ISTITUTO DI ELABORAZIONE DELLA INFORMAZIONE DEL C.N.R. - PISA

DIAGNOSABILITY OF SYSTEMS PARTITIONED INTO COMPLEX UNITS

F. Barsi*, F. Grandoni**, P. Maestrini*

Reprinted from Proceedings of "1975 International Symposium on Fault-Tolerant Computing"
Parigi, Francia, 18-20 Giugno 1975.

* Istituto di Elaborazione della Informazione del C.N.R.

** Selenia S.p.A. - Roma

Stampato in proprio

DIAGNOSABILITY OF SYSTEMS PARTITIONED INTO COMPLEX UNITS

F. Barsi°, F. Grandoni°°, P. Maestrini°
° Istituto di Elaborazione dell'Informazione del CNR. Pisa, Italy
°° Selenia S.p.A. Roma, Italy

ABSTRACT

The problem of automatic fault diagnosis of systems decomposed into a number of interconnected units is considered by using a simplified version of the diagnostic model introduced by Preparata, Metze and Chien. The model considered in this paper is supposed to be a realistic representation of systems where each unit has a considerable computational capability. For any system of n units for which the set of testing links is given, necessary and sufficient conditions for t-diagnosability are presented in both cases of one-step diagnosis and diagnosis with repair. It is shown that, if the diagnostic model introduced in this paper is applicable, the procedure for diagnosis with repair has very small complexity. The problem of optimal assignment of testing links in a system with n units in order to achieve a given diagnosability is also considered and classes of optimal t-diagnosable systems are presented for arbitrary values of t in both cases of one-step diagnosis and diagnosis with repair.

1. INTRODUCTION

Because of the expanding application of computers into areas requiring high system availability, self-diagnosability is becoming a feature of major importance in computing systems. A system is self-diagnosable if it is able to unambiguously identify malfunctioning subsystems up to a given multiplicity. As faults are localized, malfunctioning units are repaired or replaced (possibly by switching on standby spares), or faulty units are disconnected and the system reconfigured, such that computation can proceed with reduced performance.

For the purpose of self-diagnosis, a system is supposed to be partitioned into a number of subsystems, or units, and it is assumed that each unit u_i is tested by at least one diagnostic routine operated by an unit u_j ($u_j \neq u_i$), or more generally, by the concurrent action of two or more units different from u_i. Each diagnostic routine is assumed to have a binary outcome: that is, unit u_i is judged fault-free if the test passes, otherwise u_i is judged faulty. Of course, the test outcome is completely reliable only if the testing unit is fault-free (or, more generally, if none of the units cooperating for the test is faulty). The diagnostic model introduced by Preparata, Metze and Chien[1] assumes that the test outcome is not predictable in the hypothesis that the testing unit is faulty. More generally, in the model by Russel and Kime[2], each test has associated a set of invalidating units, generally a subset of the set of units cooperating for the test. When at least one unit in the invalidating set is faulty, the test outcome is unreliable.

The set of test outcomes resulting from one application of the set of tests is called the syndrome of the system. If one application of the set of tests is sufficient to identify all faulty units, one-step diagnosis is said to occur. The diagnostic process where unambiguous identification of at least one faulty unit is guaranteed is called diagnosis with repair. In both cases, the circuitry required to decode the syndrome and to identify faulty unit(s) belongs to the hard-core of the system, that is the equipment that needs to be assumed fault-free in order to make the self-diagnosis possible. The importance of reducing the complexity of the procedures required to decode the syndrome is apparent from this observation.

Two different problems arise in the investigation about self-diagnosable systems. In the analysis problem, the set of tests performed by the system is given, and the diagnosability, either one-step or with repair, is to be derived. The analysis problem has been solved for the case of one-step diagnosis, both in the Preparata's[3] and in the Russel's[2] model, while for the case of diagnosis with repair only lower and upper bounds have been published [2,4]. In the synthesis problem, which was first formulated by Preparata, Metze and Chien[1] a minimal set of tests is to be determined, such that a predetermined value of diagnosability, either one step or with repair, is achieved. Near optimal designs of systems exhibiting given values of diagnosability with repair in the Preparata's model have been recently reported[5].

