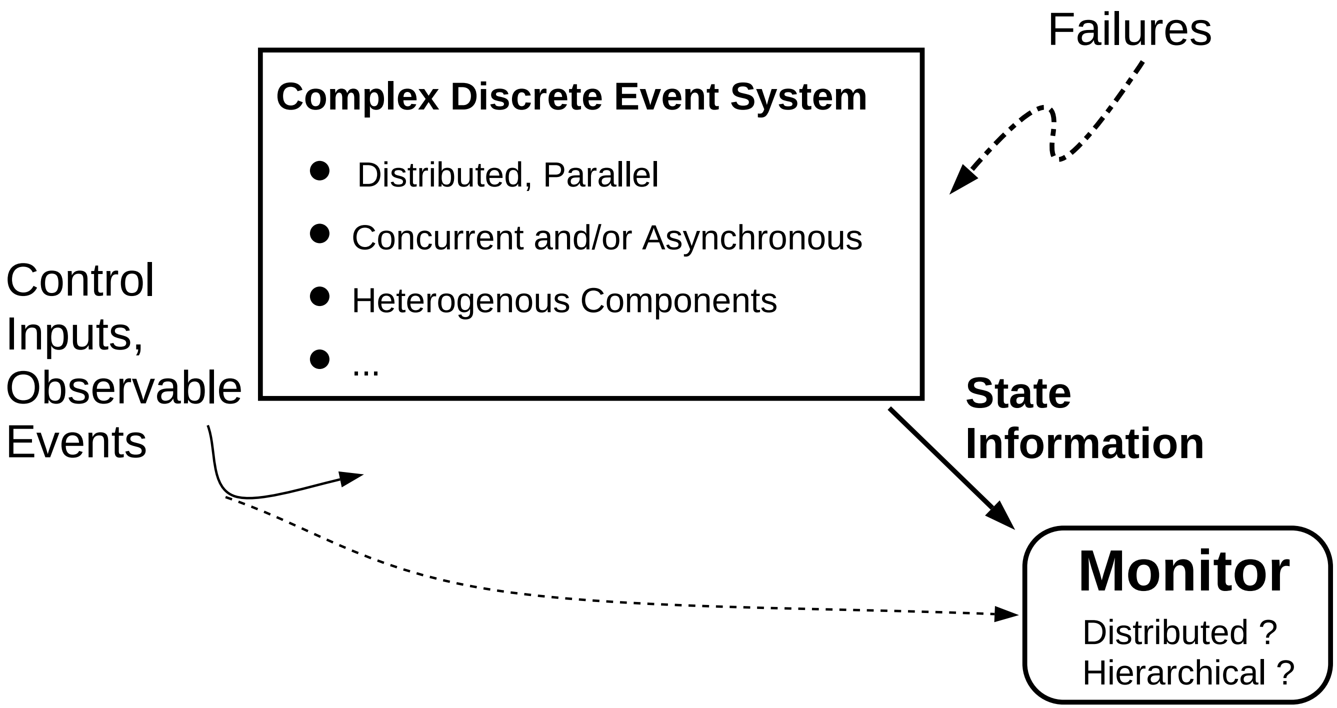
# Failure Identification in Discrete Event Systems using Encoded Petri Net States

**Yingquan Wu and Christoforos Hadjicostis**

Coordinated Science Laboratory and
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

December 13, 2002

# Motivation: Failure Monitoring in Discrete Event Systems



Failures

**Complex Discrete Event System**

- Distributed, Parallel
- Concurrent and/or Asynchronous
- Heterogenous Components
- ...

Control
Inputs,
Observable
Events

**State
Information**

## Monitor

Distributed ?
Hierarchical ?

Non-Concurrent: State information is *not* continuously available.

