Stochastic Testing of Finite State Machines

Christoforos Hadjicostis

Decision and Control Laboratory
Coordinated Science Laboratory and Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Fault Diagnosis in FSM's

Finite state machine (FSM):

- States $Q = \{q_1, q_2, ..., q_N\}$
- Inputs $X = \{x_1, x_2, ..., x_K\}$

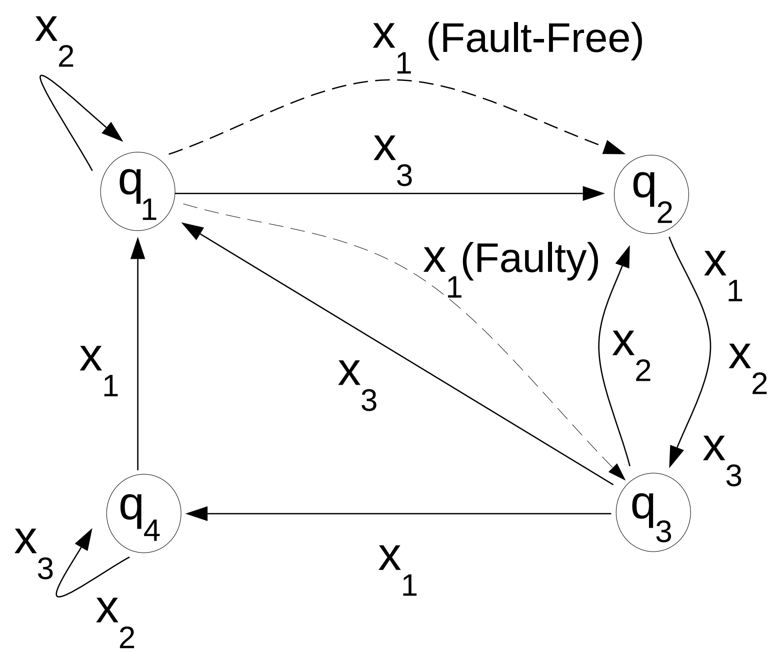
  (Outputs $Y = \{y_1, y_2, ..., y_L\}$)

- **Next-state mapping:**

  $q[k+1] = \delta(q[k], x[k])$

  (**Output mapping:**

  $y[k] = \lambda(q[k], x[k])$)



<u>Goal:</u> Detect permanent/transient fault(s) in next-state mapping

Variations of Basic Problem

- **Testing versus monitoring**
  - *Testing:* "Off-line," can control (choose) inputs (e.g., *testing sequence*)
  - *Monitoring:* "On-line," possible access to inputs (but no control)
- **Available observations**
  - Partial observations of input and state/output sequences
  - Partial, empirical averages about inputs, states and/or outputs
- **Deterministic framework**
  - Partial observations about input and state/output sequence (order is known)
  - *Optimize for:* (i) Fault coverage
    (ii) Testing sequence length
    (iii) Hardware overhead
- **Probabilistic framework**
  - Probabilistic machines, probabilistic diagnosis

Problem Formulation

$$\left.\begin{array}{c}\text{Deterministic FSM}\\ \text{Random (``white'') inputs}\end{array}\right\} \Rightarrow \text{Markov chain}$$

- **Available information:** Empirical frequencies of state occupancies
- **Goal:** Detect and identify *permanent* faults in next-state mapping of *underlying* FSM
- **Potential advantages:**
  - (i) No synchronization requirements
  - (ii) Exact order of inputs/outputs not required
  - (iii) Input not required (statistical characterization only)
  - (iv) Distributivity/observability constraints
- **Application domain:** Testing of digital systems, system diagnosis (e.g., manufacturing defects, design errors)

Related Previous Work

- **Deterministic setting (automata, languages)**
  - Conformance testing (Yannakakis)
  - Partial observations (Willsky, Varaiya, Schwartz)
  - Active diagnosis (Teneketzis, Kumar)
  - Time templates (Holloway)
- **Stochastic setting (hypothesis testing, stochastic systems)**
  - Probabilistic inference, alarm correlation (Hart, Bouloutas, Schwartz)
  - Change detection in stochastic systems (Lai, Nikiforov)
- **Main difference in our setting:**
  - Order of inputs *not* known
  - Order of states/outputs *not* known
  - **Caution:** Direct comparisons are difficult
    (*different* underlying assumptions)

