Background

- Hardware redundancy techniques
  - Duplex
  - Triple Modular Redundancy (TMR)

Background

- Classical TMR reliability
  \[ R_m^3 + 3R_m^2(1 - R_m) \]
- Pessimistic
  - Compensating faults [Siewiorek 75]
  - Multiple faults [Stroud 94]
- Optimistic
  - Common-mode failures

Compensating faults

Common-Mode Failures

- CMFs [Lala 94]
  - Affects multiple copies simultaneously
  - Generally single cause
  - Reliability detractor
    - Nuclear reactors
    - Power supply
    - Computing systems
- Diversity
  - Antidote for CMFs [Jacobs 70]
Design Diversity
- Independent design [Avizienis 85]
- Software
  - N-version programming
- Hardware
  - Function and its dual [Tamir 84]
  - Three different processors
    - Boeing 777
- Evaluate diversity
  - No metric available

Multiple Failures
- Faults in multiple copies
  - Multiple event upsets (MEU)
  - Multiple errors from single event upset
- Effect of diversity
  - More compensating faults?

Motivation
- ROAR project
  - Reconfiguration capabilities
- Metric for design diversity
- Relationship between
  - Diversity
  - Reliability
  - Mission time
  - Availability
  - Failure rate

A Metric
- n input combinational logic function
- Two copies
- Fault $f_1$ in copy 1
- Fault $f_2$ in copy 2
  - Faulty circuits remain combinational
- $T(f_i) = \text{Test set for } f_i$
- $r(f_1, f_2) = 1 - q(f_1, f_2) = \frac{|T(f_1) \cap T(f_2)|}{2^n}$

Significance of $r$
- System with redundancy
  - Fault $f_1$ in first copy
  - Fault $f_2$ in second copy
  - Probability of incorrect output
- Applicable to 3 copies
- Faults considered for illustration
  - Single stuck-at

Example
- $n = 3, f_1 : D / 1, f_2 : E / 0$
- $T(f_1) = \{000, 010, 100\}$
- $T(f_2) = \{001, 011, 101, 111, 110\}$
- $T(f_1) \cap T(f_2) = \emptyset$
  - $r = 0, q = 1$
**Example**

- \( n = 3, f_1 : D / 0, f_2 : E / 0 \)
- \( T(f_1) = \{110\} \)
- \( T(f_2) = \{001, 011, 101, 111, 110\} \)
- \( T(f_1) \cap T(f_2) = \{110\} \)
- \( r = 1/8, q = 7/8 \)

**r Spectrum**

**r Histogram**

**Important Property**

- \( T(f_1) \supseteq T(f_1) \cap T(f_2) \)
- \( r(f_1, f_1) \geq r(f_1, f_2) \)
- \( q(f_1, f_1) \leq q(f_1, f_2) \)
- **Example: design faults**

**System Model**

**Reliability**

- **Two components**
  - \( f_1, f_2 \) appear simultaneously
  - \( f_1, f_2 \) do not appear simultaneously

\[
q(f_1, f_2) = 1 - \frac{|T(f_1) \cap T(f_2)|}{2^n}
\]
Design Diversity For Redundant Systems

Reliability - First Component
- \( f_1, f_2 \) appear simultaneously at instant \( i \)

![Reliability - First Component Diagram]

Reliability - Second Component
- \( f_1 \) appears before \( f_2 \)
- \( f_1 \) appears at instant \( i \)
- \( f_2 \) appears at instant \( j \)

![Reliability - Second Component Diagram]

Reliability Analysis — CMFs
\[
R_{\text{duplex}}[T] = e^{-XT} + \sum_{f_1, f_2} \Pr(f_1, f_2)(1 - e^{-X})q\frac{[q^T - e^{-XT}]}{[q - e^{-X}]}
\]

![Reliability Analysis — CMFs Diagram]

Reliability Improvement
- Unreliability with \( q = 0.9 \)
- Unreliability with \( q = 0.99 \)
- Ratio gives reliability improvement

![Reliability Improvement Diagram]

Availability
\( q_1 = 1 - \frac{T(f_1) \cup T(f_2)}{2^n} \)

![Availability Diagram]

Availability Comparison
- \( q = 0.9 \)
- \( q = 0.99 \)

