computer system architecture and the programming language requirements impose a wide range of auxiliary operations, not closely related to the algorithm but necessary for its implementation. Even if it is impossible to eliminate T_a (or equivalently to obtain $Q = 1$), a good knowledge of the machine structure leads to an increase of Q by a clever choice of the auxiliary instructions. This quality factor may turn very useful in the evaluation of the efficiency of programs implementing image processing algorithms where the computing time generally grows quadratically with base n ($CT \propto n^2$).

ACKNOWLEDGMENT

We wish to thank M. Valenzi for his help in running the programs on the HP2116B system.

REFERENCES

[1] D. E. Knuth, *The Art of Computer Programming*, vol. 1. New York: Addison-Wesley, 1973.
[2] L. Hellerman, "A measure of computational work," *IEEE Trans. Comput.*, vol. C-21, pp. 439–446, May 1972.
[3] S. Warshall, "On computational cost," *Annual Review in Automatic Programming*, vol 5. New York: Pergamon Press, pp. 309–330, 1969.
[4] A. Rosenfeld, "Connectivity in digital picture," *J. Assoc. Comput. Mach.*, vol. 17, pp. 146–160, 1973.
[5] ——, *Digital Picture Processing*. New York: Academic Press, 1976.
[6] ——, "Arcs and curves in digital pictures," *J. Assoc. Comput. Mach.*, vol. 20, pp. 81–87, 1973.
[7] A. Rosenfeld and J. L. Pfaltz, "Sequential operation in digital picture processing," *J. Assoc. Comput. Mach.*, vol. 13, pp. 471–494, 1966.
[8] S. Levialdi, "On shrinking binary patterns," *Commun. Assoc. Comput. Mach.*, vol. 15, pp. 7–10, Jan. 1972.
[9] L. Cordela, M. J. B. Duff, and S. Levialdi, "Comparing sequential and parallel processing of picture," in *3rd Int. Joint Conf. Pattern Recognition*, Coronado, CA, pp. 703–707, Nov. 1976.
[10] V. Franchina, A. Pirri, and S. Levialdi, "VIP: An image acquisition device for digital processing," in *Proc. Conf. Assisted Scanning*, Padova, pp. 300–321, Apr. 1976.
[11] "A guide to HP computers," Hewlett-Packard Company, CA, 1972.

Connection Assignments for Probabilistically Diagnosable Systems

HIDEO FUJIWARA AND KOZO KINOSHITA

***Abstract*—This correspondence is concerned with probabilistic fault diagnosis for digital systems. A graph-theoretic model of a diagnosable system introduced by Preparata *et al.* [3] is considered in which a system is made up of a number of units with the probability of failure. The necessary and sufficient conditions are obtained for the existence of testing links (a connection) to form probabilistically t-diagnosable systems with and without repair. Methods for connection assignments are given for probabilistic fault diagnosis procedures with and without repair. Maheshwari and Hakimi [10] gave the necessary and sufficient condition for a system to be probabilistically t-diagnosable without repair. In this correspondence, we show the necessary and sufficient condition for a system to be probabilistically t-diagnosable with repair.**

Manuscript received July 8, 1976; revised November 17, 1976.
The authors are with the Department of Electronic Engineering, Osaka University, Osaka, Japan.

***Index Terms*—Automatic diagnosis, connection assignments, digital systems, graphs, probabilistic fault diagnosis, self-diagnosable systems, testing links.**

I. INTRODUCTION

Studies in self-diagnosable systems have appeared in the literature [1]–[10]. Preparata *et al.* [3] first introduced a graph-theoretic model of digital systems for the purpose of diagnosis of multiple faults, and presented methods of optimal connection assignments for instantaneous and sequential diagnosis procedure. Maheshwari and Hakimi [10] introduced a diagnosability measure t based on the probability of occurrence of faults and presented necessary and sufficient conditions for a system to be probabilistically t-diagnosable in the graph-theoretic model.

The diagnostic model employed in this correspondence is the model introduced by Maheshwari and Hakimi [10], and it is assumed that the reader is familiar with the model, assumptions, definitions, and notations given there. The concept of probabilistic diagnosability (*without* repair) was defined in [10]. Probabilistic diagnosability *with* repair can be defined similarly.

