertices are reachable from at least one input vetrex. Let $y=(y_0, y_1,\ldots, y_{n-1}) \in Z_q^n$ be an output vector for the system represented by the graph $G$, where $y_i \in Z_q$ is an output of the corresponding output vertex $(i=0,1,\ldots,n-1)$.

The problem to be considered is the problem of error detection under the assumption of single vertex failures in the graph $G$. A failure in the graph (system of processing elements) refers to a physical malfunction that cause an undesired event. We consider a fault in the graph which alter its output value to $\tilde{y}=(\tilde{y}_0, \tilde{y}_1,\ldots, \tilde{y}_{n-1})$, where $\tilde{y}_i \in Z_q$. The error in the graph's output $y$ can be characterized by the error vector $e=(e_0, e_1,\ldots, e_{n-1})$ where $e_i = \tilde{y}_i + y_i$ for $i=0,1,\ldots,n-1$.

Let us first define an error set $E(G)$ characterized by the underlying graph $G$. In our definition of an error set we assume that at most one vertex or any number of incoming edges to this vertex may fail and a fault in the graph manifest itself by distorting all successor vertices outputs, i. e. error propagates along a directed path.

Let $E_j = \left\{\left(e_0^{(j)}, e_1^{(j)}, \ldots, e_{n-1}^{(j)}\right)\right\} (j=0,\ldots,N-1)$ be a set of error patterns corresponding to a fault in vertex $X_j$, where $e_i^{(j)} \in Z_q - 0$ if there exists a directed path from $X_j$ to an output and $e_i^{(j)} = 0$ otherwise. The set $E(G) = \bigcup_{j=o}^{N=1} E_j$ of all possible error patterns corresponding to all single vertex failures in $G$ called the error set for $G$.

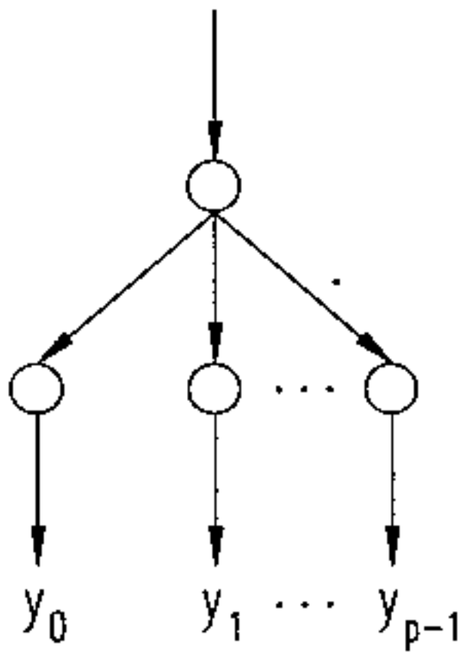

Fig. 1: $p$-ary Star Network Topology

To illustrate the above definition let us now consider the $p$-ary star network topology ( see Fig. 1). For the $p$-ary star, the single central processing element (root) is connected to all others, $N = p+1$ and $n = p$. Due to single vertex or processing element failures we have the following nonzero errors in the $p$-ary star:

$$E(G) = \left\{\begin{array}{l}(e_0, e_1, \ldots, e_{p-1}), \\ (e_0, 0, \ldots, 0), \\ (0, e_1, \ldots, 0), \\ \quad\vdots \\ (0, 0, \ldots, e_{p-1}),\end{array}\right\}, \tag{11}$$

where $e_i \in Z_q - 0$. Thus, we have $|E(G)| = (q-1)^p + p(q-1)$ nonzero error vectors for $p$-ary star over $Z_q$.

Let $Z = Hy$, where $H$ is a $(r \times n)$ $q$-ary transform matrix over $Z_q$ $\left(y \in Z_q^n,\ \ Z \in Z_q^r\right)$. Consider a graph, $G(E)$, having the error set $E(G)$ $\left(0 \notin E(G)\right)$ as a set of vertices and $U = \left\{\left(E_i, E_j\right) \middle|\ E_i, E_j \in E(G),\ \ E_i + E_j \in E(G)\right\}$ as a set of edges. Denote by $\chi(E)$ the chromatic number for $G(E)$ ($\chi(E)$ is a minimal number of colors required to color vertices of $G(E)$ in such a way that no two neighboring vertices have the same color; techniques for graph coloring with lower and upper bounds for $\chi(E)$ can be found e.g. in [14]). Then using results from [14, 15] we have for a minimal number $r_{\min}$ of transform coefficients required for detection of $E(G)$:

$$\begin{aligned}&\min\left(n - \left\lfloor \log_q\left(q^n - |E(G)|\right)\right\rfloor, \left\lceil \log_q\left(\chi(E)+1\right)\right\rceil\right) \le \\ &\le r_{\min} \le \left\lceil \log_q\left(|E(G)|(q-1)+1\right)\right\rceil\end{aligned} \tag{12}$$

We will present now solutions for the data compression problem **P1** for the two important topologies: trees and Fast Fourier Transform (FFT) networks.

Let $T_h$ be a $p$-ary full tree of height $h$ $(p \ge 2, h \ge 2)$. The height of the tree is the length of a longest path from the root to any leaf. (Here we assume that input vertex is the root and output vertices are $n = p^{h-1}$ leaves of the tree). Then