TRANSITION MATRICES

N**-dimensional state vector:** $\mathbf{q}[k]$

$\mathbf{q}_i[k] = 1$ **iff** FSM is in state q_i at time step k

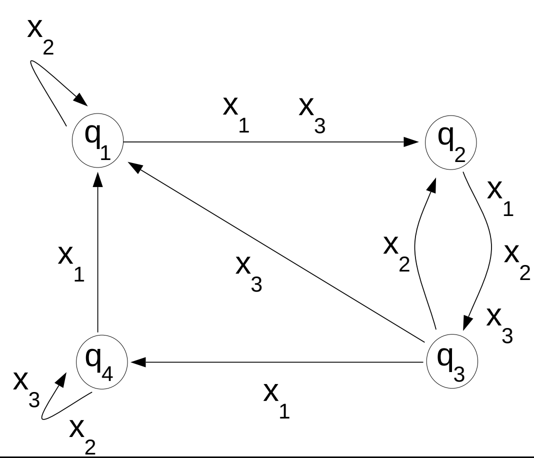
Example: $\mathbf{q}[0] = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}^T \Rightarrow$ state q_1 at time step 0

Next-state: $\mathbf{q}[k+1] = \mathbf{A}_i \mathbf{q}[k]$ **iff** $x[k] = x_i$

K **transition matrices:** $\mathbf{A}_1$, $\mathbf{A}_2$, ... $\mathbf{A}_K$ ($N \times N$, unique "1" in each column)

lth-jth entry of $\mathbf{A}_i$ is "1" **iff** $q_l = \delta(q_j, x_i)$

Example:



$$\mathbf{A}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Markov Chain Associated with FSM

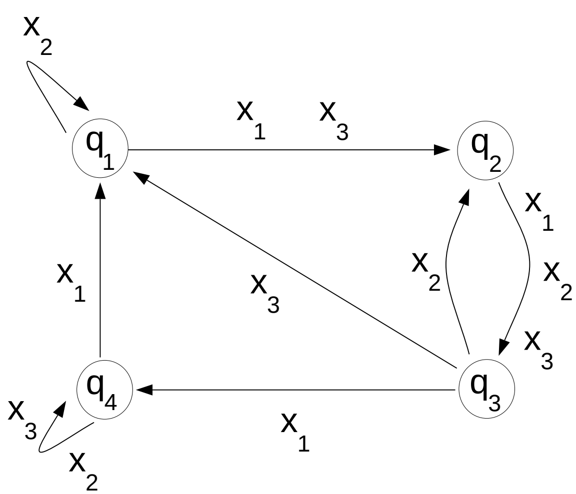
Assumptions: (i) "White" input: $x[k] = x_i$ with probability p_i

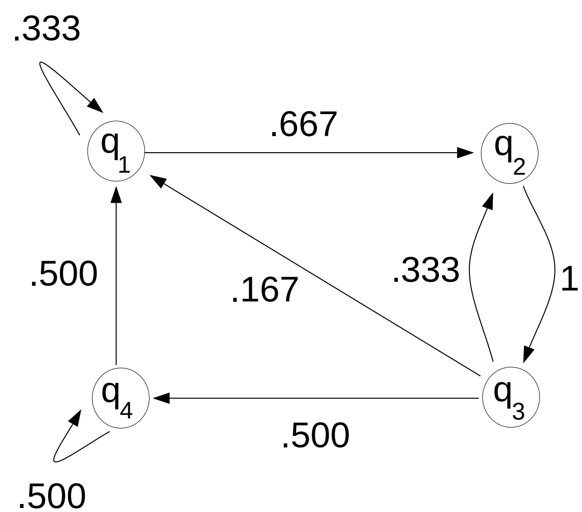
(ii) Probabilities independent of k and $\mathbf{q}[\cdot]$