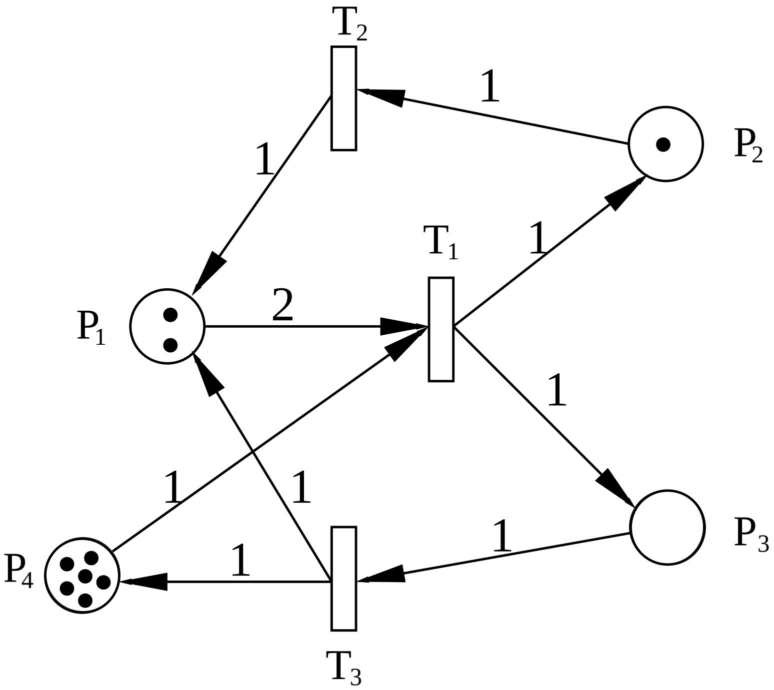
Related previous work:

Diagnosis (Tenekentzis, Lafortune, Benveniste, Kumar, Schwartz, ...)

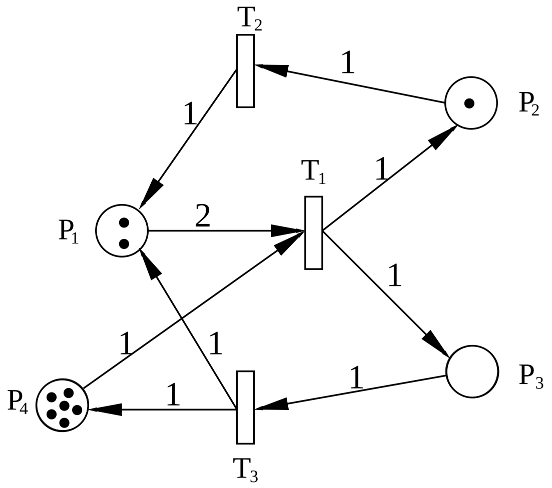
Concurrent monitoring (Kinney, McCluskey, Leveugle, ...)

Other (system-level diagnosis, testing, ...)

# PETRI NET FUNDAMENTALS AND NOTATION



- Places **P** (e.g., $P_1,\ P_2,\ P_3,\ P_4,\ n = 4$) $\longleftrightarrow$ "Storage locations"
- Transitions **T** (e.g., $T_1,\ T_2,\ T_3,\ m = 3$) $\longleftrightarrow$ "Activity"
- Tokens (denoted by "●") $\longleftrightarrow$ "Resources"



- Marking (state): $\mathbf{q}_s[t] = \left[\ 2\ \ 1\ \ 0\ \ 6\ \right]^T$
- Arc weights assembled in matrices $\mathbf{B}^- : \mathbf{P} \rightarrow \mathbf{T}$ and $\mathbf{B}^+ : \mathbf{T} \rightarrow \mathbf{P}$

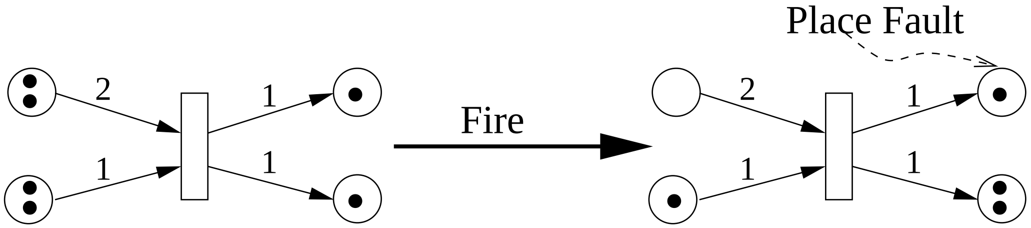
$$\mathbf{B}^+ = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{B}^- = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{B} \triangleq \mathbf{B}^+ - \mathbf{B}^- = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}$$

