RECOGNITION OF CATASTROPHIC FAULTS

Amiya Nayak†, Linda Pagli‡, Nicola Santoro†

† Center for Parallel & Distributed Computing, School of Computer Science
Carleton University, Ottawa, K1S 5B6.

‡ Dipartimento di Scienze dell'Informazione, University of Pisa
Corso Italia 40, 56100 Pisa, Italy.

I. INTRODUCTION

Fault tolerance through the incorporation of redundancy and reconfiguration is quite common. Regular systems are being designed with massive redundancy built into them [5,6,12]. These systems also make use of the redundancy to reconfigure in the event of failure in one or more components; normally, a reconfiguration process is triggered as soon as a fault is detected. Many different reconfiguration schemes [1-4,6,7,10-13] have been proposed in the literature which reconfigure regular systems in the presence of faulty components. The distribution of faults can have severe impact on the effectiveness of any reconfiguration scheme; in fact, patterns of faults occurring at strategic locations may render an entire system unusable regardless of its component redundancy and of its reconfiguration capabilities. For a given design, it is not difficult to identify a set of elements whose failure will have catastrophic consequence. There exist many patterns (random distribution) of faults, not in a block, which can be fatal for the system [9]. Therefore, the characterization of such fault patterns is crucial for the identification, testing and detection of such catastrophic events.

In this paper, we are concerned with the development of efficient recognition schemes; that is, efficient mechanisms which automatically determine whether or not an observed/detected pattern of faults will have catastrophic consequences. The problem of recognizing whether a fault pattern is catastrophic has been addressed only for specific cases. In particular, a $O(g^2)$ recognition algorithm was derived in [9] for 2−link redundant systems, where g is the length of the bypass link. In this paper, we study the more general case of recognizing catastrophic fault patterns in reconfigurable arrays with arbitrary link redundancy. For these, we prove some fundamental properties which any catastrophic fault pattern must satisfy. We then show that these properties together constitute a necessary and sufficient condition for a fault pattern to be catastrophic for k−link redundant system. As a consequence, we derive a provably correct recognition algorithm whose worse-case time complexity is $O(kg_k)$, where g_k is the length of the kth bypass link; thus, we also improve on the previous algorithm for 2−link redundant systems.

The scheme proposed in this paper can be used to determine the likelihood of a catastrophe in the system or device when some of its component fail; that is, the scheme allows the designer to recognize efficiently and effectively if the occurence of

0-8186-2837-5/92 $03.00 © 1992 IEEE

specific patterns of faults will pose a problem and cannot be reconfigured. No such other mechanism exists to our knowledge. To be able to recognize such patterns is useful not only to test the effectiveness of the employed reconfiguration scheme but also to prevent a total system shutdown.

The results of this paper complements the research on reconfiguration techniques. The results provide a set of tools which can be employed in

1. assessing the fault tolerance effectiveness of a design; this can be done by specifying the minimum number of faults which the design cannot be guaranteed to withstand,
2. testing whether a design meets the specified fault tolerance requirements; this can be achieved by comparing the requirements with the ones derived using the properties of the catastrophic fault patterns, and
3. determining redundancy requirement for the designer to meet a desired level of fault tolerance; this can be done by determining the minimal link configuration for which no catastrophic fault patterns exist below the specified amount of failure.

Furthermore, the results presented here can help to usefully incorporate knowledge of the application field into the design process as feedbacks to the designer. In particular, knowledge of the type and distribution of faults occurring in the application field can be used to determine for which designs those patterns are catastrophic; thus, the designer can remove those designs from further consideration (even though, without that knowledge, they might have been viable choices).

II. PRELIMINARIES

Let $A = \{p_0, p_2, \ldots, p_N\}$ denote a one-dimensional array of PEs (see Figure 1), where each $p \in A$ represents a processing element and there exists a direct link between p_i and $p_{i+1}, 0 \leq i < N$. Any link connecting p_i and p_j where $j > i+1$ is said to be a *bypass link*. The length of a bypass link, connecting p_i and p_j, is the distance in the array between p_i and p_j; i.e., $|j-i|$. Given an integer $g \in [1, N]$ and an array A of size N, A is said to have link redundancy g, if for every $p_i \in A$ with $i \leq N-g$ there exists a link between p_i and p_{i+g}; if $g > 1$, such a link will be called a bypass link. The array A has *link configuration* $G = \{g_1, g_2, \ldots, g_k\}$ where $g_j < g_{j+1}$ and $g_j \in [1, N]$, if A has link redundancy $g_1, g_2, \ldots, g_k$. In the following, it will be assumed that no other links exist in the array except the ones specified by G. Thus, G totally defines the *link structure* of A, and A will be called a *$k-$redundant system.* Notice that $g_1 = 1$ is the regular link, while all other g_i's correspond to bypass links.