(iii) $\sum_{i=1}^{K} p_i = 1$

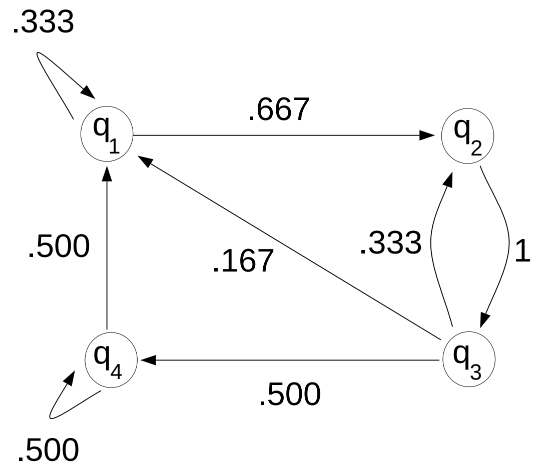
Behavior of FSM captured by Markov chain with $\boxed{\mathbf{A}_M = \sum_{i=1}^{K} p_i \mathbf{A}_i}$

<u>**Example:**</u> with $p_1 = \frac{1}{2}$, $p_2 = \frac{1}{3}$, $p_3 = \frac{1}{6}$





Steady-State Probabilities and Ergodicity



Interpretation: Weight captures transition probability (from one state to another)

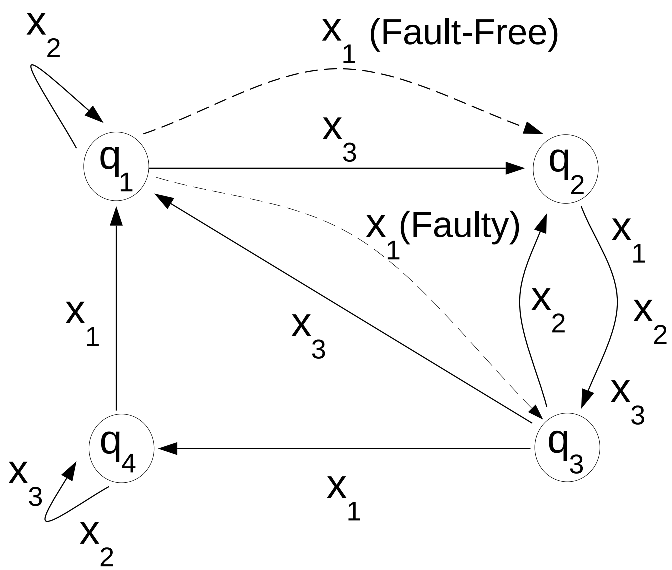
Steady-state probability vector v satisfies $\boxed{\mathbf{v} = \mathbf{A}\mathbf{v}}$

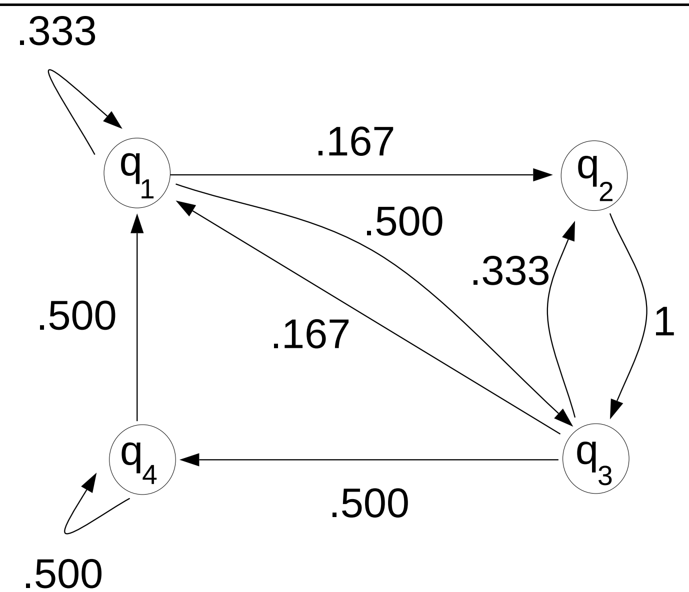
- Normalized so that $\sum_{j=1}^{N} \mathbf{v}_j = 1$
- Unique (mild assumptions)