Definition 1 [10]: A system S, represented by a digraph $G = (V,E)$, is said to be probabilistically t-diagnosable without repair (p-t-diagnosable without repair) if for any weighted digraph G_s, representing S and some set of test outcomes, there exists at most one consistent fault set $F \subseteq V$ such that $P(F) > t$.

Definition 2: A system S, represented by a digraph G, is said to be probabilistically t-diagnosable with repair (p-t-diagnosable with repair) if for any weighted digraph G_s, representing S and some set of test outcomes, there exist no consistent fault sets $F_1,F_2,\cdots,F_l$ such that

$$\bigcap_{i=1}^{l} F_i = \phi$$

and $P(F_i) > t$ for $i = 1,2,\cdots,l$.

In a p-t-diagnosable system with repair, the intersection of all consistent fault sets, whose *a priori* probability of occurrence is greater than t, is not empty so that at least the units belonging to the intersection are all faulty. Hence, there exists a sequence of applications of tests and repairs of identified faults that allows all faults originally present to be identified.

II. FUNDAMENTAL THEOREMS FOR CONNECTION ASSIGMNENTS

Given a system S with units $u_1,u_2,\cdots,u_n$ and the probability $p(u_i)$ of u_i being faulty for all $u_i \in V = \{u_1,u_2,\cdots,u_n\}$, then we consider the problems of finding a connection of S such that S is p-t-diagnosable with and without repair.

We can state the following fundamental lemmas.

Lemma 1: If a system S, represented by digraph $G = (V,E)$, is p-t-diagnosable with repair, then there exists no 2-partition $\{U_1,U_2\}$ of V such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$.

Proof: Suppose for some 2-partition $\{U_1,U_2\}$ of V, $W(U_1) < K(t)$ and $W(U_2) < K(t)$. We can easily find a weighted digraph G_s of S that has U_1 and U_2 as consistent fault sets. Thus, by Definition 2, S would not be p-t-diagnosable with repair. Q.E.D.

Lemma 2: Let V be a set of units of a system S. If there exists no 2-partition $\{U_1,U_2\}$ of V such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$, then there exists a digraph $G = (V,E)$ such that a system represented by G is p-t-diagnosable without repair.

Proof: Consider a complete digraph $G = (V,E)$ such that $(u_i,u_j) \in E$ for all $u_i,u_j \in V$. We shall prove that a system S represented by G is p-t-diagnosable without repair.

The proof is by contradiction. Assume the existence of a

0018-9340/78/0300-0280$00.75

weighted digraph G_s for which there are two consistent fault sets F_1 and F_2 with $W(F_1)$, $W(F_2) < K(t)$. Let $X = V - (F_1 \cup F_2)$, $Y = F_1 \cap F_2$, $Z = F_1 - Y$, and $Z_2 = F_2 - Y$. Without loss of generality, we have $Z_1 \neq \phi$.

If $X = \phi$, then $\{F_2, Z_1\}$ is a 2-partition of V such that $W(F_2) < K(t)$ and $W(Z_1) < K(t)$. By hypothesis, there exists no 2-partition $\{U_1, U_2\}$ of V such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$. This is a contradiction. Therefore, we have $X \neq \phi$.

Because G is complete, there exists an arc $(u_i, u_j) \in E$ such that $u_i \in X$ and $u_j \in Z_1$. Since $u_i, u_j \in \overline{F}_2$ and F_2 is a consistent fault set, we have $s(u_i, u_j) = 0$. But since F_1 is also a consistent fault set and $u_i \in \overline{F}_1$, $u_j \in F_1$, we have $s(u_i, u_j) = 1$. This is a contradiction. Hence, our initial assumption was wrong. Q.E.D.

Given a system S with units $u_1, u_2, \cdots, u_n$ and the weight $W(u_i)$ for each $u_i \in V = \{u_1, u_2, \cdots, u_n\}$, then we have the following theorems.

Theorem 1: Given a system S with a set of units V and the weight $W(u_i)$ for all $u_i \in V$, then there exists a digraph $G = (V, E)$ such that S represented by G is p-t-diagnosable without repair if and only if there exists no 2-partition $\{U_1, U_2\}$ of V such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$.

Proof-Necessity: It is obvious that every system that is p-t-diagnosable without repair is also p-t-diagnosable with repair. Hence, the necessity of the theorem follows from Lemma 1.

