Algebraic Approaches for Fault Identification in Discrete Event Systems

Yingquan Wu and Christoforos N. Hadjicostis

Abstract

In this note we develop algebraic approaches for fault identification in discrete event systems that are described by Petri nets. We consider faults in both Petri net transitions and places, and assume that system events are not directly observable but that the system state is periodically observable. The particular methodology we explore incorporates redundancy into a given Petri net in a way that enables fault detection and identification to be performed efficiently using algebraic decoding techniques. The guiding principle in adding redundancy is to keep the number of additional Petri net places small while retaining enough information to be able to systematically detect and identify faults when the system state becomes available. The end result is a *redundant Petri net embedding* that uses $2k$ additional places and enables the simultaneous identification of $2k-1$ transition faults and k place faults (that may occur at various instants during the operation of the Petri net). The proposed identification scheme has worst-case complexity of $O(k(m+n))$ operations where m and n are respectively the number of transitions and places in the given Petri net.

Keywords —Petri nets, discrete event systems, fault detection and identification, algebraic decoding.

I. Introduction

A commonly used approach to fault diagnosis in dynamic systems is to introduce analytical redundancy (characterized in terms of a parity space) and diagnose faults based on parity relations

This material is based upon work supported in part by the National Science Foundation under NSF Career Award No 0092696 and NSF ITR Award No 0085917, and in part by the Air Force Office of Scientific Research under Award No AFOSR DoD F49620-01-1-0365URI. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of NSF or AFOSR.

The authors are with the Coordinated Science Laboratory and the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign.

[1], [2]. The methodology in [3] uses a similar idea to monitor faults in discrete event systems (DESs) that can be modeled by Petri nets [4], [5]. This approach encodes the state (marking) of the original Petri net by embedding it into a redundant one in a way that enables the diagnosis of faults in the Petri net transitions and/or places via linear parity checks on the overall *encoded* state of the redundant Petri net embedding. Place faults are associated with conditions that cause the corruption of the number of tokens in a certain place of the Petri net whereas transition faults are associated with conditions that prevent tokens from being removed from (deposited at) the input (output) places of a particular transition.

In this note we consider fault identification in a Petri net where activity (transition firing) is *unobservable* but the state (Petri net marking) is *periodically observable*. More specifically, at the end of a period we observe the final state (marking) of the redundant Petri net embedding and, based on this information, we aim at detecting and identifying faults that may have occurred during this period. To achieve this, we construct redundant Petri net embeddings in which the identification of multiple and mixed (transition and/or place) faults, even when certain state information is missing, can be done systematically via algebraic coding/decoding techniques. Apart from fault detection and identification guarantees, our goal in choosing an appropriate redundant Petri net embedding is to keep the amount of redundancy (as indicated by the number of additional places/sensors) small.

As we show in this note, the use of a redundant Petri net embedding with $2k$ additional places (and the connections and tokens associated with them) allows the simultaneous identification of up to $2k-1$ transition faults and up to k place faults. The worst-case complexity of the fault identification procedure involves $O(k(m+n))$ operations where m and n are the number of Petri net transitions and places respectively. The identification procedure is based on algebraic techniques, such as traditional decoding methods (e.g., Berlekamp-Massey decoding [6]) and more recently developed methodologies for solving systems of composite power polynomial equations [7]. Note that the efficiency in the identification process comes at the cost of adding redundancy into the original Petri net — in the form of additional places (sensors) and the connections (acknowledgments) associated with them. This redundancy is chosen strategically so as to guarantee diagnosability *and* enable fast detection and identification.

II. Problem Formulation

The functionality of a Petri net $\mathcal{S}$ is best described by a directed, bipartite graph with two types of nodes: *places* (denoted by $\{P_1, P_2, ..., P_n\}$ and drawn as circles) and *transitions* (denoted by $\{T_1, T_2, ..., T_m\}$ and drawn as rectangles). Weighted directed arcs connect transitions to places and vice versa. The arc weights have to be nonnegative integers (we use b^-_{ij} to denote the weight of the arc from place P_i to transition T_j and b^+_{lj} to denote the weight of the arc from transition T_j to place P_l). Places function as storage locations for tokens (drawn as black dots).

If $\mathbf{q}_s[t]$ denotes the state/marking of the Petri net at time epoch t (i.e., it indicates the number of tokens in each place of the Petri net at time epoch t) and $\mathbf{B}^- \overset{\triangle}{=} [b^-_{ij}]$ (respectively, $\mathbf{B}^+ \overset{\triangle}{=} [b^+_{ij}]$) denotes the $n \times m$ matrix with b^-_{ij} (respectively, b^+_{ij}) at its ith row, jth column position, then the state evolution of Petri net $\mathcal{S}$ is captured by

$$\mathbf{q}_s[t+1] = \mathbf{q}_s[t] + \mathbf{B}^+\mathbf{x}[t] - \mathbf{B}^-\mathbf{x}[t] = \mathbf{q}_s[t] + \mathbf{B}\mathbf{x}[t], \tag{1}$$

where $\mathbf{B} \overset{\triangle}{=} \mathbf{B}^+ - \mathbf{B}^-$ and the input vector $\mathbf{x}[t] \in (\mathbb{Z}^+)^m$ indicates the transitions that take place (fire) at time epoch t. The input vector $\mathbf{x}[t]$ is usually assumed to be a unit vector with a single nonzero entry at its jth position indicating that transition T_j has fired. Note that transition T_j is enabled at time epoch t if and only if $\mathbf{q}_s[t] \geq \mathbf{B}^-(:, j)$ (where the inequality is taken element-wise and $\mathbf{B}^-(:, j)$ denotes the jth column of $\mathbf{B}^-$).

