フォールトトレランス

1. フォールトトレランスの基本概念を学習する
2. RAIDについて学習する
3. 信頼性評価について学習する

フォールトトレランス (Fault tolerance)

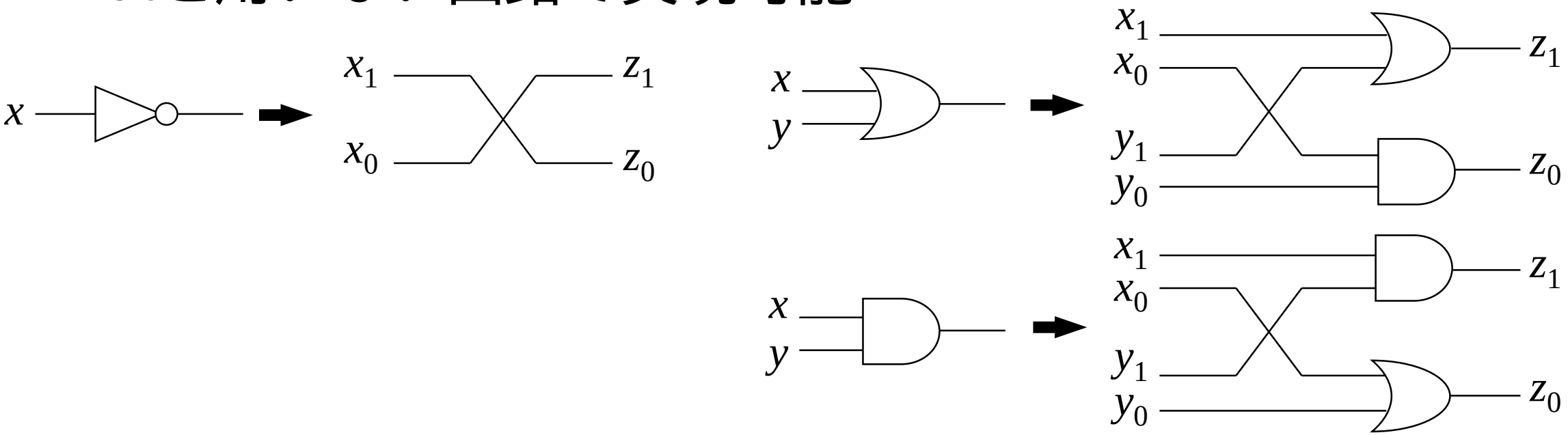
- フォールトトレランス
  - フォールトに耐えられること
- フォールトトレラントシステム
  - フォールトに耐えられるシステム
- 例.
  - パリティビット
  - 2線式論理
  - TMR
  - 商用のフォールトトレラントサーバ
  - RAID

パリティビット (parity bit)

- ビット列の1のビットの数を, 偶数, または, 奇数にたもつために付加する1ビットのこと
  - 偶数パリティ
    - パリティビットも含めて, 1の数を偶数にする方式
      - 0100010 + パリティビット 0
      - 0100011 + パリティビット 1
  - 奇数パリティ

2線式論理 (Dual-rail logic)

- 1を(1, 0), 0を(0, 1)で表現
  - 2ビットの符号語 (code word)
    - 1ビットのエラーを検出可能
- Notを用いない回路で実現可能

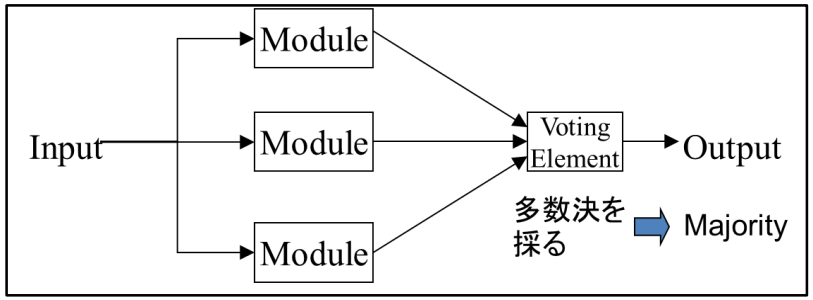


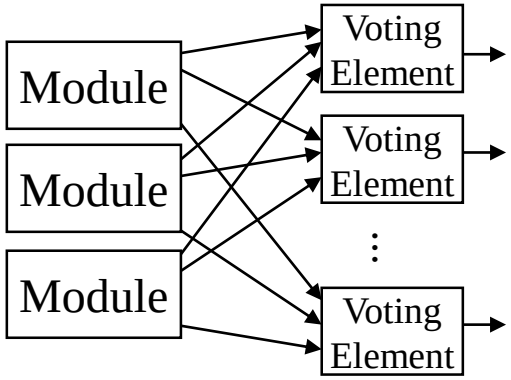
2線式論理 (Dual-rail logic)