- State evolution: $\mathbf{q}_s[t+1] = \mathbf{q}_s[t] + \mathbf{B}\mathbf{x}[t], \quad \mathbf{q}_s \geq \mathbf{0}, \ \ \mathbf{x} \geq \mathbf{0}$

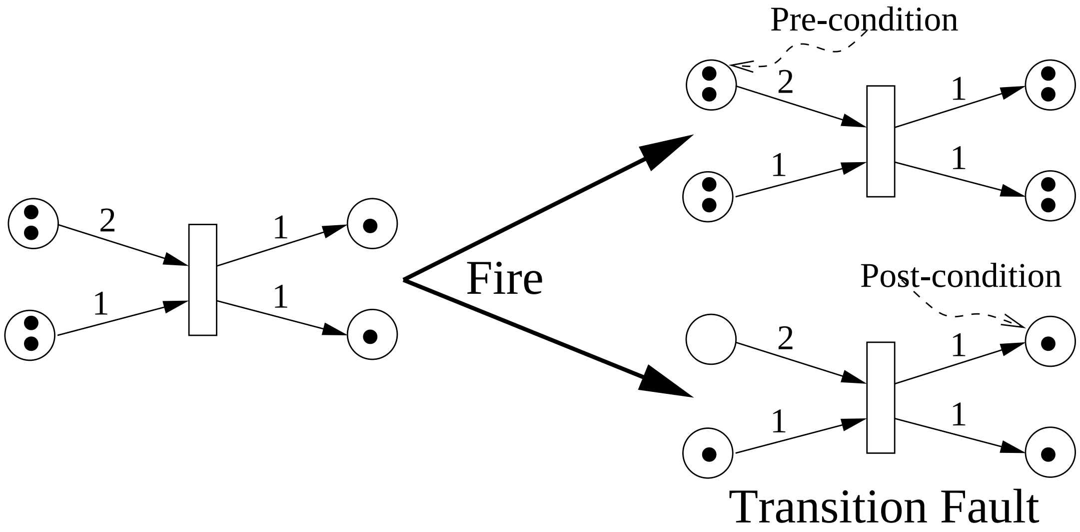
  $\mathbf{x}[t] \in \mathbb{N}_0^m$ denotes the firing vector (activity at time epoch $t$)

# FAULT MODEL

- Place fault: $\mathbf{q}_f[t] = \mathbf{q}_s[t] + \mathbf{e}_P, \quad \mathbf{e}_P = c\mathbf{U}_i, \quad 1 \leq i \leq n$

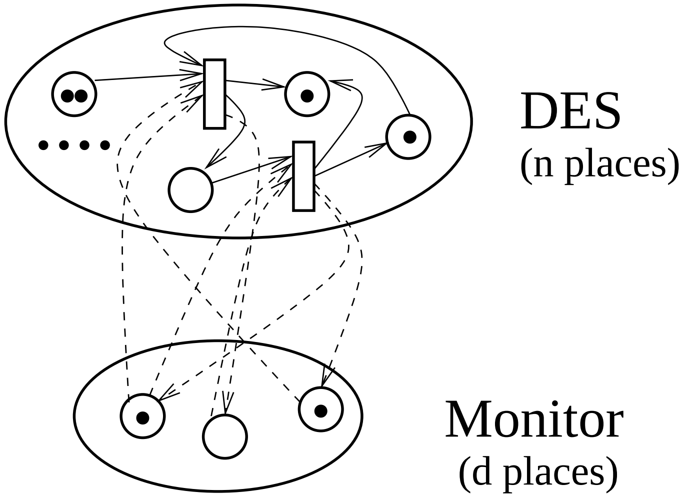


- Transition fault: $\mathbf{q}_f[t] = \mathbf{q}_s[t] - \mathbf{B}^+\mathbf{e}_T^+, \quad \mathbf{e}_T^+ = \mathbf{U}_j, \quad 1 \leq j \leq m$