2. THE DIAGNOSTIC MODEL

The diagnostic model considered in this paper is a modification of the model introduced by Preparata et al[1], in an attempt to have a more realistic representation of systems whose units have a rather complex structure. For any given system it is assumed that:

a) each test is operated by a single unit;
b) each unit has the capability of testing any other unit;
c) no unit tests itself;
d) for any pair of units u_i, u_j, at most one test of unit u_j is performed by unit u_i.

As a consequence of assumptions a) and b), every unit must have a significant computational capability and tests that are complete for a given class of faults in an unit necessarily consist of sequences of a large number of stimuli. Because of this observation it seems reasonable to assume that at least one mismatch occurs between actual and expected reaction to the stimuli whenever the tested unit is faulty, even if the testing unit itself is faulty. This hypothesis can be reinforced by assuming that a self-checking design[6] is used for some critical parts of the testing unit, e.g. the part taking the decision about the test outcome.

As a consequence of the preceding considerations, the diagnostic model of a system S

° The research reported in this paper has been supported by Selenia S.p.A. under Convenzione Selenia-Consiglio Nazionale delle Ricerche.

of units $u_1, u_2, \ldots, u_n$ is defined as follows. Assume that unit u_i tests unit u_j, that is there exists a testing link from u_i to u_j. Then:

- if u_i is fault-free, the test outcome is "0" if u_j is fault-free and "1" if u_j is faulty;
- if u_i is faulty and u_j is fault-free, both test outcomes are possible;
- if u_i and u_j are faulty, the test outcome is necessarily "1".

If the diagnostic model above defined holds, it is immediately seen that, whenever a test outcome is "0", the tested unit is unambiguously recognized to be fault-free while, if the test outcome is "1", a fault necessarily exists either in the testing, or in the tested unit, or in both.

The diagnostic model considered in this paper is given a graph theoretical representation by introducing a directed graph G=(N,A), called the diagnostic graph of S, where N is the set of the nodes and A the set of the arcs. Given a system S of units $u_1, u_2, \ldots, u_n$, each node in N is identified with an unit of S, and A has a directed arc (u_i, u_j) from u_i to u_j if and only if unit u_i tests unit u_j. The set A defines the connection of the system. Observe that, because of assumptions c) and d), the diagnostic graph is an 1-graph without self-loops[7]. For the sake of simplicity the same symbols will be used to denote units of S and the corresponding nodes in N. Following to one application of the set of tests for units of S, every arc in A is labeled with the test outcome. The set of arc labels represents the syndrome of S.

The following graph theoretic notations are also recalled for use in the subsequent sections. If G=(N,A) is a directed graph and $x \in N$, the predecessor set of x, denoted by B(x) is the set of all $y \in N$ such that $(y,x) \in A$, and $\Delta(x)$ is defined as the set B(x)-x. Similarly, the successor set of x, denoted by D(x), is the set of all $y \in N$, such that $(x,y) \in A$. For every $X \subset N$, $B(X) = \bigcup_{x \in X} B(x)$ is the union of the predecessor sets of nodes in X and $\Delta(X) = B(X) - X$. Similarly, $D(X) = \bigcup_{x \in X} D(x)$ is the union of the successor sets of nodes in X.

3. ONE-STEP DIAGNOSABILITY

A system S is said to be one-step t-diagnosable if one application of the set of tests is sufficient to identify all faulty units in S.

The number t is called the one-step diagnosability of the system. Assuming that the diagnostic model presented in Section 2 holds, an upper bound to the one-step diagnosability of digital systems is established by the following theorem. Observe that, as a consequence of the different model, the bound of $\lfloor (n-1)/2 \rfloor$ † established by Preparata et al.[1] is largely exceeded.