Given a linear array A of size N, a *fault pattern* for A is a set of integers $F = \{f_0, f_1, \ldots, f_m\}$ where $m \leq N, f_j < f_{j+1}$ and $f_j \in [0, N]$. An assignment of a fault pattern F to A means that for every $f \in F$, p_f is faulty. The *width* W_F of a fault pattern F is the number of PEs between and including the first and the last fault in F. That is, if $F = \{f_0, \ldots, f_m\}$ then $W_F = f_m - f_0 + 1$.

Definition 1 *A fault pattern F is catastrophic for an array A with link redundancy G if the array cannot be reconfigured in the presence of such an assignment of faults.*

In other words, F is a cut-set of the graph corresponding to A [8]; that is, the removal of the faulty elements and their incident links will cause the array to become disconnected. In this paper, we will consider *minimal* catastrophic fault patterns; that is, fault patterns which have exactly g_k faulty PEs.

Consider an arbitrary fault pattern $F = \{f_0, f_1, \ldots, f_{g_k-1}\}$, consisting of g_k faults for an arbitrary link configuration $G = \{g_1, g_2, \ldots, g_k\}$. Without loss of generality, assume that $f_0 = 0$. The links can be either unidirectional or bidirectional. We represent F by a Boolean matrix W of size $(W_F^+ \times g_k)$, where $W_F^+ = \lceil W_F/g_k \rceil$, defined as follows:

$$W[i,j] = \begin{cases} 1 & \text{if } ig_k + j \in F \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

In the matrix representation, each $f_l \in F$ is mapped into $W[x_l, y_l]$ where $x_l = \lfloor f_l/g_k \rfloor$ and $y_l = f_l \bmod g_k$. Notice that $W[0,0] = 1$ which indicates the location of the first fault. Refer to Figure 2 for an example of a fault pattern whose matrix representation is given in Figure 3.

Let W be the matrix representation of a minimal fault pattern F. Notice that any minimal catastrophic fault pattern satisfies the necessary condition that $\forall j$, there is only one i for which $W[i,j] = 1$. The *row coordinates* of F is the ordered set $\{x_0, x_1, \ldots, x_{g_k-1}\}$ of the row indices of W corresponding to the faults f_i $(0 \le i \le g_k - 1)$.

Let $W[x_l, y_l]$ be the location of fault f_l. The location $W[i, y_l]$, with respect to f_l, is *interior* if $i < x_l$, *border* if $i = x_l$, and *exterior* if $i > x_l$. For a given fault pattern F, $I(F)$ (i.e., *interior of* F) is the set of all interior elements, $B(F)$ (i.e., *border of* F) is the set of all border elements, and $E(F)$ (i.e., *exterior of* F) is the set of all exterior elements. Refer to Figure 4 for an example.

Now with respect to the matrix representation of F, a fault pattern F is *catastrophic* for an array A with link redundancy G if it is not possible to reach any exterior element from any interior element using the links in G.

The *area* A_F of a fault pattern F is the number of interior and border elements; that is,

$$A_F = \|I(F) \cup B(F)\| = \sum_{j=0}^{g_k-1} (x_j - 1). \tag{2}$$

III. PROPERTIES OF THE REFERENCE FAULT PATTERN

Definition 2 *Given a link configuration G, a reference fault pattern (RFP) is a catastrophic fault pattern for G which has largest width W_F and maximum area A_F.*

Let $\mathcal{F}$ be a reference fault pattern. By definition of reference fault pattern, $W_{\mathcal{F}}$ is maximal and $A_{\mathcal{F}}$ is maximal.

Consider two fault patterns $F_\alpha = \{f'_0, f'_1, \ldots, f'_{g_k-1}\}$ and $F_\beta = \{f''_0, f''_1, \ldots, f''_{g_k-1}\}$ for a given link configuration G. We define the concatenation of F_α and F_β as follows:

Definition 3 *Let $\{x'_0, x'_1, \ldots, x'_{g_k-1}\}$ and $\{x''_0, x''_1, \ldots, x''_{g_k-1}\}$ be the row coordinates of F_α and F_β respectively in their respective matrix representation. The concatenation of F_α and F_β (denoted by $F_\alpha \| F_\beta$) is a fault pattern F whose row coordinates are $\{x_0, x_1, \ldots, x_{g_k-1}\}$, where $x_i = \{max(x'_i, x''_i)\}$ for $0 \leq i \leq g_k - 1$.*

Property 1 *Let F_α and F_β be catastrophic for G. Then, their concatenation $F_\alpha \| F_\beta$ is also catastrophic for G.*

As a consequence of the above property, we can prove the following property of the reference fault pattern.

