高信頼システム 02

張山昌論

- マルコフ過程を用いた信頼度の解析
- システムの高信頼化設計
  - 概要
  - 3重化システム

私の連絡先

- 張山昌論 (はりやままさのり)
- メールアドレス: hariyama@tohoku.ac.jp
- 居室: 3号館 308号室 (地下鉄青葉山駅の後ろ)
  (事前にアポイントいただけますよう)
- 電話: 022-795-7153

授業の資料と評価方法

- 印刷して配布します
- 張山のWEBの授業のページでもPDFを公開
  - http://www.ecei.tohoku.ac.jp/hariyama
  - PC / タブレットで持ち込んでも結構です
- 基本的にはテストで成績を判定する
  - 授業中に渡した印刷資料と自筆ノートを持ち込んで良い.
- レポートなどの平常点を考慮する場合もある
- 出席はとらない

マルコフ過程を用いた信頼度解析

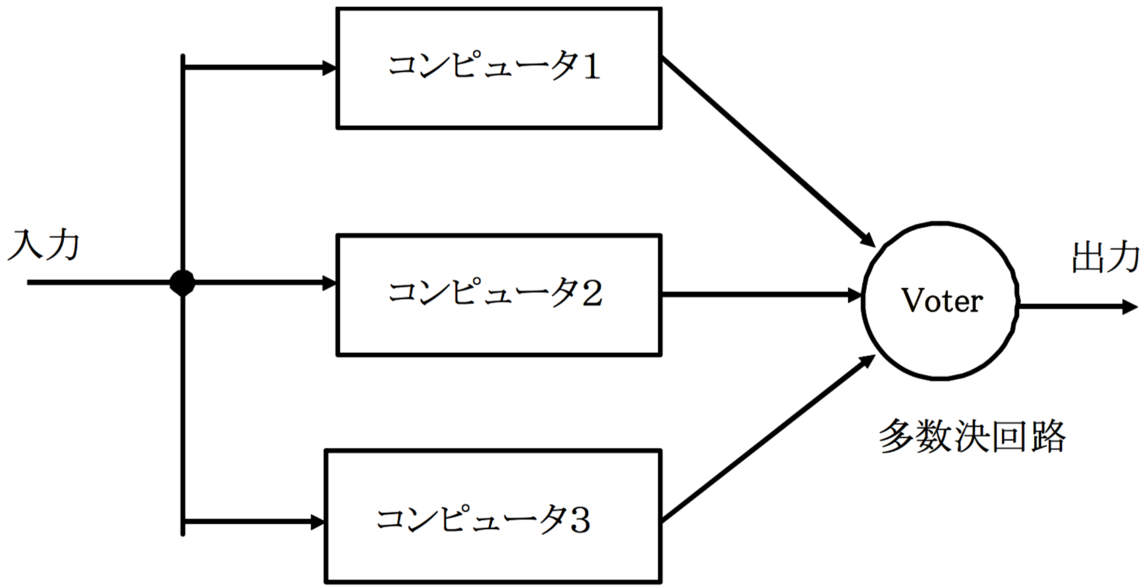
マルコフ過程

過去の有限段階前までの状態に,システムの状態遷移確率が依存する.