We consider two types of faults that may occur in a Petri net.

(i) A *transition fault* models a fault in the mechanism that implements a certain Petri net transition. We say that transition T_j has a *post-condition fault* if no tokens are deposited at its output places (even though the tokens from its input places are consumed). Similarly, we say that transition T_j has a *pre-condition fault* if the tokens that are supposed to be removed from the input places are not removed (even though tokens are deposited at the corresponding output places). As will be shown shortly, each post-condition fault can be indicated by an error of "$+1$," whereas each pre-condition fault can be indicated by an error of "-1;" thus, in terms of coding theory terminology, transition faults are measured under the Lee distance metric [6].

(ii) A *place fault* models a fault that corrupts the number of tokens in a single place of the Petri net. Note that place faults are measured in terms of the number of faulty places, independent of the number of erroneous tokens in each faulty place. Thus, in terms of coding theory terminology, place faults are measured under the Hamming distance metric [6]. Note also that, when state information from a certain place is unobservable or missing, one can treat this situation as an erasure [6].

Clearly, a pre-condition (post-condition) fault on a transition that has n_T input (output) places can also be treated as a combination of n_T place faults. In order for the fault identification algorithm to be able to resolve such conflicts, we aim at determining the *minimum* number of transition and/or place faults that explain the behavior observed in the Petri net. The underlying assumption in this formulation is that the most likely explanation is the one that involves the minimum number of faults (as would be the case if all transition and/or place faults are equally likely and independent). Note that multiple faulty firings of the same transition are allowed in our model (but count toward the maximum number of transition faults that we can tolerate).

We assume that the firing of transitions in the redundant Petri net is not directly observable while the Petri net marking is *periodically observable*. We aim to identify faults based on the observed marking at the end of a period. We use the term "non-concurrent" to capture the fact that diagnosis is performed over a period of several time epochs, in this case once every N time epochs. We assume that within the epoch interval $[1, N]$, each transition may suffer possibly multiple pre-condition or post-condition faults, but not both (actually, if a particular transition suffers both a pre-condition and a post-condition fault within $[1, N]$, their effects will be canceled, making their non-concurrent detection impossible).

III. Fault Identification

The operations involved in the Petri net state evolution in (1) are regular integer operations. The proposed fault identification schemes, however, will actually be performed based on operations in a finite field due to the simplicity of the resulting identification algorithm. More specifically, our identification algorithms will operate in GF(p), the finite field of order p where p is prime: GF(p) consists of the set $\{0, 1, 2, \ldots, p-1\}$ with all arithmetic operations taken modulo p. Due to page limitations, we omit most mathematical derivations regarding assertions about fault identifiability and the identification procedure. The readers who are interested in these mathematical details are referred to [7], [8] for the analysis of transition faults, and to [6] for the analysis of place faults.

A. Redundant Petri net embeddings

The identification of faults in a given Petri net $\mathcal{S}$ can be facilitated by the construction of a *redundant Petri net embedding* $\mathcal{H}$ [3]. More specifically, d places are added to the original Petri net $\mathcal{S}$ to form a composite Petri net $\mathcal{H}$ whose state (marking) $\mathbf{q}_h[t]$ is η-dimensional ($\eta = n + d, d > 0$) and under fault-free conditions satisfies

$$\mathbf{q}_h[t] = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t] \tag{2}$$

for all time epochs t. Here, $\mathbf{q}_s[t]$ is the state of the original Petri net $\mathcal{S}$, $\mathbf{I}_n$ denotes the $n \times n$ identity matrix and $\mathbf{C}$ is a $d \times n$ integer matrix to be designed. In order to guarantee that (2) remains valid for all t, the state evolution of $\mathcal{H}$ is chosen to be of the form

$$\mathbf{q}_h[t+1] = \mathbf{q}_h[t] + \underbrace{\begin{bmatrix} \mathbf{B}^+ \\ \mathbf{C}\mathbf{B}^+ - \mathbf{D} \end{bmatrix}}_{\mathcal{B}^+} \mathbf{x}[t] - \underbrace{\begin{bmatrix} \mathbf{B}^- \\ \mathbf{C}\mathbf{B}^- - \mathbf{D} \end{bmatrix}}_{\mathcal{B}^-} \mathbf{x}[t], \tag{3}$$

where $\mathbf{D}$ is a $d \times m$ integer matrix, also to be designed. The d additional places together with the n original places comprise the places of the *redundant Petri net embedding* $\mathcal{H}$. A valid (redundant) marking/state can be checked by using the parity check matrix $\mathbf{P} \triangleq [-\mathbf{C} \;\; \mathbf{I}_d]$ to verify that the *syndrome*

$$\mathbf{s}[t] \triangleq \mathbf{P}\mathbf{q}_h[t] = [-\mathbf{C} \;\; \mathbf{I}_d] \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t] = \mathbf{0}. \tag{4}$$

