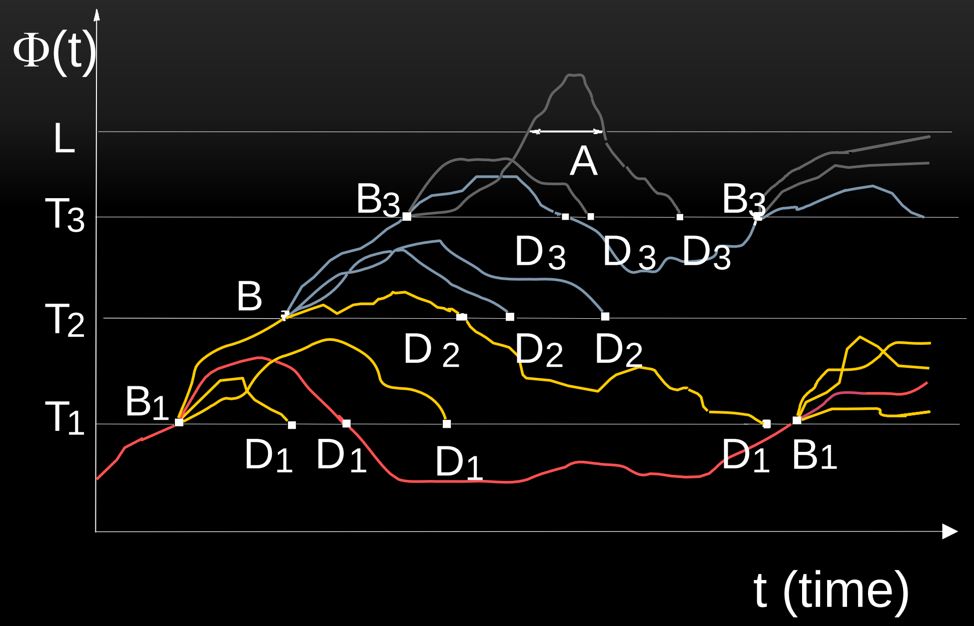
Asymptotic Analysis of RESTART Estimators in Highly Dependable Systems

José Villén-Altamirano
Universidad Politécnica de Madrid

CONTENTS

- Description of RESTART and previous results
- Model and Importance Functions
- Asymptotic analysis
- Simulation results
- Conclusions

Description of RESTART (I)



$$P = \Pr\{A\} = \Pr\{\Phi \geq L\}$$

$$\Pr\{C_i\} = \Pr\{\Phi \geq T_i\}$$

R_i:Number of trials at B_i

$$r_i = \prod_{j=1}^{i} R_j$$

$$C_1 \supset C_2 \supset C_3 \supset \ldots C_M \supset A$$

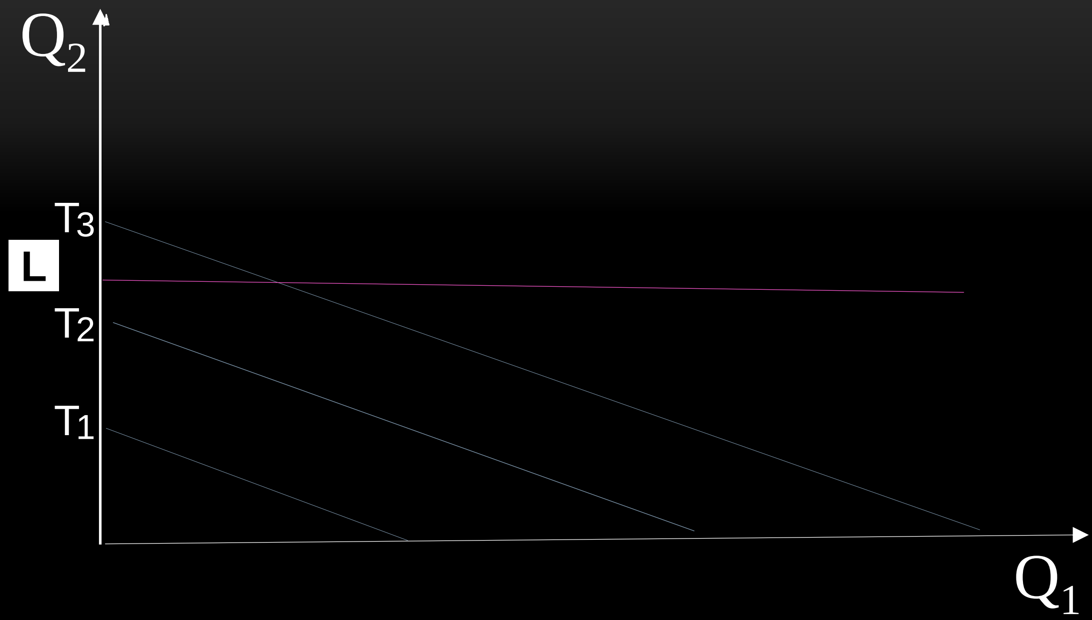
$$P\{A\} = P\{C_1\} \bullet P\{C_2 / C_1\} \bullet \ldots \bullet P\{A/C_M\}$$