1段階前のみに依存 ⇒ 単純マルコフ過程

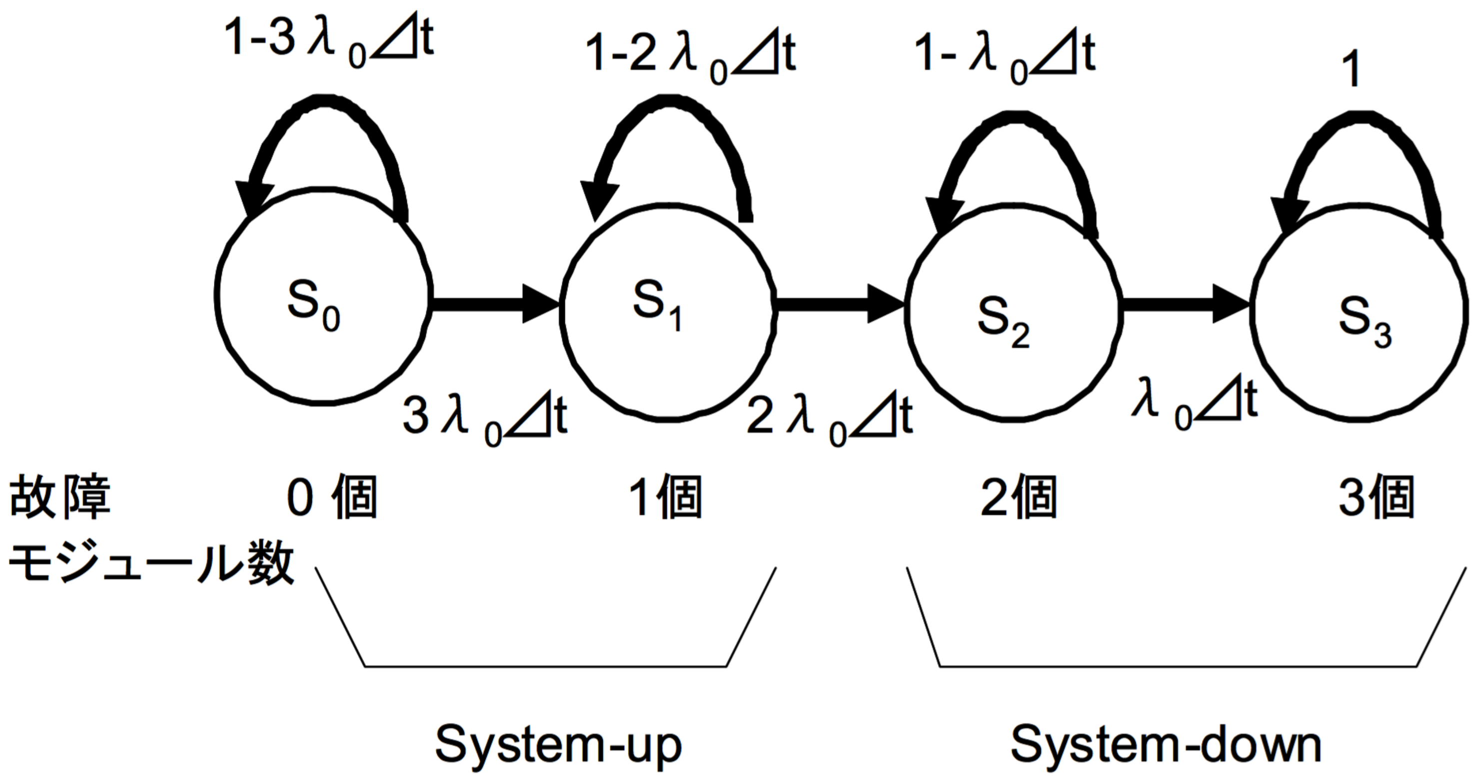
解析例）多数決による 3 重化 TMR

TMR(Triple-Modular Redundancy)



多数決により最終出力を決定

マルコフグラフに基づく TMR の信頼度解析



Si: 状態 (i=0, 1, 2, 3…)

仮定：故障は1度に1個ずつ

λ_0: 故障率

Δt: 単位時間

微小時間Δt，故障率λ_0，S_iにいる確率 P_i （$i=0, 1, 2, 3$）

$$P_0(t+\Delta t) = (1 - 3\lambda_0\Delta t)P_0(t)$$

$$P_1(t+\Delta t) = 3\lambda_0\Delta t\ P_0(t) + (1 - 2\lambda_0\Delta t)P_1(t)$$

