Dependability

Arquitetura de Computadores

Emilio Francesquini
e.francesquini@ufabc.edu.br

2020.Q1

Centro de Matemática, Computação e Cognição
Universidade Federal do ABC

Disclaimer

UFABC

- Estes slides foram preparados para o curso de Arquitetura de Computadores na UFABC.
- Este material pode ser usado livremente desde que sejam mantidos, além deste aviso, os créditos aos autores e instituições.
- O conteúdo destes slides foi baseado no conteúdo do livro *Computer Organization And Design: The Hardware/Software Interface*, 5th Edition.
- Contém algumas figuras por Silberschatz, Galvin e Gagne [SGG] e Tanenbaum e Bos [TB].

Uma hierarquia de memória da qual podemos depender

- *Dependability*
  - Traduções possíveis (nenhuma amplamente aceita): fiabilidade, fidelidade, segurança, ”dependabilidade” 
  - Indica, simplesmente, o quanto podemos depender de um serviço, tecnologia, ...

Vocês vão perceber que ao contrário das demais aulas, nesta aula preferiremos os termos em inglês por não haver um consenso para boa parte das traduções.

Failures

- Podemos modelar os *serviços* (vistos de maneira geral como software, hardware, ...) com dois estados em relação ao serviço prestado:
  1. Serviço completado com sucesso: o serviço é entregue conforme esperado
  2. Serviço interrompido: o serviço não é entregue conforme especificado
- *Failures* (falhas, erros) causam a transição de um serviço de do estado 1 para o estado 2.
  - Transientes ou Permanentes
- *Restorations* (reparos, restaurações) causam a transição de um serviço do estado 2 para o estado 1.

- Reliability (confiabilidade) - é uma medida objetiva que indica a continuidade do serviço que está sendo prestado com sucesso a partir de um ponto de referência.
  - Não confundir com *dependability* que traduzimos como fiabilidade, fidelidade...)
- MTTF - *Mean Time To Failure*: é o tempo médio, de um estado de funcionamento do sistema até a ocorrência da próxima falha.
- AFR - *Annual Failure Rate*: percentual de dispositivos que se espera falhar em um período de um ano.

MTTF *vs.* AFR para discos rígidos

UFABC

- Muitos discos hoje relatam um MTTF de 1.000.000 horas
  - $1.000.000/24/365 \approx 114$ anos
  - Parece que nunca falhariam, certo?
- Considere um data center com 50.000 computadores
  - Cada computador com 2 discos
- O AFR será:
  - 1 ano $= 365 \times 24 = 8.760$ horas
  - Um MTTF de $1.000.000$ significa um AFR de $8.760/1.000.000 = 0.876\%$
  - Como temos um data center com 100.000 discos espera-se que durante um ano falhem 876 discos
    - Ou, mais de 2 discos por dia em média!

A Backblaze publica recorrentemente valores reais observados em seus data centers para diversas marcas e modelos de HDs:

https://www.backblaze.com/b2/hard-drive-test-data.html

Interrupção do serviço e disponibilidade

- MTTR *Mean Time To Repair* - O tempo pelo qual o serviço fica interrompido.
- MTBF *Mean Time Between Failures* - Soma de MTTF + MTTR
  - Em geral, quando as pessoas se referem ao MTBF elas estavam querendo se referir ao MTTF
- *Availability* (disponibilidade) é definida como

$$\text{Availability} = \frac{\text{MTTF}}{(MTTF + MTTR)}$$

- A disponibilidade é, então, uma razão do tempo que o serviço está atuando conforme esperado pelo tempo total

- *Reliability* e *Availability* são medidas objetivas
  - Não são sinônimos para *Dependability*
- Observando a equação abaixo, fica claro que podemos melhorar a disponibilidade tanto aumentando o MTTF quando diminuindo o MTTR

$$\text{Availability} = \frac{\text{MTTF}}{(MTTF + MTTR)}$$

Noves fora...