Theorem 3.1: The one-step diagnosability of any system of n units is at most n-2.

The proof of this theorem, as well as all subsequent proofs, is omitted for the sake of brevity[8].

With the notation introduced in Section 1, the following theorem states the necessary and sufficient condition under which a system S is one-step t-diagnosable, thus providing a mean to evaluate the one-step diagnosability of any given diagnostic system.

Theorem 3.2: Let G=(N,A) be the diagnostic graph of S. Then S is one-step t-diagnosable if and only if:

a) $|\Delta(x)| \geq t$ for every $x \in N$;
b) for each pair {x,y} with $x \in N$, $y \in N$, $|\Delta(x)| = |\Delta(y)| = t$ and $y \in D(x) \cap B(x)$, there exists at least one node u such that either $u \in \Delta(x) - \Delta(y) \cap \Delta(x)$ and $\Delta(u) \neq \Delta(y)$, or $u \in \Delta(y) - \Delta(x) \cap \Delta(y)$ and $\Delta(u) \neq \Delta(x)$.

Given a system S with n units, the conditions stated by Theorem 3.2 also provide guidelines to optimally design a connection ensuring a predetermined value of one-step diagnosability. The following definition of optimality is an immediate consequence of Theorem 3.2:

Definition 3.1: A system S with n units which is one-step t-diagnosable is optimal if, in the diagnostic graph G=(N,A), $|\Delta(x)| = t$ for every $x \in N$.

A class of optimal designs for one-step t-diagnosability is defined by the following theorem. An example of an optimal one-step 2-diagnosable system with 5 units is shown in Fig. 3.1.

Theorem 3.3: For arbitrary n and t, the diagnostic graph of an optimal one-step t-diagnosable system, of units $u_0, u_1, \ldots, u_{n-1}$, is constructed by drawing, for each $0 \leq i \leq n-1$, directed arcs from units $u_{|i+1|_n}, u_{|i+2|_n}, \ldots, u_{|i+t|_n}$ † to unit u_i.

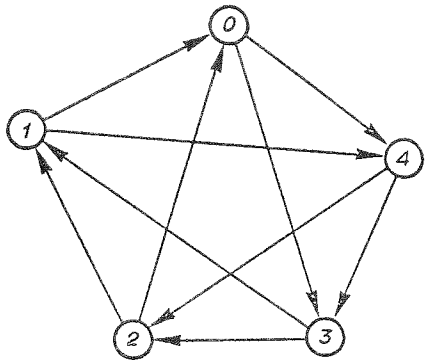

Fig. 3.1.

4. DIAGNOSABILITY WITH REPAIR: ANALYSIS

A system S is said to be t-diagnosable with repair if one application of the set of tests allows identification of at least one faulty unit, provided that the number of faulty units does not exceed t.

The number t is called the diagnosability with repair of the system. If the units that have been recognized to be faulty are repaired and the failure rate is reasonably low, the number of faulty units is decreased; this allows removing all faults through repeated

† $\lfloor a \rfloor$ denotes the greatest integer not exceeding a.

† $|a|_m$ indicates the least non negative remainder of the division of a by m.

applications of the test-repair procedure. It is easily seen that the upper bound to the one step t-diagnosability stated by Theorem 3.1 is also an upper bound to the t-diagnosability with repair.

A directed graph G=(N,A) is said to be strongly connected if there exists a directed path from any x∈N to any y∈N, y≠x. If G=(N,A) is not strongly connected, a subgraph G'(N',A') of G is called a strongly connected component of G if G' is strongly connected and any subgraph G"=(N",A") of G with N"⊃N' is not strongly connected. The diagnosability with repair of any given system represented by a diagnostic graph G which is not strongly connected is easily derived from the diagnostic capabilities of some significant strongly connected components of G, as stated by the following theorems.