# Monitoring using Separate Redundant Embeddings

## Petri Net Embedding



- Enforced encoding: $$\mathbf{q}_h[t] = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t]$$
- Evolution:

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

# SYNDROME CALCULATIONS

- Parity check: $\mathbf{s}[t] \overset{\triangle}{=} \mathbf{P}\mathbf{q}_f[t]$ where $\mathbf{P} = \left[\, -\mathbf{C} \;\; \mathbf{I}_d \,\right]$

- $\mathbf{s}[t]$ is zero if no fault (because $\mathbf{P}\mathbf{q}_h[t] = [-\mathbf{C} \;\; \mathbf{I}_d] \left( \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t] \right)$)

- With faults, $\mathbf{s}[t] = \mathbf{D}\mathbf{e}_T - \mathbf{C}\mathbf{e}_p$

$\mathbf{e}_T \in \mathbb{Z}^m$ indicator vector for transition faults ($m$-dimensional)
$\mathbf{e}_p \in \mathbb{Z}^n$ indicator vector for *plant* place faults ($n$-dimensional)

- Objective: Design $\mathbf{C}$ and $\mathbf{D}$ so that

Based on $\mathbf{s}[N]$ detect/identify multiple transition and/or place faults during [0, N]

# IDENTIFYING UP TO $k$ PLACE FAULTS

- Error syndrome

$$\mathbf{s}[N] = \mathbf{P}\mathbf{q}_f[N] = \begin{bmatrix} -\mathbf{C} & \mathbf{I}_d \end{bmatrix} \left( \mathbf{q}_h[N] + \begin{bmatrix} \mathbf{e}_P \\ \mathbf{0} \end{bmatrix} \right)$$

$$= -\mathbf{C}\mathbf{e}_P$$

- Assumption: No faults in monitoring places

- Choose $\mathbf{C}$ so that up to $k$ place faults can be detected/identified

  $(i) \Rightarrow$ Any $2k$ columns of $\mathbf{C}$ must be linearly independent

  $(ii) \Rightarrow \mathbf{C}$ must have at least $2k$ rows

  $(iii) \Rightarrow k \leq \frac{n}{2}$

# IDENTIFYING UP TO $k$ PLACE FAULTS (2)

- Matrix design: Vandermonde matrix in $GF(p)$

$$\mathbf{C}_k \triangleq \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \ldots & n^2 \bmod p \\ 1 & 2^3 \bmod p & 3^3 \bmod p & \ldots & n^3 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2k} \bmod p & 3^{2k} \bmod p & \ldots & n^{2k} \bmod p \end{pmatrix}$$

- Up to $k$ place faults are identifiable if $p \geq n$

- Identification methodology: BCH decoding algorithm

- Worst-case complexity for identification: $O(kn + k^3)$

## IDENTIFYING UP TO $k$ TRANSITION FAULTS

- Error syndrome

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

- Assumptions:

1. Total number of transition faults less than $k$: $\sum_{i=1}^{m} |e_T^i| \leq k$
2. No cancellations: $\min\{\mathbf{e}_T^+,\ \mathbf{e}_T^-\} = \mathbf{0}$

- Choose **D** so that up to $k$ transition faults can be detected/identified

# IDENTIFYING UP TO $k$ TRANSITION FAULTS (2)

- Matrix design: Vandermonde matrix in $GF(p)$

$$\mathbf{D}_k \triangleq \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 3 & \dots & m \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \dots & m^2 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^k \bmod p & 3^k \bmod p & \dots & m^k \bmod p \end{pmatrix}$$