$$\boxed{\hat{P} = \frac{N_A}{r_M \cdot N}}$$

N : No. of simulated events (retrials not included)

N_A :No. of events A (retrials included)

Description of RESTART (II)



$$P = \Pr\{A\} = \Pr\{Q_2 \geq L\}$$

$$\Pr\{C_i\} = \Pr\{\Phi \geq T_i\}$$

$$\Phi = \frac{\ln \rho_2}{\ln \rho_1} Q_1 + Q_2$$

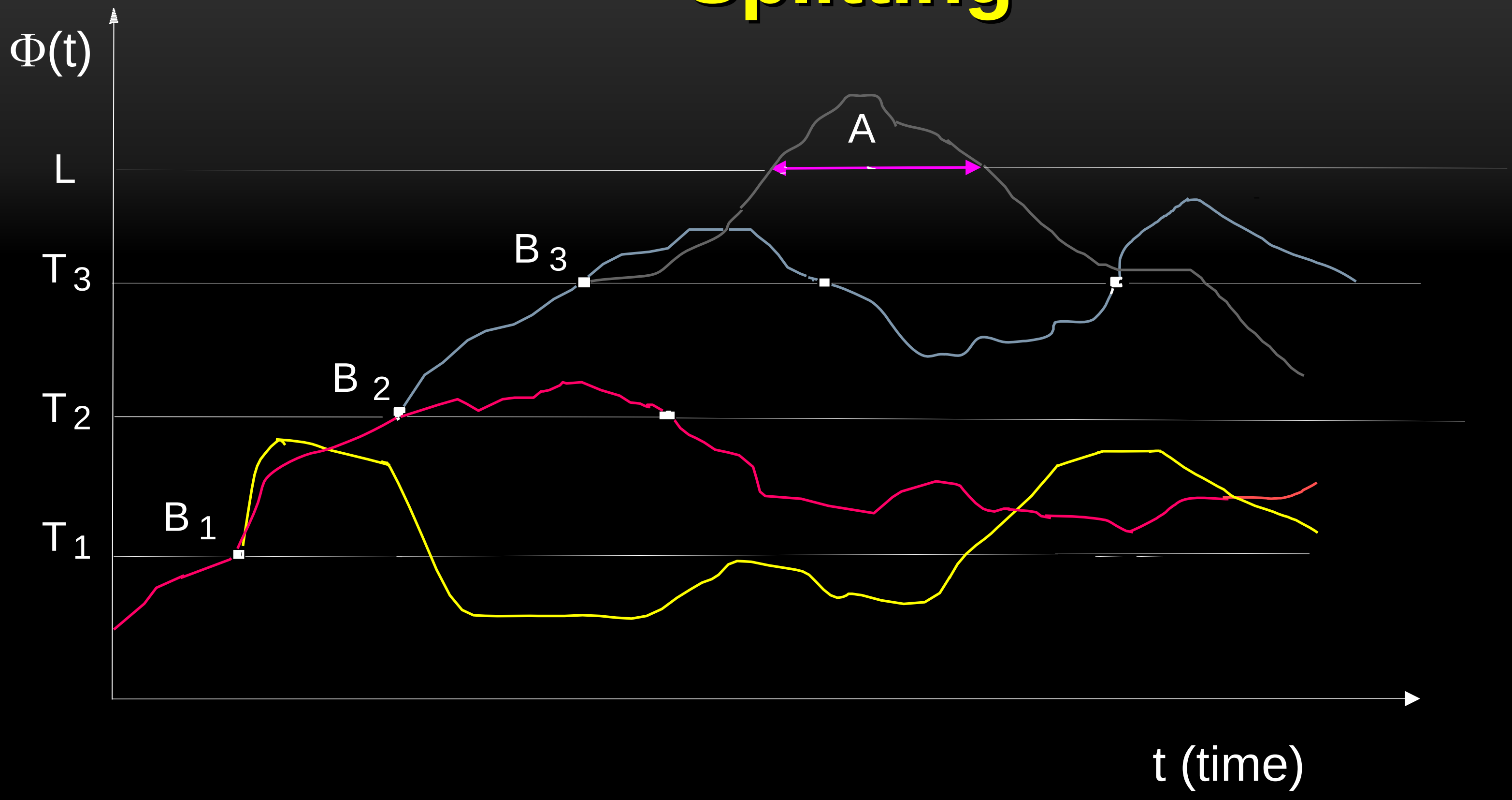
$$A \not\subset C_i \;\; i = 1, \ldots, M \;\; \text{then: } P\{A\} = \sum_{i=1}^{M} P\{C_i\} P\{A / C_i\}$$