Theorem 4.1: If the diagnostic graph G of S is not connected, let $G_1,G_2,\ldots,G_k$ be the connected components of G corresponding to the subsystems $S_1,\ldots,S_k$, whose diagnosabilities with repair are $t_1,\ldots,t_k$, respectively. Then the diagnosability with repair of S is $t=\min(t_1, t_2,\ldots,t_k)$.

Theorem 4.2: If the diagnostic graph G of S is not strongly connected, let $G_1,G_2,\ldots,G_k$ be the strongly connected components of G such that $\Delta(N_i)=\emptyset$ for each $1\leqslant i\leqslant k$, where N_i is the node set of G_i, and t_i be the diagnosability with repair of the subsystem S_i corresponding to the component G_i ($1\leqslant i\leqslant k$). Then the diagnosability with repair of S is $t=\min(t_1,t_2,\ldots,t_k)$.

Because of the properties stated by Theorems 4.1 and 4.2, as far as determination of the diagnosability with repair is concerned, our consideration will be limited to strongly connected diagnostic graphs. As a consequence of this limitation, in order to identify at least one faulty unit, it is sufficient to be able to locate at least one fault-free unit u_i, since there exists a directed path from u_i to any other unit in the system. From this observation, the sufficient condition for t-diagnosability with repair, stated by the following Theorem 4.3, is immediate, noting that, if at most t units are faulty and the hypothesis of the theorem holds, in the diagnostic graph G=(N,A) there exists at least one directed arc from $u_i\in N$ to $u_j\in N$ and this arc, being necessarily labeled with "0", diagnoses unit u_j as fault-free.

Theorem 4.3: A system S with n units is t-diagnosable with repair if the diagnostic graph G=(N,A) of S is strongly connected and $B(X)\cap X\neq\emptyset$ for each subset X⊂N with |X|=n-t.

Under the hypothesis of Theorem 4.3 the procedure for sequentially diagnosing digital systems is very simple: the nodes having at least one incoming arc labeled with "0" (the existence of at least one of such nodes is guaranteed by the theorem) are first diagnosed as fault-free; then each node u_i such that there exists a directed arc (necessarily labeled with "1") from a fault-free node to u_i is recognized to be faulty. Since the circuitry required to decode the syndrome and to identify one or more faulty units is generally a major part of the hard-core of the system, as far as the hypothesis of Theorem 4.3 holds the hard-core requirements of the diagnostic model introduced in this paper are significantly less than those of the previous models[1,2].

The condition stated by Theorem 4.3 is not necessary to ensure t-diagnosability with repair, as it is possible to realize by observing the diagnostic graph represented in Fig. 4.1, where the subset of nodes {2,4,6} does not satisfy the hypothesis of the theorem for t=4. In fact, if nodes 1,3,5 and 7 are faulty and nodes 2,4 and 6 are fault-free the syndrome where all arcs are labeled with "1"s is possible, as shown in the figure. Nevertheless, the system is 4-diagnosable with repair and, if the syndrome shown in Fig. 4.1 occurs, unit 1 is unambiguously recognized to be faulty, since the opposite assumption implies the presence of at least five faulty units. In fact, nodes 2,4,5,6,7, being connected to node 1 by arcs labeled with "1"s, are necessarily faulty.

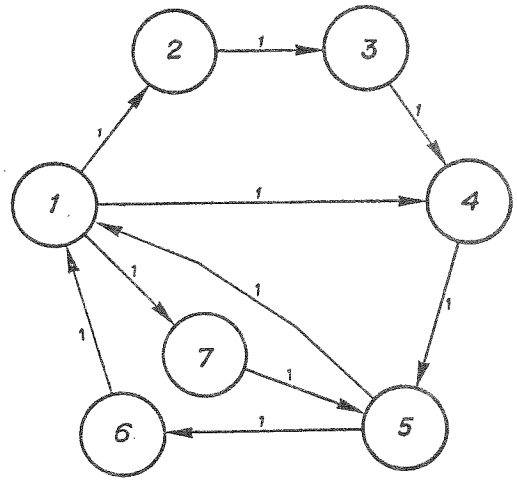

Fig. 4.1.