- Notがない回路の出力へのフォールトの影響
  - 値が1→ 0になる故障 ➡ 1→0 のみ
  - 値が0 →1になる故障➡ 0→1 のみ
- 同じ方向のエラーなら間違った符号語は出力されない
  - 例えば(0,1)→ (1,0)は起こりえない
  - 出力が符号語でない場合は, エラーが検出されたことになる
  - Fault-Secure
    - ◆誤った符号語を出力しない性質

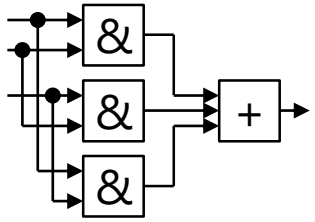
TMR (Triple Modular Redundancy)

- 3重系
  - モジュール×３＋多数決器
- 多数決器 (Voting element, voter)
  - Bit-wise voting
    - ◆1ビット毎に多数決を採る方法
    - ◆2つ以上のModuleのFaultに耐えられる場合がある





Voting Element
(Voter)



商用のフォールトトレラントコンピュータ

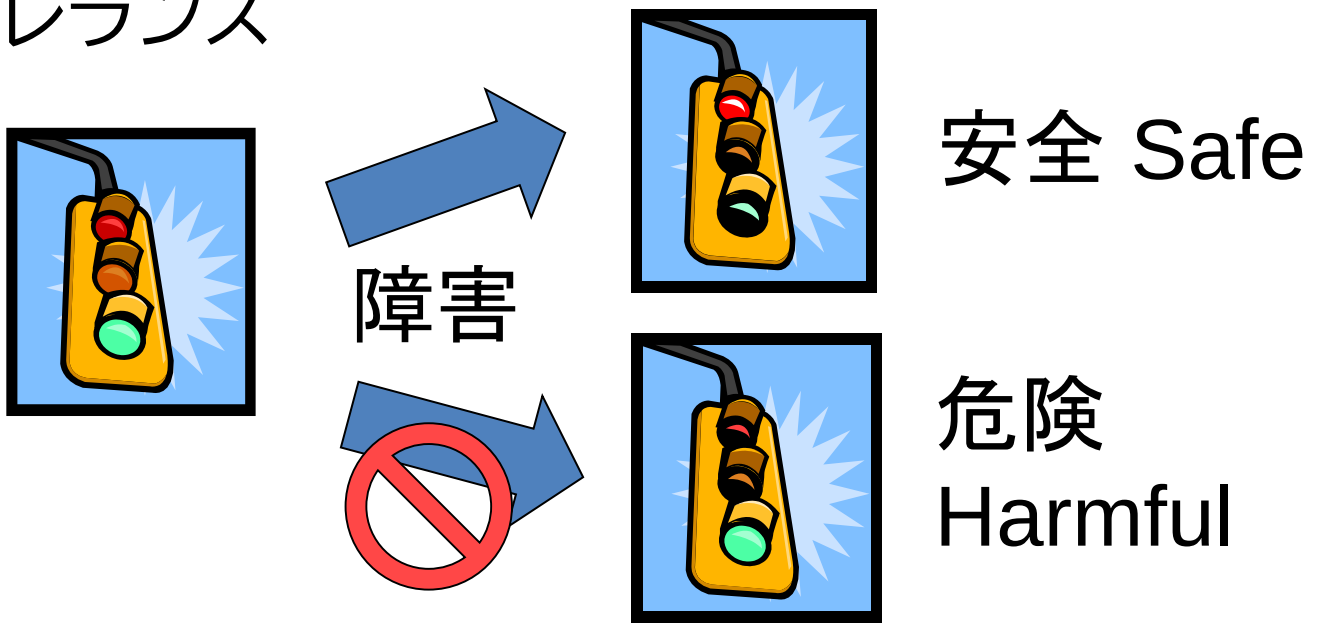
- HPE NonStopシステムファミリ

- ストラタス フォールト・トレラント・サーバ