![Availability Comparison Diagram]
Design Diversity For Redundant Systems

Self-Testing Property

- Fault $f_1$ in copy 1
- Fault $f_2$ in copy 2
- $T(f_i) = \text{Test set for } f_i$
- $T(f_i) = T(f_j)$
  - Not self-testing when $f_1$, $f_2$ present
  - Equivalent fault pairs
  - Minimize # such pairs

Example

- Equivalence classes
  - $S_1 = \{A/0, B/0, D/0\}$, $S_2 = \{C/1, D/1, E/1\}$
  - $S_3 = \{A/1\}$, $S_4 = \{B/1\}$, $S_5 = \{C/0\}$, $S_6 = \{E/0\}$
- # equivalent fault pairs
  - $3 \times 3 + 3 \times 3 + 1 + 1 + 1 + 1 = 22$

Simulation-Based Approach

- Multiple stuck-at faults
  - Exponential
- Calculation of $q$ values
  - Exponential
- $q$ values change dynamically
  - When multiple faults arrive

Simulation

- Benchmark circuits
- Synthesis of diverse copies
  - True and complemented truth tables
  - More diversity in future
  - Two-level minimization
  - Multi-level transformations
  - Mapped to G10p library

Designs

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th># Inputs</th>
<th># Outputs</th>
<th># SSF (True)</th>
<th># SSF (Complement)</th>
</tr>
</thead>
<tbody>
<tr>
<td>z5sp1</td>
<td>7</td>
<td>10</td>
<td>550</td>
<td>610</td>
</tr>
<tr>
<td>apex4</td>
<td>9</td>
<td>19</td>
<td>9636</td>
<td>8578</td>
</tr>
<tr>
<td>clip</td>
<td>9</td>
<td>5</td>
<td>698</td>
<td>664</td>
</tr>
<tr>
<td>inc</td>
<td>7</td>
<td>9</td>
<td>486</td>
<td>506</td>
</tr>
<tr>
<td>rd64</td>
<td>8</td>
<td>4</td>
<td>509</td>
<td>398</td>
</tr>
</tbody>
</table>

Simulation 1

- Multiple independent failures
- TMR systems
- 100,000 simulations
- Random variable for fault arrival
  - Proportional to module size
- Random variable for affected lead
- Random counter seed
- Report Mean Time To Failure (MTTF)
Results

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>TMR #</th>
<th>Copies</th>
<th># SSFs</th>
<th>MTTF (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z5xp1</td>
<td>1</td>
<td>T, T, T</td>
<td>1650</td>
<td>4711</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>T, C, C</td>
<td>1390</td>
<td>4612</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>T, T, C</td>
<td>1770</td>
<td>4628</td>
</tr>
<tr>
<td>apex4</td>
<td>4</td>
<td>T, T, T</td>
<td>28903</td>
<td>540</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>T, C, C</td>
<td>27550</td>
<td>516</td>
</tr>
<tr>
<td>clip</td>
<td>6</td>
<td>T, T, T</td>
<td>2034</td>
<td>4626</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>T, T, C</td>
<td>2060</td>
<td>4628</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>T, T, T</td>
<td>1545</td>
<td>6153</td>
</tr>
<tr>
<td>inc</td>
<td>9</td>
<td>C, C, C</td>
<td>1518</td>
<td>5785</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>T, T, T</td>
<td>1478</td>
<td>5978</td>
</tr>
<tr>
<td>rd84</td>
<td>11</td>
<td>T, T, T</td>
<td>1794</td>
<td>5639</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>C, C, C</td>
<td>1194</td>
<td>6681</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>T, T, C</td>
<td>1534</td>
<td>5380</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>C, C, T</td>
<td>1364</td>
<td>5735</td>
</tr>
</tbody>
</table>

Dependence on module reliabilities

Simulation 2
- Multiple independent failures
- TMR system
- 100,000 simulations
- Random variable for fault arrival
  - Constant
- Random variable for affected lead
- Random counter seed
- Report Mean Time To Failure (MTTF)