UFABC

- Disponibilidade é frequentemente expressa em *número de noves*
- Por exemplo:
  - Um serviço bom de internet pode oferecer *4 ou 5 noves* de disponibilidade. 365 dias no ano, 24 horas por dia, 60 minutos por hora = 526.000 minutos/ano
  - Um nove: 90% $\rightarrow$ 36.5 dias em manutenção por ano
  - Dois noves: 99% $\rightarrow$ 3.65 dias em manutenção por ano
  - Três noves: 99.9% $\rightarrow$ 526 minutos em manutenção por ano
  - Quatro noves: 99.99% $\rightarrow$ 52.6 minutos em manutenção por ano
  - Cinco noves: 99.999% $\rightarrow$ 5.26 minutos em manutenção por ano

Como melhorar o MTTF

UFABC

1. *Fault avoidance* (evitação/evitamento/prevenção de falhas) - Evita a ocorrência de falhas por design
2. *Fault tolerance* (tolerância a falhas) - Utiliza redundância para permitir que o serviço continue a funcionar conforme especificado apesar de falhas ocorrerem
3. *Fault forecasting* (previsão de falhas) - Prevê as falhas antes que elas ocorram permitindo que o componente seja substituído antes que ele falhe.

Detectando e corrigindo erros

UFABC

- Um Código de Detecção de Erro permite a detecção de um erro em um conjunto de dados, mas não a sua localização e, portanto, sua correção.
  - Exemplo clássico bit de paridade
- Um Código de Correção de Erros (*Error Correcting Code* - ECC) permite a detecção de erros e a sua localização/correção
  - Um exemplo de ECC é o código de Hamming
  - Rendeu ao Richard Hamming um Prêmio Turing em 1968

O código de Hamming

Bit position		1	2	3	4	5	6	7	8	9	10	11	12
Encoded data bits		p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8
Parity bit coverage	p1	X		X		X		X		X		X	
	p2		X	X			X	X			X	X	
	p4				X	X	X	X					X
	p8								X	X	X	X	X

- Exemplo: `10011010` (base 2)
  - `__1_001_1010` → `0_1_001_1010` → `011_001_101` → `0111001_1010` → `011100101010`

O código de Hamming

Bit position		1	2	3	4	5	6	7	8	9	10	11	12
Encoded data bits		p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8
Parity bit coverage	p1	X		X		X		X		X		X	
	p2		X	X			X	X			X	X	
	p4				X	X	X	X					X
	p8								X	X	X	X	X

- Suponha uma inversão no décimo bit: `011100101010` → `011100101110`

Nº Bit	1	2	3	4	5	6	7	8	9	10	11	12
Valor	0	1	1	1	0	0	1	0	1	1	1	0

  - Bit de paridade 1 é 0, paridade par. Tudo ok.
  - Bit de paridade 2 é 1. Paridade ímpar. Algo errado.
  - Bit de paridade 4 é 1. Paridade par. Tudo ok.
  - Bit de paridade 8 é 1. Paridade ímpar. Algo errado.
- $2 + 8 = 10$ o bit invertido é o bit 10. Basta invertê-lo e presto!

Outros códigos de correção e detecção de erros

UFABC

- Aumentar o número de bits de paridade permite a correção e detecção de mais do que um único erro.
- *Single Error Correcting* ou *Double Error Correcting* são frequentemente encontrados nos módulos de memória de servidores
  - Cada linha da RAM tem 72 bits (64 dados + 8 de paridade)
- Checksums, CRCs são outras alternativas empregadas para detecção de erros
- Um ECC famoso é o Reed-Solomon que utiliza campos de Galois para corrigir múltiplos bits de erros. É empregado em CDs, DVDs, Blu-rays e QR codes ...

Redundant Arrays of Inexpensive Disks

Confiabilidade e Redundância

- Reliability e Redundancy
- Tempo médio para falha (*Mean time to failure* - MTTF) - O tempo que um disco leva em média para apresentar uma falha
- Tempo médio para reparação (*Mean time to repair* - MTTR) - O tempo que se leva em média para substituir um disco e restaurar os dados
- Espelhamento (*Mirroring*) - Manter uma cópia completa de um disco em outro
  - Considere um disco com MTTF de 100.000 horas e MTTR de 10 horas
  - Tempo médio para a perda de dados é = 100.000^2 / (2 * 10) = 500 * 10^6 horas, ou 57.000 anos supondo-se que as falhas dos discos sejam eventos aleatórios independentes

A BlackBlaze divulga anualmente os MTTFs de discos de diversas marcas e modelos. Confira: https://www.backblaze.com/blog/2018-hard-drive-failure-rates/

- Várias melhorias nas técnicas de uso de discos envolvem o uso de vários discos de maneira conjunta
- O espelhamento completo pode ser matar uma mosca com um tiro de canhão