$$|E(G)| = \sum_{i=0}^{n-1} p^i (q-1)^{p^{h-1-i}}. \tag{13}$$

For example, 4-ary tree $T_3$ is represented in Fig. 2

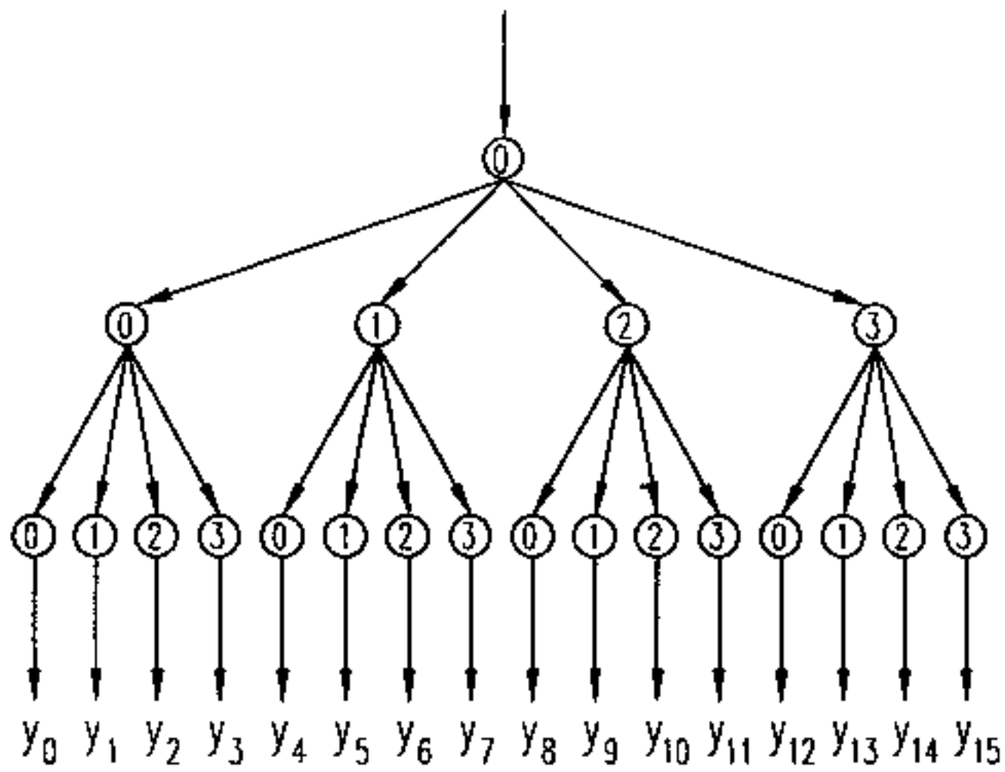

Fig. 2: 4-ary Full Tree of Height h=3

For this tree the error set $E(G)$ is:

$$\left\{\begin{array}{llllllllllllllll}
(e_0, & e_1, & e_2, & e_3, & e_4, & e_5, & e_6, & e_7, & e_8, & e_9, & e_{10}, & e_{11}, & e_{12}, & e_{13}, & e_{14}, & e_{15}), \\
(e_0, & e_1, & e_2, & e_3, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0), \\
(0, & 0, & 0, & 0, & e_4, & e_5, & e_6, & e_7, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0), \\
(0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & e_8, & e_9, & e_{10}, & e_{11}, & 0, & 0, & 0, & 0), \\
(0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & e_{12}, & e_{13}, & e_{14}, & e_{15}), \\
(e_0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0), \\
(0, & e_1, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0), \\
 & & & & & & & \cdots & & & & & & & \vdots & \\
(0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & e_{15}),
\end{array}\right\},$$

$$\text{where } e_i = Z_q - 0. \tag{14}$$

It is possible to show [15, 16], that for a $p$-ary full tree with $h \le \left(\log_p\left(1+(q-1)^{-1}\right)\right)$ for any $p$, $r_{\min} = h$ and

$$H = H^{(h)} = \left[\begin{array}{c} \overbrace{H^{(h-1)} \quad H^{(h-1)} \quad \cdots \quad H^{(h-1)}}^{p} \\ W \end{array}\right],$$

where W is a row of one 1 followed by $n-1 = p^h - 1$ zeros, and

$$H^{(2)} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{15}$$

For example, for $T_3$ represented by Fig. 2 ($p$=4, $h$=3) we have

$$H = H^{(3)} = \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 1000 & 1000 & 1000 & 1000 \\ 1000 & 0000 & 0000 & 0000 \end{bmatrix}.$$

For the n-point FFT, there are $N = n\log_2 n$ vertices interconnected with $\log_2 n$ levels of butterfly structures, e.g., the graph for the 8-point FFT with decimation-in-frequency (DIF) is shown in Fig. 3.

If we consider input fanout branches as possible source of errors, then there are $n\left(\log_2 n + 1\right)$ single faults in the $n$-point FFT graph. Due to these single faults we have the following nonzero errors for the 8-point FFT graph of Fig. 3:

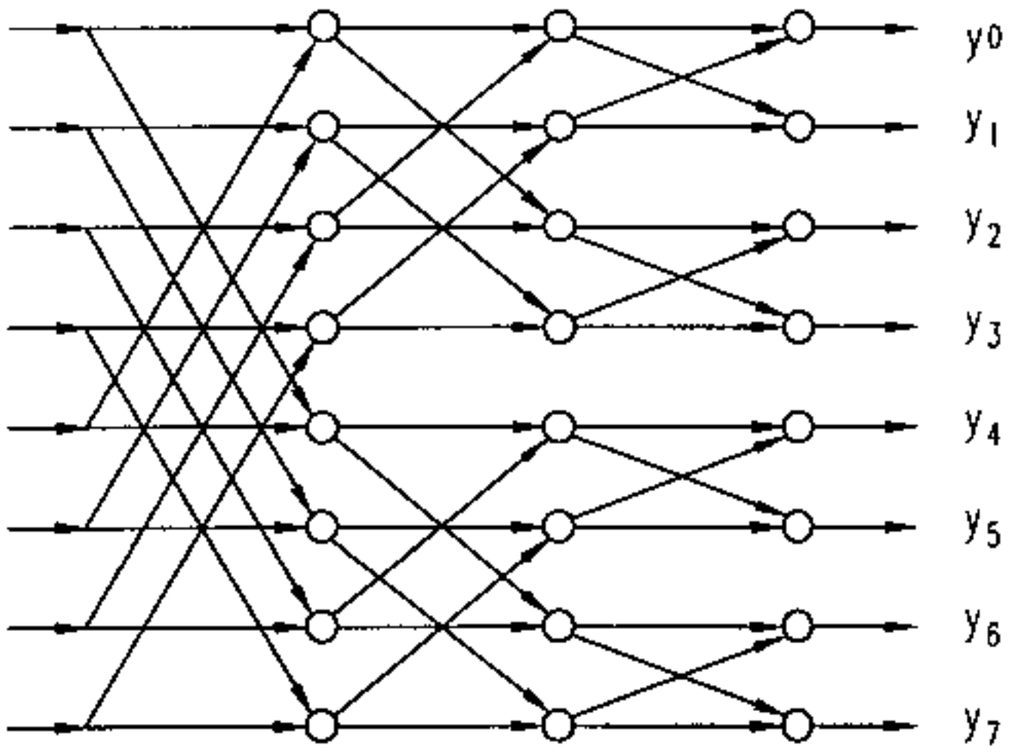

Fig. 3: Eight-Point DIF FFT Network Topology

$$E(G) = \left\{\begin{array}{llllllll}
(e_0, & e_1, & e_2, & e_3, & e_4, & e_5, & e_6, & e_7), \\
(e_0, & e_1, & e_2, & e_3, & 0, & 0, & 0, & 0), \\
(0, & 0, & 0, & 0, & e_4, & e_5, & e_6, & e_7), \\
(e_0, & e_1, & 0, & 0, & 0, & 0, & 0, & 0), \\
(0, & 0, & e_2, & e_3, & 0, & 0, & 0, & 0), \\
(0, & 0, & 0, & 0, & e_4, & e_5, & 0, & 0), \\
(0, & 0, & 0, & 0, & 0, & 0, & e_6, & e_7), \\
(e_0, & 0, & 0, & 0, & 0, & 0, & 0, & 0), \\
(0, & e_1, & 0, & 0, & 0, & 0, & 0, & 0), \\
 & & & \cdots & & & \vdots & \\
(0, & 0, & 0, & 0, & 0, & 0, & 0, & e_7),
\end{array}\right\},$$

where $e_i \in Z_q - 0$ and

$$|E(G)| = \sum_{i=0}^{t} 2^i (q-1)^{2^{t-i}}, n = 2^t.$$

The recursive construction for matrices $H$ for DIF FFT topologies is given by

$$H = H^{(n)} = \begin{bmatrix} H^{(n/2)} & H^{(n/2)} \\ & W \end{bmatrix}, \quad (16)$$

$$W = 100..0, \quad H^{(2)} = \begin{bmatrix} 11 \\ 10 \end{bmatrix}.$$

For example, for the 8-point DIF FFT graph represented by Fig. 3 :

$$H = H^{(8)} = \begin{bmatrix} 11 & 11 & 11 & 11 \\ 10 & 10 & 10 & 10 \\ 10 & 00 & 10 & 00 \\ 10 & 00 & 00 & 00 \end{bmatrix}.$$

(A construction similar to (16) can be used for FFTs with decimation-in-time [16] ).

Thus for a $n$-point FFT we have

$$r_{\min} = \log_2 n + 1. \quad (17)$$

The flow graph of the Walsh-Hadamard Transform (WHT) [3, 4] differs from the flow graphs of the FFT only in the values of twiddle factors ($\pm 1$ for WHT). Thus, solution (16) is valid also for networks computing WHT. Solutions for multidimensional FFTs and for Fast Chrestenson Transforms can be found in [16].

To conclude this section we note that elements of matrices $H$ for trees and FFTs are zeros and ones only.

## II. Robust Quadratic Transforms for Testing of Computer Systems.

In the previous section we considered linear data compressors $Z = Hy, \left(Z \in Z_q^r,\ y \in Z_q^n\right)$. For any linear transform we have for the probability, $P_{AL}(e)$, of masking (aliasing probability) for a given error pattern $e$

$$P_{AL}(e) = \text{Prob}\{H(y+e) = H(y)\} =$$

$$= \text{Prob}\{He = 0\} = \begin{cases} 1, e \in \text{ Kern } H; \\ 0, e \notin \text{ Kern } H. \end{cases} \quad (18)$$

Thus, performances of linear compressors are very sensitive to error distributions

$$P = \{P_0, P_1, \ldots, P_{M-1}\} \left(M = q^n, P_i = \text{Prob}\{e = i\}\right).$$

We will describe in this section a class of nonlinear (quadratic) *robust* transforms, such that their performances do not depend on error distributions. We will show that for optimal robust transforms described by $r$ quadratic $q$-ary functions, we have

$P_{AL}(e) = q^{-r}$ for any $e \neq 0$.

Suppose $n = 2rs$. Consider the following nonlinear mapping $Z_q^n \mapsto Z_q^r$

$$Z = (Z_0, \ldots, Z_{r-1}) = H(y_0, \ldots, y_{n-1}) = Y_0 Y_1 + \\ + Y_2 Y_3 + \ldots + Y_{2s-2} Y_{2s-1}, \quad (19)$$

where $Y_i = (y_{ir}, \ldots, y_{(i+1)r-1})$ $(i = 0, \ldots, 2s-1)$, and all operations in the quadratic form (19) are in $Z_q^r$.

For $q=2$ and $r=1$ these quadratic forms are known as bent functions [ 3, 5, 18, 19, 20, 21]. In this case $n = 2s$, $Y_i = y_i$,

$$Z = y_0 y_1 + y_2 y_3 + \ldots y_{n-2} y_{n-1}, \quad (20)$$

and we have for the autocorrelation for bent functions

$$B(e) = \sum_{y \in Z_2^n} H(y) H(y+e) = \begin{cases} 2^{n-1} - 2^{n/2-1}, e = 0; \\ 2^{n-2} - 2^{n/2-1}, e \neq 0. \end{cases} \quad (21)$$

Thus, $B(e) = \underset{e \neq 0}{\text{Const}}$. (We note that $B(e)$ can be computed by applying twice the Walsh-Hadamard Transform using the Wiener -Khinchin theorem [3] ).

For any linear function $f(y_0, \ldots, y_{n-1})$ $(y_i \in Z_2)$ such that $f(y_0, \ldots, y_{n-1}) = 1$, when $(y_0, \ldots, y_{n-1}) \in V$ and $f(y_0, \ldots, y_{n-1}) = 0$ otherwise, where $V$ is a subspace of $Z_2^n$, we have for its autocorrelation

$$B(e) = \sum_{y \in Z_2^n} f(y) f(y+e) = \begin{cases} |V|, e \in V; \\ 0, \ e \notin V. \end{cases} \quad (22)$$

Since for bent functions defined by (20), we have $B(e) = \underset{e \neq 0}{\text{Const}}$, one can say that bent functions are at the maximal distance from any linear function [5].