Sufficiency: Follows from Lemma 2. Q.E.D.

It can be easily verified that Theorem 1 is valid for p-t-diagnosability with repair also.

Example: Consider a system consisting of three units such that $p(u_1) = 1/5$, $p(u_2) = 1/4$, $p(u_3) = 1/3$, and $t = 1/20$. Then we have $W(u_1) = \log 4$, $W(u_2) = \log 3$, $W(u_3) = \log 2$, and $K(t) = \log 8$. Let $U_1 = \{u_1\}$ and $U_2 = \{u_2, u_3\}$, then we have $W(U_1) = \log 4 > K(t)$ and $W(U_2) = \log 6 > K(t)$. Thus, from Theorems 1 and 2, it can be seen that there exists no digraph G such that the system represented by G is p-t-diagnosable with repair or without repair.

III. Connection Assignments for Diagnosability

It has been shown in the last section that for a system S which is p-t-diagnosable, the set of units V must satisfy the condition of Theorem 1, i.e., there exists no 2-partition $\{U_1, U_2\}$ of V such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$. In this section we consider the design of p-t-diagnosable systems provided that the above condition holds.

Given a system S with a set of units V and weight $W(u_i)$ for all $u_i \in V$, a subset U of V satisfying the following condition is called a *base set* of S.

Condition: There exists no 2-partition $\{U_1, U_2\}$ of U such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$.

Definition 3: A system S with digraph $G = (V, E)$ is said to belong to a design D_0 if for some base set U of S, 1) $\langle U \rangle$ is a complete digraph, and 2) $\Gamma^{-1}(u_i) \subseteq U$ and $W(\Gamma^{-1}(u_i)) \geq K(t)$ for all $u_i \in V - U$.

Definition 4: A system S with digraph $G = (V, E)$ is said to belong to a design D_1 if for some base set U of S,

1) $(u_i, u_{i+1}) \in E$ for $1 \leq i \leq n - 1$,
2) $(u_n, u_1) \in E$,

and

3) $(u_i, u_s) \in E$ for $1 \leq i \leq s - 1$,

where $U = \{u_1, u_2, \cdots, u_s\}$ and $V = \{u_1, u_2, \cdots, u_n\}$.

To illustrate the designs D_0 and D_1, we consider a system S_1 which consists of five units $u_1, u_2, \cdots, u_5$. Suppose $p(u_1) = 1/7$, $p(u_2) = 1/6$, $p(u_3) = 1/5$, $p(u_4) = 1/4$, $p(u_5) = 1/3$, and $t = 1/35$, then we have $W(u_1) = \log 6$, $W(u_2) = \log 5$, $W(u_3) = \log 4$, $W(u_4) = \log 3$, $W(u_5) = \log 2$, and $K(t) = -\log 1/35 + \log 6/7 + \log 5/6 + \log 4/5 + \log 3/4 + \log 2/3 = \log 10$. Let $U = \{u_1, u_2, u_3\}$. Since $W(U) = \log 120 \geq 2K(t)$, there exists no 2-partition $\{U_1, U_2\}$ of U such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$. Therefore U is a base set of S_1.

In Fig. 1 two designs are illustrated for system S_1. D_0 is shown in Fig. 1(a) and D_1 is shown in Fig. 1(b). In Fig. 1(a), $\langle U \rangle$ is a complete digraph, $\Gamma^{-1}(u_4) = \Gamma^{-1}(u_5) = \{u_1, u_2\} \subseteq U$, and $W(\Gamma^{-1}(u_4)) = W(\Gamma^{-1}(u_5)) = \log 30 \geq K(t)$. Therefore, system S_1 represented by a digraph shown in Fig. 1(a) belongs to design D_0. It can easily be shown that system S_1 represented by a digraph shown in Fig. 1(b) belongs to design D_1.

We shall prove that a system is p-t-diagnosable without repair if it employs design D_0 and that a system is p-t-diagnosable with repair if it employs design D_1.

Theorem 2: If a system S employs design D_0, then S is p-t-diagnosable without repair.

Proof: The proof is by contradiction. Assume the existence of a weighted digraph G_s for which there are two consistent fault sets F_1 and F_2 with $W(F_1)$, $W(F_2) < K(t)$. Let $X = U - (F_1 \cup F_2)$, $Y = F_1 \cap F_2$, $Z_1 = F_1 - Y$, and $Z_2 = F_2 - Y$, where U is a base set of S in design D_0. Without loss of generality, assume $Z_1 \neq \phi$. The following cases are possible.