- Up to $k$ transition faults are identifiable if $p \geq m$

- Identification methodology: Novel decoding algorithm

- Worst-case complexity for identification: $O(k^2 m)$

# SYNTHESIS FOR MIXED FAULTS

- Choose $p > \max(m, n)$, choose matrices

$$\mathbf{C}^* \triangleq p\mathbf{C}_k \ , \qquad \mathbf{D}^* \triangleq \mathbf{D}_{2k-1}$$

- Error syndrome

$$\mathbf{s}[N] = \mathbf{P}\mathbf{q}_f[N] = \mathbf{D}^*\mathbf{e}_T - \mathbf{C}^*\mathbf{e}_P$$

- Transition fault syndrome

$$\mathbf{s}_T \triangleq \mathbf{P}\mathbf{q}_f[N] \equiv \mathbf{D}^*\mathbf{e}_T \pmod{p}$$

- Place fault syndrome

$$\mathbf{s}_P \triangleq (\mathbf{D}^*\mathbf{e}_T - \mathbf{s})/p = (\mathbf{C}^*/p)\mathbf{e}_P = \mathbf{C}\mathbf{e}_P$$

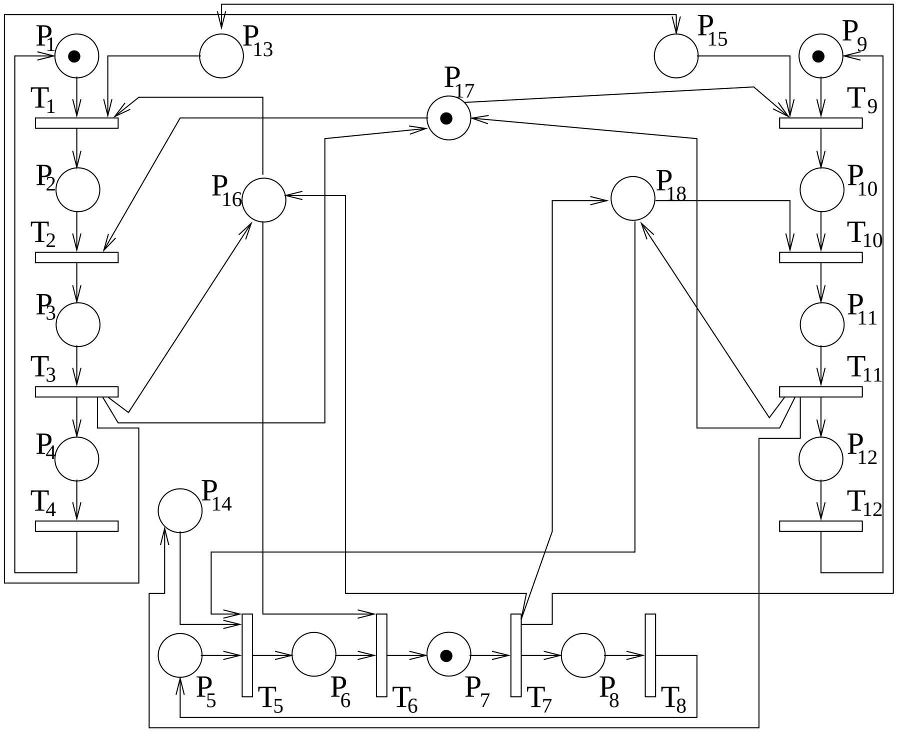
# MATRIX DESIGN SUMMARY

$$\mathbf{D}^* \triangleq \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 3 & \dots & m \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \dots & m^2 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2k-1} \bmod p & 3^{2k-1} \bmod p & \dots & m^{2k-1} \bmod p \end{pmatrix}$$

$$\mathbf{C}^* \triangleq p \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \dots & n^2 \bmod p \\ 1 & 2^3 \bmod p & 3^3 \bmod p & \dots & n^3 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2k} \bmod p & 3^{2k} \bmod p & \dots & n^{2k} \bmod p \end{pmatrix}$$