Let us introduce a system of characteristic functions $h_i(y)$ $(i = 0, \ldots, q^r - 1)$ for nonrepetative quadratic form H over $Z_q^r$ defined by (19):

$$h_i(y) = 1 \text{ iff } H(y) = i. \quad (23)$$

Autocorrelation functions $B_i(e)$ for $h_i(y)$ can be defined as

$$B_i(e) = \sum_{y \in Z_q^n} h_i(y) h_i(y+e) = \left| \{ y \mid H(y) = H(y+e) = i \} \right|. \quad (24)$$

(Autocorrelation functions $B_i(e)$ can be computed by the Wiener-Khinchin theorem using the Chrestenson transform over $Z_q^r$ [3, 4] ).

It is possible to show [22, 23] that for $i \neq 0$

$$B_i(e) = \begin{cases} q^{2rs-r} - q^{rs-r}, e = 0; \\ q^{2rs-2r} \pm q^{rs-r}, e \neq 0; \end{cases} \quad (25)$$

and we have for the total autocorrelation

$$B(e) = \sum_i B_i(e) = \left|\left\{ y \mid H(y) = H(y+e) \right\}\right| =$$

$$= \begin{cases} q^{2rs}, e = 0; \\ q^{2rs-r}, e \neq 0; \end{cases} \quad (26)$$

where $H(y)$ defined by (19).

Thus, quadratic forms defined by (19) have the flat total autocorrelation and compressors implementing these forms are robust with a probability of masking any error

$$P_{AL}(e) = q^{-r} = 2^{-mr}. \quad (27)$$

Let $C$ be a quadratic $q$-ary error-detecting code defined as $y \in C$ iff

$$H(y) = Y_0 Y_1 + \ldots, Y_{2s-2} Y_{2s-1} = 1, \quad (28)$$

where $Y_i = (y_{ir}, \ldots, y_{(i+1)r-1})$ and all operations in (28) are in $Z_q^r$. Then $C$ is a code with the length $n=2rs$ and the number of codeworks $\left| C \right| = q^{2sr-r} - q^{sr-r}$. These codes provide for an equal protection against all possible errors for large $q$ or large $n$ and are optimal for the minimax criterion on error detection [22]. For a given block size, n, and the number of codeworks, $\left| C \right|$, these codes minimize $\max_{e \neq 0} Q(e)$, where $Q(e)$ is the conditional error masking probability given the error pattern e. For these codes for any $e \neq 0$

$$\left(q^{2rs-2r} - q^{rs-r}\right)\left(q^{2rs-r} - q^{rs-r}\right)^{-1} \leq Q(e) \leq$$

$$\leq \left(q^{2rs-2r} + q^{rs-r}\right)\left(q^{2rs-r} + q^{rs-r}\right)^{-1} \quad (29)$$

and

$$Q(e) \sim q^{-r} \quad (30)$$

for large $n$ or large $q$.

Simple encoding and decoding procedures for these codes are presented in [22].

## III. Spectral Techniques for Soft Decision Diagnosis of Computer Systems.

Let $y = (y_0, y_1, \ldots, y_{n-1})$, $y_i \in Z_q, q = 2^m$ be a test response for a system-under-test. As a result of faults in the system $y$ may be destorted into $y+e$, where $e = (e_0, \ldots, e_{n-1})$, $e_i \in Z_q, e \in E(G)$, and the set of errors, $E(G)$, is defined by the topology of the system. Denote

$\mathrm{supp}(e) = \left(\mathrm{supp}(e_0), \ldots, \mathrm{supp}(e_{n-1})\right)$, where

$$\mathrm{supp}(e_i) = \begin{cases} 1, e_i \neq 0; \\ 0, e_i = 0. \end{cases}$$

The soft decision diagnosis problem can be formulated in the following way. For a given $E(G) \subseteq Z_q^n$ construct a transform $Z = H(y)$ over $Z_q$

$$Z_j = H_j\left(y_0, \ldots, y_{n-1}\right) \quad \left(j = 0,1,\ldots,r-1\right) \quad (31)$$

with minimal $r$ such that

$$H\left(y + e^{(1)}\right) \neq H\left(y + e^{(2)}\right) \quad (32)$$

for any $e^{(1)}, e^{(2)} \in E(G)$ and $\mathrm{supp}(e^{(1)}) \neq \mathrm{supp}(e^{(2)})$.

We will consider the case when $H$ is linear. Then (32) can be written as:

$$He^{(1)} \neq He^{(2)} \quad (33)$$

for any $e^{(1)}, e^{(2)} \in E(G)$, $\mathrm{supp}(e^{(1)}) \neq \mathrm{supp}(e^{(2)})$ and all operations are in $Z_q$. We will call $H(y)$ a fault-free signature, $H(y+e)$ a faulty signature and $S=He$ a syndrome of error $e$.

If (33) is satisfied, than the location, $\mathrm{supp}(e)$, of an error $e$ can be computed by analysis of the distortion $H(y)+H(y+e)$ in the fault-free signature. The bounds on a minimal number of spectral coefficients in transforms satisfying (33) can be obtained from bound (12) for error detection by replacing the error set $E(G)$ with

$$E(G) \bigcup \left\{ e^{(1)} + e^{(2)} \middle| \mathrm{supp}\left(e^{(1)}\right) \neq \right.$$

$$\left. \neq \mathrm{supp}\left(e^{(2)}\right); e^{(1)}, e^{(2)} \in E(G) \right\}.$$

We note that any matrix H satisfying (33) is a parity check matrix of a linear $q$-ary $(n, n\text{-}r)$ code locating the error set E(G). We note also that a linear $(n, n-r)$ code with a parity check matrix $H$ locating an error set $E(G)$, $0 \notin E(G)$ corrects $E(G)$ if and only if for every distinct $e^{(1)}, e^{(2)} \in E(G)$ with $\mathrm{supp}\left(e^{(1)}\right) = \mathrm{supp}\left(e^{(2)}\right)$, there exists a pair $e^{(3)}, e^{(4)} \in E(G) \bigcup 0$ with $\mathrm{supp}\left(e^{(3)}\right) \neq \mathrm{supp}\left(e^{(4)}\right)$ such that $e^{(1)} + e^{(2)} = e^{(3)} + e^{(4)}$.