$$P_2(t+\Delta t) = 2\lambda_0\Delta t\ P_1(t) + (1 - \lambda_0\Delta t)P_2(t)$$

$$P_3(t+\Delta t) = \lambda_0\Delta t\ P_2(t) + P_3(t)$$

$$\{P_0(t+\Delta t) - P_0(t)\}/\Delta t = -3\lambda_0 P_0(t)$$

$\Delta t \to 0$ $$dP_0(t)/dt = -3\lambda_0 P_0(t)$$

$$P_0(t) = \exp(-3\lambda_0 t)$$

他も同様にして解くと

$$P_1(t) = 3\exp(-2\lambda_0 t) - 3\exp(-3\lambda_0 t)$$

$$P_2(t) = 3\exp(-\lambda_0 t) - 6\exp(-2\lambda_0 t) + 3\exp(-3\lambda_0 t)$$

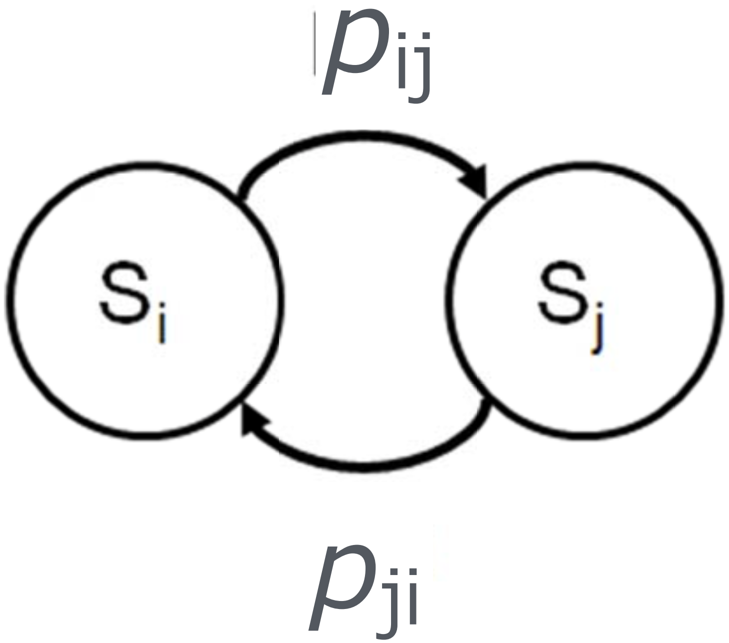
$$P_3(t) = 1 - 3\exp(-\lambda_0 t) + 3\exp(-2\lambda_0 t) - \exp(-3\lambda_0 t)$$

TMR の信頼度 R_{TMR} は,

$$R_{TMR} = P_0(t) + P_1(t) = 3\exp(-2\lambda_0 t) - 2\exp(-3\lambda_0 t)$$

マルコフ過程の一般化

マルコフグラフ



状態遷移確率：p_{ij} ，　$\sum_{j=1}^{r} p_{ij} = 1$

$$P = \begin{array}{c} \\ S_1 \\ S_2 \\ \\ S_r \end{array} \begin{array}{c} \begin{array}{cccc} S_1 & S_2 & & S_r \end{array} \\ \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1r} \\ p_{21} & p_{22} & \cdots & p_{2r} \\ & & & \\ p_{r1} & p_{r2} & \cdots & p_{rr} \end{pmatrix} \end{array}$$