  - 2重系
  - 高可用性

https://www.hitachi-systems.com/campaign/02/ftserver/

フェイルセイフ（fail-safe）

- 障害がおきても安全な出力・状態に移行
  - 一種のフォールトトレランス



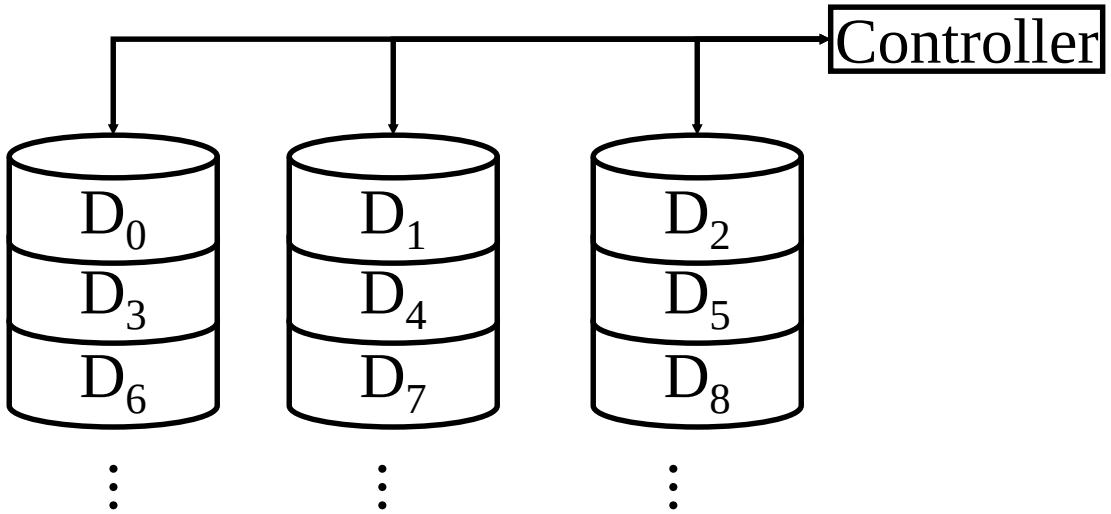
近い概念. Fail-operational
制御システムが障害となっても，機能を縮退してシステム自体は動作を継続

2. RAID

- Redundant Array of Inexpensive Disks
  → Redundant Array of Independent Disks
  - 複数のハードディスクを用いて，フォールトトレラントな記憶領域を実現
- Striping
  - 記憶領域をStripeに分割し，複数のディスクに分散させること
  - 1ストライプ = 負荷の分散
    - 典型的な大きさ：128KB, 256KB, 512KB

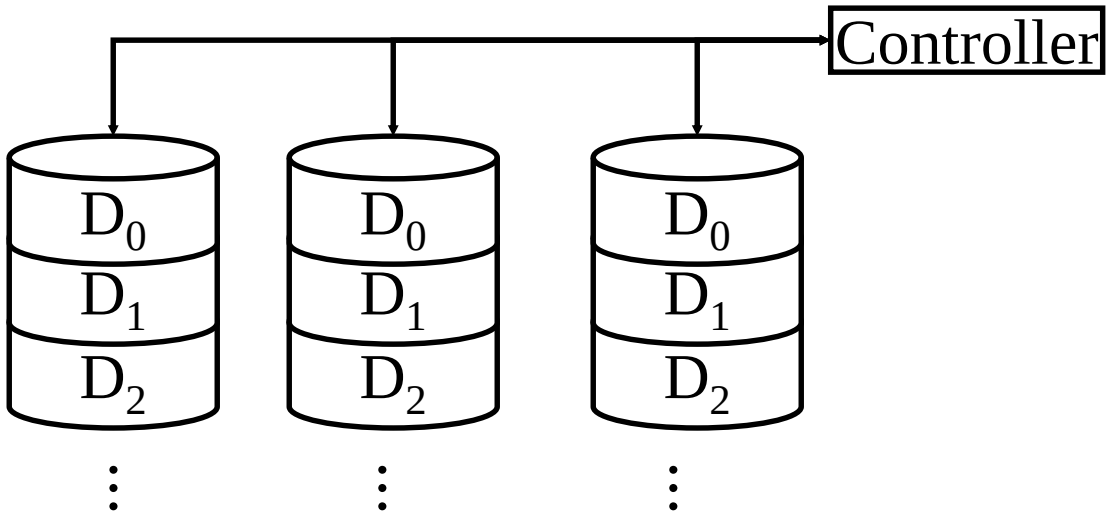
RAID-0 (Striping)

