# EXAM–3 Fault Tolerant Systems 05/13/2002

## READ CAREFULLY BEFORE BEGINNING

1. This exam comprises 25% for 400 level, 20% for 500 level of your total grade. Points are indicated for each question/section.
2. This is an **open book/notes** exam.
3. This is an 1 hour exam but you have 2 hour to finish.
4. Make sure your copy has **6** questions.
5. Read each question completely before answering. Be sure you understand all assumptions and constraints.
6. **Show all work and state all assumptions**. Partial credit can not be given for work not shown. Use the back of the page, if necessary.

| | |
|---|---|
| REG MAXIMUM | 100 |
| DEDUCTIONS | − |
| **TOTAL SCORE** | |

PRINTED NAME _____

SIGNATURE _____

1. (10) Assume a critical application needs 4 fail-stop-processors (FSP) to function, i.e. there must be $\geq 4$ good FSPs. If we want to tolerate 2 faults, how many p-processors and s-processors do we need if faults must be assumed independent?

2. (20) With respect to the Boeing 777 flight control (paper by Bob Yeh):

   (a) How are *Byzantine faults* dealt with? Can the triple-TMR handle such faults? Justify your answer.

   (b) Show a scenario that indicates the *maximum* number of faults the triple-triple redundant system could possibley handle and still function correctly.

   (c) Now show a scenario that indicates the *minimum* number of faults that could cause the triple-triple redundant system to fail. (Note, this is a very different scenario from the previous question.)

   (d) What happens if more than the previous number of processors would fail? Does the plane crash, or is there an alternative? (justify your answer!!)

   (e) Assume the flight computer configuration is changed from a triple-triplex to a dual-quadruplex, i.e. two 4MRs. Recall, that a 4MR in this context is nothing but a 2-of-4 configuration. Now, consider benign and symmetric faults. Draw the Petri-net of this system.

3. (20) A system consists of processing units numbered $U_0, ..., U_7$ configured as a ring. The connection assignment for the PMC diagnosability model is that each unit tests its successor in the ring.

   (a) If, at most, two units are faulty, is this ring (in general) one-step 2-fault-diagnosable? Justify your answer.

   (b) Given that $U_0$ and $U_2$ are faulty, show how these two faults are diagnosed by using syndromes. Show your steps.

   (c) In the Adaptive Distributed System Diagnostics of Bianchini and Buskens, what would be the value of the TESTED_UP$_3$ array? Assume that $U_0$ and $U_2$ are faulty.

4. (20) With respect to RAID storage:

   (a) Assume we have a total of $N$ identical disks ($N$ is even) in a RAID level 1 configuration and that the MTTF for a single disk is given. Now assume that this RAID system is at a remote location with no access for repair. The drive mirror mapping is such that drive $i$, $1 \leq i \leq N/2$, is mirrored to drive $i + N/2$. What is the probability that this system will fail within $t$ hours? This is unreliability $F(t)$. Hint, think of a RAID level 1 using minimal $N$ and go from there.

   (b) What level of redundancy is assume in a RAID level 0 system?

   (c) What is the main advantage of using interleaving at the sector level over interleaving at the bit level? Indicate which RAID level uses which interleaving approach.

   (d) Draw a Petri-Net for a RAID level 5 with a total of $N$ drives, assuming we are given fail rate $\lambda$ and repair rate $\rho$.

5. (20) With respect to agreement:

   (a) State the minimum number of processors and round used for

      i. Lamport's model (Oral Messages)

      ii. Thambiturai & Park Model

   (b) Which of the two models above results in better reliabilities? Justify your answer – you may use an example fault scenario.

   (c) Using Lamport's OM(m) algorithm, what is the number of messages that are sent in the *simplex* scenario (remember that implies a single initial general) if we want to tolerate 5 faults?

   (d) Does running a "simplex agreement" on a critical task imply fault-tolerance or what does it take to actually achieve fault tolerance?

6. (10) We have considered diagnosability of a ring, which is a graph $G = (V, E)$ where $V$ is the set of $n$ vertices (units) and $E$ the set of $N$ edges (test assignments). Now consider an extension, called power graph, which is denoted by $G^p$. Assume that $G^p$ is an undirected graph, i.e. the edges are undirected. The $p$th power $G^p$ of $G$ has the same vertex set $V$, and nodes $u$ and $v$ are adjacent in $G^p$ if their distance in $G$ is at most $p$. You can envision $G^p$ as a "ring" where each vertex is connected to $p$ neighbor vertices in each direction. Note, that $G^1$ is a simple ring.

   (a) Draw the graph $G^2$ for $V = \{v_0, v_1, ..., v_7\}$.

   (b) Derive an explicit formula for the number of tests (test-count $c$) performed in a diagnosability scenario which uses $G^p$ as the test assignment graph, assuming one edge constitutes one test.

   (c) What is the connectivity $C$ of the $G^p$?

   (d) Is $G^p$ a regular graph? Justify your answer.

# extra work sheet