次の状態

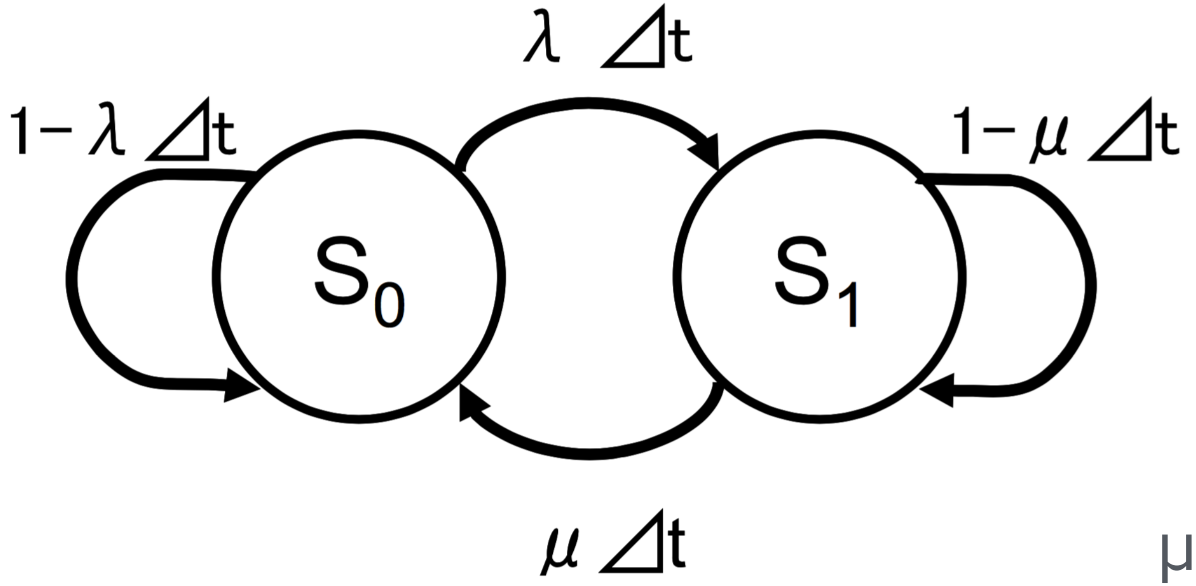
今の状態

⊿t の間の遷移確率

⊿t　≠　0　⇒　離散的マルコフ過程　⇒　解析：差分方程式

⊿t　→　0　⇒　連続マルコフ過程　⇒　解析：微分方程式

例）修復を伴うシステム



μ：修復率

$$P = \begin{bmatrix} 1-\lambda \Delta t & \lambda \Delta t \\ \mu \Delta t & 1-\mu \Delta t \end{bmatrix}$$

修復率(Repair Rate) μ= 1/MTTR

※MTTR (Mean-Time-To-Repair):

平均修復時間

遷移行列の性質

$X(t)=(X1(t), X2(t), \cdots, Xn(t))$

時刻 t に状態S1, S2, …, Snにいる確率

$$X(t+\Delta t) = X(t)\mathbf{P}$$

定常状態においてSiにいる確率は？

時間が十分に経つと，

$X(t) \to X$（定数ベクトル）

$$X = X\mathbf{P}$$

例

$$(x_1 \ \ x_2 \ \ x_3) \begin{bmatrix} 0.5 & 0.25 & 0.25 \\ 0.5 & 0 & 0.5 \\ 0.25 & 0.25 & 0.5 \end{bmatrix} = (x_1 \ \ x_2 \ \ x_3)$$

$$x_1 + x_2 + x_3 = 1$$

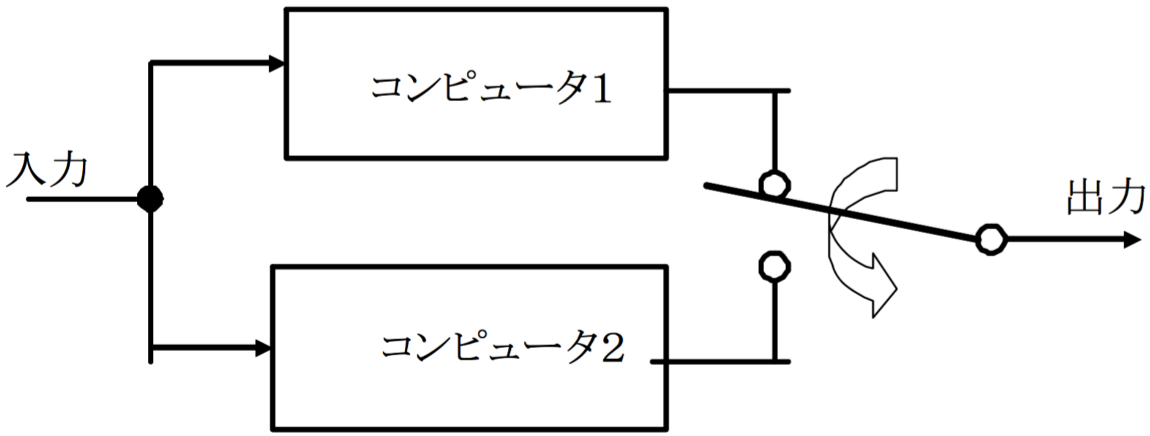
$$(1/2)\,x_1 + (1/2)\,x_2 + (1/4)\,x_3 = x_1$$

$$(1/4)\,x_1 + 0 + (1/4)\,x_3 = x_2$$

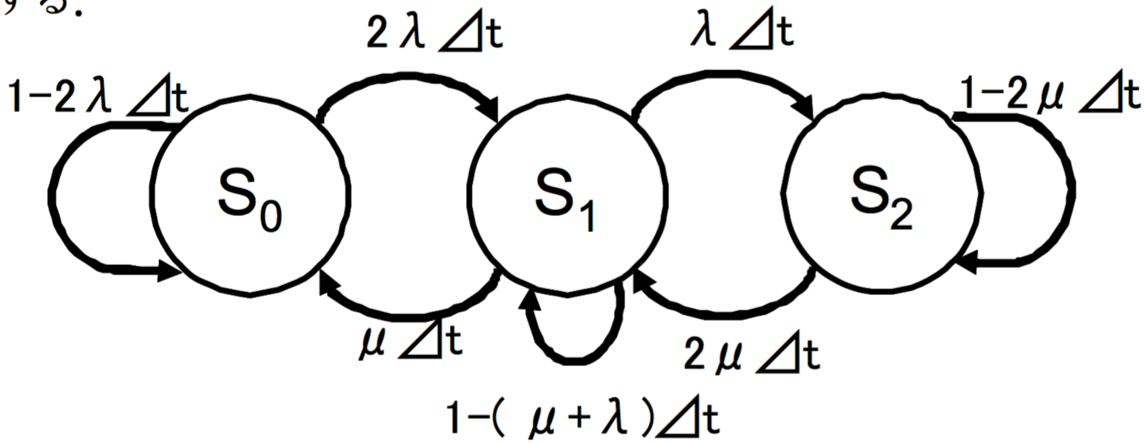
$$(1/24)\,x_1 + (1/2)\,x_2 + (1/4)\,x_3 = x_3$$