Results

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>TMR #</th>
<th>Copies</th>
<th>MTTF (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z5xp1</td>
<td>1</td>
<td>T, T, T</td>
<td>63572</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>T, C, C</td>
<td>63467</td>
</tr>
<tr>
<td>apex4</td>
<td>3</td>
<td>T, T, T</td>
<td>95505</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>T, C, C</td>
<td>95652</td>
</tr>
<tr>
<td>clip</td>
<td>5</td>
<td>T, T, T</td>
<td>79594</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>T, T, C</td>
<td>74954</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>T, T, T</td>
<td>74964</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>C, C, C</td>
<td>71462</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>T, T, C</td>
<td>73410</td>
</tr>
<tr>
<td>inc</td>
<td>10</td>
<td>T, T, T</td>
<td>73331</td>
</tr>
<tr>
<td>rd84</td>
<td>11</td>
<td>C, C, C</td>
<td>66005</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>T, T, C</td>
<td>63931</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>C, C, T</td>
<td>64771</td>
</tr>
</tbody>
</table>

Diversity does not always help

Results

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>TMR #</th>
<th>Copies</th>
<th>MTTF (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z5xp1</td>
<td>1</td>
<td>T, T, T</td>
<td>3396</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>T, T, T</td>
<td>3389</td>
</tr>
<tr>
<td>apex4</td>
<td>3</td>
<td>T, T, T</td>
<td>3658</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>T, T, C</td>
<td>3967</td>
</tr>
<tr>
<td>clip</td>
<td>5</td>
<td>T, T, T</td>
<td>3747</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>T, T, C</td>
<td>3776</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>T, T, T</td>
<td>5277</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>T, T, C</td>
<td>4648</td>
</tr>
<tr>
<td>inc</td>
<td>9</td>
<td>T, T, T</td>
<td>4772</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>T, T, C</td>
<td>3741</td>
</tr>
</tbody>
</table>

Significance of \( q \) metric

Simulation 3
- 100,000 simulations
- TMR system
- Random fault triples
- Report error latency

Results

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>TMR #</th>
<th>Copies</th>
<th>Latency (cycles)</th>
<th>% compensating fault triples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z5xp1</td>
<td>1</td>
<td>T, T, T</td>
<td>3389</td>
<td>33.76</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>T, T, T</td>
<td>3568</td>
<td>35.49</td>
</tr>
<tr>
<td>apex4</td>
<td>3</td>
<td>T, T, T</td>
<td>3658</td>
<td>35.49</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>T, T, C</td>
<td>3967</td>
<td>0</td>
</tr>
<tr>
<td>clip</td>
<td>5</td>
<td>T, T, T</td>
<td>3747</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>T, T, C</td>
<td>3776</td>
<td>53.32</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>T, T, T</td>
<td>5277</td>
<td>52.29</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>T, T, C</td>
<td>4648</td>
<td>46.34</td>
</tr>
<tr>
<td>inc</td>
<td>9</td>
<td>T, T, T</td>
<td>4772</td>
<td>47.37</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>T, T, C</td>
<td>3741</td>
<td>37.02</td>
</tr>
</tbody>
</table>

Simulation 4
- CMFs in duplex system
- Replicated systems
  - Corresponding faults
  - Report error latency
- Diverse systems
  - No known model
  - Many possible candidates
  - Report error latency
  - Averaged over candidates
  - Unbiased estimation
Design Diversity For Redundant Systems

### Results

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>Duplex #</th>
<th>Copies</th>
<th>Error Latency (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z5xp1</td>
<td>1</td>
<td>T, T</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>T, C</td>
<td>6669</td>
</tr>
<tr>
<td>apex4</td>
<td>3</td>
<td>T, T</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>T, C</td>
<td>3006</td>
</tr>
<tr>
<td>clip</td>
<td>5</td>
<td>T, T</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>T, C</td>
<td>7669</td>
</tr>
<tr>
<td>inc</td>
<td>7</td>
<td>T, T</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>T, C</td>
<td>7516</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>T, C</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>T, T</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>T, C</td>
<td>6797</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>C, C</td>
<td>24</td>
</tr>
</tbody>
</table>

Results

Diversity helpful for CMFs

### Simulation 5

- Self-testing property
- Duplex system
  - Replicated system
  - CMFs undetectable
- Report % detectable fault pairs

### Conclusions

- New design diversity metric $q$
- Simple relationship between
  - Reliability, availability
  - Metric $q$
  - Mission Time
  - Failure Rate
- Common-mode failures
  - Diverse designs better
    - Bounded mission time

### References