Aula 3 - Diagnósticos em nível de sistema

Wednesday, March 9, 2016 14:02

System-level Diagnosis

Uma teoria antiga: o primeiro modelo é de 1967.
Antes: esforços para diagnóstico de falhas de componentes do hardware

Existem limites óbvios ao diagnóstico.

- Unidades trocam rapidamente de estado
- Todas as unidades estão falhas

Diagnóstico é baseado em TESTES.

Um teste é um procedimento, uma bateria de testes, que permitem determinar o estado da unidade testada.

O primeiro modelo de diagnóstico: PMC (iniciais dos autores: Preparata, Metze, Chien)

Um sistema S = $\{u_1, u_2, \ldots, u_n\}$ consiste de N unidades que não podem ser decompostas.
Estados: uma unidade pode estar em um de dois estados: falha (faulty) ou sem-falha (fault-free)

Uma unidade sem-falha executa corretamente.

Uma unidade sem-falha executa corretamente.
Por outro lado, uma unidade falha tem comportamento arbitrário.

Uma premissa importante do modelo PMC:
Uma unidade sem-falha executa testes "perfeitos": determina com precisão se a unidade tes stada está falha ou sem-falha e reporta resultados de testes com precisão.

No contexto de sistemas distribuídos, a execução de testes envolve trocas de mensagens e ex xecução de tarefas. Pense na premissa do modelo PMC no contexto de sistemas síncronos (OK! Impleme ntável) e assíncronos (impossível diferenciar uma unidade falha de uma unidade lenta).
Assim, por enquanto consideramos apenas sistemas síncronos.

O que é possível determinar na execução de testes no modelo assíncrono? É possível determi inar com precisão se a unidade testada está sem falha. Se a resposta não chega, a unidade está suspe eita de falha.

Outra premissa do PMC:
Uma unidade não muda de estado antes do diagnóstico completar. Não é possível garantir is sso num sistema real, então o resultado um teste realizado durante uma mudança de estado deve se r descartado.

No modelo PMC, as unidades executam testes entre si, de acordo com um "assinalamento d le testes" (*testing assignment*) e reportam os resultados dos testes para um observador central, entida ade fora do sistema. Esta unidade central processa os resultados dos testes e completa o diagnóstico: de etermina quais unidades estão falhas/sem-falhas.

Síndrome do sistema: conjunto dos resultados de todos os testes realizados.

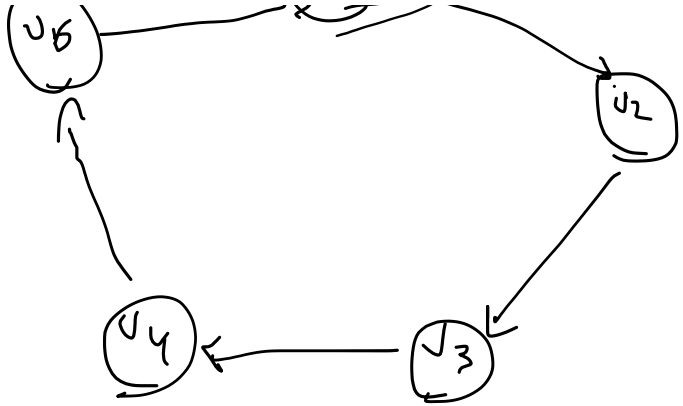
Se a unidade i testa a unidade j, o resultado de teste r_{ij}.

$r_{ij} = 0$ se u_i está sem-falha
e u_j está sem-falha

$r_{ij} = 1$ se u_i está sem-falha
e u_j está falha

$r_{ij} = *$ se u_i está falha

Exemplo



O assinalamento de testes pode ser representado como um grafo direcionado $G = (V, E)$, V é o conjunto de unidades e ∃ arco (i, j) se a unidade i testa a unidade j.

Síndrome deste sistema:

$\{*, 0, 0, 0, 1\}$ -> $\{0, 0, 0, 0, 1\}$ ou $\{1, 0, 0, 0, 1\}$

Se o número de falhas é limitado, i.e. $t = 1$

No exemplo é possível provar que, se $t = 1$, então este assinalamento permite identificar co rretamente TODAS as situações de falhas possíveis.

Diagnosability
O número máximo de unidades que podem estar falhas e o diagnóstico completa corretame nte.

Em 1974, Hakimi & Amin provaram que um sistema no modelo PMC é t-diagnosticável se

1. $N \geq 2t + 1$
2. Cada unidade é testada por pelo menos t testadoras.
3. Duas unidades não se testam mutuamente.

Exercício/exemplo

Projete um sistema 2-diagnosticável