Reliability Engineering and System Safety 130 (2014) 115–124

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

# Asymptotic optimality of RESTART estimators in highly dependable systems

J. Villén-Altamirano *

Department of Applied Mathematics, Technical University of Madrid, Calle Arboleda s/n, 28031 Madrid, Spain

ARTICLE INFO

*Article history:*
Received 7 May 2013
Received in revised form
6 May 2014
Accepted 22 May 2014
Available online 2 June 2014

*Keywords:*
Rare event
RESTART simulation
Subset simulation
Reliability
HRMS systems
Asymptotic optimality

ABSTRACT

We consider a wide class of models that includes the highly reliable Markovian systems (HRMS) often used to represent the evolution of multi-component systems in reliability settings. Repair times and component lifetimes are random variables that follow a general distribution, and the repair service adopts a priority repair rule based on system failure risk. Since crude simulation has proved to be inefficient for highly-dependable systems, the RESTART method is used for the estimation of steady-state unavailability and other reliability measures. In this method, a number of simulation retrials are performed when the process enters regions of the state space where the chance of occurrence of a rare event (e.g., a system failure) is higher. The main difficulty involved in applying this method is finding a suitable function, called the importance function, to define the regions. In this paper we introduce an importance function which, for unbalanced systems, represents a great improvement over the importance function used in previous papers. We also demonstrate the asymptotic optimality of RESTART estimators in these models. Several examples are presented to show the effectiveness of the new approach, and probabilities up to the order of $10^{-42}$ are accurately estimated with little computational effort.



## 1. Introduction

Estimating dependability for a highly-dependable multi-component system is a problem of great interest in different areas such as computer systems, telecommunications, mechanics, aircraft design, power utilities, and many other engineering fields. Increasing demand for system reliability cannot depend on the increasing reliability of components due to technological restrictions. The alternative is a fault-tolerant system which, through the use of redundancy, has the ability to operate properly in the presence of faults. Any system failure should have a small probability of occurring; that is, it should be a rare event. It is important to estimate such probabilities because when a rare event does occur, its consequences may be catastrophic. For example, network servers (studied in Section 5.3) play an increasingly important role due to the rapid growth in demand for internet services, and a server breakdown event may cause significant financial losses. As a result, redundancy is usually built in to prevent services from breaking down.

Even assuming exponential distributions for component failures and repairs, analytical or numerical solution methods are impractical due to the excessive number of states of the continuous time Markov chain (CTMC). For generally distributed failure and repair times, effective numerical techniques, for all practical purposes, do not exist. Thus, simulation becomes the only viable technique for analysis. However, any estimation of rare event probability with the "crude" Monte Carlo technique requires a prohibitively large number of trials in most cases. Thus, fast simulation methods for rare events are required. Several techniques that use importance sampling have been developed to force the system to fail more frequently within a simulation experiment; see [1] for an overview of these methods, [2] for a recent application in reliability and [3,4] for the related Cross–Entropy method. In the literature [5], a CTMC model with finite state space, whose transitions correspond to component failures and repairs, is usually adopted.

The other important method for rare event simulation is RESTART (Repetitive Simulation Trials After Reaching Thresholds). This method has a precedent, of much more limited scope [6], in the splitting method described in [7]. Recent applications of splitting to reliability problems can be seen in [8,9]. M. and J. Villén-Altamirano coined the name RESTART in 1991 [10] and made a theoretical analysis that yields the variance of the estimator and the gain obtained with one threshold. A detailed analysis with multiple thresholds is made in [11], where optimal values for thresholds and the number of retrials that maximize the

* Tel.: +34 913367525; fax: +34 913367877.
*E-mail address:* jvillen@eui.upm.es

http://dx.doi.org/10.1016/j.ress.2014.05.012
0951-8320/

gain were derived. In the RESTART method a more frequent occurrence of a formerly rare event is achieved by performing a number of simulation retrials when the process enters regions of the state space where the importance is greater, i.e., regions where the chance of occurrence of the rare event is higher. These importance regions are defined by comparing the value taken by a function of the system state, the importance function, with certain thresholds.

In reliability problems related to mechanics, a technique called Subset simulation with Splitting was presented in [12]. However, this technique should be considered a variant of RESTART, which is also based on the observation that a small failure can be expressed as a product of larger conditional failure probabilities that can be estimated with much less computational effort.

The application of RESTART to particular models requires a suitable importance function to be chosen. An inefficiency factor related to the importance function was analyzed in [6] and guidelines for selecting such a function heuristically were provided. An importance function useful for estimating reliability measures is provided in [13]. This function is valid for simulating balanced and some unbalanced systems. Balanced systems are those whose components have the same redundancy and failure rates of the same order of magnitude. In this paper we introduce an importance function that matches a previous one for systems with the same redundancy, but which is much better for systems with components of different degrees of redundancy.

One limitation of RESTART methodology in simulating highly reliable systems with low redundancy is the difficulty of defining thresholds that are close and for which the probability of reaching the next threshold is reasonably great and, thus, close to the optimal. For this reason, [14,15] suggested that this methodology is not appropriate for this type of system. However, as will be shown, very low probabilities can be accurately estimated with reasonable computational effort even for systems with a low level of redundancy in their components. Unlike importance sampling, RESTART works better with "significant" redundancies in the system. In this sense, they can be considered complementary methods. The advantages of RESTART are that, for Markovian models, the state space of the CTMC does not have to be finite (as it does in importance sampling), that the extension to non-Markovian models is relatively straightforward and that it is not so dependent on particular features of the system.