$$\boxed{\hat{P} = \sum_{i=1}^{M} \frac{N_{Ai}}{r_i \cdot N}}$$

N : No. of simulated events (retrials not included)

N_{Ai} : No. of events A in retrials from sets C_i

Splitting



- Useful only for short samples. Inefficient for steady-state simulation

- DPR, Subset Simulation: Particular implementations of RESTART or Splitting

Gain Obtained with RESTART

- Computational time for a given relative error proportional to

$$\boxed{f_V\, f_O\, f_R\, f_T \left(-\ln P + 1\right)^2}$$

$$\text{Gain} = \frac{1}{f_V \;\; f_0 \;\; f_R \;\; f_T} \quad \frac{1}{P\left(-\ln P + 1\right)^2}$$

Factors $f \geq 1$ reflect inefficiency due to:

f_T - not optimal thresholds f_0 - algorithm overhead

f_R - not optimal R_i f_V - variance at B_i

Factor f_R

- Optimal values of R_i

$$R_i = \frac{1}{\sqrt{P_{i+1/i-1}}} \quad \Rightarrow \quad f_R \simeq 1$$

Round R_i to the closest integer number.

Factor f_T

- The thresholds must be set as close as possible

$$P_{\min} = Min\left(P_{i/i-1}\right)$$

$$f_T = \frac{\left(\sum_{i=0}^{M} \frac{1 - P_{i+1/i}}{\sqrt{P_{i+1/i}}} + 1\right)^2}{\left(-\ln P + 1\right)^2}$$

$P_{\min}$	f_T
1	1
0.5	1.04
0.1	1.5
0.01	4.6
0.001	20.9

Factor f_O

- $f_0 \leq Max(y_i)$
- **Affects to computational time, not to number of events**

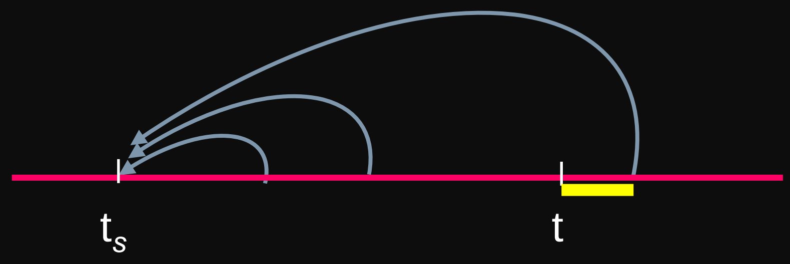
- y_e **= overhead per event: evaluate ϕ, compare with T_i, …**
- y_{ri} **= overhead per retrial: restore state at B_i, re-schedule, ...**
- $y_0 = y_e$ $y_i = y_e \; y_{ri}$