RAID - Redundant Array of Inexpensive Disks

UFABC

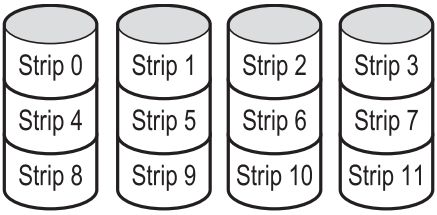
- O uso vários discos **pioram** o MTTF
  - 100 discos com MTTF de 100.000 horas
  - 100.000/100 = 1.000 horas ou 41.66 dias
- A solução envolve utilizar redundância nos 100 discos
- Disk striping - Dividir os bits (ou blocos) entre vários discos
  - bit-level striping - Os bits de um byte são espalhados entre os vários discos
  - block-level striping - Os blocos de um arquivo são espalhados entre vários discos
- Por exemplo, se desejamos fazer um RAID de 8 discos podemos escrever o *i*-ésimo bit de um byte no *i*-ésimo disco. O conjunto dos 8 discos pode então ser tratado como um único disco, com setores com 8x o tamanho padrão e, mais importante, com 8x o desempenho

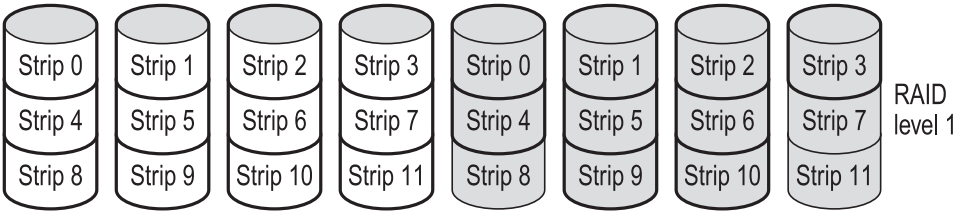
- Estruturas de RAID aumentam o desempenho e a confiabilidade utilizando redundância de dados
- O RAID como um todo ainda pode falhar
  - Replicar os dados entre RAIDs é comum
    - Escritas duplicadas entre sites separados geograficamente
    - A redundância provê a possibilidade de recuperação de desastres
    - Pode ser feita de maneira síncrona ou assíncrona
  - Frequentemente uma pequena quantidade de discos reservas quentes (*hot spare disks*) são mantidas conectados, porém não alocados, para substituir automaticamente um disco que falhou (e receber a sua cópia dos dados)