In order to derive the necessary and sufficient condition for t-diagnosability with repair, the syndrome where all test outcomes are "1"s is denoted by Σ_1. Furthermore, given a diagnostic graph G=(N,A), any subset X⊂N is said to be stable[7] if $B(X)\cap X=\emptyset$; the stable subsets of N whose cardinality is a maximum are called maximal stable subsets in G. It is immediately seen that if the nodes in any stable subset X are fault-free and the nodes in N-X are faulty, the syndrome Σ_1 is possible. For a given x∈N, let G_1^x denote the subgraph of G whose node set is N-x and X_1^x be an arbitrary maximal stable subset in G_1^x: with this notation the index $f_1(x)=|N|-|X_1^x|$ equals the minimum number of faulty units that can give rise to the syndrome Σ_1 in the system S, with the constraint that unit x is faulty. Similarly, if for a given x∈N G_0^x denotes the subgraph of G whose node set is $N-B(x)\cup D(x)$ and X_0^x is an arbitrary maximal stable subset in G_0^x, the index $f_0(x)=|N|-|X_0^x|$ equals the minimum number of faulty units that can give rise to the

syndrome Σ_1, with the constraint that unit x is fault-free. It is immediately seen that if $f_0(x)<f_1(x)$ $[f_1(x)<f_0(x)]$ and the syndrome Σ_1 occurs, in the hypothesis that the number of faulty units is smaller than $f_1(x)$ $[f_0(x)]$, the unit x is unambiguously diagnosed as fault-free [faulty]. From the preceding analysis, the following theorem is derived:

Theorem 4.4: A system S of units $u_1,u_2,\ldots,u_n$ is t-diagnosable with repair if and only if $t=\max[f_0(u_1),f_0(u_2),\ldots,f_0(u_n), f_1(u_1),f_1(u_2),\ldots,f_1(u_n)]-1$.

Furthermore, whenever the syndrome Σ_1 occurs in S, every unit u_i such that $f_0(u_i)=t+1$ $[f_1(u_i)=t+1]$ is faulty [fault-free] in the hypothesis that the number of faulty units does not exceed t.

Observe that the capability of identifying at least one faulty, or fault-free, unit in the presence of the syndrome Σ_1, resulting from Theorem 4.4, does not imply a more complex procedure to decode the syndrome, or equivalently a larger hard-core, as compared to the procedure resulting from Theorem 4.3, since whenever each test outcome is "1" the state of at least one unit is known in the hypothesis that the faulty units are at most t.

As an example, consider again the diagnostic graph shown in Fig. 4.1. The following values of the indices $f_0(u_i)$ and $f_1(u_i)$ are immediately verified: $f_0(u_1)=5$, $f_0(u_2)=3$, $f_0(u_3)=4$, $f_0(u_4)=3$, $f_0(u_5)=5$, $f_0(u_6)=3$, $f_0(u_7)=3$, $f_1(u_1)=3$, $f_1(u_2)=4$, $f_1(u_3)=3$, $f_1(u_4)=4$, $f_1(u_5)=3$, $f_1(u_6)=4$, $f_1(u_7)=4$. From Theorem 4.4 it follows that the system is 4-diagnosable and, whenever the syndrome Σ_1 occurs, units u_1 and u_5 are necessarily faulty in the hypothesis that at most four units are faulty.

5. DIAGNOSABILITY WITH REPAIR: SYNTHESIS

Given a system S with n units, where each unit is supposed to be able to test any other unit, there exist, in general, several different connections ensuring a predetermined value of diagnosability with repair. It is interesting to investigate how the connection can be designed such that the system is t-diagnosable with repair and the number of testing links is as low as possible.