Note: $p$ is a prime number larger than both $m$ and $n$

# EXAMPLE: THREE MACHINES AND THREE ROBOTS



- Goal: Identify up to two transition faults and/or one place fault
- Example: Borrowed from Al-Jaar and Desrochers book
- $m = 12$, $n = 18 \Rightarrow p = 19$

# PARAMETER DESIGN

- Matrix design (with $p = 19$)

$$\mathbf{D}^* = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 & 11^2 & 12^2 \end{pmatrix} \pmod{19}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 9 & 16 & 6 & 17 & 11 & 7 & 5 & 5 & 7 & 11 \end{pmatrix}$$

$$\mathbf{C}^* = 19 \left[ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 & 11^2 & 12^2 & 13^2 & 14^2 & 15^2 & 16^2 & 17^2 & 18^2 \end{pmatrix} \pmod{19} \right]$$

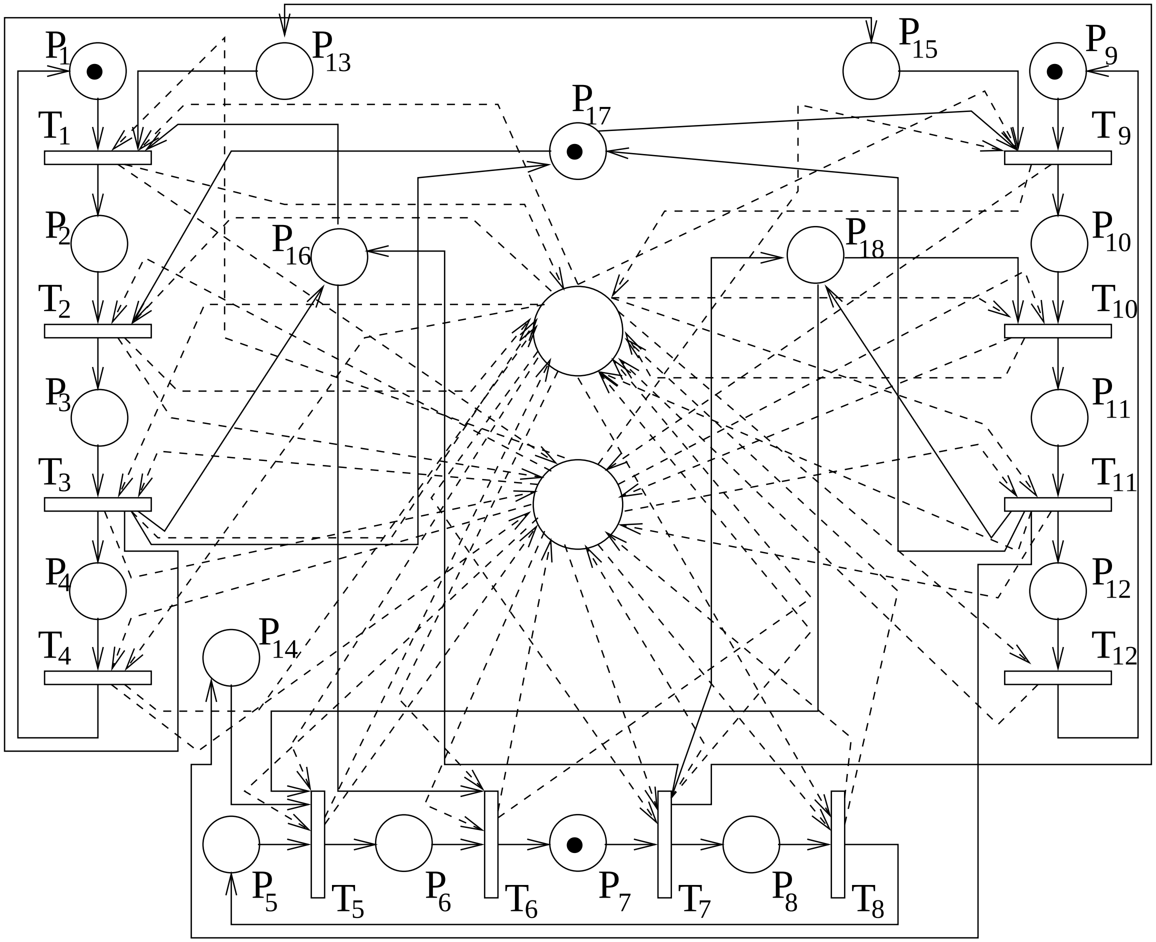
$$= \begin{pmatrix} 19 & 38 & 57 & 76 & 95 & 114 & 133 & 152 & 171 & 190 & 209 & 228 & 247 & 266 & 285 & 304 & 323 & 342 \\ 19 & 76 & 171 & 304 & 114 & 323 & 209 & 133 & 95 & 95 & 133 & 209 & 323 & 114 & 304 & 171 & 76 & 19 \end{pmatrix}$$