これを解くと $X = (0.4 \quad 0.2 \quad 0.4)$

レポート）並列冗長系の定常アベイラビリティ



ここでは，２台のコンピュータが故障した場合は，修理は２台並列に可能であるものとする．



１個以上のモジュールが正常に動作している確率の総和，すなわち定常アベイラビリティを求めよ．

※定常アベイララベリティ＝定常状態での稼働率

システムの高信頼化設計

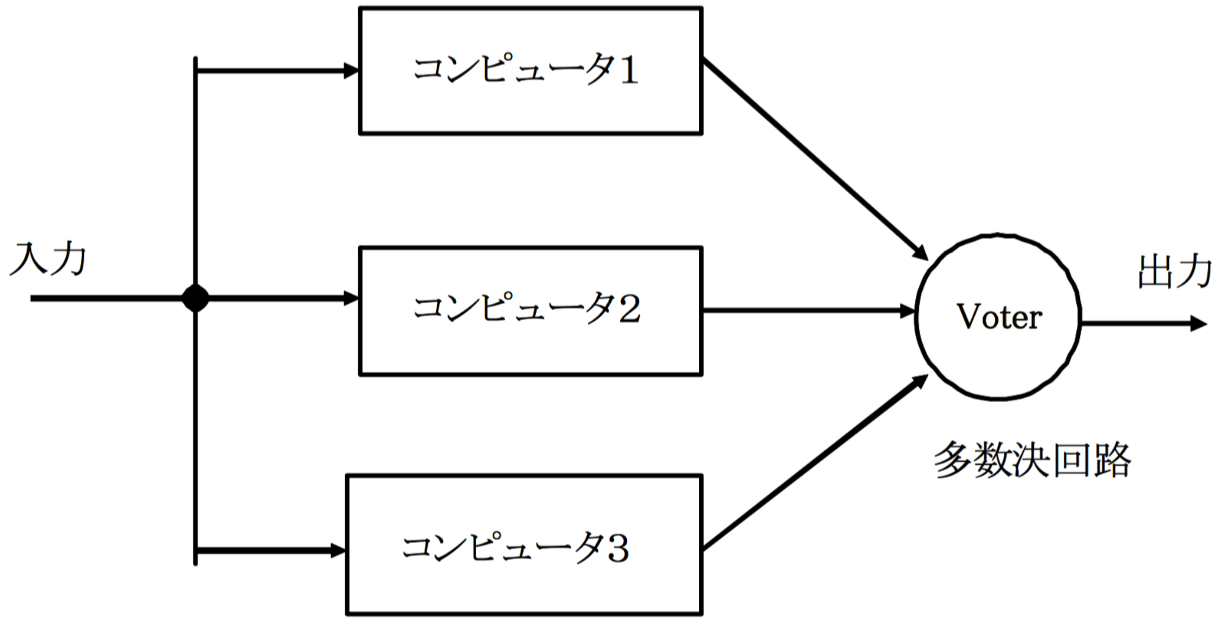
概要

システムの信頼性向上技術の分類

- **故障回避（Fault avoidance）**
  - （理想的には）すべての故障を事前に排除
  - （実際は）容認できる程度に故障の確率を減らす
  - 例）部品のスクリーニングにより信頼性の高い部品のみを使うなど
- **耐故障化（Fault tolerance）**
  - フォールトの存在を認めた上で，システム全体として冗長性を利用して高信頼化 を達成する
  - 冗長性をシステムに組み込む
→ 故障が存在しても正しい処理の続行を可能とする
  - 例）非常用電源装置