We note that the above condition is a necessary and sufficient condition on the error set $E(G)$ such that if and only if this condition is satisfied any linear code locating $E(G)$ will also correct $E(G)$.

For example, for the p-ary star with $p=5$ and $q=2^2$,
$E(G)=\{(e_0,e_1,e_2,e_3,e_4),(e_0,0,0,0,0),(0,e_1,0,0,0),$
$(0,0,e_2,0,0),(0,0,0,e_3,0),(0,0,0,0,e_4)\}$,
where $e_i \in \{1=01,\alpha=10,\alpha^2=11\}$. A code locating $E(G)$ does not guarantee error correction since for two errors $e^{(1)}=(1,1,1,1,1), e^{(2)}=(1,1,\alpha,\alpha,\alpha)$ there is no pair $e^{(3)},e^{(4)}$ with different .support such that $e^{(1)}+e^{(2)}=e^{(3)}+e^{(4)}=(0,0,\alpha^2,\alpha^2,\alpha^2)$ (note that $\alpha^2+\alpha+1=0$).
Using the above arguments one can see that any code over $Z_q$ locating up to $l$ independent errors $(E(G)=\{e \mid 0<\|e\|\le 2l\})$ can also correct $l$ errors. The same is also true for codes locating burst errors.

Let us consider now the case when at most $l$ components in $y=(y_0,\ldots,y_{n-1})$ may be distorted $(E=\{e \mid 0<\|e\|\le l\})$.
In this case $H$ can be taken as the check matrix of the $q$-ary Reed-Solomon code of length $n$ [5]

$$H=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ & & \cdots & & \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(r-1)(n-1)} \end{bmatrix}, \quad (34)$$

where $\alpha$ is primitive in $Z_q$, $n \le q-1$ and $r=2l$. For this matrix any $r$ columns are linearly independent over $Z_q$.
Computing $Z=Hy$, where $H$ is defined by (34), requires $n$ clocks and $r$ LFSRs with parallel input. An error locating procedure for this case identifies supp$(e)$ for a given $He$. This procedure based on the Euclidean algorithm [12] has a complexity $L=O(lm)+O(\log_2 n)$. ($L$ is a number of equivalent two-input gates, $q=2^m$). For example, for $n=100$, $m=32$ and $l=5$ we have $L \sim 28{,}000$ [12].
We note also that H defined by (34) with $r=2l$ can be used for location of more than $l$ errors. It was shown in [13] that if $\|e\|=t>l$, then the fraction $w$ of localizable errors with $\|e\|=t$, $l<t<2l$, is lowebounded by

$$w \ge (1-q^{-1})^{\binom{n}{t}-1} \sim e^{-\binom{n}{t}q^{-1}}. \quad (35)$$

For example, if $t=5$, $r=6$, $n=100$, $q=2^{32}$ ($m=32$), then $w=0.979$. Thus, by allowing a small fraction of errors not to be located , one can reduce substantially the required redundancy from $r=2l$ to $r=l+1$.

Let us consider now the error-locating problem when the original system is the full $p$-ary tree of height $h$ ($n=p^{h-1}$) (the 4-ary full tree of height $h=3$ is presented in Fig. 2, the error set for this tree is given by (14)).

The following recursive procedure can be used for construction of $H=H^h$ for $p$-ary trees[16].

$$H^{(h)}=\begin{bmatrix} H^{(h-1)} & H^{(h-1)} & \cdots & & H^{(h-1)} & & \\ 11\cdots1 & \alpha\alpha\cdots\alpha & \cdots & \alpha^{p-1} & \alpha^{p-1} & \cdots & \alpha^{p-1} \\ 10\cdots0 & 00\cdots0 & \cdots & 0 & 0 & \cdots & 0 \\ 00\cdots0 & 10\cdots0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}, \quad (36)$$

where

$$H^{(2)}=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-1} \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{bmatrix}_{4\times p}, \quad (37)$$

$4 \le p < q$, and $\alpha$ is primitive in $Z_q$. Thus, for any $p$-ary, $(4 \le p < q)$ tree $r=3h-2$. For the case of $p=3$ one can also use the above construction (36) with $H^{(2)}=I_3$ ($I_3$ is and identity matrix of 3 by 3). Therefore, for the $p$-ary tree with $p=3$, $q>p$, $r=3h-3$.
For binary trees over $Z_q$ the following recursive construction can be used :

$$H^{(h)}=\begin{bmatrix} H^{(h-1)} & H^{(h-1)} \\ 10\cdots0 & 00\cdots0 \\ 00\cdots0 & 10\cdots0 \end{bmatrix}, \quad (38)$$

where $H^{(2)}=I_2$. Thus, for the binary tree over $Z_q$ of height $h$, $r=2h-2$.
The complexity $L$ for the syndrome computing network implementing $H^{(h)}y$ in terms of nubmers of $Z_q$ adders and multipliers is [16]:

$$L=\left(2\left(p^{h-1}-p\right)+h(p-1)\right)L_{\oplus}+\left((h-1)(p-1)\right)L_{\otimes}, \quad (39)$$

where $L_{\otimes}$ is a complexity of a multiplier that multiplies a field element from $Z_q$ by a fixed element from the same field. This network for $h=3$ is represented at Fig. 4.

The error locating procedure for tree errors is very simiple. Let us denote

$$S = H^{(h)} y = \begin{bmatrix} S^{h-1} \\ S^h_1 \\ S^h_2 \\ S^h_3 \end{bmatrix}, \qquad (40)$$

where $S^{h-1}$ are syndroms due to the $\left[H^{(h-1)} H^{(h-1)} \cdots H^{(h-1)}\right]$ part of $H^{(h)}$ (see(36)) and $S^h_1, S^h_2, S^h_3$ are syndroms for the last three rows of the parity check matrix $H^{(h)}$. Let $S^1$ denotes the syndrome for the all 1 row.