Case 1: $Z_1 \cap U \neq \phi$ and $F_2 \cap U \neq \phi$. If $X = \phi$, then $\{Z_1 \cap U, F_2 \cap U\}$ is a 2-partition of U such that

$$W(Z_1 \cap U) \leq W(Z_1) \leq W(F_1) \leq K(t)$$

and

$$W(F_2 \cap U) \leq W(F_2) \leq K(t).$$

This contradicts the hypothesis that U is a base set of S. Therefore, we have $X \neq \phi$. Because $\langle U \rangle$ is complete, there exists an arc $(u_i, u_j) \in E$ such that $u_i \in X$ and $u_j \in Z_1$. Since $u_i, u_j \in \overline{F}_2$ and F_2 is a consistent fault set, we have $s(u_i, u_j) = 0$. But since F_1 is also a consistent fault set and $u_i \in \overline{F}_1$, $u_j \in F_1$, we have $s(u_i, u_j) = 1$. This is a contradiction.

Case 2: $Z_1 \cap U = \phi$, i.e., $Z_1 \subseteq V - U$. Let $u_j \in Z_1$. If $\Gamma^{-1}(u_j) \subseteq F_2$, then we have $W(\Gamma^{-1}(u_j)) \leq W(F_2) < K(t)$, but this contradicts the hypothesis that S belongs to design D_0. Therefore, there exists $u_i \in \overline{F}_2 \cap \Gamma^{-1}(u_j)$. Since $\Gamma^{-1}(u_j) \subseteq U$, we have $u_i \in \overline{Z}_1$ and thus $u_i \in \overline{F}_1 \cap \overline{F}_2$. Since $u_i, u_j \in \overline{F}_2$ and F_2 is a consistent fault set, we have $s(u_i, u_j) = 0$. But since F_1 is also a consistent fault set and $u_i \in \overline{F}_1$, $u_j \in F_1$, we have $s(u_i, u_j) = 1$. This is a contradiction.

Case 3: $F_2 \cap U = \phi$, i.e., $F_2 \subseteq V - U$. Let $u_j \in Z_1$. Since $\Gamma^{-1}(u_j) \subseteq U$, we have $\Gamma^{-1}(u_j) \cap F_2 = \phi$. If $\Gamma^{-1}(u_j) \subseteq Z_1$, then we have $W(\Gamma^{-1}(u_j)) \leq W(Z_1) \leq W(F_1) < K(t)$, but this contradicts the hypothesis. Therefore $\Gamma^{-1}(u_j) \cap \overline{Z}_1 \neq \phi$. Hence, there exists $u_i \in \Gamma^{-1}(u_j) \cap \overline{F}_1 \cap \overline{F}_2$. Since $u_i, u_j \in \overline{F}_2$ and F_2 is a consistent fault set, we have $s(u_i, u_j) = 0$. But since F_1 is also a consistent fault set and $u_i \in \overline{F}_1$, $u_j \in F_1$, we have $s(u_i, u_j) = 1$. This is a contradiction. Hence, our initial assumption was wrong. Q.E.D.

Theorem 3: If a system S employs design D_1, then S is p-t-diagnosable with repair.

Proof: The proof is by contradiction. Assume the existence of a weighted digraph G_s for which there are consistent fault sets $F_1, F_2, \cdots, F_l$ such that

$$\bigcap_{i=1}^{l} F_i = \phi$$

and $W(F_i) < K(t)$ for all $F_i \in \{F_1, F_2, \cdots, F_l\}$. Let $U = \{u_1, u_2, \cdots, u_s\}$ be a base set of S in design D_1 and let $V = \{u_1, u_2, \cdots, u_n\}$. The following cases are possible.

Case 1: $u_s \in \overline{F}_i$ for all $F_i \in \{F_1, F_2, \cdots, F_l\}$. In the weighted digraph G_s, there exists a vertex u_k such that $s(u_{i-1}, u_i) = 0$ for all $i = s + 1, s + 2, \cdots, k - 1$, $s(u_{k-1}, u_k) = 1$, and $u_k \in F_k$ for some $F_k \in \{F_1, F_2, \cdots, F_l\}$. Then, we have $u_{s+1}, u_{s+2}, \cdots, u_{k-1} \in \overline{F}_i$ for all $F_i \in \{F_1, F_2, \cdots, F_l\}$.