フォールトトレランス（Fault Tolerance）の例

多数決による 3 重化 TMR(Triple-Modular Redundancy)



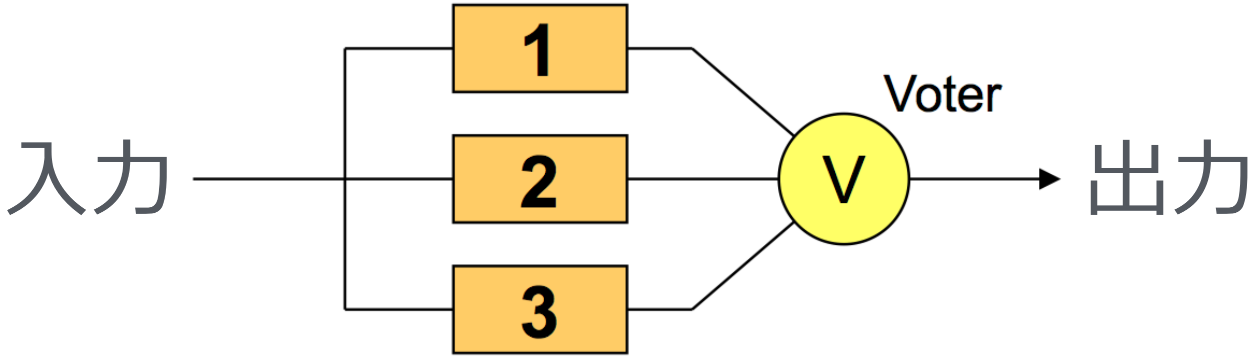
フォールトトレラント技術の分類

- フォールトトレラント技術
  - 誤り検出
    - 回復のきっかけ
      - ２重化
      - 誤り検出符号
    - セルフチェッキング
    - フェールセーフ
    - ウォッチドックタイマ(Watch Dog Timer)
    - タイムアウト
    - 出力結果の妥当性検証
  - 静的冗長
    - クラシカルＴＭＲ
    - 誤り訂正符号
    - マスク論理
  - 動的冗長
    - 再構成(Reconfiguration)
      - 回復(Recovery)
    - ロールバック
    - 縮退