- **This factor usually takes low values with exponential times. However the rescheduling of Weibull or Erlang times is more time consuming.**

FACTOR F_V (I): RESCHEDULING

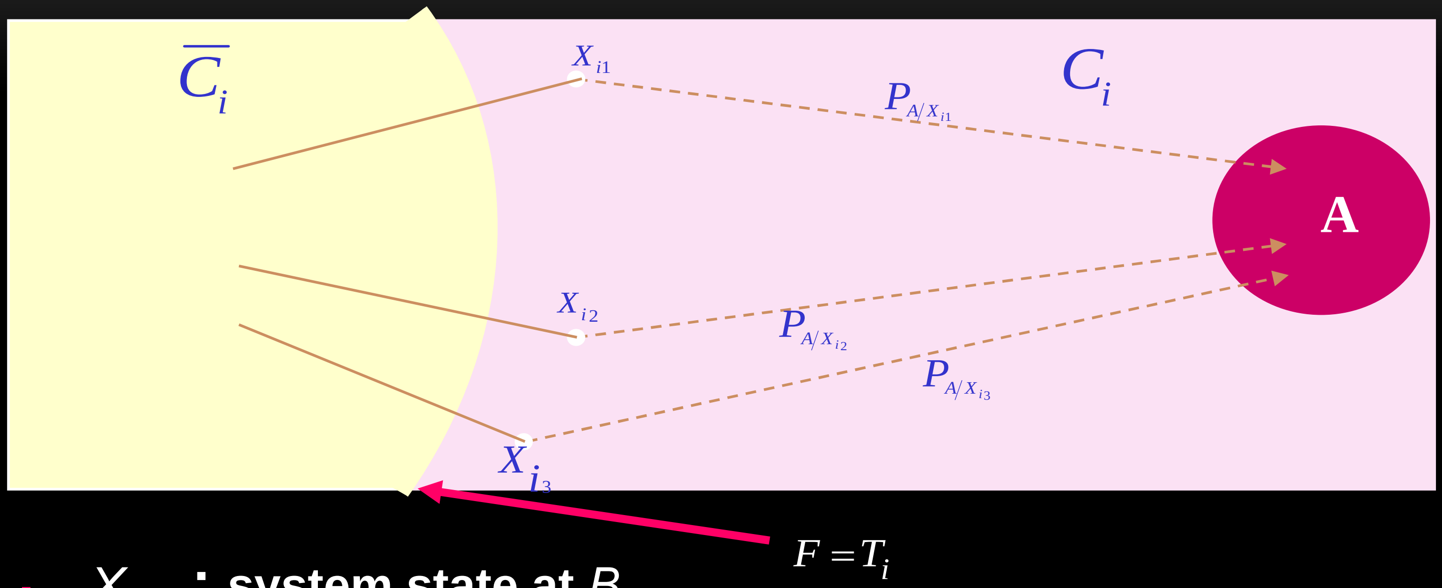
- It is convenient to reschedule at $B_{i,}$ for each retrial, the scheduled components lifetimes and repaired times. Otherwise, there would be high correlation between retrials.
- If these times are exponentially distributed, the rescheduling is straightforward, due to the memory-less property of this distribution.
- For other distributions we use the following procedures: we obtain a random value of the whole e.g., lifetime of a component. If the end of the lifetime is greater than the value of the clock at the current time (B_i), the residual lifetime is obtained as the difference between the two amounts. Otherwise a new random value is obtained and so on.

If after 50 attempts the new end of lifetime is lower than the value of the clock at the current time (B_i), it is not rescheduled.