The location algorithm to find a faulty vertex is described as follows:

1.If $S_i = 0, i = 1,2,\ldots, 3h-2$: no error, end.

2. Let $j = h$.

3.If both $S^j_2 \neq 0$ and $S^j_3 \neq 0$: error location is the root of the tree of height j, end.

4. For $j > 2$, if either $S^j_2 = 0$ and $S^j_3 = 0$: error location is in the subtree $k$, $0 \le k \le p-1$, where $\alpha^k = S^j_1 / S^{j-1}_2$; for $j = 2$, if either $S^2_2 = 0$ or $S^3_2 = 0$: error location is in vertex (leaf) k, $0 \le k \le p-1$, where $\alpha^k = S^2_1 / S^1_2$.

5.Repeat steps 3 and 4 for tree of height $j = j-1$.

6. End.

The transform matrix $H_3$ for the 4-ary tree of height $h=3$ is

$$H^{(3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & 1 & \alpha & \alpha^2 & \alpha^3 & 1 & \alpha & \alpha^2 & \alpha^3 & 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & \alpha & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad (41)$$

Suppose that a root of subree 1 (See Fig. 2) is faulty and

$$e = \left(0,0,0,0,\alpha,\ 1,\alpha^3,0,\ 0,0,0,0,0,0,0,0,\right). \qquad (42)$$

Then

$$S = H^{(3)} e = \left(\alpha,\alpha^5,\alpha,\alpha,\alpha^2,\ 0,\ \alpha,\right). \qquad (43)$$

This yields $S^3_2 = 0$, therefore the error is in the subtree 1 since $S^3_1 / S^3_2 = \alpha^2 / \alpha = \alpha$, $i = 1$. Since $S^2_2 \neq 0$ and $S^3_2 \neq 0$, error is in the root of subtree 1 of height 2.

We note that the number, $r$, of rows in $H^{(h)}$ for $p$-ary trees of height $h$ can be drastically decreased (from $r=3h$-2 to $r=h$) if we allow a small probability of misdiagnosis. In this case one can take [16]

$$H^{(h)} = \begin{bmatrix} H^{(h-1)} & H^{(h-1)} & \cdots & H^{(h-1)} \\ 11\ldots1 & \alpha\,\alpha\ldots\alpha & \cdots & \alpha^{p-1}\alpha^{p-1}\ldots\alpha^{p-1} \end{bmatrix}, \qquad (44)$$

where

$$H^{(2)} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{bmatrix},\ n=p<q.$$

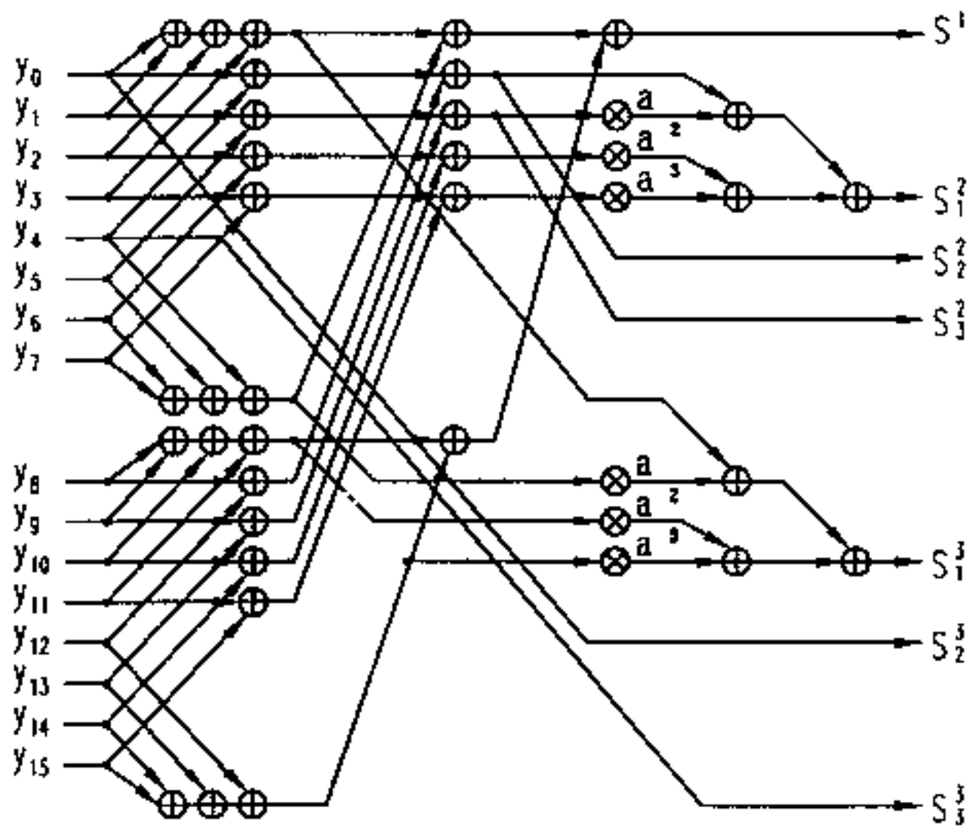


Fig.4 Network for Computing $S = H^{(3)} y$

The number of rows in $H^{(h)}$, defined by (44) is equal to $h$. The location procedure in this case is very simple, and the probability of correct diagnosis for this procedure can be estimated as [ 16]

$$w = 1 - \left(1 - pq^{-1}\right)^{h-1} \qquad (45)$$

which is small for large $q$.

## IV. Spectral Techniques for Hard Decision Diagnosis of Computer Systems.

The hard decision diagnosis problem can be formulated in the following way. For a given $E(G) \subseteq Z^n_q$ construct a binary

matrix $H$ with a minimal number of rows such that for any $e^{(1)}, e^{(2)} \in E(G)$ with $\mathrm{supp}\left(e^{(1)}\right) \neq \mathrm{supp}\left(e^{(2)}\right)$

$\mathrm{supp}\left(He^{(1)}\right) \neq \mathrm{supp}\left(He^{(2)}\right)$, where (46)

$\mathrm{supp}\left(Z = Z_0, \ldots, Z_{r-1}\right) = \left(\mathrm{supp}\left(Z_0\right), \ldots, \mathrm{supp}\left(Z_{r-1}\right)\right)$.