If $u_k \in \overline{F}_j$ for some F_j, then we have $u_{k-1} \in \overline{F}_j \cap \overline{F}_k$ and $u_k \in \overline{F}_j \cap F_k$. Since $u_{k-1}, u_k \in \overline{F}_j$ and F_j is a consistent fault set, we have $s(u_{k-1}, u_k) = 0$. But since F_k is also a consistent fault set and $u_{k-1} \in \overline{F}_k$, $u_k \in F_k$, we have $s(u_{k-1}, u_k) = 1$. This is a con-

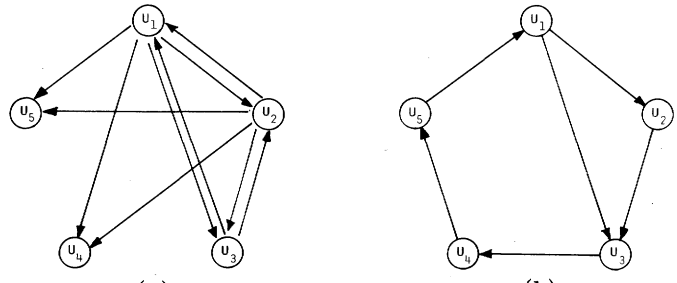

Fig. 1. Designs (a) D_0 and (b) D_1.

tradiction. Therefore, $u_k \in F_j$ for all F_j. However, this contradicts that

$$\bigcap_{i=1}^{l} F_i = \phi.$$

Case 2: $u_s \in F_j$ for some $F_j \in \{F_1,F_2,\cdots,F_l\}$. If $\overline{F}_j \cap U = \phi$, then $F_j \supseteq U$ and thus $W(F_j) \geq W(U)$. Since $W(F_j) < K(t)$, we have $W(U) < K(t)$. But this contradicts that U is a base set. Therefore $\overline{F}_j \cap U \neq \phi$.

Since

$$\bigcap_{i=1}^{l} F_i = \phi,$$

we have $u_s \in \overline{F}_k$ for some $F_k \in \{F_1,F_2,\cdots,F_l\}$. Now, we shall show that $\overline{F}_j \cap U \subseteq F_k$. Assume that there exists a vertex $u_\alpha \in \overline{F}_j \cap \overline{F}_k \cap U$. Since F_k is a consistent fault set and $u_\alpha,u_s \in \overline{F}_k$, we have $s(u_\alpha,u_s) = 0$. But since F_j is also a consistent fault set and $u_\alpha \in \overline{F}_j$, $u_s \in F_j$, we have $s(u_\alpha,u_s) = 1$. This is a contradiction. Therefore, we have $\overline{F}_j \cap U \subseteq F_k$.

Let $U_1 = F_j \cap U$ and $U_2 = \overline{F}_j \cap U$. Clearly, $U_1 \neq \phi$, $U_2 \neq \phi$, $U_1 \cup U_2 = U$ and $U_1 \cap U_2 = \phi$. Since $U_1 \subseteq F_j$ and $U_2 \subseteq F_k$, we have $W(U_1) \leq W(F_j) < K(t)$ and $W(U_2) \leq W(F_k) < K(t)$. Hence, there exists a 2-partition $\{U_1,U_2\}$ of U such that $W(U_1) < K(t)$ and $W(U_2) < K(t)$. This contradicts that U is a base set. Q.E.D.

Theorems 2 and 3 show that if one can find a base set U of a system, then one can easily construct p-t-diagnosable systems with and without repair using designs D_1 and D_0, respectively. Hence, we shall show a method for finding a base set of a given system.

Given a system S with a set of units $V = \{u_1,u_2,\cdots,u_n\}$ and weight $W(u_i)$ for all $u_i \in V$, then without loss of generality assume $W(u_1) \geq W(u_2) \geq \cdots \geq W(u_n)$. If the system S satisfies the necessary and sufficient condition of Theorem 1, we can find a base set U of S as follows.