In [3] it is shown that if matrices $\mathbf{C}$ and $\mathbf{D}$ have integer nonnegative entries and satisfy $\mathbf{C}\mathbf{B}^+ - \mathbf{D} \geq \mathbf{0}$ and $\mathbf{C}\mathbf{B}^- - \mathbf{D} \geq \mathbf{0}$ (element-wise), then a properly initialized redundant Petri net embedding $\mathcal{H}$ (i.e., one that satisfies Eq. (2) at $t = 0$) admits any firing sequence that is admissible in the original Petri net $\mathcal{S}$.

B. Identification of transition faults

Recall that within the epoch interval $[1, N]$ each transition may suffer multiple pre-condition or post-condition faults, but not both. Let $\mathbf{e}_T^+ \in (\mathbb{Z}^+)^m$ denote an indicator vector of post-condition faults and $\mathbf{e}_T^- \in (\mathbb{Z}^+)^m$ denote an indicator vector of pre-condition faults within the epoch interval $[1, N]$. Assuming no place faults, the erroneous state $\mathbf{q}_f[N]$ at time epoch N is given by

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^- \ , \tag{5}$$

where $\mathbf{q}_h[N]$ is the state that would have been reached under fault-free conditions. The fault syndrome at time epoch N is then

$$\begin{aligned}\mathbf{s}_T[N] &= [-\mathbf{C} \ \ \mathbf{I}_d](\mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^-) \\ &= [-\mathbf{C} \ \ \mathbf{I}_d]\left(\mathbf{q}_h[N] - \begin{bmatrix} \mathbf{B}^+ \\ \mathbf{C}\mathbf{B}^+ - \mathbf{D} \end{bmatrix}\mathbf{e}_T^+ + \begin{bmatrix} \mathbf{B}^- \\ \mathbf{C}\mathbf{B}^- - \mathbf{D} \end{bmatrix}\mathbf{e}_T^-\right)\end{aligned}$$

and is easily calculated to be

$$\mathbf{s}_T[N] = \mathbf{D}\mathbf{e}_T \ , \tag{6}$$

where $\mathbf{e}_T \triangleq \mathbf{e}_T^+ - \mathbf{e}_T^-$. Clearly, the identification of transition faults based on the syndrome $\mathbf{s}_T[N]$ is completely determined by matrix $\mathbf{D}$. Note that a transition fault corresponds to a Lee (“± 1”) error [6], with “$+1$” meaning a single post-condition fault and “-1” meaning a single pre-condition fault as indicated by (6).

Let $\mathbf{D}$ take the form

$$\mathbf{D}_{k+1} \triangleq \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_m^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^k & \alpha_2^k & \alpha_3^k & \dots & \alpha_m^k \end{pmatrix} \ , \tag{7}$$

where $\alpha_1, \alpha_2, \dots, \alpha_m$ are m distinct nonzero elements in GF(p) (note that this requires $p > m$) and α_i^j is exponentiation in GF(p) (the subscript “$_{k+1}$” is used to indicate the row dimension of $\mathbf{D}$, which corresponds to the number of additional places).

When up to k transition faults (i.e., “± 1” errors) occur, Proposition 3(i) in [7] indicates that the syndrome $\mathbf{s}_T = [s_0 \ s_1 \ s_2 \ \dots \ s_k]$ is nonzero and uniquely determines those erroneous locations. Furthermore, by adopting the approach in [7], we can identify up to k transition faults with complexity of $O(km)$ operations. The details of translating these results to the set-up here can be found in [8]. Note that matrix $\mathbf{C}$ does not directly enter the development here and we consider it later when we discuss the identification of place faults.

Note that, for $k = 1$, the first row of matrix $\mathbf{D}$ in (7) is redundant; thus, we only need

$$\mathbf{D}_1 \triangleq (1, 2, \ldots, m), \quad k = 1. \tag{8}$$

For $k = 2$, the first row is again redundant. This is justified by the fact that the equations $x_1 \equiv x_2 + x_3$ and $x_1^2 \equiv x_2^2 + x_3^2$ do not have a nonzero (non-trivial) solution in GF(p); thus, there is no confusion about the number of faults. Therefore, for $k = 2$, we can use the following matrix $\mathbf{D}$:

$$\mathbf{D}_2 \triangleq \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ 1 & 2^2 & 3^2 & \ldots & m^2 \end{pmatrix} \bmod p\,, \quad k = 2. \tag{9}$$

C. Identification of place faults

We now focus on the identification of place faults under the assumption of no transition faults. Let the place faults within the time epoch interval $[1, N]$ result in a corrupted state

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] + \mathbf{e}_P, \tag{10}$$

where $\mathbf{q}_h[N]$ is the state that would have been reached under fault-free transitions and $\mathbf{e}_P \in \mathbb{Z}^\eta$ denotes the (accumulated) place fault vector. Note that $\mathbf{e}_P$ is an η dimensional vector and can model faults on *all* places of the Petri net, including the redundant ones. We are interested in identifying up to k place faults, which implies that $\mathbf{e}_P$ has Hamming weight up to k. The place fault syndrome is given by

$$\mathbf{s}_P[N] = [-\mathbf{C}\ \ \mathbf{I}](\mathbf{q}_h[N] + \mathbf{e}_P) = [-\mathbf{C}\ \ \mathbf{I}]\mathbf{e}_P, \tag{11}$$

i.e., the identifiability of place faults is exclusively determined by matrix $\mathbf{C}$.