システムの高信頼化設計

3重化システム

モジュール3重化



多数決回路（Voter）が故障しないと仮定

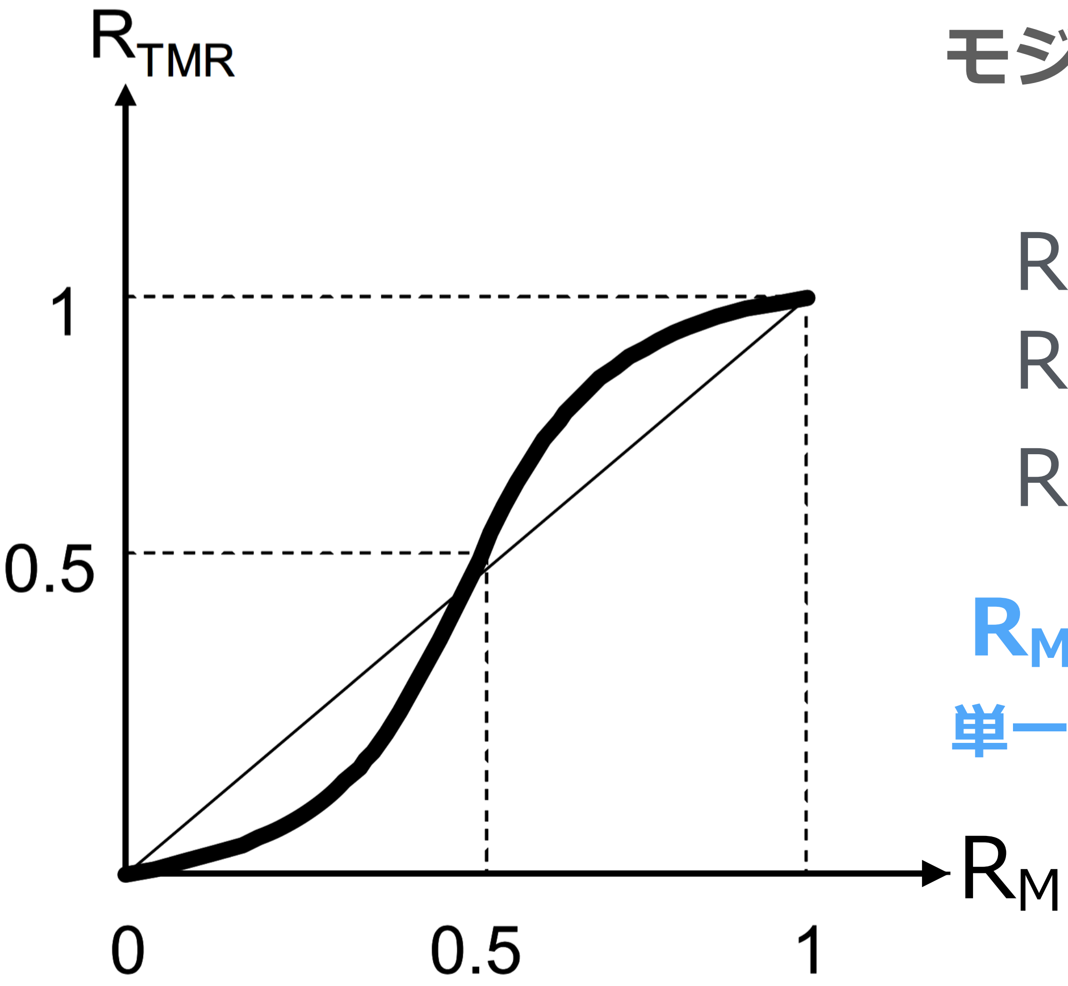
→ 1個のモジュールの信頼度 R_M で決定

R_{TMR}＝3個のモジュールが全て機能している確率

＋ いずれか2個のモジュールが機能している確率

$$= R_M^3 + 3R_M^2(1-R_M) = 3R_M^2 - 2R_M^3$$

ＴＭＲの信頼度



モジュールの信頼度が低いと．．．

R_M = 0.8 → R_{TMR}=0.896
R_M = 0.7 → R_{TMR}=0.784
R_M = 0.5 → R_{TMR}=0.5

R_M = 0.4 → R_{TMR}=0.352 !!

単一のモジュールよりも信頼性が低い！

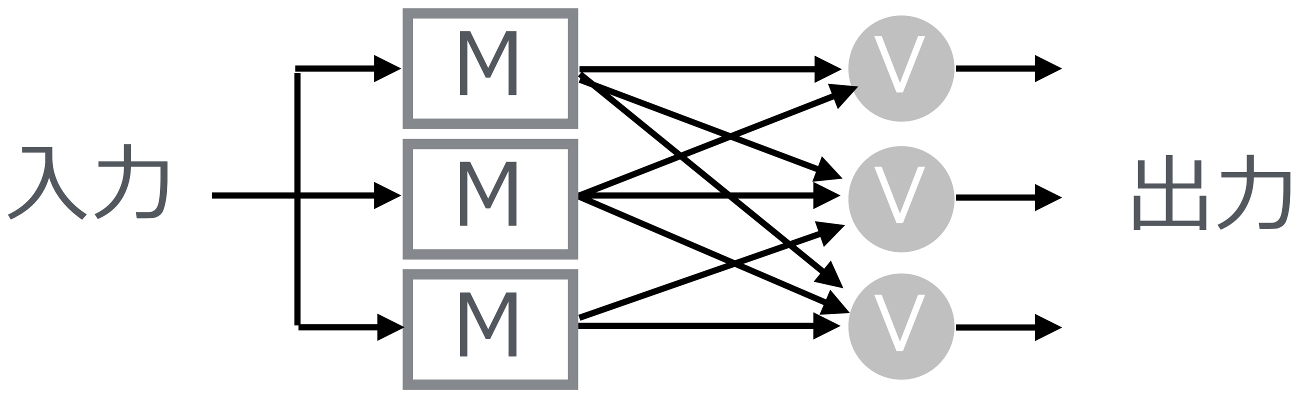
多数決回路（Voter）の信頼度を考慮

Voterが故障すると，他のモジュールの故障とは関係なくシステムが故障

R_{TMR}＝Voterの信頼度 × モジュール部分の信頼度

＝$R_V(3R_M^2 - 2R_M^3)$

3重化TMRシステム



3つのシステム出力のうち2つが正常である

→3対のVoter/Module対の複製のうち2対が正しく機能

$$R_{sys}=(R_M R_V)^3+3(R_M R_V)^2(1-R_M R_V)$$

R_V: Voterの信頼度