1) If $W(V) \geq 2K(t)$, then let $U = \{u_1,u_2,\cdots,u_s\}$ such that

$$\sum_{i=1}^{s-1} W(u_i) < 2K(t)$$

and

$$\sum_{i=1}^{s} W(u_i) \geq 2K(t).$$

2) If $W(V) < 2K(t)$, then let $U = V$.

Example: Consider the system S_1 with $W(u_1) = \log 6$, $W(u_2) = \log 5$, $W(u_3) = \log 4$, $W(u_4) = \log 3$, $W(u_5) = \log 2$, and $K(t) = \log 10$.

$$W(V) = \sum_{i=1}^{5} W(u_i) = \log 720 > 2K(t) = \log 100.$$

$W(u_1) + W(u_2) = \log 30 < 2K(t)$ and $W(u_1) + W(u_2) + W(u_3) = \log 120 > 2K(t)$. Hence, we have $U = \{u_1,u_2,u_3\}$, which is a base set of S_1.

IV. Necessary and Sufficient Condition for Diagnosability

So far we have discussed connection assignment problem for probabilistically diagnosable systems. In this section we present the necessary and sufficient condition for a system represented by a digraph to be probabilistically diagnosable. Maheshwari and Hakimi [10] gave the necessary and sufficient condition for a system to be p-t-diagnosable without repair. We can state the necessary and sufficient condition for a system to be p-t-diagnosable with repair in the following.

Theorem 4: A system S with digraph $G = (V,E)$ is p-t-diagnosable with repair if and only if for all $U \subseteq V$ with $\Gamma^{-1}(U) = \phi$, whenever there exist subsets of $U,F_1,F_2,\cdots,F_l$ such that $\bigcup_{i=1}^{l} F_i = U$, $\bigcap_{i=1}^{l} F_i = \phi$ and $W(F_i) < K(t)$ for all $F_i \in \{F_1,F_2,\cdots,F_l\}$, then $\Gamma^{-1}(F_\alpha \cap \overline{F}_\beta) \cap \overline{F}_\alpha \cap \overline{F}_\beta \neq \phi$ for some $F_\alpha,F_\beta \in \{F_1,F_2,\cdots,F_l\}$.

Proof-Necessity: Suppose the condition of the theorem does not hold. Then, for some $U \subseteq V$ with $\Gamma^{-1}(U) = \phi$, there exist subsets of $U,F_1,F_2,\cdots,F_l$ such that $\bigcup_{i=1}^{l} F_i = U$, $\bigcap_{i=1}^{l} F_i = \phi$, $W(F_i) < K(t)$ for all F_i, and $\Gamma^{-1}(F_\alpha \cap \overline{F}_\beta) \cap \overline{F}_\alpha \cap \overline{F}_\beta = \phi$ for all $F_\alpha,F_\beta \in \{F_1,F_2,\cdots,F_l\}$.

Construct a weighted digraph G_s as follows. For each arc $(u_i,u_j) \in E$,

$$s(u_i,u_j) = \begin{cases} 1, & \text{if } u_i \in \overline{F}_k, u_j \in F_k \text{ for some } F_k \\ 0, & \text{otherwise.} \end{cases}$$

For any $F_i \in \{F_1,F_2,\cdots,F_l\}$, we shall show that F_i is a consistent fault set for the above weighted digraph G_s.

1) For any arc $(u_i,u_j) \in E$ such that $u_i \in \overline{F}_i$, $u_j \in F_i$, we have $s(u_i,u_j) = 1$ by the definition of G_s.

2) For any arc $(u_i,u_j) \in E$ such that $u_i,u_j \in \overline{F}_i$, we can show that $s(u_i,u_j) = 0$ as follows. Suppose that $s(u_i,u_j) = 1$, then from the definition of G_s, $u_i \in \overline{F}_k$, $u_j \in F_k$ for some F_k. This implies $u_i \in \Gamma^{-1}(F_k \cap \overline{F}_i) \cap \overline{F}_k \cap F_i$. But, this contradicts the hypothesis. Therefore $s(u_i,u_j) = 0$.

Hence, $F_1,F_2,\cdots,F_l$ are all consistent fault sets for G_s. Moreover, $\bigcap_{i=1}^{l} F_i = \phi$, $W(F_i) < K(t)$ for all F_i. Therefore, the system is not p-t-diagnosable with repair.