Property 2 *For any link configuration G, the reference fault pattern is unique.*

IV. NECESSARY & SUFFICIENT CONDITIONS FOR CATASTROPHE

The first necessary condition establishes an important relationship between a fault pattern F and the reference fault pattern $\mathcal{F}$.

Definition 4 *For any two fault patterns F_α and F_β, F_α and F_β cross if $I(F_\alpha) \not\subseteq I(F_\beta)$ and $I(F_\beta) \not\subseteq I(F_\alpha)$.*

Lemma 1 *Given G, let $\mathcal{F}$ be the reference fault pattern and F be any fault pattern for G. If F and $\mathcal{F}$ cross, then F is not catastrophic for G.*

Figure 5 shows an example of a fault pattern which crosses $\mathcal{F}$ and therefore not catastrophic.

Lemma 1 expresses a necessary condition for a fault pattern to be catastrophic. However, not crossing $\mathcal{F}$ is not sufficient for a fault pattern to be catastrophic (see Figure 6 for an example).

Lemma 2 *Let the links be unidirectional. If F does not satisfy the following property then F is not catastrophic for G: for any column y_i $(0 \leq y_i \leq g_k - 1)$ in W and for any link $g \in G = \{g_1, g_2, \ldots, g_k\}$*

$$x_i \leq \begin{cases} x_{i+g} + 1 & \text{if } i + g \leq g_k - 1 \\ x_j & \text{otherwise} \end{cases} \tag{3}$$

where $j = (i + g) \bmod g_k$.

Lemma 2 can be extended to the case of bidirectional links as follows:

Lemma 3 *For bidirectional links, if F does not satisfy the following property then F is not catastrophic for G: for any column y_i $(0 \leq y_i \leq g_k - 1)$ in W and for any link $g \in G = \{g_1, g_2, \ldots, g_k\}$*

$$1) \quad x_i \leq \begin{cases} x_{i+g} + 1 & \text{if } i + g \leq g_k - 1 \\ x_j & \text{otherwise} \end{cases} \tag{4}$$

$$2) \quad x_i \leq \begin{cases} x_{i-g} + 1 & \text{if } i - g \geq 0 \\ x_{[i+g_k-g]} + 2 & \text{otherwise} \end{cases} \tag{5}$$

where $j = (i + g) \bmod g_k$.

The above lemmas state necessary conditions for a fault pattern to be catastrophic. We will now show that the combination of the conditions expressed by Lemmas 1, 2, and 3 constitute a necessary and sufficient condition.

Theorem 1 *A fault pattern F is catastrophic for a link configuration G if and only if*

i) it does not cross the reference fault pattern corresponding to G, and

ii) it satisfies Lemma 2 in the case of unidirectional links and Lemma 3 in case of bidirectional links.

V. AN IMPROVED RECOGNITION STRATEGY

We use the preceding results to construct an efficient recognition algorithm. In particular, the algorithm will verify whether the necessary and sufficient conditions expressed by Theorem 1 are met.

The recognition algorithm is outlined in Appendix A. The algorithm includes a pre-testing phase, ensuring that the width and area of F are not greater than the ones of the reference fault pattern $\mathcal{F}$. The major steps of the algorithm are: Test for Crossing and Test for Property. Test for Crossing requires only the determination of the maximal row coordinate of F and $\mathcal{F}$; thus, it can be done in time $O(g_k)$. For each row coordinate and for each link, Test for Property requires either one or two tests depending on whether the links are unidirectional or bidirectional, respectively; hence, the entire process can be completed in time $O(kg_k)$.

Property 3 *The algorithm requires $O(kg_k)$ time.*

Notice that the complexity of this algorithm represents an improvement on the $O(g_k^2)$ complexity of the existing algorithm for 2–link redundant systems (i.e., $G = \{1, g_k\}$ and $k = 2$); in fact, in this case, the proposed algorithm requires only $O(g_k)$ time.

REFERENCES

[1] K. P. Belkhale and P. Banerjee, "Reconfiguration Strategies in VLSI Processor Arrays," in *Proc. Int'l Conf. on Computer Design*, 1988, pp. 418-421.

[2] D. M. Blough, "On the Reconfiguration of Memory Arrays containing Clustered Faults," in *Proc. 21st Int'l Conf. on Fault-Tolerant Computers*, 1991, pp. 444-451.