We next associate the design of matrix $\mathbf{C}$ with well-known algebraic decoding techniques. Let $\mathbf{H}_{2k}$ be defined as

$$\mathbf{H}_{2k} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_{\eta-1} & \alpha_\eta \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \ldots & \alpha_{\eta-1}^2 & \alpha_\eta^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \ldots & \alpha_{\eta-1}^3 & \alpha_\eta^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{2k} & \alpha_2^{2k} & \alpha_3^{2k} & \ldots & \alpha_{\eta-1}^{2k} & \alpha_\eta^{2k} \end{pmatrix}, \tag{12}$$

where $\alpha_1, \alpha_2, \dots, \alpha_\eta$ are η distinct nonzero elements in GF(p) (note that this requires $p > \eta$)[1]. It is well-known that syndrome $\mathbf{s}$ in the form

$$\mathbf{s} = \mathbf{H}_{2k}\mathbf{e} \tag{13}$$

uniquely determines $\mathbf{e}$ as long as the Hamming weight of $\mathbf{e}$ is up to k (cf. [6]). Furthermore, the Berlekamp-Massey algorithm can be used to identify up to k Hamming errors with computational complexity of $O(k\eta)$ operations (cf. [6]). Note that, in the case of place faults, the syndrome in (12) is a linear combination of columns of $\mathbf{H}_{2k}$ where the weights with which columns are combined are arbitrary integers; in the case of transition faults, however, the syndrome in (7) is a linear combination of columns of $\mathbf{D}_{k+1}$ where the weights with which columns are combined are restricted to be ± 1. Since the all "1's" row that is present in $\mathbf{D}_{k+1}$ is not useful for the Berlekamp-Massey algorithm, it is not included in the construction of $\mathbf{H}_{2k}$.

To transform our problem to the algebraic decoding problem in (13), we make the reasonable assumption that the number of erroneous tokens in a place is bounded. More specifically, we assume that e_{P_i}, the erroneous number of tokens in place P_i, is within the interval $[-\frac{p-1}{2},\ \frac{p-1}{2}]$. Under this assumption, e_{P_i} can be interpreted to fall within $[0,\ p-1]$ in GF(p) (by naturally mapping e_{P_i} to $[e_{P_i} \bmod p]$).

The transformation from (11) to (13) can be achieved by setting $d = 2k$, and $\eta = n + 2k$ and by enforcing the transformation

$$\mathbf{H}_{2k} = \mathbf{\Phi}[-\tilde{\mathbf{C}}\ \ \mathbf{I}_{2k}] \text{ or } \mathbf{P}_{2k} = \mathbf{\Phi}^{-1}\tilde{\mathbf{H}}_{2k}, \tag{14}$$

where the multiplication and inversion operations are defined in GF(p) and matrix $\mathbf{\Phi}$ denotes the last $2k$ columns of $\mathbf{H}_{2k}$

$$\mathbf{\Phi} \triangleq \begin{pmatrix} \alpha_{n+1} & \alpha_{n+2} & \alpha_{n+3} & \cdots & \alpha_{\eta-1} & \alpha_\eta \\ \alpha_{n+1}^2 & \alpha_{n+2}^2 & \alpha_{n+3}^2 & \cdots & \alpha_{\eta-1}^2 & \alpha_\eta^2 \\ \alpha_{n+1}^3 & \alpha_{n+2}^3 & \alpha_{n+3}^3 & \cdots & \alpha_{\eta-1}^3 & \alpha_\eta^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{n+1}^{2k} & \alpha_{n+2}^{2k} & \alpha_{n+3}^{2k} & \cdots & \alpha_{\eta-1}^{2k} & \alpha_\eta^{2k} \end{pmatrix}. \tag{15}$$

[1] The code whose parity check matrix is defined by (12) is called a Reed-Solomon code whereas the code whose parity check matrix is defined by (7) is called an extended Reed-Solomon code (cf. [6]).

Note that $\mathbf{\Phi}$ forms a nonsingular Vandermonde matrix. Clearly, if we set $\mathbf{P} = [-\tilde{\mathbf{C}} \;\; \mathbf{I}_{2k}] = \mathbf{\Phi}^{-1}\mathbf{H}_{2k}$ (by interpreting the entries as integer entries in $[0,\ p-1]$, i.e., by inverting the natural mapping mentioned above), then we can easily convert (11) to the decoding problem (13). By taking both sides of (11) modulo p we obtain

$$\mathbf{s}_P[N] = \mathbf{P}\mathbf{q}_f[N] = [-\tilde{\mathbf{C}} \;\; \mathbf{I}_{2k}]\mathbf{e}_P \quad \Rightarrow \quad \mathbf{\Phi}\mathbf{s}_P[N] \equiv \mathbf{H}_{2k}\mathbf{e}_P,$$

where the symbol "$\equiv$" denotes equality modulo p.

