EC500
Design of Secure and Reliable Hardware

Lecture 4

Mark Karpovsky

Error Models

Chip-Level Models

Let $\tilde{y}$ be a $(T \times n)$ binary output matrix possibly distorted by error. T is the number of input vectors and n is the number of primary outputs. Similarly, y is a $(T \times n)$ binary matrix of fault free responses and $E = \tilde{y} \oplus y$ is an error matrix, then $E = \begin{bmatrix} e(1) \\ e(2) \\ \vdots \\ e(T) \end{bmatrix}$. $y(t), \tilde{y}(t), e(t) \in F_q^n$.

Uniform errors

All $E \neq 0$ are equiprobable

Correlated errors

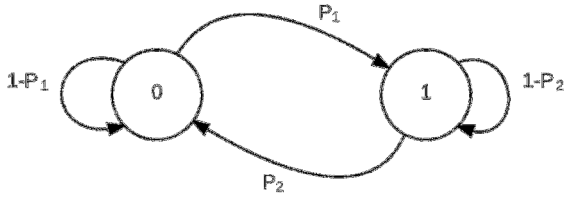
Temporal Models

a. **Time Independent Errors**

$e(t), t = 1,2, \ldots, T$ are statistically independent. Most popular model for combinational devices, random test.

b. **Time Correlated Errors**

Markov Chain Model



$0 -$ no errors
$1 -$ error

$$P_1 = Prob(e(t+1) \neq 0 | e(t) = 0)$$
$$P_2 = Prob(e(t+1) = 0 | e(t) \neq 0)$$

Difficult to compute (P_1, P_2)

c. **Lazy Errors**

A channel is lazy if P_2 is close to 1 (errors are repeating with high probability)

d. **Burst Errors**

A burst error is an error that will distort not more than consecutive bits of length b.

Spatial Models

Space Independent Errors

Let $\|e(t)\| = l$

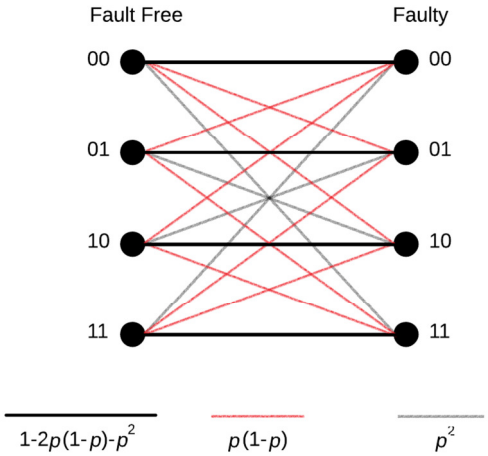
$\|e(t)\| = l$ is the number of ones in $e(t)$ (Hamming norm of $e(t)$), number of bits at the output distorted at moment t

For any l:

$Prob\{\|e(t)\| = l\} = \binom{n}{l} p^l (1-p)^{n-l}$, where p is the bit distortion rate and $Prob(0 \to 1) = Prob(0 \to 1)$ distortions.

This model is efficient for networks with limited fanouts.

Example: Independent Errors ($n = 2$)



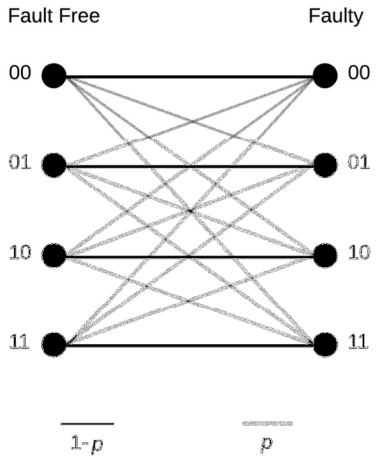
Space Symmetrical Models

a. For any t:
All $e(t) \neq 0$ are equiprobable.

$$Prob\{e(t) = i\} = \begin{cases} 1 - (2^n - 1)p & , i = 00 \ldots 0 \\ p & , i \neq 00 \ldots 0 \end{cases}$$

Space symmetrical model is very popular. This model is efficient for networks with large fanouts.

Example: Symmetrical Errors ($n = 2$)



b. Space Errors of a Given Magnitude
For any t:

$$Prob\{e(t) = i\} = \begin{cases} 1 - p, i = 0 \ldots 0 \\ p, i = a \\ 0, otherwise \end{cases}$$ for some n-bit vector a

This model is efficient for networks where every fault affects only a fixed set of ouputs for all input vectors.

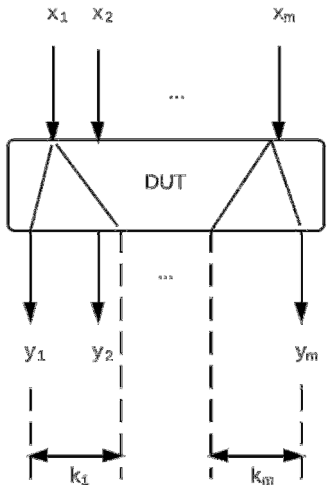
General Spatial Model

$\{P_0, P_1, \ldots, P_{2^n-1}\}$ – error distribution in space
$P_0 = Prob\{e(t) = 0\}$ – no errors
$P_1 = Prob\{e(t) = i\}$

Space error distribution is difficult to compute. It depends on a DUT and the input for the DUT.