- Initial marking

$$\mathbf{q}_h[0] = \begin{bmatrix} \mathbf{I}_{18} \\ \mathbf{C}^* \end{bmatrix} \mathbf{q}_s[0]$$

$$= (1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 646\ 399)^T$$

# Monitor Construction



# FAULT DETECTION AND IDENTIFICATION

- Firing sequence, faults and state evolution

$$T_7 : \ \mathbf{q}_f[1] = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1 \quad 1558 \quad 836)^T, \quad \mathbf{q}_f[1] = \mathbf{q}_h[1]$$

$$T_1 : \ \mathbf{q}_f[2] = (0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \quad 1026 \quad 399)^T, \quad \mathbf{q}_f[2] = \mathbf{q}_h[2]$$

$$T_2 : \ \mathbf{q}_f[3] = (0\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1 \quad 1081 \quad 566)^T, \quad \text{Pre-condition fault at } T_2$$

$$T_8 : \ \mathbf{q}_f[4] = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1 \quad 1024 \quad 547)^T$$

$$T_3 : \ \mathbf{q}_f[5] = (0\ 1\ 0\ 1\ 1\ 0\ 2\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \quad 1955 \quad 1231)^T, \quad P_7 \text{ corrupted by } +2$$

$$T_9 : \ \mathbf{q}_f[6] = (0\ 1\ 0\ 1\ 1\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1 \quad 1185 \quad 761)^T, \quad \text{Post-condition fault at } T_9$$

- Resulting syndrome $\mathbf{s}[6] = [-\mathbf{C} \ \ \mathbf{I}_2]\mathbf{q}_f[6] = \begin{pmatrix} -259 \\ -417 \end{pmatrix}$

- Transition fault identification

$$\mathbf{D}\mathbf{e}_T \equiv \mathbf{s}[6] \equiv \begin{pmatrix} 7 \\ 1 \end{pmatrix} \quad \Longrightarrow \quad \mathbf{e}_T = \mathbf{U}_9 - \mathbf{U}_2$$

- Place fault identification

$$\mathbf{C}\mathbf{e}_P = (\mathbf{D}\mathbf{e}_T - \mathbf{s}[6])/p = \begin{pmatrix} 9-2-(-259) \\ 5-4-(-417) \end{pmatrix} /19 = \begin{pmatrix} 14 \\ 22 \end{pmatrix} = 2\mathbf{C}(:,7) \ \Longrightarrow \ \mathbf{e}_P = 2\mathbf{U}_7$$

# CONCLUSIONS

- Contribution:

  Fault detection and identification in discrete event systems using algebraic decoding techniques

- Highlights:
  - Non-concurrency
  - Multiple additive/mixed faults

- Remaining question: Complexity trade-off

# Transition Fault Identification Algorithm (1)

- Transition fault identification

$$\begin{cases} e_1 + e_2 + \ldots + e_k \equiv S_0 \\ e_1x_1 + e_2x_2 + \ldots + e_kx_k \equiv S_1 \\ e_1x_1^2 + e_2x_2^2 + \ldots + e_kx_k^2 \equiv S_2 \\ \vdots \\ e_1x_1^k + e_2x_2^k + \ldots + e_kx_k^k \equiv S_k \end{cases}$$