Sufficiency: The proof is by contradiction. Assume the existence of a weighted digraph G_s for which there are consistent fault sets $F_1,F_2,\cdots,F_l$ such that $\bigcap_{i=1}^{l} F_i = \phi$ and $W(F_i) < K(t)$ for all F_i.

Let $U = \bigcup_{i=1}^{l} F_i$. If $\Gamma^{-1}(U) \neq \phi$, then there exists an arc $(u_i,u_j) \in E$ with $u_i \in U$ and $u_j \in U$. Moreover, since $\bigcap_{i=1}^{l} F_i = \phi$, we have $u_j \in F_j \cap \overline{F}_k$ for some F_j,F_k. Since $u_i,u_j \in \overline{F}_k$ and F_k is a consistent fault set, we have $s(u_i,u_j) = 0$. But since F_j is also a consistent fault set and $u_i \in \overline{F}_j$, $u_j \in F_j$, we have $s(u_i,u_j) = 1$. This is a contradiction. Therefore, we have $\Gamma^{-1}(U) = \phi$.

Thus, by hypothesis, $\Gamma^{-1}(F_\alpha \cap \overline{F}_\beta) \cap \overline{F}_\alpha \cap \overline{F}_\beta \neq \phi$ for some F_α,F_β, i.e., there exists an arc $(u_i,u_j) \in E$ with $u_i \in \overline{F}_\alpha \cap \overline{F}_\beta$, and $u_j \in F_\alpha \cap \overline{F}_\beta$. Since $u_i \in \overline{F}_\alpha$, $u_j \in F_\alpha$, and F_α is a consistent fault set, we have $s(u_i,u_j) = 1$. But since F_β is also a consistent fault

set and $u_i, u_j \in \overline{F}$, we have $s(u_i, u_j) = 0$. This is a contradiction. Hence, our initial assumption was wrong. Q.E.D.

V. Conclusions

In this correspondence we have presented the necessary and sufficient conditions for the existence of a connection to form probabilistically t-diagnosable systems with and without repair, and also presented the designs D_1 and D_0 for p-t-diagnosable systems with and without repair, respectively. However, these designs are not optimal, and hence the investigation of optimal connection assignments for probabilistically diagnosable systems with and without repair is an open research problem.

Acknowledgment

The authors wish to acknowledge the support and encouragement of Prof. H. Ozaki of Osaka University, Osaka, Japan.

References

[1] R. E. Forbes, D. H. Rutherford, C. B. Stieglitz, and L. H. Tung, "A self-diagnosable computer," in *1965 Fall Joint Comput. Conf., AFIPS Conf. Proc.*, vol. 27, Washington, DC: Spartan, 1965, pp. 1073–1086.

[2] E. Manning, "On computer self diagnosis—Part I: Experimental study of a processor—Part II: Generalizations and design principle," *IEEE Trans. Electron. Comput.*, vol. EC-15, pp. 873–881, 882–890, Dec. 1966.

[3] F. P. Preparata, G. Metze, and R. T. Chien, "On the connection assignment problem of diagnosable systems," *IEEE Trans. Electron. Comput.*, vol. EC-16, pp. 848–854, Dec. 1967.

[4] C. V. Ramamoorthy and W. Mayeda, "Computer diagnosis using the blocking gate approach," *IEEE Trans. Comput.*, vol. C-20, pp. 1294–1299, Nov. 1971.

[5] N. Seshagiri, "Completely self-diagnosable digital systems," *Int. J. Syst.*, vol. 1, pp. 235–246, Jan. 1971.

[6] S. L. Hakimi and A. T. Amin, "Characterization of connection assignment of diagnosable systems," *IEEE Trans. Comput.* (Corresp.), vol. C-23, pp. 86–88, Jan. 1974.

[7] A. D. Friedman, "A new measure of digital system diagnosis," in *Proc. Fault Tolerant Computing Conf.*, pp. 167–170, June 1975.

[8] J. D. Russell and C. R. Kime, "System fault diagnosis: Closure and diagnosability with repair," *IEEE Trans. Comput.*, vol. C-24, pp. 1078–1089, Nov. 1975.

[9] J. D. Russell and C. R. Kime, "System fault diagnosis: Masking, exposure, and diagnosability without repair," *IEEE Trans. Comput.*, vol. C-24, pp. 1155–1161, Dec. 1975.