To efficiently identify k place faults, we pre-process the syndrome $\mathbf{s}_P[N] = \mathbf{P}_{2k}\mathbf{e}_P$ by (left) multiplying by matrix $\mathbf{\Phi}$, i.e., we obtain the modified syndrome $\mathbf{s}'_P[N] \overset{\triangle}{=} \mathbf{\Phi}\mathbf{s}_P[N]$, which satisfies $\mathbf{s}'_P[N] \equiv \mathbf{H}_{2k}\mathbf{e}_P$ and can be solved efficiently for $\mathbf{e}_P$ using the Berlekamp-Massey algorithm. The complexity of the identification procedure is $O(k\eta)$ operations [6].

When a few places are unobservable, we can set the number of tokens in the unobservable places to zero[2] and apply error-and-erasure decoding which is again empowered by the Berlekamp-Massey algorithm (cf. [6]). In such case, the error correction capability is characterized by $f + 2t \leq 2k$, where f denotes the number of unobservable places and t denotes the number of place faults (among observable places).

D. Simultaneous Identification of Transition and Place Faults

In this section we show that with $2k$ additional places it is possible to *simultaneously* identify $2k-1$ transition faults *and* k place faults. As in the previous sections, we assume that no transition suffers simultaneous pre-condition and post-condition faults during the epoch interval $[1, N]$ and that the number of erroneous tokens added to or subtracted from each place does not exceed $+\frac{p-1}{2}$.

By combining Eqs. (6) and (11), we have the following fault syndrome at time epoch N:

$$\begin{aligned} \mathbf{s}[N] &= \mathbf{P}(\mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^- + \mathbf{e}_P) \\ &= \mathbf{D}\mathbf{e}_T + \mathbf{P}\mathbf{e}_P \; . \end{aligned} \tag{16}$$

Recall that the identification schemes for transition faults and place faults that we presented earlier were essentially based on operations in GF(p) (modulo p operations). To identify both

[2] Essentially here we are treating a place whose number of tokens is unobservable as an *erasure* [6].

types of faults simultaneously, the key idea is to incorporate regular integer operations into the design of matrices $\mathbf{D}$ and $\mathbf{C}$, as well as in the identification procedure (note that the marking consists of nonnegative integers rather than elements in GF(p)). For notational simplicity, we ignore the subscript "${}_{2k}$" in the sequel. Let p be a prime number larger than both m and η, and let $\mathbf{D}$ follow the design in (7) and $\mathbf{C}$ be chosen such that $\mathbf{P} \stackrel{\triangle}{=} [\mathbf{C} \quad \mathbf{I}] \pmod p$ satisfies (14). Define $\mathbf{D}^*$ and $\mathbf{P}^*$ by

$$\mathbf{D}^* \stackrel{\triangle}{=} -p \cdot \mathbf{D}, \tag{17}$$

$$\mathbf{C}^* \stackrel{\triangle}{=} p \cdot \mathbf{1} - \mathbf{C}, \quad \mathbf{P}^* \stackrel{\triangle}{=} [-\mathbf{C}^* \quad \mathbf{I}] = [\mathbf{C} - p \cdot \mathbf{1} \quad \mathbf{I}], \tag{18}$$

where $\mathbf{1}$ is a $2k \times n$ matrix with all entries being 1.

Note that the design in Eqs. (17) and (18) satisfies $\mathbf{C}^* > \mathbf{0}$, $\mathbf{D}^* < \mathbf{0}$ (element-wise). This guarantees that the marking of the additional places $\mathbf{C}^*\mathbf{q}_s[\cdot]$ is nonnegative and that the arc weights associated with the additional places (given by $\mathbf{C}^*\mathbf{B}^- - \mathbf{D}^*$ and $\mathbf{C}^*\mathbf{B}^+ - \mathbf{D}^*$) are nonnegative. It is possible, however, that after the occurrence of a fault some firings that are enabled in the original Petri net become disabled in the redundant Petri net embedding due to the (erroneous) marking of the additional places. Clearly, this is not an issue if the enabling and disabling of transitions is *not* influenced by the number of tokens in the additional places. Even when the additional places function as controllers (as in [9] for instance), this problem can be avoided in straightforward ways (e.g., by adding a sufficiently large number of extra tokens to each additional place and ignoring this extra number of tokens when performing parity checks at the end of time epoch N).