Ergodicity (mild assumptions): machine eventually reaches steady-state

$\boxed{\text{state } q_j \text{ visited with frequency } \mathbf{v}_j}$

FAULTS IN UNDERLYING (DETERMINISTIC) FSM





New input transition matrix:

$$\mathbf{A}'_i = \mathbf{A}_i + \mathbf{E}_i$$

New Markov transition matrix:

$$\mathbf{A}'_M = \mathbf{A}_M + p_i\mathbf{E}_i$$

New Markov chain reaches new steady-state $\mathbf{v}'$

Goal: Detect and identify faults by looking at how $\mathbf{v}'$ deviates from $\mathbf{v}$

Perfect Knowledge of State Frequencies

Assumption: $\mathbf{v}'$ known exactly
(i.e., empirical frequencies = steady-state probabilities)

Definition of steady state $\mathbf{v}' = \mathbf{A}'_M \mathbf{v}' = (\mathbf{A}_M + p_i \mathbf{E}_i)\mathbf{v}'$ implies

$$\boxed{p_i \mathbf{E}_i \mathbf{v}' = (\mathbf{I}_N - \mathbf{A}_M)\mathbf{v}' = \mathbf{e}}$$

Single fault: From state q_j, input x_i takes transition to state q_m *instead of* q_l

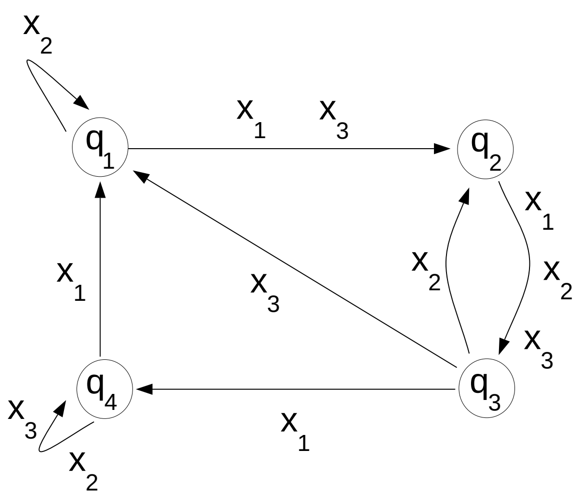
Structure of $\mathbf{E}_i$: Zeros everywhere except

- "+1" at mth-jth entry
- "-1" at lth-jth entry

Observation: $\mathbf{e}$ has exactly two non-zero entries
$\Rightarrow$ Structure of $\mathbf{E}$ can potentially be determined from $\mathbf{e}$

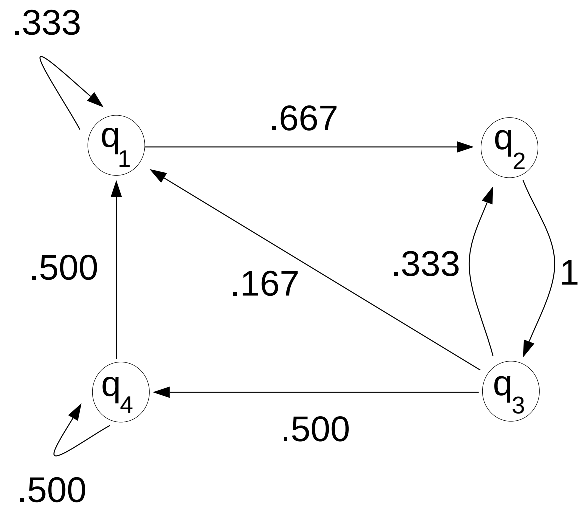
Caution: Estimate of $\mathbf{v}'$ is not perfect $\Rightarrow$ Confidence levels

Example (1)