- データが重複しないようにストライプを分散
  - アクセスの並列化による
    性能の向上
  - No fault tolerance
  - 利用効率(記憶容量に対する使用可能容量の割合)＝ 100%



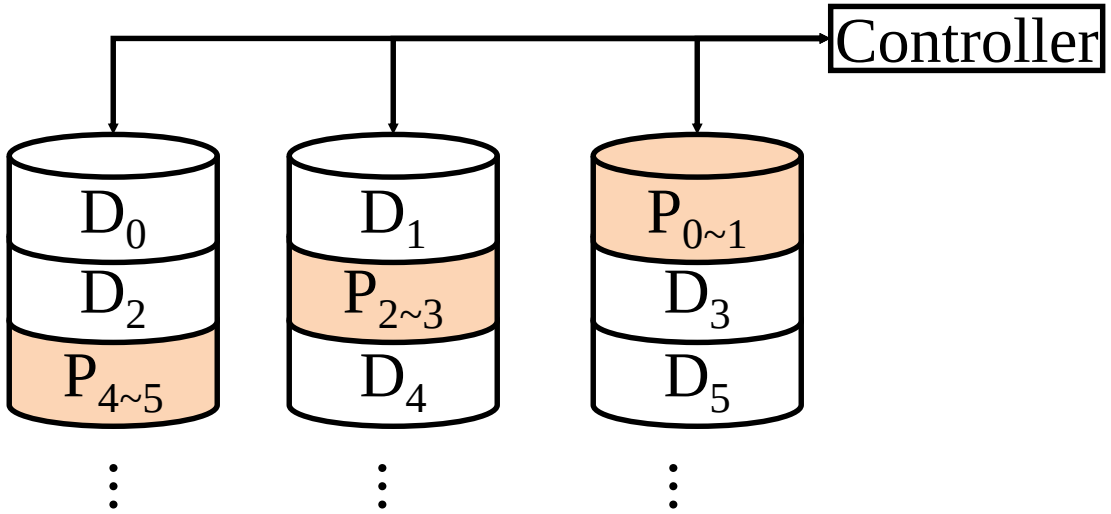
RAID-1 (Mirroring)

- 同一のデータを複数(N台)のディスクで保持
  - 高いFault tolerance (N-1台の障害への耐性)
  - 高速な読み出し
  - 低速な書き込み
  - 利用効率=100/N %