Definition 5.1: A system S with n nodes and a testing links, which is t-diagnosable with repair, is said to be optimal if the diagnosability with repair of any system with n nodes and a testing links is at most t and any system with n nodes and a-1 testing links is at most (t-1)-diagnosable with repair.

In section 4 it has been shown that the diagnosability with repair of an arbitrary system S is determined by analyzing the strongly connected components of the diagnostic graph of S. The importance of strongly connected diagnostic graphs is further emphasized by observing that, as far as the synthesis of optimal systems which are t-diagnosable with repair is concerned, consideration can be limited to systems whose diagnostic graph is strongly connected, as stated by the following theorem.

Theorem 5.1: If S is t-diagnosable with repair and the diagnostic graph G=(N,A) of S is not strongly connected, there exists at least one S', whose diagnostic graph G'=(N,A') has $|A'|=|A|$ and is strongly connected, which is at least t-diagnosable with repair.

As an example of an optimal connection for diagnosability with repair, consider the case of n units connected in a simple loop, whose diagnostic graph is shown, for n=5, in Fig. 5.1. Since it is immediately seen that $f_0(u_i)=f_1(u_i)=\left\lceil\frac{n}{2}\right\rceil$† for each unit u_i in the system, it follows from Theorem 4.4 that the system is $(\left\lceil\frac{n}{2}\right\rceil-1)$-diagnosable with repair. Since any graph with n nodes and n arcs different from the simple loop is not strongly connected, and any graph with n nodes and n-1 arcs is 0-diagnosable because of Theorems 4.1 and 4.2, it is immediate from the preceding discussion that the system under consideration is optimal for $(\left\lceil\frac{n}{2}\right\rceil-1)$-diagnosability with repair.

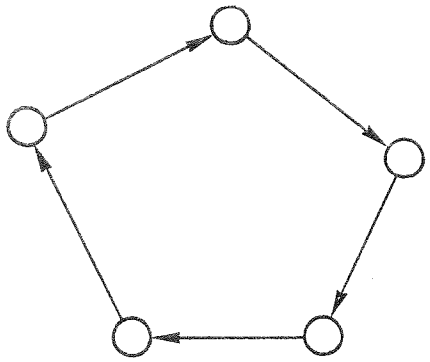

Fig. 5.1.

In order to identify classes of optimal systems with n units for any value of diagnosability with repair in the range $\left\lceil\left\lceil\frac{n}{2}\right\rceil-1,\ n-2\right\rceil$, the following lemma is introduced.

Lemma 5.1: If S is t-diagnosable with repair and the diagnostic graph G=(N,A) of S has $|A|>|N|$ and is strongly connected, there exists a connection of the units in S with $|A|-1$ testing links such that the diagnostic graph is strongly connected and the diagnosability with repair is at least t-1.

Recalling that the optimal design with n units and $t=\left\lceil\frac{n}{2}\right\rceil-1$ has n testing links, (i.e., the simple loop connection is an optimal design for $t=\left\lceil\frac{n}{2}\right\rceil-1$) the following theorem is an immediate consequence of Lemma 5.1.

† $\lceil a\rceil$ indicates the smallest integer greater than, or equal to a.

Theorem 5.2: Any system with n units which is t-diagnosable with repair, with $t \geq \left\lceil \frac{n}{2} \right\rceil - 1$, has at least $n+t-\left\lceil \frac{n}{2} \right\rceil + 1$ testing links.