[3] F. Distante, F. Lombardi, and D. Sciuto, "Array Partitioning: A Methodology for Reconfigurability and Reconfiguration Problems," in *Proc. Int'l Conf. on Computer Design*, 1988, pp. 564-567.

[4] J. W. Greene and A. E. Gamal, "Configuration of VLSI Arrays in the Presence of Defects," *Journal of the ACM*, Vol. 31, No. 4, 1984, pp. 694-717.

[5] I. Koren and D. K. Pradhan, "Introducing Redundancy into VLSI Designs for Yield and Performance Enhancement," in *Proc. 15th Int'l Conf. on Fault-Tolerant Computers*, 1985, pp. 330-335.

[6] S. Kuo and W. K. Fuchs, "Efficient Spare Allocation for Reconfigurable Arrays," *IEEE Design and Test*, Feb. 1987, pp. 24-31.

[7] F. Lombardi, D. Sciuto and R. Stefanelli, "A Technique for Reconfiguring Two-Dimensional VLSI Arrays," in *Proc. Real Time Symposium*, 1987, pp. 44-53.

[8] A. Nayak, L. Pagli and N. Santoro "Combinatorial and Graph Problems arising in the Analysis of Catastrophic Fault Patterns," in *23rd SE Conf. on Combinatorics, Graph Theory and Computing*, 1992, to appear.

[9] A. Nayak, N. Santoro and R. Tan, "Fault-Intolerance of Reconfigurable Systolic Arrays," in *20th Int'l Symp. on Fault-Tolerant Computers*, 1990, pp. 202-209.

[10] R. Negrini, M. G. Sami, and R. Stefanelli, "Fault-Tolerance Techniques for Array Structures used in Supercomputing," *IEEE Computer*, Vol. 19, No. 2, 1986, pp. 78-87.

[11] A. L. Rosenberg, "The Diogenes Approach to Testable Fault-Tolerant Arrays of Processors," *IEEE Trans. on Computers*, Vol. C-32, No. 10, Oct. 1983, pp.902-910.

[12] G. Saucier, J. L. Patry and E. F. Kouka, "A Reconfigurable Wafer Scale Array for Image Processing," in *Proc. Int'l Conf. on Wafer Scale Integration*, 1989, pp. 277-288.

[13] R. Venkateswaran, P. Mazumder and K. G. Sin, "Hex-Repair: A New Approach to Hexagonal Array Reconfiguration," in *Proc. IEEE Int'l Workshop on Defect and Fault Tolerance on VLSI Systems*, 1991, pp. 288-291.

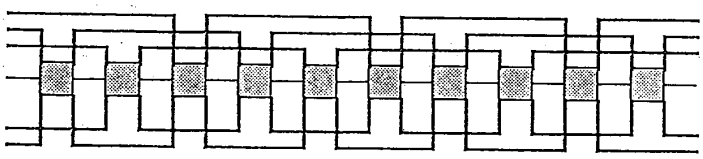


Figure 1: One dimensional array of processors. Bypass links are shown in bold.

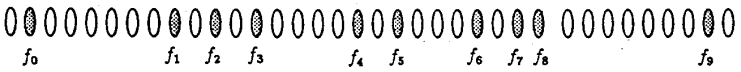


Figure 2 : A fault pattern F_1 for $G = \{1, 10\}$ with bidirectional links. $\|F_1\| = 10$ and $W_F = 34$.

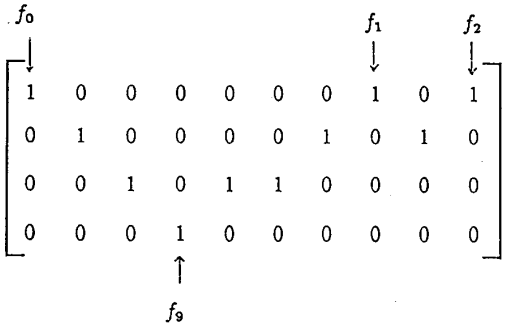


Figure 3 : The matrix representation for F_1 in Figure 2

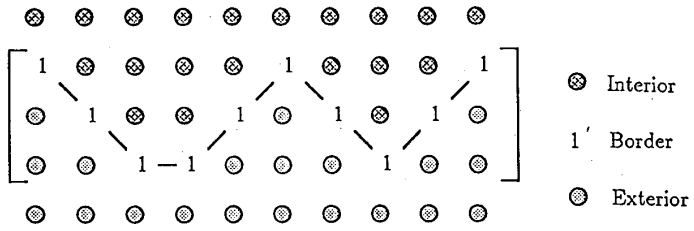
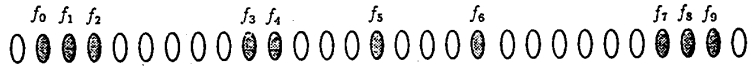


Figure 4 : *Interior*, *exterior* and *border* of a fault pattern $F = \{0, 5, 9, 11, 14, 16, 18, 22, 23, 27\}$ for $G = \{1, 5, 10\}$ in which all links are bidirectional. The first and last row in Figure 4 correspond to elements in the array which are outside of W_F and not part of W.