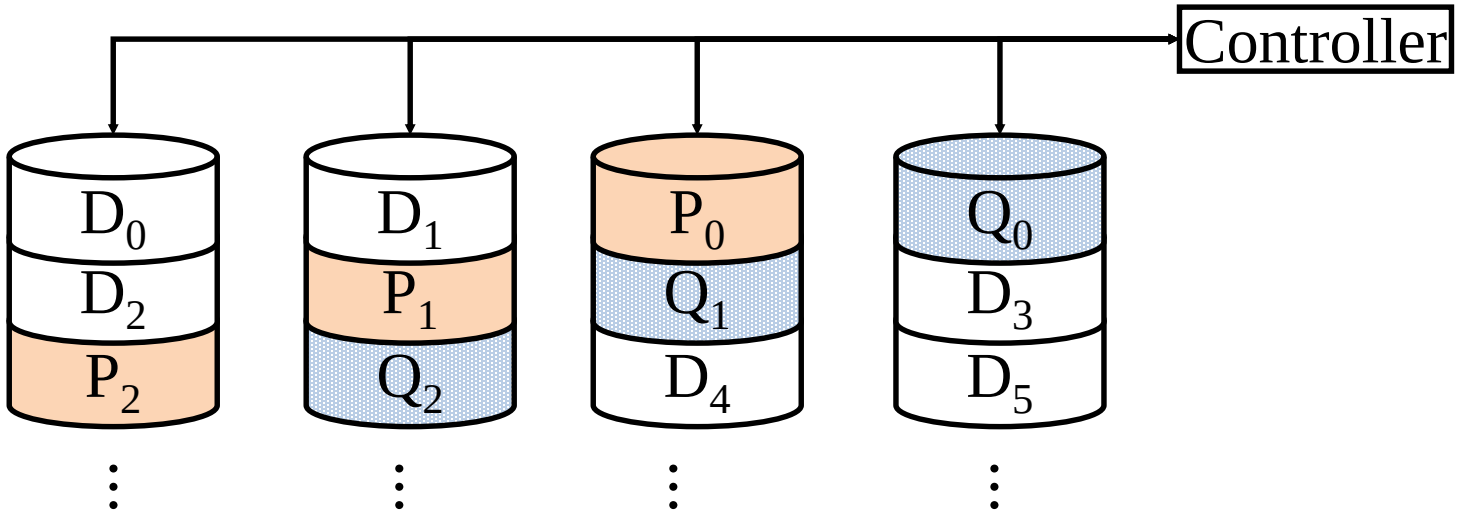
RAID-5

- パリティをディスクに分散
  - Disk 1台のフォールトをmask
  - 高速な読み出し・書き込み
  - 利用効率 100×(N-1/N) %



RAID-6

- 2重パリティ
  - Disk 2台のフォールトをmask
  - 利用効率 100×(N-2/N) %



3. 信頼性評価について学習する

- 評価尺度
  - 信頼度 reliability
  - 可用度 availability
  - MTTF

- 参考. 正常・障害以外の状態をもつシステム
  - 漸次縮退(gracefully degrading)システム
    - ◆ 正常と障害の間に, 機能が縮退した状態が存在
  - 評価尺度
    - ◆Performability: Performance + Reliability

Reliability (信頼度)とMTTF

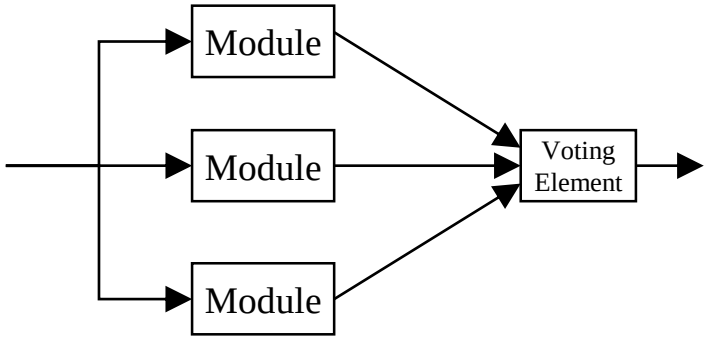
- Reliability
  - 時刻 t までシステムが正しく動き続ける確率
  - failure rate (障害率) λ ($\lambda \geq 0$)が一定の場合

    $R(t) = \mathrm{e}^{-\lambda t}$
    - t: 時刻 ($t \geq 0$), e: 自然対数の底
- MTTF
  - 障害までの平均時間

    MTTF=$\int_0^\infty R(t)dt$
  - $R(t) = \mathrm{e}^{-\lambda t}$のとき，MTTF = $\frac{1}{\lambda}$

TMRのReliabilityとMTTF

- $R(t) = 3\mathrm{e}^{-2\lambda t} - 2\mathrm{e}^{-3\lambda t}$
  - モジュールの信頼度: $R_m(t) = \mathrm{e}^{-\lambda t}$
  - Voting element (多数決器, voter)は, 故障しない
  - 2台以上のモジュールが故障していなければ, 正常