A strongly connected directed graph $G=(N,A)$ which has k simple loops, with $k>1$, is said to be a k-rosace[7] if $|B(u_0) \cup D(u_0)| > 2$ for only one $u_0 \in N$. Denoting by N_i $(1 \leq i \leq k)$ the node set of the i.th loop, relations $u_0 \in N_i$ $(1 \leq i \leq k)$ and $\bigcup_{i=1}^{k} N_i = N$ are immediate from the definition. It is also immediate that each k-rosace with n nodes has n+k-1 arcs and for every $1 \leq k \leq \frac{n}{2}$ there exist k-rosaces where $|N_i|$ is even for at most one N_i. From an analysis of the diagnostic capabilities of systems whose diagnostic graph is a k-rosace, the following theorem is derived:

Theorem 5.3: Any system with n units, whose diagnostic graph is a k-rosace where $|N_i|$ is even for at most one N_i, is an optimal t-diagnosable system for $t=k+\left\lceil \frac{n}{2} \right\rceil - 2$.

As an example, consider the diagnostic graph shown in Fig. 5.2, which satisfies the hypothesis of Theorem 5.3. Since it is easily verified that $f_0(u_0)=6$ and $f_1(u_0)=4$, it follows that the diagnosability with repair of the system is at least 5 and, whenever the syndrome Σ_1 occurs, unit u_0 is diagnosed as faulty in the hypothesis that the number of faulty units does not exceed 5. Furthermore, from Theorem 5.2 it is known that the diagnosability of the system under consideration cannot exceed $a-(n-\left\lceil \frac{n}{2} \right\rceil + 1)=5$. It is concluded that the system whose diagnostic graph is shown in Fig. 5.2 is an optimal design for 5-diagnosability with repair.

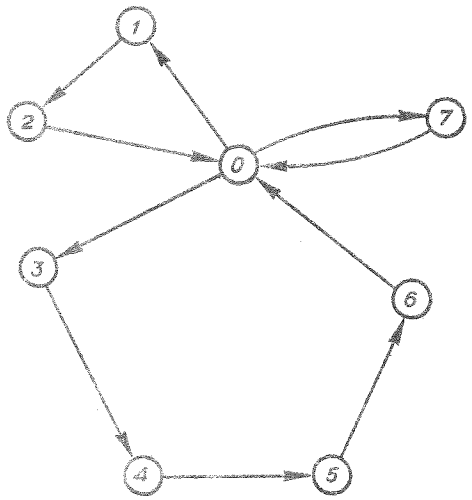

Fig. 5.2.

AKNOWLEDGMENT

The authors wish to thank Prof. F.P. Preparata of University of Pisa for suggestions and stimulating discussions.

REFERENCES

1. F.P. Preparata, G. Metze, R.T. Chien: "On the Connection Assignment Problem of Diagnosable Systems", IEEE Trans. Comp., Vol. C-16, pp. 848-854, Dec.1967 .

2. J.D. Russel and C.R. Kime: "On the Diagnosability of Digital Systems", Digest of Int. Symp. on Fault Tolerant Comp., Palo Alto, Cal., June 1973.

3. S.L. Hakimi and A.T. Amin: "Characterization of Connection Assignment of Diagnosable Systems", IEEE Trans. Comp., Vol. C-23 pp. 86-87, Jan. 1974.

4. P. Ciompi, L. Simoncini: "The Boundary Graphs: an approach to the Diagnosability with Repair of Digital Systems", Proc. of the third Texas Conference on Computing Systems, Austin, Texas, Nov. 1974, IEEE CSPO n. 74 CHO895-3C.

5. P. Ciompi, L. Simoncini: "On the Diagnosability with Repair of Digital Systems", Convenzione Selenia-CNR, Rapporto 75004/P/E.

6. D.A. Anderson and G. Metze: "Design of Totally Self-Checking Check Circuits for m-Out-of-n Codes", IEEE Trans. Comp., Vol. C-22, pp. 263-269, Mar. 1973.

7. C. Berge: "Graphes et Hypergraphes", Paris: Dunod, 1970.

8. F. Barsi, F. Grandoni, P. Maestrini: "A Study on self-diagnosis of Digital Systems", Convenzione Selenia-CNR, Rapporto 75003/P/E.