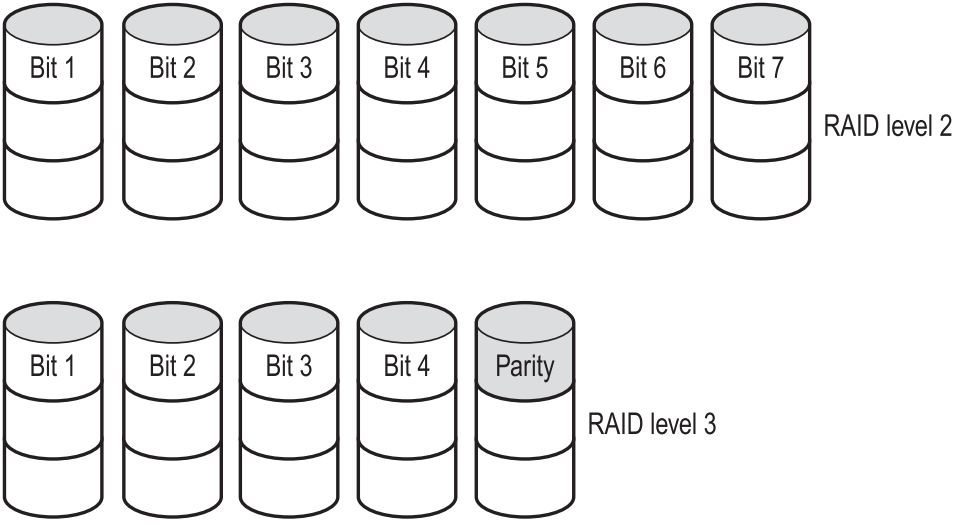
Tipos de RAID

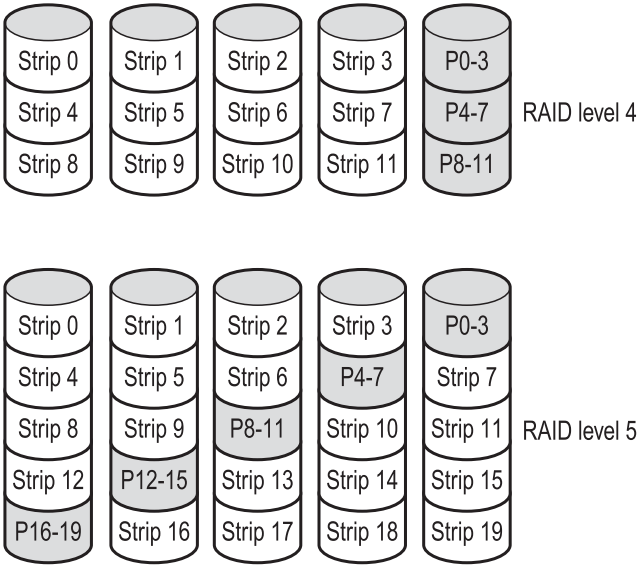
UFABC

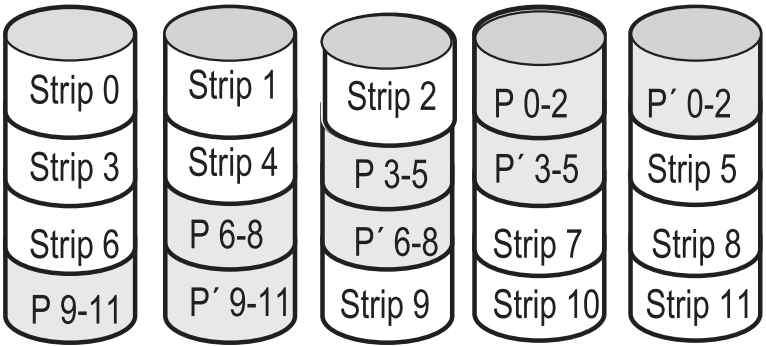
- RAID 0 - Nome que não tem muito sentido, pois não há redundância, mas é oferecido como opção aos usuários.
- RAID 1 - Espelhamento
- RAID 2 - Código de detecção e correção de erros (na prática caiu em desuso)
- RAID 3 - Paridade de dados intercalada. Um disco dedicado à paridade.
- RAID 4 - Paridade intercalada por blocos.
- RAID 5 - Paridade distribuída intercalada por blocos.
- RAID 6 - Redundância P + Q


Strip 0
Strip 1
Strip 2
Strip 3
Strip 4
Strip 5
Strip 6
Strip 7
Strip 8
Strip 9
Strip 10
Strip 11
RAID level 0


Strip 0
Strip 1
Strip 2
Strip 3
Strip 4
Strip 5
Strip 6
Strip 7
Strip 8
Strip 9
Strip 10
Strip 11
Strip 0
Strip 1
Strip 2
Strip 3
Strip 4
Strip 5
Strip 6
Strip 7
Strip 8
Strip 9
Strip 10
Strip 11
RAID
level 1


Bit 1
Bit 2
Bit 3
Bit 4
Bit 5
Bit 6
Bit 7
RAID level 2
Bit 1
Bit 2
Bit 3
Bit 4
Parity
RAID level 3


Strip 0
Strip 1
Strip 2
Strip 3
P0-3
Strip 4
Strip 5
Strip 6
Strip 7
P4-7
RAID level 4
Strip 8
Strip 9
Strip 10
Strip 11
P8-11
Strip 0
Strip 1
Strip 2
Strip 3
P0-3
Strip 4
Strip 5
Strip 6
P4-7
Strip 7
Strip 8
Strip 9
P8-11
Strip 10
Strip 11
RAID level 5
Strip 12
P12-15
Strip 13
Strip 14
Strip 15
P16-19
Strip 16
Strip 17
Strip 18
Strip 19


Strip 0
Strip 3
Strip 6
P 9-11
Strip 1
Strip 4
P 6-8
P´ 9-11
Strip 2
P 3-5
P´ 6-8
Strip 9
P 0-2
P´ 3-5
Strip 7
Strip 10
P´ 0-2
Strip 5
Strip 8
Strip 11

RAID level 6

E o tal do RAID 10 e RAID 01?

UFABC

- RAID 10/RAID 01 - Mirroring + Striping e vice-versa
- RAID 10 - 8 discos - 4 pares espelhados (cada par em RAID 1) e dados em stripes nos 4 pares.
- RAID 01 - 8 discos - 2 conjuntos de 4 discos (em RAID 0) com escritas espelhadas entre os conjuntos (dentro do conjunto escritas com stripes)