- MTTF = _____
  - モジュールのMTTF: $\mathrm{MTTF}_m = \frac{1}{\lambda}$

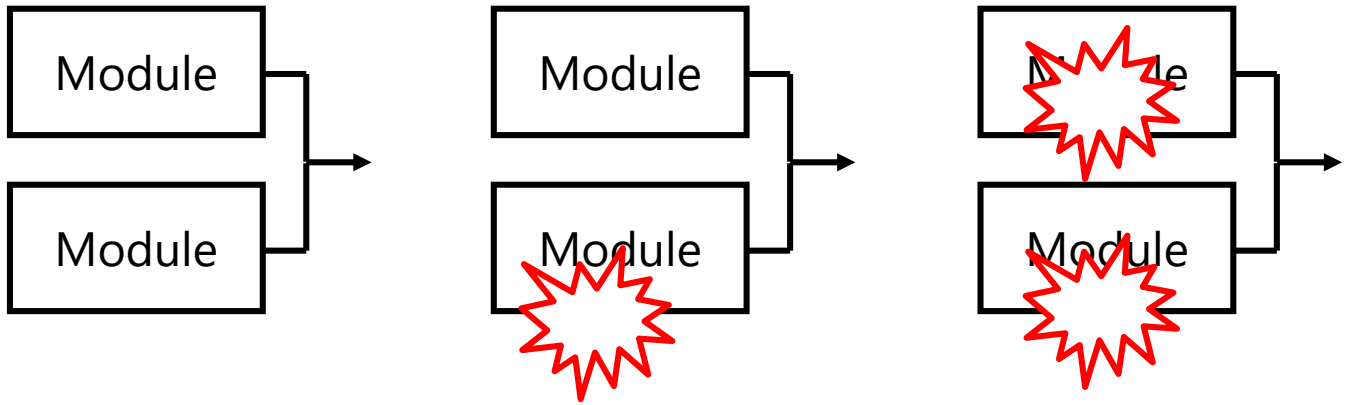
参考

$$\int a^x \, dx = \frac{a^x}{\log a} + C$$

$$\int e^{ax} \, dx = \frac{1}{a} e^{ax} + C$$

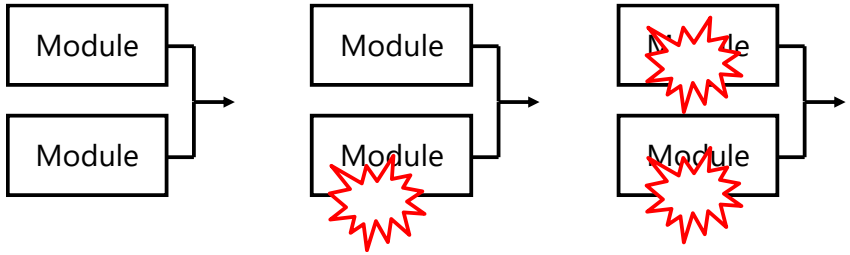
マルコフモデル (Markov models)

- 状態変化をマルコフ連鎖で表現
  - 状態＋遷移率
  - 詳細な動作を表現可能
- 例. 2重系＋修復人1

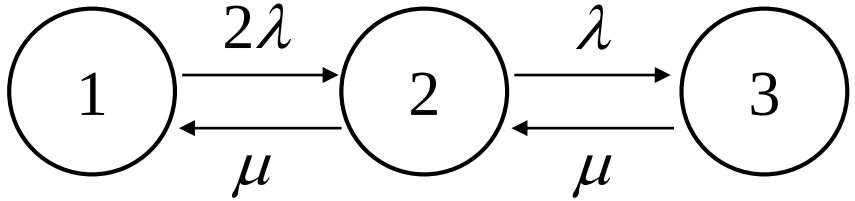


マルコフモデル (Markov models)

- 状態変化をマルコフ連鎖で表現
  - 状態＋遷移率
  - 詳細な動作を表現可能
- 例. 2重系＋修復人1

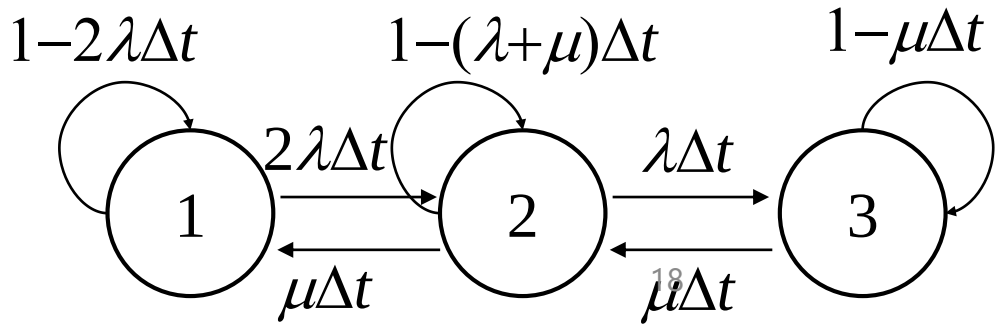


連続時間



λ: 障害率(failure rate)
μ: 修復率(repair rate)

離散時間



定常アベイラビリティの解析

- 定常アベイラビリティ
  - システムが正常である確率
  - 例の場合. 状態1か2にいる確率
- 求め方
  - π_i: 状態iにいる確率として，連立方程式をとく

$$\begin{cases} 0 = \mu\pi_2 - 2\lambda\pi_1 \\ 0 = 2\lambda\pi_1 + \mu\pi_3 - (\mu + \lambda)\pi_2 \\ 0 = \lambda\pi_2 - \mu\pi_3 \\ \pi_1 + \pi_2 + \pi_3 = 1 \end{cases}$$