We now address the identification procedure. Clearly, the syndrome $\mathbf{s}[N] \stackrel{\triangle}{=} \mathbf{P}^*\mathbf{q}_f[N]$ at time epoch N satisfies

$$\mathbf{s}_P \equiv \mathbf{s}[N] \equiv [\mathbf{C} \quad \mathbf{I}]\mathbf{e}_P \pmod p. \tag{19}$$

Left multiplying by $\mathbf{\Phi}$ on both sides of (19), we obtain the modified syndrome

$$\mathbf{s}'_P \stackrel{\triangle}{=} \mathbf{\Phi}\mathbf{s}_P \equiv \mathbf{\Phi}[\mathbf{C} \quad \mathbf{I}]\mathbf{e}_P \equiv \mathbf{H}\mathbf{e}_P \pmod p. \tag{20}$$

When k or less place faults occur, they can be identified by the Berlekamp-Massey algorithm based on $\mathbf{s}'_P$. Once the place faults have been successfully identified and $\mathbf{e}_P$ has been obtained, we can compute

$$\mathbf{s}_T \stackrel{\triangle}{=} (\mathbf{s}[N] - \mathbf{P}^*\mathbf{e}_P)/p = (\mathbf{D}^*/p)\mathbf{e}_T = -\mathbf{D}\mathbf{e}_T, \tag{21}$$

which immediately enables us to identify up to $2k-1$ transition faults using the algorithm discussed in the previous section (note that the symbol "=" denotes integer equality). Overall, the identification of place faults requires $O(k\eta) = O(k^2+kn)$ operations and the identification of transition faults requires $O(km)$ operations; thus, the entire identification complexity is $O(k(m+n))$ operations.

Note that in the approach presented above the identification of transition and place faults is essentially separated. As a result, no matter how many transition faults occur, place faults are always identifiable, as long as no more than k place faults happen.

E. Distributed Fault Identification

Consider a Petri net can be conveniently decomposed into a set of M interacting subsystems $\{\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_M\}$ that have disjoint sets of transitions and share (a small number of) places. If we design a redundant Petri net embedding for each of the subsystems *separately* (utilizing our developments in this section), then when a transition associated with a shared place fires in subsystem $\mathcal{S}_i$, its effect on the other subsystems $\mathcal{S}_j$, $j \neq i$, will be treated as a place fault in the shared place. One way to overcome this limitation is to *compensate* for the fault syndrome in each subsystem $\mathcal{S}_j$, $j \neq i$, by appropriately adjusting the number of tokens in its additional places. Note that the decomposition of a Petri net into subsystems with disjoint sets of transitions and shared places is essentially an arbitrary assignment of transitions into subsystems; a good choice, however, would be one that minimizes the interactions between the transitions of one subsystem and the places of another. This would be the case, for example, if the number of shared places is small. More details can be found in [8].

IV. Example

The Petri net shown in Figure 1 appears in [10] and represents the control logic for three machines and three robots. There are twelve transitions (i.e., $m = 12$) and eighteen places (i.e., $n = 18$). The initial marking of the Petri net, as indicated in Figure 1 by the number of tokens in each place, is

$$\mathbf{q}_s[0] = (1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0)^T\ .$$

We describe the details for a fault diagnosis scheme in which we aim to simultaneously detect and identify two transition faults and one place fault. We assume that the number of faulty tokens

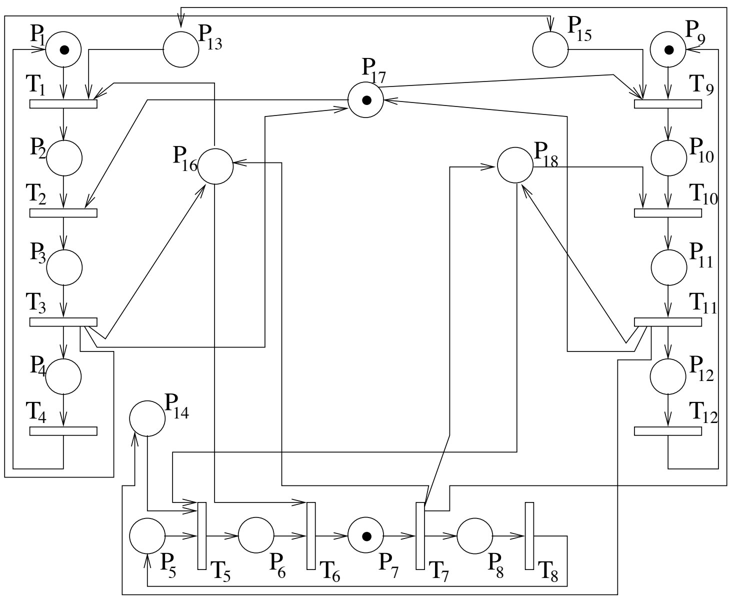

Fig. 1. Petri net model of a manufacturing system with three machines and three robots.

in any place is bounded by $[-5, 5]$. By our development in Section III, we need two redundant places ($d = 2$) and, since the smallest prime number that it is greater than both $m = 12$ and $\eta = 18 + 2 = 20$ is 23, we set $p = 23$. Following the construction in Section III, we obtain $\mathbf{D}^*$, $\tilde{\mathbf{H}}$ and $\mathbf{C}^*$ as in Figure 2.