- Unknowns:

$$e_i \in \{-1, 0, 1\}, \;\; i = 1, 2, \ldots, k$$

$$x_i \in \mathrm{GF}(p), \;\; i = 1, 2, \ldots, k$$

- Identifiability: Equation array has at most one solution if $k \leq p$

- Equation array

$$\begin{cases} x_1 & +x_2 & +\ldots & +x_r & = S_1 \\ x_1^2 & +x_2^2 & +\ldots & +x_r^2 & = S_2 \\ & & & & \vdots \\ x_1^r & +x_2^r & +\ldots & +x_r^r & = S_r \end{cases}$$

- Definition $\Lambda_\tau(x_1, x_2, \ldots, x_r) \overset{\triangle}{=} (-1)^\tau \sum_{1 \le i_1 < i_2 < \ldots < i_\tau \le r} x_{i_1} x_{i_2} \ldots x_{i_\tau}, \quad \tau \le r$

- Newton's identity

$$\Lambda_\tau = \frac{1}{\tau!} \begin{vmatrix} S_1 & 1 & 0 & \ldots & 0 & 0 \\ S_2 & S_1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{\tau-1} & S_{\tau-2} & S_{\tau-3} & \ldots & S_1 & \tau-1 \\ S_\tau & S_{\tau-1} & S_{\tau-2} & \ldots & S_2 & S_1 \end{vmatrix}$$

- Solution

$$x^r + \Lambda_1 x^{r-1} + \Lambda_2 x^{r-2} + \ldots + \Lambda_{r-1} x + \Lambda_r = 0$$

- Decomposition

$$\begin{cases} x_1 & +x_2 & +\dots & +x_i & = S_1 & +x_{i+1} & +\dots & +x_k & \overset{\triangle}{=} S_1 + T_1 \\ x_1^2 & +x_2^2 & +\dots & +x_i^2 & = S_2 & +x_{i+1}^2 & +\dots & +x_k^2 & \overset{\triangle}{=} S_2 + T_2 \\ & & & & \vdots & & & & \\ x_1^k & +x_2^k & +\dots & +x_i^k & = S_k & +x_{i+1}^k & +\dots & +x_k^k & \overset{\triangle}{=} S_k + T_k \end{cases}$$

- Observation

$$\Lambda_j(x_1, x_2, \dots, x_i) = 0, \quad j = i+1, \dots, k$$

- Resulting equation array

$$\begin{vmatrix} S_1+T_1 & 1 & \dots & 0 & 0 \\ S_2+T_2 & S_1+T_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{j-1}+T_{j-1} & S_{j-2}+T_{j-2} & \dots & S_1+T_1 & j-1 \\ S_j+T_j & S_{j-1}+T_{j-1} & \dots & S_2+T_2 & S_1+T_1 \end{vmatrix} = 0, \quad j = i+1, \dots, k$$

# TRANSITION FAULT IDENTIFICATION ALGORITHM (2)

## Proposition (Algorithmic key)

$$\begin{vmatrix} S_1+T_1 & 1 & \dots & 0 & 0 \\ S_2+T_2 & S_1+T_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{r-1}+T_{r-1} & S_{r-2}+T_{r-2} & \dots & S_1+T_1 & r-1 \\ S_r+T_r & S_{r-1}+T_{r-1} & \dots & S_2+T_2 & S_1+T_1 \end{vmatrix}$$

$$= \sum_{i=0}^{r} \binom{r}{i} \begin{vmatrix} S_1 & 1 & \dots & 0 & 0 \\ S_2 & S_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{i-1} & S_{i-2} & \dots & S_1 & i-1 \\ S_i & S_{i-1} & \dots & S_2 & S_1 \end{vmatrix} \cdot \begin{vmatrix} T_1 & 1 & \dots & 0 & 0 \\ T_2 & T_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ T_{r-i-1} & T_{r-i-2} & \dots & T_1 & r-i-1 \\ T_{r-i} & T_{r-i-1} & \dots & T_2 & T_1 \end{vmatrix}$$