[10] S. N. Maheshwari and S. L. Hakimi, "On models for diagnosable systems and probabilistic fault diagnosis," *IEEE Trans. Comput.*, vol. C-25, pp. 228–236, Mar. 1976.

Semi-Fast Fourier Transforms over $GF(2^m)$

DILIP V. SARWATE

***Abstract*—An algorithm which computes the Fourier transform of a sequence of length n over $GF(2^m)$ using approximately $2nm$ multiplications and $n^2 + nm$ additions is developed. The number of multiplications is thus considerably smaller than the n^2 multiplications required for a direct evaluation, though the number of additions is slightly larger. Unlike the fast Fourier transform, this method does not depend on the factors of n and can be used when n is not highly composite or is a prime.**

***Index Terms*—Analysis of algorithms, computational complexity, error-correcting codes, finite fields, Fourier transforms.**

I. Introduction

The discrete Fourier transform (DFT) of a sequence of n elements of a finite field can be computed by means of the fast Fourier transform (FFT) algorithm over the finite field [1]. This algorithm is just the well-known complex field FFT algorithm (e.g., [2]) with the primitive nth root of unity $\exp(j2\pi/n)$ in the complex field being replaced by a primitive nth root of unity in the finite field. When n is composite, with factors $n_1, n_2, \cdots, n_s$, the finite field FFT is essentially what is called a mixed-radix FFT and requires $n(n_1 + n_2 + \cdots + n_s)$ multiplications and $n(n_1 + n_2 + \cdots + n_s)$ additions as compared to the n^2 multiplications and n^2 additions required to evaluate the DFT in the most obvious way. If n is not highly composite, (or if n is a prime), the saving in computation is quite small (or nonexistent). In such cases, the DFT can be computed from the cyclic convolution of two appropriately defined sequences of length approximately $2n$ or more [3]–[5]. This convolution itself can be computed by computing the forward transforms of the two sequences, a pointwise multiplication of the transforms, and an inverse transform. If the length of the sequence is chosen to be highly composite, the FFT algorithm can be used to compute the three transforms and significant savings in computation can be achieved.

The problem that arises in using the convolution method is that the finite field may not contain an appropriate primitive root of unity, and computations may have to be done in a much larger field [6]. In such a case, one can transform the problem of computing a finite field convolution into one of computing a convolution of arrays of integers. If the array convolution is computed by means of a two-dimensional complex field FFT algorithm, then the DFT over $gf)p^m)$ can be computed [6] using $O(nm \log nmM(q))$ bit operations where $M(q)$ is the number of bit operations required to multiply two q-bit numbers and $q \approx 2 \log_2 n + 4 \log_2 m + 4 \log_2 p$. However, this method is not very efficient for small values of n.

The algorithm proposed in this correspondence requires $2(n-1)(m-1)$ multiplications and $(n-1)(n+m-1)$ additions in $GF(2^m)$ to compute a transform of length n, n a prime, over $GF(2^m)$. If n is not a prime, the number of multiplications is somewhat less and the number of additions is somewhat more. Since multiplications require more time than additions, the algorithm is somewhat faster than the direct method, though both require $O(n^2)$ arithmetic operations. However, the proposed algorithm requires $O(n^2 \log n)$ bit operations only, which is better by a factor of $\log n$ over the direct method. For small values of n, the proposed method is superior to the cyclic convolution technique and to the usual FFT algorithm based on the factors of n. Asymptotically, of course, the cyclic-convolution technique requires $O(n \log^4 n)$ bit operations only, and is vastly superior. For these reasons, the proposed algorithm is dubbed a semi-fast Fourier transform (SFFT) algorithm.

II. The SFFT Algorithm

Let n be an odd integer, m the multiplicative order of 2 mod n, α a primitive nth root of unity in $GF(2^m)$, and β an element of degree m in $GF(2^m)$. It is convenient, but not necessary, to take β to be a primitive element. Let $A(x) = A_0 + A_1 x + A_2 x^2 + \cdots$

Manuscript received June 28, 1976; revised April 27, 1977. This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DAAB-07-72-C-0259.

The author is with the Coordinated Science Laboratory and the Department of Electrical Engineerig, University of Illinois at Urbana-Champaign, Urbana, IL 61801.

0018-9340/78/0300-0283$00.75