Thus, the weights to (from) the redundant places from (to) the transitions in the original system (shown in Figure 3 with dotted arcs) are given by

$$\mathbf{C}^*\mathbf{B}^+ - \mathbf{D}^* = \begin{pmatrix} 29 & 52 & 123 & 114 & 120 & 147 & 219 & 205 & 222 & 233 & 306 & 277 \\ 27 & 103 & 266 & 372 & 52 & 300 & 108 & 425 & 278 & 190 & 189 & 148 \end{pmatrix}$$

and

$$\mathbf{C}^*\mathbf{B}^- - \mathbf{D}^* = \begin{pmatrix} 70 & 73 & 75 & 97 & 159 & 158 & 170 & 197 & 242 & 265 & 256 & 285 \\ 43 & 117 & 218 & 382 & 65 & 319 & 70 & 430 & 317 & 193 & 144 & 160 \end{pmatrix} .$$

Furthermore, the initial marking of the overall system is

$$\mathbf{q}_h[0] = \begin{bmatrix} \mathbf{I}_{18} \\ \mathbf{C}^* \end{bmatrix} \mathbf{q}_s[0] = (1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 53\ 36)^T .$$

Assume that the applied firing sequence is $T_7, T_1, T_2, T_8, T_3, T_9$, and that the following faults occur: a pre-condition fault in transition T_2 (during time epoch 3), a place fault that corrupts the

$$\mathbf{D}^* = \begin{pmatrix} -23 & -46 & -69 & -92 & -115 & -138 & -161 & -184 & -207 & -230 & -253 & -276 \\ -23 & -92 & -207 & -368 & -46 & -299 & -69 & -414 & -276 & -184 & -138 & -138 \end{pmatrix}$$

$$\begin{aligned} \tilde{\mathbf{H}} &= \begin{pmatrix} 1 & 5 & 2 & 10 & 4 & 20 & 8 & 17 & 16 & 11 & 9 & 22 & 18 & 21 & 13 & 19 & 3 & 15 & 6 & 7 \\ 1 & 2 & 4 & 8 & 16 & 9 & 18 & 13 & 3 & 6 & 12 & 1 & 2 & 4 & 8 & 16 & 9 & 18 & 13 & 3 \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} 6 & 7 \\ 13 & 3 \end{pmatrix}}_{\mathbf{\Phi}} \underbrace{\begin{pmatrix} 1 & 17 & 17 & 18 & 2 & 18 & 14 & 10 & 22 & 8 & 20 & 14 & 13 & 20 & 10 & 8 & 2 & 3 & 1 & 0 \\ 19 & 19 & 12 & 9 & 12 & 17 & 22 & 7 & 13 & 21 & 17 & 1 & 21 & 22 & 13 & 9 & 2 & 16 & 0 & 1 \end{pmatrix}}_{[\mathbf{C}\ \ \mathbf{I}]} \end{aligned}$$

$$\mathbf{C}^* = \begin{pmatrix} 22 & 6 & 6 & 5 & 21 & 5 & 9 & 13 & 1 & 15 & 3 & 9 & 10 & 3 & 13 & 15 & 21 & 20 \\ 4 & 4 & 11 & 14 & 11 & 6 & 1 & 16 & 10 & 2 & 6 & 22 & 2 & 1 & 10 & 14 & 21 & 7 \end{pmatrix}$$

Fig. 2. Matrices associated with the monitoring scheme for the system of Figure 1.

number of tokens in P_7 by $+2$ (during time epoch 5), and a post-condition fault in transition T_9 (during time epoch 6). The sequence of markings is

$$\begin{array}{lll} T_7: \ \mathbf{q}_f[1] = (1\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1 \quad 102 \quad 74)^T & & \text{Fault-free} \\ T_1: \ \mathbf{q}_f[2] = (0\,1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1 \quad 61 \quad 58)^T & & \text{Fault-free} \\ T_2: \ \mathbf{q}_f[3] = (0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1 \quad 113 \quad 161)^T & & \text{Pre-condition fault in } T_2 \\ T_8: \ \mathbf{q}_f[4] = (0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1 \quad 121 \quad 156)^T & & \text{Fault-free} \\ T_3: \ \mathbf{q}_f[5] = (0\,1\,0\,1\,1\,0\,2\,0\,1\,0\,0\,0\,0\,0\,1\,1\,2\,1 \quad 169 \quad 204)^T & & P_7 \text{ corrupted by } +2 \\ T_9: \ \mathbf{q}_f[6] = (0\,1\,0\,1\,1\,0\,2\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1 \quad -73 \quad -113)^T & & \text{Post-condition fault in } T_9 \end{array}$$

The resulting syndrome is $\mathbf{s}[6] = [-\mathbf{C}^* \ \ \mathbf{I}_2]\mathbf{q}_f[6] \equiv \begin{pmatrix} 5 & 21 \end{pmatrix}^T \pmod{23}$ and, by left multiplying by $\mathbf{\Phi}$, we obtain the modified place fault syndrome as $\mathbf{s}'_P = \mathbf{\Phi}\mathbf{s}[6] \pmod{23} \equiv \begin{pmatrix} 16 & 13 \end{pmatrix}^T$. By inspecting the punctured parity check matrix $\tilde{\mathbf{H}}$, we easily identify place P_7 as faulty with the erroneous number of tokens being $+2$. This is consistent with what took place during the operation of the system. Next, utilizing (21), we obtain $\mathbf{D}\mathbf{e}_T = -(\mathbf{s}[6] - \mathbf{P}^*\mathbf{e}_P)/23 = \begin{pmatrix} 7 & 8 \end{pmatrix}^T$. We note that the above syndrome does not coincide with any column of $\pm\mathbf{D}$, so there must be two transition faults (if identifiable). We first consider the case of both faults undergoing pre-