A fault pattern F_2

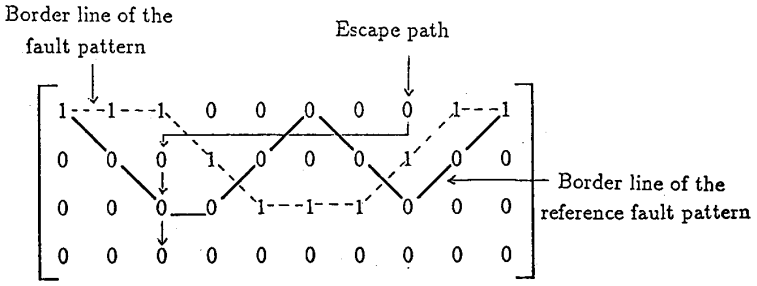


Figure 5 : A fault pattern F_2 which crosses the reference fault pattern for $G = \{1, 5, 10\}$ in which the links are bidirectional. The solid line and dashed line indicate the border of $\mathcal{F}$ and F_2 respectively.

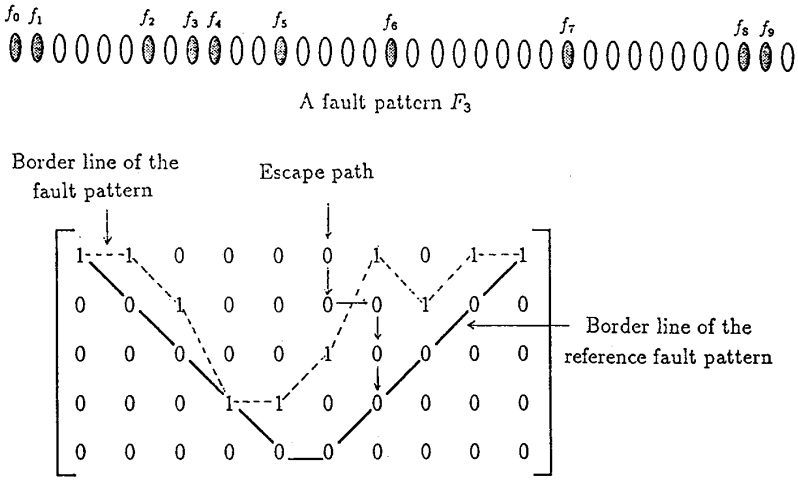


Figure 6 : A fault pattern F_3 which does not cross the reference fault pattern for $G = \{1, 10\}$ when the links are bidirectional. The solid line and dashed line indicate the border of $\mathcal{F}$ and F_3 respectively.

APPENDIX A

Algorithm: Recognizing if F is catastrophic for G

```
Begin
    TEST := True;
    Test for violation of maximal area and width;
    if TEST then
        Test for crossing;
        if TEST then Test for property;
    endif
End.
```

Test for violation of maximal area and width (Pre-Testing)

```
Begin
    if W_F < W_F or A_F < A_F then
        TEST := false
    endif
End;
```

Test for Crossing

```
Begin
    Let {x_i} and {x̄_i} be the row coordinates of F and F̄, respectively.
    i := 0;
    repeat
        if x_i > x̄_i then
            TEST := False
        endif
        i := i + 1;
    until i > g_k or not(TEST)
End;
```

Test for Property

```
Begin
    i := 0;
    repeat
        j := 1;
        repeat
            if i + g_j ≤ g_k − 1 then x_p := x_{i+g_j} + 1 else x_p := x_{(i+g_j) mod g_k};
            if i − g_j ≥ 0 then x_q := x_{i−g_j} + 1 else x_q := x_{⌊i+g_k−g_j⌋} + 2;
            Case link orientation of
            unidirectional:
                if x_i > x_p then
                    TEST := False
                endif
            bidirectional:
                if (x_i > x_p) and (x_i > x_q) then
                    TEST := False
                endif
            endcase
            j := j + 1;
        until j > k or not(TEST)
        i := i + 1;
    until i > g_k or not(TEST)
End;
```