FSM with input probabilities

$p_1 = \frac{1}{2}, \quad p_2 = \frac{1}{3}, \quad p_3 = \frac{1}{6}$



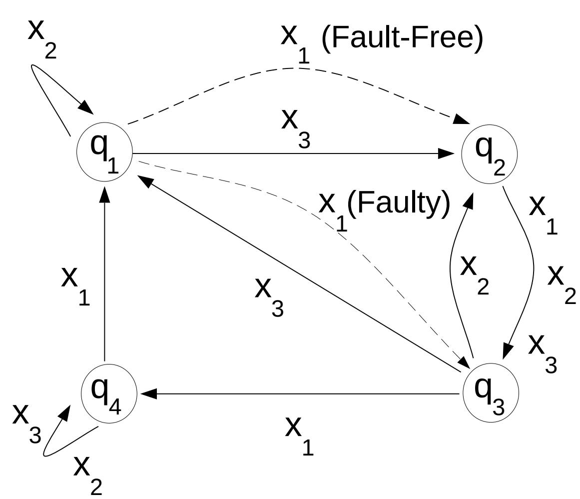
Markov chain with transition matrix

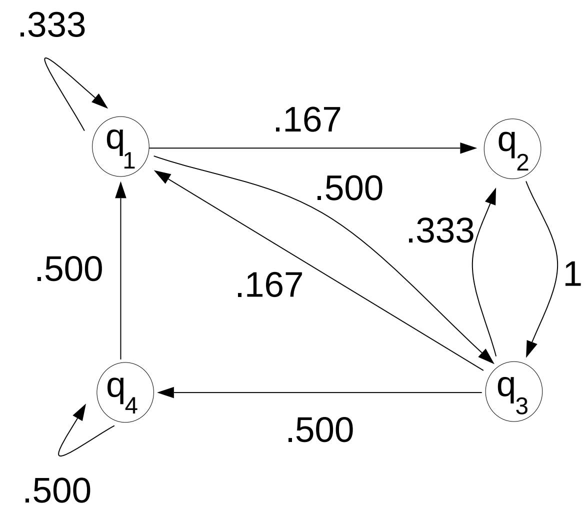
$$\mathbf{A}_M = \sum_{i=1}^{3} p_i \mathbf{A}_i = \begin{bmatrix} .333 & 0 & .167 & .500 \\ .667 & 0 & .333 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & .500 & .500 \end{bmatrix}$$

$$\mathbf{v}' = \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix}^T$$

States visited with equal frequencies

Example (2)





$$
\begin{aligned}
\mathbf{A}'_1 &= \mathbf{A}_1 + \mathbf{E}_1 \\
&= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}
\end{aligned}
$$

where $\mathbf{E}_1$ is given by

$$
\mathbf{E}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}
$$

Markov chain with transition matrix

$$
\begin{aligned}
\mathbf{A}'_M &= \mathbf{A}_M + p_1\mathbf{E}_1 \\
&= \begin{bmatrix} .333 & 0 & .167 & .500 \\ .167 & 0 & .333 & 0 \\ .500 & 1 & 0 & 0 \\ 0 & 0 & .500 & .500 \end{bmatrix}
\end{aligned}
$$

$$
\mathbf{v}' = \begin{bmatrix} 0.286 & 0.143 & 0.286 & 0.286 \end{bmatrix}^T
$$

State q_2 visited half as often

EXAMPLE (3)

$$\mathbf{e} = (\mathbf{I}_N - \mathbf{A}_M)\mathbf{v}' = \begin{bmatrix} 0 \\ -0.143 \\ 0.143 \\ 0 \end{bmatrix} .$$

Note: $0.143 = p_i \mathbf{v}'_j$ for *some* $i = 1, 2, 3$ and *some* $j = 1, 2, 3, 4$

Possible pairs: $(p_1, \mathbf{v}'_1)$, $(p_1, \mathbf{v}'_3)$, $(p_1, \mathbf{v}'_4)$

Physical considerations imply that only possibility is $(p_1, \mathbf{v}'_1)$

Conclusion: The next-state from state q_1 on input x_1 has been corrupted so that

$$\mathbf{E}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Conclusions and Future Work

Potential Advantages:

- Exact input sequence is *not* required (statistical characterization *is* required)
- No synchronization constraints
- Out-of-order observations acceptable (applications to networked systems)

Future Work:

- Deviations of empirical state frequencies from actual steady-state probabilities (large deviations, ergodic theory)
- Bounds on probability of error (Bayesian setting, confidence intervals)
- Bounds on length of observation window
- "Optimal set" of required statistical observations