Asymptotic optimality with importance sampling has been studied for cases where the failure rates of the components tend to zero. In this paper, we will prove the asymptotic optimality of RESTART estimators in a wide class of models that include the highly reliable Markovian systems (HRMS) for cases where the redundancy tends to infinity. Several examples are presented to show the effectiveness of the approach. Simulation results will be provided for some Markovian models that have appeared in the literature and for non-Markovian models with Weibull lifetime distributions and Erlang repair times.

The paper is organized as follows: Section 2 presents a review of the method. Section 3 describes a wide class of highly dependable systems and gives the importance function. Section 4 provides the asymptotically optimal analysis. In Section 5 several application examples are shown and, finally, conclusions are stated in Section 6.

## 2. Description of RESTART

This method has been described in detail in several papers, e.g., [11,13], and a tutorial on it can be seen in [16]. Nevertheless it is described here in order to make this paper more self-contained.

Let $\Omega$ denote the state space of a process $X(t)$ and $A$ the rare set whose probability must be estimated. A nested sequence of sets of states $C_i$, $(C_1 \supset C_2 \supset \ldots C_M)$ is defined, which determines the partitioning of the state space $\Omega$ into regions $C_i - C_{i+1}$; the higher the value of $i$, the higher the importance of the region $C_i - C_{i+1}$. These sets are defined by means of a function, $\Phi : \Omega \to \Re$, called the importance function. Thresholds $T_i$ $(1 \le i \le M)$ of $\Phi$ are defined so that each set $C_i$ is associated with $\Phi \ge T_i$.

The rare set probability, $P = \Pr\{A\}$, may be defined as the probability of the system being in a state of set $A$ at the instant certain events, denoted reference events, occur. A reference event at which the system is in a state of the set $A$ is referred to as an event $A$. In the examples of Section 5, (component) failure events are reference events, but not repair events. Two additional events, $B_i$ and $D_i$, are defined as follows:

$B_i$: event at which $\Phi \ge T_i$, having been $\Phi < T_i$ at the previous event;
$D_i$: event at which $\Phi < T_i$, having been $\Phi \ge T_i$ at the previous event.

RESTART works as follows:

- A simulation path, called main trial, is performed in the same way as if it were a crude simulation. This lasts until it reaches a predefined "end of simulation" condition.
- Each time an event $B_1$ occurs in the main trial, the system state is saved, the main trial is interrupted, and $R_1 - 1$ retrials $[B_1, D_1)$ are performed. Each of these retrials is a simulation path that starts with the state saved at $B_1$ and finishes when an event $D_1$ occurs.
- After the $R_1 - 1$ retrials $[B_1, D_1)$ have been performed, the main trial continues from the state saved at $B_1$. Note that the total number of simulated paths $[B_1, D_1)$, including the portion $[B_1, D_1)$ of the main trial, is $R_1$. Each of these $R_1$ paths is called a trial $[B_1, D_1)$. The main trial, which continues after $D_1$, leads to new sets of retrials $[B_1, D_1)$ if new events $B_1$ occur.
- Events $B_2$ may occur during any trial $[B_1, D_1)$. Each time an event $B_2$ occurs, an analogous process is set in motion: $R_2 - 1$ retrials $[B_2, D_2)$ are performed, leading to a total number of $R_2$ trials $[B_2, D_2)$. The trial $[B_1, D_1)$, which continues after $D_2$, may lead to new sets of retrials $[B_2, D_2)$ if new events $B_2$ occur.
- In general, $R_i$ trials $[B_i, D_i)$ $(1 \le i \le M)$ are performed each time an event $B_i$ occurs in a trial $[B_{i-1}, D_{i-1})$. The number $R_i$ is constant for each value of $i$.
- A retrial that starts at $B_i$ also finishes if it reaches the "end of simulation" condition before the occurrence of event $D_i$.

Observe that splitting occurs each time a trial crosses a threshold, and trials are killed when they leave the threshold at which they were born.

Fig. 1 illustrates a RESTART simulation with $M=3$, $R_1=R_2=4$, $R_3=3$, in which the chosen importance function $\Phi$ also defines set $A$ as $\Phi \ge L$. Bold, thin, dashed and dotted lines are used to distinguish the main trial and the retrials $[B_1, D_1)$, $[B_2, D_2)$, and $[B_3, D_3)$, respectively.

Note that for the statistics referring to all the trials, the weight assigned to a trial when it is in the region $C_i - C_{i+1}$ ($C_M$ if $i=M$) must be the inverse of the cumulative number of trials, $1/r_i = 1/\Pi_{j=1}^{i} R_j$ $(1 \le i \le M)$.

Some more notations:

- $P = \Pr\{A\}$; $C_{M+1} = A$; $C_0 = \Omega$;
- $P_{h/i}$ $(0 \le i \le h \le M+1)$: probability of the set $C_h$ at a reference event, knowing that the system is in a state of the set $C_i$ at that reference event. For $h \le M$, since $C_h \subset C_i, P_{h/i} = \Pr\{C_h\}/\Pr\{C_i\}$;