Computation of Space Error Distributions

Let k_i outputs depend on x_i for the DUT.



k_i is the size of dependence cone for input x_i, $(i = 1, 2, \ldots, m)$

Then, the number of different error patterns N_e due to single stuck-at faults is uppderbounded by $N_e \leq \sum_{i=1}^{m}(2^{k_i} - 1)$

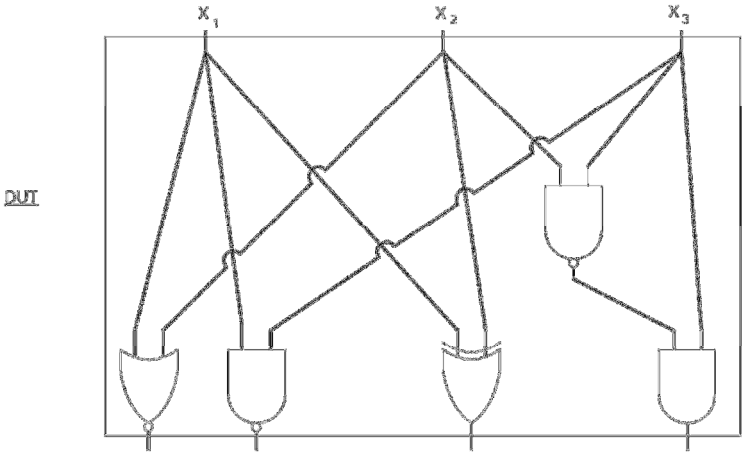
Example:
$m = 32$, $n = 32$, $\max_i k_i = 10$
$N_e \leq 32 \times (2^{10} - 1) \ll 2^{32}$

Improvement for the Upperbound on N_e

Let Y_i be the set of outputs that depend on input x_i, $(i = 1, 2, \ldots, m)$
Let $|Y_i| = k_i$, $|Y_i \cap Y_j| = k_{ij}$, $|Y_i \cap Y_j \cap Y_r| = k_{ijr}$, ...
Then, $N_e \leq \sum_i(2^{k_i} - 1) - \sum_{i,j}(2^{k_{ij}} - 1) + \sum_{i,j,r}(2^{k_{ijr}} - 1) - \cdots$

Time independent, space symmetrical models are the most popular models.

Example: Single Stuck-at Faults



$N_e \leq (2^3 - 1) + (2^3 - 1) + (2^2 - 1)$
$k_1 = 3,\ k_2 = 3,\ k_3 = 2$
$k_{12} = 2,\ k_{13} = 1,\ k_{23} = 1,\ k_{123} = 0$

$$N_e \leq \sum_i (2^{k_i} - 1) - \sum_{i,j} (2^{k_{ij}} - 1) + \sum_{i,j,r} (2^{k_{ijr}} - 1) - \cdots$$

For the previous example,

$$N_e \leq [(2^3 - 1) + (2^3 - 1) + (2^2 - 1)] - [(2^2 - 1) + (2^1 - 1) + (2^1 - 1)] + (2^0 - 1) = 12$$

Board or System Level Error Models

Independent Errors

Probability of l component being faulty is $\binom{S}{l} p^l (1-p)^{S-l}$, where

$S -$ is the size of a board or system

$p -$ probability of an error at the output of a component

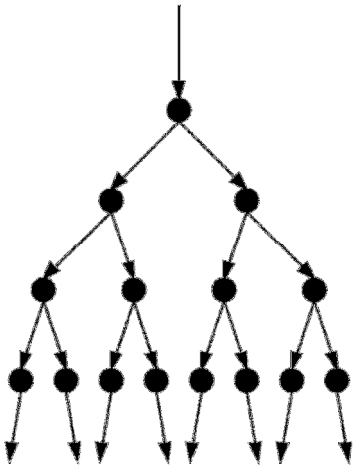
(p can be computed by using one of the chip level error models)

Conclusion on Chip Level Error Models

Space independent model predicts maximum probability of missing an error (pessimistic estimation) and space symmetrical model predicts minimum hrobablity of missing(optimistic estimation). Symmetrical model predicts in large networks more precisely than other models.

System Correlated Errors
Equiprobable single node failures.

Example: Tree Processor



Possible error patterns are:

10000000
01000000
00100000
00010000
00001000
00000100
00000010
00000001
11000000
00110000
00001100
00000011
11110000
00001111
11111111

In this table, 1 indicates that output of the corresponding processor is distorted.

All errors due to a fault is a single node of in a single link are equiprobable.

Errors in y_i are distributed according to one of the chip error models!