Factor f_v (II)

$$f_v \leq Max(s_i) \qquad s_i = \frac{a_i}{K_A}\left[K'_i + \frac{V(P^*_{A/X_i})}{(P^*_{A/i})^2}\gamma_i\right] \simeq 1 + \frac{V(P^*_{A/X_i})}{(P^*_{A/i})^2}$$



- X_i : **system state at** B_i
- P^*_{A/X_i}: **importance of state** X_i
- $P^*_{A/i}$: **expected value of** P^*_{A/X_i}
- γ_i : **factor reflecting the autocovariance of** P^*_{A/X_i}

CONTENTS

THE HRMS MODEL

- k types of components
- n_i identical components of each type
- The system works if at least r_i components of each type i work
- Failure propagation
- Exponential lifetimes and repaired times

Generalization of the model:

- Redundancy can be active or passive
- Critical components have priority to be repaired
- General lifetime and repaired distributions (not only exponential)

IMPORTANCE FUNCTION (I)

- **The first importance function is**:

$$\Phi\left(t\right) = cl - oc(t)$$

- *cl* : cardinality of the minimal cut set with lowest cardinality
- *oc*(*t*): number of components that are operational at time *t* in the cut set with lowest number of operational components.

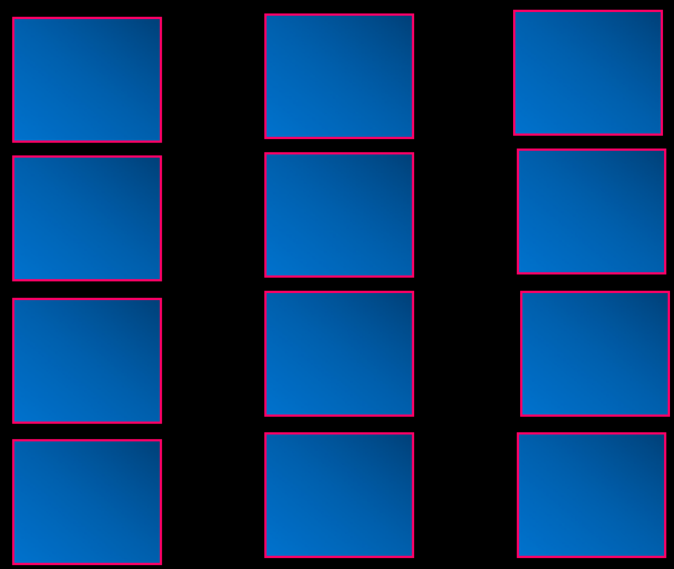
For systems with the same redundancy for all types of components:

$$\Phi\left(t\right) = Max_i\left\{ fc_i\left(t\right)\right\}$$

- fc_i: number of components that are failed at time *t* in the *i*th minimal cut set

IMPORTANCE FUNCTION (II)

Example: Model with k = 3 types of components, n_i=4 components of each type. The system fails if all the components of one type fail (r = 1).



- We define 3 thresholds, each of one is hit if i components of the same type are failed.

IMPORTANCE FUNCTION (III)

- **The second importance function is**:

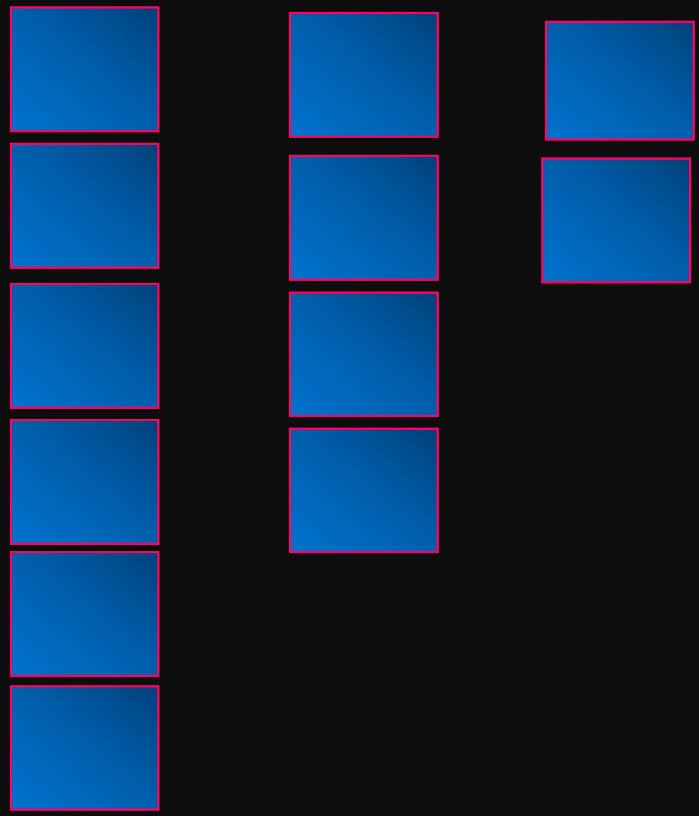
$$\Phi(t) = Max_i \left\{ fc_i(t) / (n_i - r_i + 1) \right\}$$

- fc_i: number of components that are failed at time t in the ith minimal cut set
- $(n_i - r_i + 1)$: Amount of redundancy of components of type i.

The lower the redundancy of a type, the greater the importance of a failure of a component of that type. We can observe that this IF matchs the previous one if all the types have the same redundancy.

IMPORTANCE FUNCTION (IV)

Example 2: Model with $k = 3$ types of components, $n_1 = 6$ components of the first type, $n_2 = 4$ of the second type and $n_3 = 2$ of the third type. The system fails if all the components of one type fail ($r_i = 1$).



- We could define 1 threshold, which is hit if 1 component of the third type, or 2 of the second type or 3 of the first type fail.

$1/P_{i+1/i}$

ASIMPTOTIC OPTIMALITY (I)

- **Sufficient conditions:**

a) The importance function Φ leads to s_i values that are bounded or have subexponential growth when $1/P$ grows exponentially;

b) The number of retrials is such that both the ratio between the acumulated number of retrials and the optimal one and the inverse of that ratio are bounded or have subexponential growth;

c) Enough thresholds are defined to have $1/P_{i+1/i}$ bounded or with subexponential growth.

Condition b) is never restrictive.

Condition c) is satisfied given that as the redundancy of each type of component tends to infinity, we can define enough thresholds.

Condition a) is satisfied if:

$$\lim_{l\to\infty} \frac{Q^*_{A/h}}{P^*_{A/h}} < \infty$$

Asimptotic Optimality (II)

Reliability estimation of a non-repairable balanced system in the interval (0, t_e).

Let us consider a system with k types of identical components. Assume that threshold h is hit at an instant t. Then: $\Phi(t) = h$. Let call $l = cl - h$.

- *The system state with greatest importance is an state with a cut set with l operating components (for example of type j) and the other cut sets with l +1 operating components.* Thus the supreme of the importance is given by:

$$Q^*_{A/h} = p^l + (k-1)\,p^{l+1}$$

- Let us consider the set Ω_{hj} of system states when the process enters set C_h with a failure of a component of type j. All the states of this set have a cut set with l operating components of type j and the other cut sets with at least l +1 operating components. A lower bound of the importance of each of these states is: p^l. The probability of entering set C_h with a system state of set Ω_{hj}, is 1/k. Thus:

$$P^*_{A/h} > \sum_{j=1}^{k} p^l \cdot 1/k = p^l \quad \text{and} \quad \lim_{l\to\infty} \frac{Q^*_{A/h}}{P^*_{A/h}} \le \lim_{l\to\infty} \frac{p^l + (k-1)\,p^{l+1}}{p^l} = 1 + (k-1)\,p < \infty$$

Asimptotic Optimality (III)

The proofs are made for:

- *Reliability estimation of a non-repairable balanced system in the interval* $(0, t_e)$.
- *Reliability estimation of a non-repairable unbalanced system in the interval* $(0, t_e)$.
- *Reliability estimation of a repairable balanced system in the interval* $(0, t_e)$.
- *Reliability estimation of a repairable unbalanced system in the interval* $(0, t_e)$.
- Steady state availability of a repairable system (balanced or unbalanced).