The hard decision approach allows identification of errors $e$ by analyzing supports of their syndromes $S=He$. Magnitudes of distortions in components of a syndrome are not important for the hard decision diagnosis. The identification of locations of errors is possible if there is a one-to-one mapping

$$E(G) \leftrightarrow \left\{\mathrm{supp}(He) \,\middle|\, e \in E(G)\right\}.$$

In general, this approach requires more rows in $H$ (more observation points for the compressed response $Z=Hy$) but a decoding procedure is very simple and has a straightforward hardware implementation.

Denote $H \otimes \mathrm{supp}(e)$ the Boolean multiplication of an $(r \times n)$ binary matrix $H$ by an $n$-bit binary vector $\mathrm{supp}(e) = \left(\mathrm{supp}(e_0), \ldots, \mathrm{supp}(e_{n-1})\right)$ with addition being replaced by logical summation (OR). Then with probability $1 - q^{-1}$ if

$H \otimes \mathrm{supp}\left(e^{(1)}\right) \neq H \otimes \mathrm{supp}\left(e^{(2)}\right)$, (47)

then $He^{(1)} \neq He^{(2)}$; $e^{(1)}, e^{(2)} \in E(G) \subseteq Z_q^n$ and $\mathrm{supp}\left(e^{(1)}\right) \neq \mathrm{supp}\left(e^{(2)}\right)$.

Let us consider now the hard decision diagnosis problem for the case of $l$ independent errors $\left(E = \left\{e \,\middle|\, 0 < \|e\| \leq l\right\}\right)$. We note that in this case any check matrix of a $l$-th order binary superimposed code [24, 25, 26, 27] can be chosen as the transform matrix $H$.

A binary superimposed code of order $l$ consists of a set of codewords such that componentwise Boolean sum (OR) of any $l$ codewords differs from every other componentwise sum of $l$ or fewer codewords.

Thus, in a view of (47), any check matrix of a $l$-th order linear superimposed code can be chosen as a hard decision diagnostic matrix $H$.

Since there are $|E| = \sum_{i=0}^{l} \binom{n}{i}$ different locations of $l$ errors, we have the following lower bound on the minimal number $r=r(n,l)$ of required spectral coefficients (rows in $H$)

$$r(n,l) \geq \left\lceil \log_2 \sum_{i=0}^{l} \binom{n}{l} \right\rceil. \quad (48)$$

For the case of single errors $\left(l = \|e\| = 1\right)$, one can take as $H$ any binary matrix with different nonzero columns. Thus

$$r(n,1) = \left\lceil \log_2 (n+1) \right\rceil. \quad (49)$$

The case of multiple errors ($l>1$) is not as simple and it is difficult even to estimate $r=r(n,l)$. Several good constructions of check matrices for linear superimposed codes can be found in [24, 25, 26].

A hardware implementation of the hard decision diagnostic algorithms for $l = 1, n = 100, q = 2^{32}$ requires about 10,000 equivalent two-input gates [27].

Let us consider now a general case of hard decision diagnosis, when the error set $E(G)$ is defined by the topology $G$ of the system.

Let $N$ be the number of processing elements in the systems (nodes in $G$) and $d$ is the length (number of nodes) of the longest path in $G$.

Then we have the following attainable bounds on a minimal number of rows in $H$

$$\max\left(\left\lceil \log_2(N+1) \right\rceil, d\right) \leq r \leq n. \quad (50)$$

These bounds can be improved if we have additional information about the topology of the system..

Let $N(j)$ be the number of paths of length at least $j$ which do not have any endpoints in common. The following two lower bounds on $r$ have been proven in [28, 29]:

$$\sum_{i=1}^{r-j+1} \binom{r}{i} \geq N(j), \quad (51)$$

$$\sum_{i=1}^{\lceil (r-j)2^{-1} \rceil} \binom{r}{i} + \sum_{r=\lceil (r+j)2^{-1} \rceil}^{r} \binom{r}{i} \geq M(j). \quad (52)$$

Lower bounds (51), (52) are valid for all values of $j = 1,2,\ldots,d$.

For the $p$-ary full tree of height $h$ we have $d = h, n = p^{h-1}$, $N = \frac{p^h - 1}{p-1}$ and $N(d) = p^{d-1}$. Thus, by (50), (51) we have the following lower bounds for the minimal number $r = r(d)$ of spectral coefficients required for hard diagnosis of $p$-ary trees of height $h = d$.

$$r(d) \geq \left\lceil \log_2 \left( \frac{p^{d-1} - 1}{p-1} + 1 \right) \right\rceil \quad (53)$$

and

$$\sum_{i=1}^{r(d)-d+1}\binom{r(d)}{i}\geq p^{d-1}\ . \qquad (54)$$

Solving (54) for $d >> 1$ we have asymptotically

$$r(d) > \begin{cases} 1.29(d-1), & p=2; \\ 1.64(d-1), & p=3; \\ (\log_2 p)(d-1), & p\geq 4. \end{cases} \qquad (55)$$

We note, that for $p \geq 4$ and $d >> 1$ (53) gives better lower bounds than (55).

The best known upper bounds on $r$ for binary trees [29] are given by

$$r(d) \leq \begin{cases} 1.5\,(d-1), d=4r+1; \\ \lceil 1.5\,(d-1)\rceil + 1, \text{ otherwise.} \end{cases} \qquad (56)$$

Values of $r(d)$ for binary trees with $N < 2^{12}$ are given in the following table:

| $d$ | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| $r(d)$ | 2 | 4 | 5 | 6 | 8 | 9-10 |

| $d$ | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|
| $r(d)$ | 10-11 | 12 | 13-14 | 14-16 | 16-17 |

Table 1: Minimal Numbers, $r(d)$, of Spectral Coefficients Required for Hard Diagnosis of Binary Trees of Height $h=d$

Optimal or near optimal constructions for $\left(r(d)\times p^{d-1}\right)$ transform matrices $H$ for $p$-ary trees $h$, together with lower and upper bounds for $r(d)$ for different $p>2$ and $N=\dfrac{p^d-1}{p-1}<5{,}000$ can be found in [28, 29]. The gap between bounds is small.