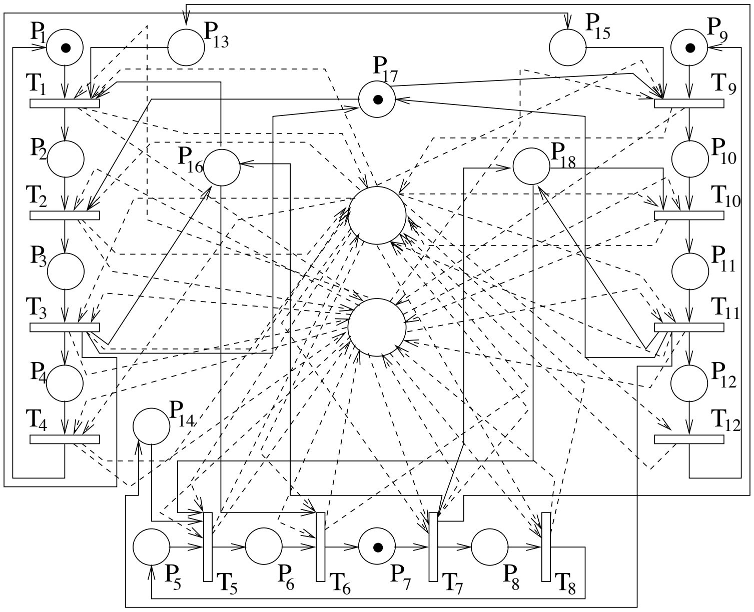

Fig. 3. Fault detection and identification for the manufacturing system of Figure 1 using a redundant Petri net embedding.

condition faults, which results in the following equation array:

$$\begin{cases} -x_1 - x_2 \equiv 7, \\ -x_1^2 - x_2^2 \equiv 8\ . \end{cases}$$

We quickly realize that there does not exist a proper solution. Similarly, we eliminate the possibility of both faults being post-condition faults. We then try the case of a pre-condition fault and a post-condition fault, which translates to solving

$$\begin{cases} x_1 - x_2 \equiv 7, \\ x_1^2 - x_2^2 \equiv 8. \end{cases}$$

These equations are easily shown to have a unique solution with $x_1 = 9$ and $x_2 = 2$. Therefore, we conclude that transition T_2 suffered a pre-condition fault and transition T_9 suffered a post-condition fault, which is consistent with what took place during the operation of the system.

Note that, during the operation of the redundant Petri net system in our example, the number of tokens in the additional places becomes negative (at time epoch 6). If the additional places function as controllers (as in [9]), then this implies that the firing of transition T_9 during time epoch 6 would be inhibited. This issue can be avoided by adding a sufficiently large number of extra tokens to each redundant place (and ignoring this extra number of tokens when performing parity checks).

V. Conclusions

In this note we have presented algebraic approaches to fault identification schemes in discrete event systems that are described by Petri nets. Our setting assumes that system events (transition firings) are not directly observable but that the system state (marking) is periodically observable, and aims at capturing faults in both Petri net transitions and places. To achieve this, we introduce redundancy and construct a redundant Petri net embedding whose additional places encode information in a way that enables error detection and identification to be performed using algebraic decoding techniques. Our approach does not need to reconstruct the various possible state evolution paths associated with a given discrete event system and the identification algorithm has low complexity.

References

[1] J. Gertler, *Fault Detection and Diagnosis in Engineering Systems*. Marcel Dekker, New York, 1998.

[2] E. Y. Chow and A. S. Willsky, "Analytical redundancy and the design of robust failure detection systems," *IEEE Trans. Automatic Control*, vol. 29, pp. 603–614, July 1984.

[3] C. N. Hadjicostis and G. C. Verghese, "Monitoring discrete event systems using Petri net embeddings," *Application and Theory of Petri Nets 1999 (Series Lecture Notes in Computer Science, vol. 1639)*, pp. 188–207, 1999.

[4] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Kluwer Academic Publishers, Boston, MA, 1999.

[5] T. Murata, "Petri nets: properties, analysis and applications," *Proc. of the IEEE*, vol. 77, pp. 541–580, April 1989.

[6] R. E. Berlekamp, *Algebraic Coding Theory*, Revised ed., Aegean Park Press, Laguna Hills, CA, 1984.

[7] Y. Wu and C. N. Hadjicostis, "On solving composite power polynomial equations," *Mathematics of Computation*, vol. 74, pp. 853–868, 2005.

[8] Y. Wu and C. N. Hadjicostis, "Algebraic approaches for centralized and distributed fault identification in discrete event systems," *Technical Report*, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 2004. Available at `http://decision.csl.uiuc.edu/∼chadjic/`

[9] K. Yamalidou, J. Moody, M. Lemmon and P. Antsaklis, "Feedback control of Petri nets based on place invariants," *Automatica*, vol. 32, pp. 15–28, Jan. 1996.

[10] R. Y. Al-Jaar and A. A. Desrochers, "Petri nets in automation and manufacturing," *Advances in Automation and Robotics,* G. N. Saridis, Ed., vol. 2, Greenwich, CT: JAI Press, 1990.