CONTENTS

SIMULATION RESULTS (I)

- ***Example 1:*** *k = 1, so the system has n components of the same type. One repair service. The system fails if all the components fail (r = 1).*

Table I: Unavailability and MTBF for the HRMS system with *k* = 1, *r* = 1, *λ* = 0.001 and *μ* = 1. Relative error = 0.1.

n	U	f_T	Time minutes	Actual ratio	Theor ratio	$f_T\, f_R\, f_V\, f_0$ ratio
5	1.2×10^{-13}	11.3	0.32	1	1	1
10	3.6×10^{-24}	8.5	0.85	2.67	3.20	0.83
15	1.3×10^{-33}	7.0	1.86	5.81	6.22	0.93
20	2.4×10^{-42}	6.2	4.36	13.60	9.91	1.37

- Recall: computational time proportional to $f_V\, f_O\, f_R\, f_T \left(-\ln P + 1\right)^2$

SIMULATION RESULTS (II)

- *Example 2: k = 3, n components of each type. Ample repair service. The system fails if n-1 components of the same type fail (r = 2).*

Table II: Unavailability and MTBF for the HRMS system with *k* = 3, *r* = 2, λ_1= 0.01, λ_2= 0.015, λ_3= 0.0002 and μ = 1. Relative error = 0.1.

n	U	f_T	Time minutes	Actual ratio	Theor ratio	$f_T\ f_R\ f_V\ f_0$ ratio
8	1.3×10^{-12}	4.0	0.67	1	1	1
12	8.8×10^{-20}	4.5	2.33	3.48	2.50	1.39
16	5.5×10^{-27}	4.8	3.60	5.38	4.70	1.14
20	3.3×10^{-34}	5.2	9.60	14.33	7.59	1.89

SIMULATION RESULTS (III)

- *Example 3: c = 6, different redundancies and failure rates for each type. One repair service. The system fails if $n_i - r_i$ components of some type fail*

Table III: Unavailability and MTBF for the HRMS system with *c* = 6, *n* = (4, 3, 5, 10, 10, 10), ... , *n* = (20, 19, 21, 26, 26, 26) *r* = (1,1,1,5,5,5), *λ* = (0.0015, 0.00025, 0.0025, 0.002, 0.002, 0.002) and *μ* = 1.

n	*U*	Time IF 1	Time IF 2	Actual ratio	Theor ratio	f_T f_R f_V f_0 ratio
4,3,5,10,10,10	7.4×10^{-11}	236.2	10.6	1	1	1
+ 1	1.4×10^{-12}	350.1	16.7	1.58	1.37	1.15
+ 6	6.4×10^{-20}	166.2	19.3	1.82	3.49	0.52
+ 11	1.4×10^{-25}	175.2	85.3	8.05	5.80	1.39
+ 16	5.2×10^{-30}	127.3	132.6	12.50	7.99	1.56

Simulation Results (IV)

Analogous results have been obtained for these 3 models with the following distributions:

- *Component lifetimes: Weibull*
- *Service times: Erlang*

Computational times were around 2.5 - 3 times greater than with exponential times for estimating probabilities of the same order of magnitude, It is due to:

- It is more time consuming to generate random numbers from these distributions
- The rescheduling with exponential distribution is straightforward, but with Weibull and Erlang distributions it is much more slowly.

CONCLUSIONS

- RESTART is an appropriate method to simulate highly dependable systems, particulary when there are significant redundancies in the system.
- The new importance function greatly improves the previous one for systems for which the types of components with greater probability of failure have also the greater redundancy.
- We have proved the asymptotic optimality of RESTART estimators in a wide class of models that include the HRMS systems for the case where the redundancy tends to infinity.
- Asymtotic optimality does not guarantee a close to the optimal application for estimating probabilities of interest.