Constructions for optimal or near optimal transforms for hard diagnosis for two dimensional meshes and multidimensional cube topologies can be found in [29].

## References


[1] Bardell, P. H., McAnney, W. H., and Savir, J., "Built-In Test For VLSI: Pseudorandom Techniques,", John Wiley & Sons, 1982.

[2] Konemann, B., Mucha, J., and Zwieholf, G., "Built-In Test for Complex Digital Integrated Circuits", *IEEE J. Solid State Circuits*, Vol. SC-15, pp. 315-318, June 1980.

[3] Karpovsky, M. G., "Finite Orthogonal Series in the Design of Digital Devices", John Wiley & Sons, 1976.

[4] Karpovsky, M. G., (Editor), "Spectral Techniques and Fault Detection", Academic Press, 1985.

[5] MacWilliams, F. J., Sloane, N. J. A., "The Theory of Error Correcting Codes", North Holland, 1978.

[6] Karpovsky, M. G., Gupta, S. K., Pradhan, D. K., "Aliasing and Diagnosis Probability in MISR ...", *Proc. Int. Test Conf.*, 1991, pp. 828-840.

[7] Pradhan, D. K., Gupta, S. K., "A Framework for Designing and Analyzing New BIST Techniques ...", *IEEE Trans. On Computers*, Vol. 40, No. 6, pp. 743-763, June 1991.

[8] Pradhan, D. K., Gupta, S. K., Karpovsky, M. G., "Aliasing Probability for Multiple Input Signature Analyzer", *IEEE Trans. on Computers*, Vol. 39, No. 4, pp. 586-591, April 1990.

[9] Damiani, M., et al, "Aliasing in Signature Analysis Testing with Multiple Input Shift Registers", *IEEE Trans. on CAD*, Vol. 9, No. 12, pp. 1344-1353, December 1990.

[10] Iwasaki, K., Arakawa, F., "An Analysis of the Aliasing Probability of Multiple Input Signature Registers in the Case of a $2^m$-ary Symmetrical Channel", *IEEE Trans. on CAD*, Vol. 9, No. 4, pp. 427-438, April 1990.

[11] Iwasaki, K., Yamaguchi, N., "Design of Signature Circuits Based on Weight Distributions of Error-Correcting Codes", *Proc. Int. Test Conf.*, 1990.

[12] Karpovsky, M. G., Chaudhry, S., "Design of Self-Diagnostic Boards by Multiple Signature Analysis", *IEEE Trans. on Computers*, Vol. 42, No. 9, September, 1993, pp. 1035-1044.

[13] Karpovsky, M. G., Chaudhry, S., Levitin, L. B., "Multiple Signature Analysis: a Framework for Built-In Self-Diagnostic", *Proc. 22-nd Fault-Tolerant Computing Symp.*, 1992, pp. 112-120.

[14] Berge, C., "Graphs and Hypergraphs", North Holland, N. Y., 1973.

[15] Karpovsky, M. G., Milman, V. D., "On Subspaces Contained in Finite Homogeneous Spaces", *Discrete Mathematics*, Vol. 22, 1978, pp. 273-280.

[16] Karpovsky M. G., Chaudhry, S., Levitin, L. B., Moraga, C., "Detection and Location of Given Sets of Errors by Nonbinary Linear Codes", to appear in Springer in Verlag, 1994.

[17] Karpovsky, M. G., Roziner, T., Moraga, C., "Error Detection in Multiprocessor Systems and Array Processors", to appear *in IEEE Trans. on Computers*, 1994.

[18] Rothaus, O. S., "On "Bent" Function", *J. Comb. Theory*, A 20, 1976, pp. 300-305.

[19] McFarland, R. L., "A Family of Difference Sets in Non-Cycle Groups", *J. Comb. Theory*, A 15, 1976, pp. 1-10.

[20] Olsen, J. D., Scholtz, R. A., Welch, L. R., "Bent-Function Sequences", *IEEE Trans. Inform. Theory*, IT-28, No. 6, 1982, pp. 858-864.

[21] Lempel, A., Cohn, M., "Maximal Families of Bent Sequences", *IEEE Trans. Inform. Theory*, IT.-28, No. 6, 1982, pp. 865-868.

[22] Karpovsky, M. G., Nagvajara. P., "Optimal Codes for the Minimax Criterion on Error Detection ", *IEEE Trans. Inform. Theory,* IT-35, No. 6, November 1989, pp. 1299-1305.

[23] Karpovsky, M. G., Nagvajara, P., "Function with Flat Autocorrelation and Their Generalizations", *Proc. Third Int. Workshop on Spectral Techniques*, Germany 1988, to appear in Springer and Verlag in 1994.

[24] Stiassny, S., "Mathematical Analysis of Various Superimposed Coding Methods", *IBM Res. Report*, No. RC 103, April 1959.

[25] Kautz, W. H., Singleton, R. C., "Nonrandom Binary Superimposed Codes", *IEEE Trans. Inform. Theory*, IT-10, October 1964.

[26] Dyachkov, A. G., Rykov, V. V., "A Survey on Superimposed Codes Theory", *Problems of Information and Control*, Vol. 12, No. 4, 1983.

[27] Karpovsky, M. G., Chaudhry, S., "Built-In Self-Diagnostic by Space-Time Compression of Test Responses", *Proc. IEEE VLSI Test Symp.*, 1992, pp. 1035-1044.

[28] Karpovsky, M. G., Levitin. L. B., Vainstein, F. S., "Identification of Faulty Processing Elements by Space-Time Compression of Test Responses", *Proc. Int. Test Conf.*, 1990, pp. 638-647.

[29] Karpovsky, M. G., Levitin, L. B., Vainstein, F. S., "Diagnosis by Signature Analysis of Test Responses", *IEEE Trans. on Computers*, Vol. 43, No. 1, January 1994.